Unclassified **NEA/CSNI/R(2002)1/VOL1**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

10-Jun-2002

English - Or. English

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2002)1/VOL1
Unclassified

CNRA/CSNI WORKSHOP ON LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS

WORKSHOP PROCEEDINGS

Hluboka nad Vltavou, Czech Republic
25th-27th September, 2001

English - Or. English

JT00127842

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of 27 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON NUCLEAR REGULATORY ACTIVITIES

The Committee on Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency (NEA) is an international committee made up primarily of senior nuclear regulators. It was set up in 1989 as a forum for the exchange of information and experience among regulatory organisations and for the review of developments which could affect regulatory requirements.

The Committee is responsible for the programme of the NEA, concerning the regulation, licensing and inspection of nuclear installations. The Committee reviews developments which could affect regulatory requirements with the objective of providing members with an understanding of the motivation for new regulatory requirements under consideration and an opportunity to offer suggestions that might improve them or avoid disparities among Member Countries. In particular, the Committee reviews current practices and operating experience.

The Committee focuses primarily on power reactors and other nuclear installations currently being built and operated. It also may consider the regulatory implications of new designs of power reactors and other types of nuclear installations.

In implementing its programme, CNRA establishes co-operative mechanisms with NEA's Committee on the Safety of Nuclear Installations (CSNI), responsible for co-ordinating the activities of the Agency concerning the technical aspects of design, construction and operation of nuclear installations insofar as they affect the safety of such installations. It also co-operates with NEA's Committee on Radiation Protection and Public Health (CRPPH) and NEA's Radioactive Waste Management Committee (RWMC) on matters of common interest.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers. It was set up in 1973 to develop and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety amongst the OECD Member countries.

CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of its programme of work. It also reviews the state of knowledge on selected topics of nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus in different projects and International Standard Problems, and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups and organisation of conferences and specialist meeting.

The greater part of CSNI's current programme of work is concerned with safety technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment and severe accidents. The Committee also studies the safety of the fuel cycle, conducts periodic surveys of reactor safety research programmes and operates an international mechanism for exchanging reports on nuclear power plant incidents.

In implementing its programme, CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

CNRA/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS
Hluboká nad Vltavou, Czech Republic

25th-27th September, 2001

A Contents

B Summary and Conclusions

C Programme

D Papers

E Participants

A TABLE OF CONTENTS

Page

Volume I

B Summary and Conclusions 11

C Programme 37

D Papers 45

OPENING SESSION:
ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I&C SYSTEMS
Chairmen: M. Chiramal - P. Krs

Electricité de France Experience of Computer-based I&C Systems 47
François Poizat, Edf, France

The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan 55
Yoichi Mito, the Kansai EP Co., Inc.
Masafumi Utsumi, Mitsusbishi HI Ltd., Japan

Independent Assessment of the Temelin Software Safety System 63
Petr Zavodsky, CEZ a.s., Czech Republic

Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor 75
D.I. Kim, B.R. Kim and S.H. Oh, Korea Institute of Nuclear Safety, Korea

Decision Support for Approval of Safety Critical Programmable Systems 83
Gustav Dahll, Bjørn Axel Gran, OECD Halden Reactor Project, Norway
Bo Liwång, Swedish Nuclear Power Inspectorate, Sweden

TECHNICAL SESSION 1:
NATIONAL AND INTERNATIONAL COMPUTER-BASED STANDARDS AND GUIDES FOR SAFETY SYSTEMS 95
Chairmen: J.P. Bouard, Z. Ogiso

International Standardisation in Nuclear I&C Engineering 97
Jean-Paul Bouard, EdF, France

Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety 109
Gary Johnson, Lawrence Livermore National Laboratory, USA

The New IAEA Safety guide and the Common Position of European Regulators on Software for Systems Important to Safety 117
Pierre-Jacques Courtois, Association Vinçotte Nuclear, Brussels, Belgium

Approach to the Application of the State Regulatory Requirements, Legislation and Standards in Modernization of I&C Systems, Concerning Especially the Digital Computer-Based Systems **129**
J. Zatloukal, P. Krakora, NRI Rez, Czech Republic

Standard Base for Regulatory Activity in NPP I&C Systems Area **139**
V. Goldrin, M. Yastrebenetsky, Yu. Rozen, S. Vinogradskaya
State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

TECHNICAL SESSION 2: REGULATORY ASPECTS **147**
Chairmen: K. Hamar, A. Lindner,

EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Power Industry
Christina Antonescu, USNRC, **149**
Paul D. Ewing, Richard T. Wood, Oak Ridge National Laboratory, USA

Pre-Qualification of Digital Platform - U.S. NRC Regulatory Review of the Common Q Platform **159**
W.K. Mortensen, M. Chiramal

Survey and Evaluation of Digital I & C Licensing Experience **165**
Swu Yih, Chin-Feng Fan, Chan-Fu Chuang

Collecting Data from Operational Experience of Computer-Based I&C Systems - A Regulatory Perspective on Goals and Tasks **177**
G. Schnürer, ISTec, Garching, F. Seide, BfS, Salzgiter, Germany

Digital Projects in the Near Past and their Consequences in Safety Regulations in Hungary **187**
K. Hamar, HAEC, Hungary

Volume II

TECHNICAL SESSION 3
ANALYSIS AND ASSESSMENT OF DIGITAL I&C SYSTEMS **11**
Chairmen: M. L. Järvinen, M. Kersken

Preliminary Evaluation of Computerized Procedures from Safety Viewpoints **16**
Yun H. Chung, Sung N. Choi, Bok R. Kim, Korea Institute of Nuclear Safety, Korea

Modernization of the I&C System for ANP Dukovany by the Use of Computer-based Equipment **21**
F. Dalik, K. Wagner, M. Ris, SKODA, Czech Republic
Jean-Pierre Burel, Schneider Electric, Jean-Paul Mauduit, Framatome-ANP, France

FMEA Performed on the SPINLINE3 Operational System Software as Part of the TIHANGE1 NIS Refurbishment Safety Case **37**
L. Ristord, C. Esmenjaud, Schneider Electric Industries, France

Qualification of Pre-Developed Software for Safety-Critical I&C Application in NPPs **51**
M. Kersken, ISTec, Garching, Germany

A Bayesian Approach to Risk Informed Performance Based Regulation for Digital I&C QA Programs **69**
Swu Yih, Sun-Li Chyou, Li-Sing Wang, AEC INER
Chin-Feng Fan, Yuan-Ze University, Chinese Taipei

TECHNICAL SESSION 4
SOFTWARE LIFE CYCLE ACTIVITIES **81**
Chairmen: G. Dahll, F. Krizek

Implementation of Software Independent Verification Distributed Control and Information Systems and Validation for Lungmen **83**
Jiin-Ming Lin, Jeen-Yee Lee, Taiwan Power Company, Chinese Taipei

Static Analysis of the Software Used in Safety Critical System of the NPP Temelin **91**
Z. Piroutek, S. Roubal, J. Rubek, I & C Energo, a.s., Czech Republic

Assessment Methodology of the Temelin NPP Control System Performance and Quality **99**
Ivan Petruzela, Karel Bednarik, I & C Energo, a.s., Czech Republic

Methodology of NPP I&C System Algorithms and Software Expert Analysis **109**
V.S. Kharchenko, L.M. Lyubchik, M.A. Yastrebenetsky, State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

TECHNICAL SESSION 5
EXPERIENCE WITH APPLICATIONS SYSTEM ASPECTS, POTENTIAL LIMITS AND FUTURE TRENDS AND NEEDS **119**
Chairmen: B. Liwång - M. Hrehor

Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No. 6 and 7 **121**
Makino Shigenori, Tokyo Electric Power Company, Japan

Technical Requirements on Maintenance of Digital I&C Systems Important to Safety **131**
G. Schnürer, ISTec, Garching, F. Seidel, BfS, Salzgitter, Germany

Requirements Management of I & C System Refurbishment of NPP Dukovany **141**
Jiri Pliska, I & C Energo, a.s., Czech Republic

Licensing Process of the Digital Computer-based I&C Systems to be Implemented Within the NPP Dukovany I & C Refurbishment Project **151**
Ceslav Karpeta, Scientech Inc., Josef Rosol, CEZ, a.s., Czech Republic

Temelin Nuclear Power Plant Westinghouse - I&C Change Process (Paper not available)
Dennis M. Popp, John L. Duryea, USA

E List of Participants **169**

CNRA/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF
COMPUTER-BASED I&C SYSTEMS
Hluboká nad Vltavou, Czech Republic

25th-27th September, 2001

B. Summary and Conclusions

CNRA/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF
COMPUTER-BASED I&C SYSTEMS

EXECUTIVE SUMMARY

The OECD Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, was held from 25th to 27th September, 2001, in Hluboká nad Vltavou, Czech Republic, sponsored by both the Committee on Nuclear Regulatory Activities (CNRA) and the Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA). It was organised in collaboration with the Czech State Office for Nuclear Safety (SÚJB), the Czech Power Board CEZ a.s., I&C Energo a.s. and the Nuclear Research Institute, Rez near Prague.

The objectives of the Workshop were to exchange the experience gained by both the regulators and the industry in different countries in the licensing and operation of computer-based I&C systems, to discuss the existing differences in their licensing approaches in various countries, to consider the safety aspects of their practical use, and to discuss the ways of promoting future international co-operation in the given area.

The scope of the Workshop included:

- review of the progress made since the CNRA/CSNI workshop which was held in 1996
- current and future regulatory needs and/or requirements for the computer-based I&C systems
- progress made in software life cycle activities, including verification and validation, and safety/hazards analysis
- benefits of applying the computer-based I&C systems to improve plant performance and safety.

The Technical Sessions and Discussion Sessions covered the following topics:

Opening Session: Advances made in the use and planning of computer-based I&C systems
Topic 1: National and international standards and guides for computer-based safety systems
Topic 2: Regulatory aspects
Topic 3: Analysis and assessment of digital I&C systems
Topic 4: Software life cycle activities
Topic 4: Experience with applications, system aspects, potential limits and future trends and needs
Final Session: Workshop summary.

The workshop provided a unique opportunity for people with experience in licensing, developing, manufacturing, implementing, maintaining or researching computer-based systems important to safety to get together and to discuss their insights learned from their actual activities. The Workshop was successful in this point. It was attended by 65 people from 15 countries and by 2 international organizations.

Progress since the previous workshop

At the first workshop the basic concern was whether it is possible to safely implement and operate software-based systems in nuclear power plants. During the 5 years following the first OECD workshop, computer-based I&C systems have been installed and operated in both safety and non-safety systems in a number of nuclear plants all over the world. These countries have developed the systems in their own manner and universal measures to implement computer-based safety systems have not yet been obtained. This status has not changed since the previous Workshop. In parallel, the nuclear industry (consisting of the utilities, vendors, designers, and constructors) and the regulators have universally reached a somewhat stable state in addressing the issues and concerns which were identified during that first workshop. This state was achieved by accepting, in principle, that a computer-based safety system designed, implemented and reviewed based on a structured life-cycle process would provide an acceptable safety system.

The life cycle processes adopted by most of the countries are based on the requirements of national or international standards which have similar structures and methodologies. The process consists of a series of hardware- and software- related activities including design, review, tests, verification and validation, configuration management, safety analyses, and associated documentation.

In comparison with the last meeting, it is evident that great progress has been made in the application of digital computer-based I&C systems. At the same time, it was reported in several papers that new problems had emerged during these five years, for example, COTS, certification of software, obsolescence of digital spare parts, re-classification of some computer-based systems (for example, overall plant computer that controls main control panels or consoles), regulatory efficiency and effectiveness on computer-based systems important to safety, etc. Future problems from the regulatory point of view refer to both the adoption of the established qualification methods for software-based I&C systems to new developments in software technology and to the improvement of the licensing procedures.

As the progress of digital technology is very rapid from day to day, there is a need to continue following the progress of digital technology and surveying the measures for application with accumulating operating experience of previous installations. Collecting and evaluating operational experience of computer-based systems as initiated by the CSNI Task Force on Computer-Based Control Systems Important to Safety (COMPSIS) will be essential for the evaluation of reliability characteristics of such systems and devices.

Findings and Recommendations

The purpose of this Workshop was to recognize the progress of technology concerning the items that the previous Workshop and the CNRA Special Issue Meeting had indicated.

In this context, the insight from this Workshop can be summarized as follows:

Complexity: The complexity of functions required of the modern computer systems and its basic elements (cpu, graphic tools, compilers, etc.,) is increasing with technological advances. As a consequence, there are two diverging trends which need to be addressed - added functionality and capability of the system versus verifying that adequate safety is maintained. Methodologies for demonstrating software safety, including the issue of verification and validation are still controversial.

Reliability: Many papers indicated that simplicity was most important to assure the reliability of computer-based systems important to safety, but did not indicate "how simple is simple enough for safety application". At the same time, some analytical approaches were introduced but did not succeed in showing quantitative values. This status has been left unchanged since the previous Workshop. International co-operation should help in obtaining the analytical measures.

Diversity: The functional diversity is considered in most of the applications which were presented at this Workshop, while some indicated other digital diverse systems.

Digital technology evolution**:** The rapid pace of the digital technology evolution has identified the need for addressing obsolescence of components, equipment, and tools; consideration of spare parts, human resources and expertise for operating and maintaining NPP digital systems for the life of the systems. Suggestions made at the workshop, such as sharing resources and knowledge base through some vehicles like Owner's Groups, are worthy of consideration.

International and national standards: Considerable progress has been achieved on this issue. Many international standards and guides covering software lifecycle were developed and revised during these five years, while many countries have developed their own standards or guides.
Some people felt that there are too many standards that are often complex, inconsistent, and misleading. As stated in the papers at this workshop, the various standards committees are aware of these shortcomings and co-ordination activities between the various national and international standards organizations have been initiated. Such efforts should be encouraged so that the fundamental requirements and acceptance criteria for all computer system life-cycle activities in both national and international standards are clear and consistent.

Independent V&V: All of the presentations related to this issue indicated that they followed the similar style of V&V as the ones endorsed in IEC 880 and also reported that it cost too much time and human resources, with a large amount of documentation. Meanwhile, many approaches on independent V&V were reported but the insights on the degree of independence were divided. It seems difficult to reach a general consensus on the degree of independence. In particular, the independent V&V performed in NPP Temelin gave the impression that "independence" is a very costly and time-consuming activity. It seems that we stand at a turning point, that is, which way should we adopt. One way is to produce a complex system and to perform cost-ineffective independent V&V on it. The other is to pursue simplicity that does not need to perform independent V&V. For some systems, such as French SPIN/SPINELINE3, German Teleperm-XS, Japanese POL, and American Eagle it was shown that they have been already verified and moved to the stage of design certification or product certification for reuse in safety application. The

approach "Independent V&V for first application and certification of design or product for second use" is expected.

***Maintaining human competencies*:** An area of concern expressed during the workshop was that the human resources and competencies necessary to maintain the current computer-based safety and non-safety systems is not likely be available in the near future. Most of the participants agreed that addressing the problem on human resources is essentially important as well as the development of safety critical digital systems. Methods and policies for retaining the knowledge, expertise and competencies should be initiated in the industry and regulatory bodies.

COTS, PDS, PES: The use of commercial off-the-shelf (COTS) products, previously developed software (PDS), and previously existing software (PES) and other legacy systems in safety system applications is an issue that was identified as an immediate concern. Standards addressing the requirements and acceptance criteria and detailed guidance on how to implement them in a manner that is internationally applicable are needed immediately.

Conclusion

As a general conclusion, the Workshop can be considered representative of the progress made towards reaching the targets set at the Munich workshop almost five years ago. The Munich workshop had identified areas where further development and specific improvements were needed. The Hluboka workshop has reviewed the development achieved since then. Based on the papers presented at this workshop and on the discussions by the workshop participants, it is evident that the details of the life-cycle activities and the associated acceptance criteria are still in flux and have yet to be universally acceptable. The basic trends from Munich still hold and are reaffirmed in the frame of evolving regulatory and commercial environments.

Future international co-operation should strive to reach universally acceptable positions in the above areas.

OECD/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF
COMPUTER-BASED I&C SYSTEMS

MEETING SUMMARY

Sponsorship

The OECD Workshop on **Licensing and Operating Experience of Computer-Based I&C Systems,** was held from 25h to 27th September, 2001, in Hluboká nad Vltavou, Czech Republic, it was sponsored by both the Committee on Nuclear Regulatory Activities (CNRA) and the Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA). It was organised in collaboration with the Czech State Office for Nuclear Safety (SÚJB), the Czech Power Board CEZ a.s., and I&C Energo a.s.

2. Background:

In March 1996 the CNRA and CSNI organised a Workshop on Technical Support for Licensing Issues of Computer-Based Systems Important to Safety. The workshop was hosted by GRS/ISTec in Munich, Germany. The main purpose of the Workshop was to provide a forum for the exchange of information on the technical issues of computer-based systems important to safety. In June 1996 there was a joint CNRA/CSNI Special Issue meeting to discuss the technical support required for licensing issues of computer-based systems important to safety, utilising the results of the workshop. Follow-up activities were discussed at the December 1996 annual meetings of the CNRA and CSNI. Both meetings confirmed the general recommendations of the workshop, such as:

· Digital systems can be used in safety systems provided that they meet local regulatory requirements

· A wide spectrum of licensing approaches exists

· Further co-operation between the regulatory bodies is necessary to understand the regulatory basis for differences

· It is important to collect information on actual experience in utilising software systems.

In response to the CSNI and CNRA annual meetings in 1996, a Task Group on Computer-Based Systems Important to Safety was established under the CSNI Working Group on Operating Experience. The Task Group has developed a database (COMPSIS) on operational experience related to computer-based systems and follows up on the state of knowledge on the issues. Also, a guideline document, NEA/CSNI/R(99)14 "COMPSIS, Computer-based Systems Important to Safety, Reporting Guidelines", was issued in 1999. The data collection has already been initiated by the Task Group under a trial experiment.

The use of digital systems in NPPs is expanding rapidly. As this technology improves, more and more of these systems are being installed at existing and new plants. The most extensive applications of digital I&C systems have been made at the Darlington NPP in Canada, Sizewell B NPP in the UK, Chooz B1 (France), Kashiwazaki-Kariva 6,7 in Japan, Wolsong 2,3,4 (Korea) and Temelin NPP in the Czech

Republic. Recently, partial refurbishment of the obsolete I&C systems at some VVERs, e.g. Bohunice 1,2 (Slovakia) or Paksh 1,2 (Hungary) by digital ones was done, as well.

At the present time, there is generally a greater experience with computer-based I&C systems on both sides, the industry and among regulators, than there was five years ago. Progress has also been made in developing international regulatory guides and recommendations related to the digital I&C systems.

Based on the progress made in the development of digital I&C systems in recent years and their practical applications in many NPPs in NEA member states, the two committees, CNRA and CSNI, decided to organise a joint CNRA/CSNI Workshop in the second half of 2001 on "Licensing and Operating Experience of Computer-Based Systems Important to Safety", as a follow-up to the one which was held in 1996. The purpose was to exchange the experience gained by both the regulators and the industry in different countries in the licensing and operation of computer-based I&C systems, to discuss the existing differences in their licensing approaches in various countries, to consider the safety aspects of their practical use and to discuss the ways of future international co-operation in the given area.

3. Scope and Technical Content of the Workshop

The scope of the Workshop included:

- review of the progress made since the CNRA/CSNI workshop in 1996
- current and future regulatory needs and/or requirements for the computer-based I&C systems
- progress made in software life cycle activities, including verification and validation, and safety/hazards analysis
- benefits of applying the computer-based I&C systems to improve plant performance and safety.

The Technical Content of the Workshop included:

Opening Session: Advances made in the use and planning of computer-based I&C systems
Topic 1: National and international standards and guides for computer-based safety systems
Topic 2: Regulatory aspects
Topic 3: Analysis and assessment of digital I&C systems
Topic 4: Software life cycle activities
Topic 5: Experience with applications, system aspects, potential limits and future trends and needs
Final Session: Workshop summary.

In general terms, the Workshop attempted to give answers to questions in the following areas:

- What are the benefits of using computer-based I&C systems?
- What national and international standards and guidance could be universally acceptable from the safety perspective?
- What are the regulatory requirements for the current and future generations of digital I&C systems?
- What are the major technical issues and challenges associated with applications of digital technology in I&C systems?

4. Programme Committee of the Workshop

For the preparation of the workshop, its agenda and all the other organisational aspects, the existing CSNI Task Force on Computer-Based Control Systems Important to Safety (COMPSIS) set up the core of the workshop Programme Committee (PC). It was the responsibility of the Programme Committee to evaluate the abstracts of the proposed papers, select the papers for presentation, organise the Sessions, develop the final programme of the workshop, appoint the Session Chairmen, etc. The members of the Programme Committee were:

Mr. Jean-Paul BOUARD, EdF, France
Mr. Matthew CHIRAMAL, NRC, USA ,(COMPSIS Chairman)
Mr. Pierre J. COURTOIS, AVN, Belgium
Mr. Gustav DAHLL, OECD Halden Project
Mr. Karoly HAMAR , HAEC, Hungary
Mr. Hartmuth HEINSOHN, GRS, Germany
Dr. Marja-Leena JÄRVINEN, STUK, Finland
Mr. Karel KRIZEK, CEZ a.s., Czech Republic
Mr. Petr KRS, SÚJB, Czech Republic (PC Chairman)
Dr. Arndt LINDNER, ISTec, Germany
Mr. Bo LIWÅNG , SKI, Sweden
Mr. Zen-ichi OGISO, NUPEC, Japan
Mme. Brigitte SOUBIES , DSIN, France
Prof. Björn WAHLSTRÖM, VTT, Finland
Mr. Bob Yates, NII, United Kingdom
Mr. Miroslav Hrehor, OECD/NEA, (Scientific Secretary).

On the occasion of the Workshop there was an opportunity for participants to visit NPP Temelin with its VVER-1000 reactors equipped with the Westinghouse's digital I&C system.

OPENING SESSION : ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I&C SYSTEMS

Session Chairmen: M. Chiramal, P. Krs

Electricité de France Experience of computer-based I&C systems

Poizat Francois, EdF , France

The presentation focused on the experience gained by EdF in the transition from the electro-magnetic relay-based analog I&C systems in the 34 900 Mwe NPP units (commissioned during 1977 to 1983) to the first digital integrated protection system (SPIN) based on Motorola 6800 microprocessors in the 20 1300 Mwe P4 ad P'4 units (1984 - 1991) to the fully computerized I&C system in the 4 1450 Mwe N4 units (1997) in which the protection system (SPIN), control systems (Contronic E and uREC), control room (KIC) including plant operating procedures are computerized.
To revamping/refurbishment of the steam generator level control system, and the nuclear instrumentation system at the oldest 900 Mwe units during 1998 -99.

The presentation traced these changes, discussed the problems encountered, and the lessons learned. As NPPs trend towards more computerization and reliance on digital components, consideration should be given to the short life cycles of these products and difficult-to-maintain software skills. The presentation concluded that the trend towards the use of COTS to develop NPP I&C systems is a viable solution, provided that safety requirements are met in a cost-effective manner.

The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan

Yoichi Mito, The Kansai EP Co., Inc.
Masafumi Utsumi, Mitsubishi HI Ltd., Japan

The presentation addressed the problem now facing the Japanese nuclear power plants of aging, obsolescence, and the high cost of maintenance of conventional analog I&C system components and equipment. The industry is studying and developing long-range plans for systematic maintenance and replacement of the analog I&C components and equipment. The latest generation of NPPs in Japan are designed with digital safety and non-safety I&C systems. The study considers the differences between the existing plants and the new plants in the area of system safety functions, redundant architecture, interfaces. Included in the study is the consideration of upgrading the main control room boards with advanced computer-based Human-machine Interface systems.

Independent Assessment of the Temelín Safety System Software

Petr Závodský, CEZ a.s., Czech Republic

The presentation covered the activities carried out by Data System and Solutions LLC (DSAS), under contract to the utility CEZ , for the independent assessment (IA) of the Temelin Plant's safety I&C system software.

The I&C system for the Temelin Nuclear Power Plant was designed and implemented by Westinghouse Electric Co. Westinghouse had performed independent verification and validation of the safety I&C system software in accordance with the requirements of standards IEC-880/1986, IEEE Std. 7-4.3.2/1993, ANSI NQA-2a/1990 Part 2.7. In addition, to provide confidence in the integrity of the safey system software, SUJB required that independent assessment be performed on the safety system software that

included independent verification and confirmation that the software design met the requirements of the standards, and an independent review and evaluation of the system software.The presentation included accounts of the following tasks performed by DSAS and its sub-contractors, and the lessons learned from these activities:

Independent audit of the software development process
Assessment of system software tools
Verification of system and software requirements
Verification of software design
Static analysis of source code
Dynamic testing
Assessment of system common mode
Verification and validation of configuration and calibration data

Based on the IA program it was concluded that there were no findings to undermine the confidence in the quality of the software design implementation process and the system software, and that the processes used by Westinghouse were generally in compliance with the requirements of the reference standards.

Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor
D. I. Kim, B. R. Kim and S. H. Oh,
Korea Institute of Nuclear Safety

The presentation provided the regulatory review approach and results of an interim evaluation by the KINS staff with regard to the review of the standard safety analysis report of the Korea Next Generation Reactor (KNGR -AP1400).
The review raised new issues related to the system architecture of the KNGR digital plant protection system (DPPS) regarding the integration of the DPPS bistable processor and the local coincidence logic processor in each of the redundant protection channels. Another item of concern identified is the use of soft controllers in the plant digital engineered safety features actuation system (DESFAS) and the classification and qualification of such controls. The presentation also provided details the of defense-in-depth and diversity analysis for the postulated common mode/cause failure of software, and of the design of the diverse manual controls for DPPS and DESFAS.

Decision Support for Approval of Safety Critical Programmable Systems
Gustav Dahll, Bjørn Axel Gran, OECD Halden Reactor Project
Bo Liwång, Swedish Nuclear Power Inspectorate

The subject of the presentation was the application practices of the three principles of licensing and regulatory requirements - rule-based, consensus-based, and risk-based - as they pertain to software-based NPP I&C systems. The Swedish nuclear regulatory body is drafting a new inspection handbook, where these principles are applied to the lifecycle activities of the software-based system. The presentation provided a methodology for systematically combining the three principles using Bayesian Belief Nets. An experimental study that used the BBN method in combination with a software safety standard was applied to a safety critical software-based system - a computerized system for aiding helicopter landing in various locations during rescue operation. The project consisting of several tasks was discussed during the presentation.

TECHNICAL SESSION 1: NATIONAL AND INTERNATIONAL STANDARDS FOR COMPUTER-BASED SAFETY SYSTEMS AND GUIDES

Session Chairmen: J.P. Bouard, Z. Ogiso

International Standardisation in Nuclear I&C Engineering

Bouard Jean-Paul, EdF, France

The presentation on international standardisation in nuclear I&C, first introduced the global context and the international and regional relationships developed by the International Electrotechnical Commission (IEC), which, together with the International Standards Organisation (ISO) are responsible for the preparation and maintenance of many of the world's International Standards. Then it focuses on standardisation in the nuclear instrumentation and control sector and highlights the work currently being done within IEC SC45A (Instrumentation reactor). More particularly, on projects dealing with software for computer in the safety systems of NPP, classification, the sector translation of the generic standards for the nuclear domain.

Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety

Gary Johnson, Lawrence Livermore National Laboratory, USA

The presentation comparing IEC and IEEE (Institute of Electrical and Electronics Engineers) standards, recognises that, if in the past the IEC and IEEE developed two sets of standards for I&C used in NPP, today, due to the shrinking of the market, the nuclear business is a global one and thus in this environment the harmonisation of the activities of these two bodies is vital. The contents of the two sets of standards are surveyed and opportunities to improve consistency between the two sets are identified.

The New IAEA Safety Guide and the Common Position of European Regulators on Software for Systems Important to Safety

Courtois Pierre-Jacques, Association Vinçotte Nuclear, Belgium

The presentation introducing the new IAEA safety guide on software important to safety and the European report on the common position of European regulators on the same subject gave an overview of some of the distinctive aspects of those two international documents which provide guidance on the design and licensing of computer based systems. It focused on their coherence and complementarities, on their strong and original points and on the issues left open.

Approach to the Application of the State Requirements, Legislation and Standards in Modernization of I&C Systems, Concerning Especially the Digital Computer-Based Systems
J. Zatloukal, P. Krakora, NRI Rez, Czech Republic

The licensing base for computer-based systems important to safety in NPP Temelin and NPP Dukovany was introduced in this presentation. The regulatory requirements for NPP Temelin were based on the US standards related to computer-based safety systems. The adoption of US standards came from the fact that Czech standards were addressed only to analog systems and not to the digital systems at the time when digital safety systems in NPP Temelin were decided to be adopted and subsequently US standards were introduced with the adopted digital system. Meanwhile, the regulatory requirements for NPP Dukovany were based on the Czech standards namely, "Set of USJB Positions" which was developed as the licensing base for implementation of digital safety systems. The licensing stage for digital safety systems in NPP Dukovany is still under way.

Standard Base for Regulatory Activity in NPP I&C Systems Area
M. Yastrebenetsky, V. Goldrin, Yu. Rozen, S. Vinogradskaya
State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

The standard base for regulation on digital I&C systems in Ukraine NPP was introduced, together with some samples of digital systems. The Ukraine standards are basically based on 3 dominant documents but these were harmonized with international standards and some foreign national standards. The criteria for digital application in I&C systems and the main features of the assessment methods for compliance with the criteria were also introduced.

During the **panel session** some important points were brought up:

First, the ***complexity of modern basic components*** (micro processors, compilers, graphic tools etc.) and the power of the tools used for safety demonstration of computer based systems (CBS) are increasing. Those two antagonist trends maintain the situation of balanced nuclear safety when introducing CBS in NPP. Today, as always, the absolute demonstration of safety of software is out of reach, the V&V of CBS is still an open and controversial question. Over the past ten years, CBS have been introduced in many NPPs in numerous countries without any major problems. This introduction was done using basic design rules (determinism proven by design, restricted use of component, rigorous QA…) to use generic component and it appears that this sound approach can be used and trusted to face the accelerating evolution of IT.

Secondly, the ***international context of standardisation*** is deemed to be complex, misleading and even disconcerting. Co-ordination between the different bodies would be valuable. In a first step the inconsistencies should be identified, a roadmap proposing the way to deal with them could be drawn. The responsibilities and relationships between the different bodies should be clearly defined.

Finally the problem of ***maintaining human competencies*** was raised. It appeared during the debate that there was no general consensus to answer that question and to guarantee that the skills necessary for the maintenance, the licensing activities related to the modifications concerning the CBS currently in operation will be there in the future. Nevertheless, some examples of measures taken by industrial companies are given based on defining long term contract to address the problem or in recruiting staff in different domain, automation for example and training them to IT.

TECHNICAL SESSION 2 REGULATORY ASPECTS

Session Chairmen: A. Lindner, K. Hamar

In the Technical Session 2 “Regulatory Aspects” four papers were presented. They dealt with the different aspects of regulations for digital safety I&C. The first paper describes the activities and the status of the generic pre-qualification of a digital platform, the second one includes an approach to investigate several licensing procedures and to derive from this investigation improved licensing procedures, the third paper deals with the collection of data from the operational experience of computer-based I&C systems and the last one describes digital projects in Hungary and their consequences with respect to safety regulation.

PRE-QUALIFICATION OF DIGITAL PLATFORM – U.S. NRC REGULATORY REVIEW OF THE COMMON Q PLATFORM

W. K. MORTENSEN, M. CHIRAMAL

The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform is to be loaded with plant-specific application software to implement various nuclear plant safety system applications. The basis of pre-qualification is compliance with the NRC-approved EPRI Topical Report TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications". The NRC staff reviewed the basic operation of the system, life cycle process and documentation associated with the Common Q hardware and software. The procedure was introduced by the lecturer as a type testing procedure, where the outcome also declares legal statements about the compliance with key requirements in the US, 10CFR50 appendix “B”, about quality assurance. The staff has completed the review of the qualification of nearly all of the Common Q platform components and the staff’s evaluation of the completed activities has been documented in the safety evaluation report (SER) issued on August 11, 2000.

Survey and Evaluation of Digital I&C Licensing Experience

Swu Yih, Chin-Feng Fan, Chan-Fu Chuang

This paper describes the licensing experiences of digital I&C systems based on USNRC regulations for Taiwan’s fourth NPP (Lungmen Project). The contents consist of three parts. In the first part, it is described how the licensing process was conducted, how the licensing strategy was adopted, and how the manufacturers, utility, consultant companies and regulators interact. Some statistics of licensing- related activities and events listed in chronological order are also presented to help understand the scope and complexity of this licensing. In the second part, the paper describes an in-depth analysis of USNRC digital I&C regulations. The internal logical structure, strengths and weaknesses of those regulatory codes, guides, and standards are investigated to identify the efficiency shaping factors. In the third part, modifications are proposed for the current regulation structure and regulation practice. These modifications may improve the current digital I&C licensing efficiency and effectiveness. There was a presentation of a licensing process model which can be used to evaluate the effectiveness of different licensing approaches. The original USNRC regulations and proposed modifications are then evaluated under this model to show the improvement of efficiency.

Collecting Data from Operational Experience of Computer-Based I&C Systems – A Regulatory Perspective on Goals and Tasks
G. Schnürer, F. Seidel

The paper deals with the methods and goals of the collection of data from computer-based I&C systems which are developed, qualified and maintained using a unique platform. The main goal of the data collection is to contribute to the further qualification of these systems by the evaluation and optimization of the qualification procedure, demonstration of the achieved systems' dependability and utilizing the experience of the system applications of lower safety significance within the licensing procedure for computer-based systems important to safety. The content of the records and the evaluation methods for operational experience should have been agreed by the involved experts of the licensees, manufacturers, technical support organizations and regulatory bodies. Not only the failures and the reported events are of interest, but also periods of operation without significant failures. As a long-term goal of the collection of operational experience, the achieved performance of the system might be estimated in quantitative terms. To calculate the reliability, it is crucial to establish an evaluation model in order to identify the necessary parameters as early as possible and to collect them continuously during the operation.

Digital Projects In The Near Past And Their Consequences In Safety Regulations In Hungary
K. Hamar

The paper describes from the regulatory point of view the operational experiences with digital I&C systems in Hungary. There are systems with different importance to safety used like reactor protection systems, core monitoring systems, process computers and others. Errors and problems of the digital systems and related components are listed. The lecturer emphasises the great importance of type testing for the successful licensing of the Teleperm XS system as a reactor protection system for the NPP Paks. From the ongoing licensing processes it can been seen that qualification of class "B" (following IEC 61226) may be more difficult, because of more complex static and dynamic system properties of class "B" systems. As the most important system property, the deterministic behaviour is identified. The existing experiences will be addressed in the new Hungarian safety regulations.

DISCUSSIONS AND CONCLUSIONS, SESSION 2:

During the discussion of the papers, questions regarding some of the details of the presentations were dealt with. In particular, several aspects of the model for the licensing process, presented in the second paper, were discussed. Establishing a model of the licensing process seems to be an interesting approach, but further work is necessary.

Compared to the last meeting in 1996 in Munich the great progress in the application of digital computer-based I&C systems was evident. Future problems from the regulatory point of view refer to both the adoption of the established qualification methods for software-based I&C systems to new developments in software technology and to the improvement of the licensing procedures. Collecting and evaluation of operational experience of computer-based systems will be helpful for the evaluation of reliability characteristics of such systems and devices.

The following conclusions could be drawn:

1. Type testing is an important and desired institution in licensing, beneficial for licensees, and regulatory bodies, and hopefully for developers and manufacturers, too.

2. The efficiency of the licensing process may promote or suppress the utilization of digital technology.

3. The regulator behaves as a transformer between the ”evidence” and the “confidence”.

4. The conservative approach is still present in the licensing, and the licensees and the developers are not satisfied with it. They are waiting for relaxation, and searching for the feasible techniques to support it.

5. Safety is manifest in a set of system properties, like deterministic behaviour, constant system load, simplicity, transparency, etc. At the same time, these are the “easy to license” system properties. The simplicity is in contradiction with nearly all of the another system characteristics: functionality, testability, diversity.

6. The SW reliability data collection suffers that loss, if the reported events and error cases are dependent on the licensee event reporting systems. If reporting criteria do not meet, the result is that the statistically valuable cases remain hidden.

7. From the aspect of data collection efficiency, the comparable operational profile and the unique platforms are desired.

TECHNICAL SESSION 3 ANALYSIS AND ASSESSMENT OF DIGITAL I&C SYSTEMS

Session Chairmen: M.L. Järvinen, M. Kersken

The following five papers were presented:

Preliminary Evaluation of computerized procedure from safety viewpoints

Yun H. Chung, Sung N. Choi, Bok R. Kim, KINS

The paper presents the preliminary safety assessment made to the Computerized Procedure Systems (CPS) to be implemented at the Korean Next Generation Reactor, which is planned to start commercial operation in 2010. The computer-based procedures are being used at various nuclear power plants. This change can support and enhance the operators' performance and safety. However there are safety issues which should be discussed when implementing these systems such as the impact on operators and shift performance, situation assessment and response planning, handling of complex situations particularly in failures of the CPS and change over to paper-based procedures, design for navigation and communication and software quality. The paper presents the preliminary assessment results.

MODERNIZATION OF THE I&C SYSTEM FOR ANP DUKOVANY BY THE USE OF COMPUTER-BASED EQUIPMENT

Jean Pierre Burel, Schneider El., F. Dalik, K. Wagner, M. Říš, ŠKODA
Jean-Paul Mauduit, Framatome-ANP

The paper describes the replacement of existing systems important to safety (category A and B) by computer based systems which are realized by SPINELINE 3 technology. Special parts of the system are units executing functions connected directly with the VVER reactor technology; these are developed by means of an industrial microcomputer-based system as used by Skoda. The features of SPINLINE 3 and Skoda technology are described with emphasis on their contribution to safety.

FMEA performed on the SPINLINE 3 operational system software as part of the Tihange 1 NIS refurbishment safety case

L. Ristord, C.Esmenjaud, Schneider El. Industries

The paper presents the FMEA analysis made for the new Tihange 1 Nuclear Instrumentation System which became operational in March 2001. The choice of the software based technology raised the issue of the risk of a CCF due to the use of the same software in redundant independent units. In addition to the demonstration of the application of the safety requirements for the software in safety systems, a FMEA oriented towards the significant CCF risk was required as part of the safety case. The paper presents the FMEA experience, including the adaptation of the principles of FMEA to the analyses of the software, an approach to identify the components to be analyzed, definitions of the software failure modes associated with the components, examples of the analyses performed on the operational system software and feedback of the experience. Performing the FMEA has proven to be a good way to discuss in depth safety aspects of software based systems.

Qualification of pre-developed software for safety-critical I&C application in NPP's
M. Kersken, ISTec Garching

Implementation of I&C functions important to safety in nuclear power plants are increasingly realized with computer-based systems, i.e. by its software. These so called equipment families are often used to develop these I&C functions. Extensive research work has been made, mainly during last ten years, to tackle the problem of qualifying pre-developed software to be included in the systems important to safety. Due to the great variety of software types and differences in the applications, no unique solution has yet been developed. The objective of the paper is to provide a set of staggered criteria for the qualification of pre-developed software to be used in different categories for the safety critical I&C. An attempt is made to demonstrate an exemplary procedure as to how the different approaches can be brought together, to form a useable set of staggered criteria for the acceptance of the pre-developed software. The first examples show that there will be no principal difficulty for a unified approach, because there are no major contradictions in the requirements or recommendations of the analyzed documents. The acceptance of such a unified procedure, however, needs the involvement of a broad international group of experts.

A Bayesian approach to risk informed performance based regulation for digital I&C QA programs
Swu Yih, Sun-Li Chyou, Li-Sing Wang, AEC INER,
Chin-Feng Fan, Yuan-Ze University

A proposal for a systematic way to reduce unnecessary conservatism in regulatory processes is given. Bayesian Belief Networks BBN are applied as a modelling technique to describe the assessment processes as e.g. independent V&V.
The method first enumerates major influence factors, and constructs the BBN for system risk; an event tree based on same influence factors is then generated. Tree trimming is performed to delete the impossible branches and thus control the exponentially explosive problem in the event tree construction. The numbers of occurrences of final outcomes of the tree are then counted to draw the risk profile graph. The graph can help in identifying the potential areas of unnecessary conservatism. It can also help in determining whether the resulting outcomes of proposed QA program changes are acceptable or not.

CONCLUSIONS FROM SESSION 3

As can be seen from these topics, the session comprised a quite large variety of analysis techniques which can be applied to computer-based systems in I&C important to safety. These reached from review and evaluation of computerized operating procedures for future reactors (Korea) to constructive and analytical techniques which are applied at the moment during the replacement of systems important to safety in an actual plant (Czech Republic). The application of FMEA to computer based technology (Belgium), especially to software, is quite innovative, and has been used in a safety demonstration to show low risk of common cause failure due to software.

A practical systematic approach for an acceptance procedure for pre-developed software was proposed. This approach was based on widely discussed international documents concerning this topic. Another proposal which dealt with the assessment of the effectiveness of regulation procedures based on modeling via Bayesian Belief Networks is highly interesting, because this may be a sound basis for directing the limited resources which can be spent during the development and safety demonstration of computer-based systems important to safety into the most effective combination of techniques which should be applied.

The session did not focus so much on an independent verification and validation IV&V. Discussions after this and other sessions showed, however, that IV&V has an important role in the safety demonstration, but the focus and methods can still be further developed. The application of different tools and methods - as against those which are used in V&V during development – can bring additional assurance to the safety

demonstration. The use of pre-qualified software and the associated IV&V can be one of the ways of reducing the costs of the safety demonstrations. Also in this area future work is needed in the international community.

With respect to this variety of techniques which were presented in the session and their actual or envisaged application in the near future, the session reflects an image of the whole workshop. In most of the sessions there were possibilities to exchange experience of applying well known constructive and analytical techniques to actual implementations of computer based technology. Other contributions, however, were more directed towards opening the door for new applications by providing proposals for their assessment. This mixture of direct application-oriented presentations on the one hand and others oriented towards the near future on the other side, made the workshop very valuable for the experts working in the field of I&C important to safety.

The information also provided new guides and standards for computer-based technology important to safety, which was very helpful, because this gives a better feeling of the internationally agreed principal regulatory requirements.

TECHNICAL SESSION 4: SOFTWARE LIFE CYCLE ACTIVITIES

Session Chairmen: G. Dahl , F. Krizek

The overall theme of the session was the description of the V&V methods used in the licensing process for NPPs. This includes both the methods which have been used and methods planned to be used in NPPs in Taiwan, the Czech Republic and Ukraine. Four papers were presented:

Implementation of Software Independent Verification and Validation for Lungmen Distributed Control and Information Systems
Jiin-Ming Lin, Jeen-Yee Lee, Taiwan Power Company

Static Analysis of the Software Used in Safety Critical System of the NPP Temelin
Piroutek Z., Roubal S., Rubek J., I&C Energo a.s., Czech republic

Assessment Methodology of the Temelin NPPControl System Performance and Quality
Ivan Petruzela, Karel Bednarík, CEZ a.s.,, Czech republic

Methodology of NPP I&C System Algorithms and Software Expert Analysis
V.S. Kharchenko, L.M. Lyubchik, M.A., Yastrebenetsky State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

The first paper, presented by Jeen-Yee Lee from Taiwan Power Company (TPC), dealt with the implementation of the software independent verification and validation (IV&V) for the Distributed Control & Information Systems of the Lungmen NPP. It covered the codes and standards as applicable, the scope of the software IV&V and the documents reviewed, the organisational structure and activities for performing the IV&V work. Teams from GE and TPC performed software V&V for the Lungmen project, based on the USNRC Standard Review Plan Chapter 7, BTP-14 and USNRC Regulatory Guide 1.168 respectively. Two recommendations for performing future software IV&V activities can be made on the basis of the experiences so far. One is to fully understand the regulatory requirements on software IV&V before an IV&V project gets started. The other is to establish a tracking system for IV&V activities in IV&V project to facilitate control and monitoring of the issues identified.

The next two papers described the methods used in the evaluation of safety critical software at the Temelin NPP. The first paper, presented by J. Rubek from I & C Energo s.r.o, gave an overview over the static analysis methods used in this process. The method used was influenced by the one used for the licensing of the Sizewell B protection system, although it is not a direct copy. For the analysis they used the tool MALPAS for analysis of control flow, data use, information flow and semantic compliance. The approach used was cost consuming, but made it possible to discover software anomalies which could be not found in manual check.

In the other Temelin paper, presented by I. Petruzela, also from I & C Energo, described assessment methodology of the control system performance and quality. A methodology has been developed in I&C Energo for the test assessment of the control process quality. This is based on the evaluation of the

behaviour of the main controlled quantities in the course of transients of the test. A set of criteria is defined which serve to check the performance of the Temelín NPP unit control against the design. They determine the borders of the area in which the numeric values of the assessed parameters should vary if the work is made in compliance with the design. The fulfillment of the criteria makes it possible to determine the achieved quality of the NPP Temelín unit major controllers after the completed test.

The fourth paper, presented by V. Kharchenko from the State Scientific and Technical Center on Nuclear and Radiation Safety in Ukraine, described a methodology for verification and validation and expert analysis of algorithms and software in I&C systems. The method was approved for application in Ukrainian NPP, and was in particular applied during the evaluation of the computer-based control system ASUT-1000M for Zaporozhey NPP.

These papers gave a valuable contribution to the workshop as they presented methods actually applied in the licensing of safety critical I&C systems in different NPPs, and that they cover complementary aspects of the licensing process, from general principles to more detailed techniques.

TECHNICAL SESSION 5 EXPERIENCE WITH APPLICATIONS, ASPECTS, POTENTIAL SYSTEM LIMITS AND FUTURE TRENDS AND NEEDS

Session Chairmen: B. Liwång, M. Hrehor

Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No. 6 and 7

Makino Shigenori, Tokyo Electric Power Company

The paper presented the development of digital safety systems for the Kashiwazaki-Kariwa Unit 6 & 7. Digital control and network systems has been applied to the I&C systems of Japanese BWR's since the 1980s. The introduction has been stepwise and the scope of the application has been widened gradually. Based on the experience almost all of the I&C systems, including the safety-related systems, were finally digitised in K-6/7. The system consists of 4 divisions with a 2 out of 4 logic. As for the consideration for common mode failures, some hard-wired back-up countermeasures were installed.

In the paper the development process and the different activities for the V&V were presented. In the validation process, the semi-dynamic simulation tests were also performed additionally to investigate the integrity for system requirement.

The NUREG/CR-6430 introduced several techniques for the hazard analysis. TEPCO performed the hazard analysis utilising the FTA methodology.

For the top hazard two events was defined; failure to initiate trip signal on request and unnecessary (erroneous) trip signal without request. For each of these the underlying structures were developed step by step until the bottom hazard elements were identified. Each of the identified bottom elements were examined against their verification process.

The conclusions from the experience from the performed development, installation and operation is that the following policies should be applied to digital safety systems:

- utilisation of digital systems with good performance and operating experience
- simple software architecture
- static memory allocation, avoidance of external interrupts etc.
- use of graphical language in order to keep transparency and traceability
- modularization of the software for its reuse and effective V&V
- considerations for common mode failures and suitable backup measures

Technical Requirements on Maintenance of Digital I&C Systems Important to Safety
G. Schnürer, ISTec, Garching
F. Seidel, BfS, Salzgitter, Germany

The paper presents work which has already started in Germany.

The paper deals with the necessity of requirements on maintenance and upgrading of safety relevant digital I&C systems as a basis for the elaboration of proper maintenance and upgrade guidelines. Requirements which are treated and discussed are technical solution-oriented versus guidelines so as to have an overall general character. The adoption of existing rules and guidelines is also taken into account for the definition of these additional requirements for safety relevant I&C.

The goal of the paper is the introduction of possible safety relevant requirements with respect to
- maintenance of digital safety relevant and safety I&C
- tracing and route cause analysis of incidents caused by I&C maintenance
- support the regulatory body as well as technical experts concerning state of the art

In the paper it is shown that the international standard IEC 60880 contains the necessary elements for an acceptable modification process and discussed some areas of special interest for handling modification requests, including the configuration management system.

As a summary the following aspects are to be considered:

- Completeness and applicability of the existing requirements concerning maintenance and upgrading of digital safety systems.

- Software maintenance requirements for systems of lower safety categories.

- Maintenance requirements concerning automatically generated software.

Requirements Management of I&C System Refurbishment of NPP Dukovany
Jiri Pliska, I&C Energo a.s., Czech republic

Using an example of the Requirements Management System as implemented in the project "I&C System Refurbishment for NPP Dukovany" the paper presented the system analysis methods and the corresponding tools – generally designed CASE systems as a necessary preconditions for the organisation, management, co-ordination, inspection and evaluation of the extensive project, both from the viewpoint of the contractor and customer, as well as from the viewpoint of the national regulatory body. It is a tool for systematic identification, requirement structuring, communication, control, monitoring and verification of user requirements.

The system is based on a list of individual requirements. The user requirements are organised within a hierarchical structure which observes the structure of the application area. Individual requirements are mutually interrelated in various ways. Each requirement is expressed in the form of a written description. Some significant features of the requirements are clearly and simply expressed with a set of assigned attributes. The practical experience has proven that a good CASE system provides many more options for solutions in Requirements Management Systems than common specialised tools.

The entire system of requirements is in the HTML format represented with 14 000 files with the total size of 50 MB. Any evaluation or sorting takes from several seconds to several minutes. The most time-consuming is fulltext search, taking less than 10 minutes in the whole system. When limiting conditions are used, the search is significantly faster.

Licensing Process of the Digital Computer-based I&C Systems to be Implemented within the NPP Dukovany I&C Refurbishment Project
Ceslav Karpeta, Scientech Inc. - CR, Josef Rosol, CEZ a.s., Czech republic

The paper provided a brief outline of the NPP Dukovany I&C system refurbishment project with a particular focus on specific regulatory requirements related to the digital I&C systems and ways which the utility has adopted in order to ensure that these requirements are met. The licensing process applied to the refurbishment of the Dukovany NPP I&C system is structured to the several stages with the final objective of obtaining the regulatory permission for permanent operation of the refurbished unit. Also, an overall quality assurance programme was established in line with the regulatory requirements covering processes, activites, products, organizations, personnel, etc. The utility intends to perform various audits in order to ensure that the installed equipment will operate as intended, and to provide information needed to support the licensing process. An Audits Plan has been developed to provide the basis for those activities.

Temelin Nuclear Power Plant Westinghouse -I&C Change Process
Dennis M. Popp, John. L. Duryea, USA

During the course of the I&C Systems upgrade at Temelin NPP numerous engineering changes were incorporated in the design and then implemented onsite. From the early stages of installation, Westinghouse has implemented a controlled process to manage these changes. Since the onset of commissioning, Westinghouse has adapted a flexible approach to managing this change process so as to be responsive, during various upgrade efforts, to the needs of the Czech design organizations, as well as those of the start up team. The paper provided an outline of the development of this process.

Under the change process, all modifications to the various digital systems are reviewed to ensure that correct system functionality is maintained and integrated with other plant systems, regulatory requirements, commitments and software configuration controls.

C PROGRAMME

CNRA/CSNI WORKSHOP ON

LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS

Hluboká nad Vltavou, Czech Republic
25-27 September, 2001

Tuesday, 25 September 2001

08:00 - 09:00	**Registration and Coffee**	
09:00 - 09:10	**Welcome**	**P. Krs** **SUJB, Deputy Chairman** **Mr. Krizek - CEZ a.s.**
09:10 - 09:20	**Introductory Remarks**	**M. Hrehor -OECD/ NEA**
	OPENING SESSION: **ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I&C SYSTEMS**	**Chairmen:** **M. Chiramal** **P. Krs**
09:20 - 09:50	**Electricité de France Experience of computer-based I&C systems** Poizat Francois, EdF	**FRANCE**
09:50 - 10:20	**The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan** J Masafumi Utsumi, Mitsubishi HI Ltd Yoichi Mito, Kansai Electric Power	**JAPAN**
10:20-10:40	**Coffee Break**	
10:40 - 11:10	**Independent Assessment of the Temelín Software Safety System** Petr Závodský, CEZ a.s.,	**CZECH REPUBLIC**
11:10 - 11.40	**Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor** D. I. Kim, B. R. Kim and S. H. Oh Korea Institute of Nuclear Safety	**REP. OF KOREA**

11.40 - 12.10	**Decision Support for Approval of Safety Critical Programmable Systems** Gustav Dahll, Bjørn Axel Gran OECD Halden Reactor Project Bo Liwång, Swedish Nuclear Power Inspectorate	**OECD/HALDEN/SWEDEN**

TECHNICAL SESSION 1

	NATIONAL AND INTERNATIONAL COMPUTER-BASED STANDARDS AND GUIDES FOR SAFETY SYSTEMS	**Chairmen:** **J.P. Bouard** **Z. Ogiso**
14:00 - 14:30	**International Standardisation in Nuclear I&C Engineering** Bouard Jean-Paul, EdF	**FRANCE**
14:30 - 15:00	**Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety** Gary Johnson, Lawrence Livermore National Laboratory	**USA**
15:00 - 15:30	**The New IAEA Safety Guide and the Common Position of European Regulators on Software for Systems Important to Safety** Courtois Pierre-Jacques, Association Vincotte Nuclear, Brussels	**BELGIUM**
15:30-15:50	**Coffee Break**	
15:50 - 16:20	**Approach to the Application of the State Regulatory Requirements, Legislation and Standards in Modernization of I&C systems, Concerning Especially the Digital Computer-Based Systems** J. Zatloukal, P. Krakora, NRI Rez	**CZECH REPUBLIC**
16:20 - 16.50	**Standard Base for Regulatory Activity in NPP I&C Systems Area** V. Goldrin, M. Yastrebenetsky Yu. Rozen, S. Vinogradskaya State Scientific Technical Center on Nuclear and Radiation Safety	**UKRAINE**
16:50 - 18:00	**Discussion Opening Session & Session 1**	

Wednesday, 26 September 2001

TECHNICAL SESSION 2 — **REGULATORY ASPECTS** — **Chairmen: K. Hamar, A. Lindner**

09:00 - 09:30	**EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Power Industry** Christina Antonescu, U.S. NRC Paul D. Ewing, Richard T. Wood Oak Ridge National Laboratory	**USA**
09:30 - 10:00	**Pre-Qualification of Digital Platform - U.S. NRC Regulatory Review of the Common Q Platform** W. K.Mortensen, M. Chiramal**,** US NRC	**USA**
10:00 - 10:30	**Survey and Evaluation of Digital I&C Licensing Experiences** Swu Yih, INER, AEC Chin-Feng Fan,Yuan-Ze University Chan-Fu Chuang,, Nuclear Regulation Division, AEC	**CHINESE TAIPEI**
10:30-10:50	**Coffee Break**	
10:50 - 11:20	**Collecting Data from Operational Experience of Computer-Based I&C Systems- A Regulatory Perspective on Goals and Tasks** G. Schnürer, ISTec, Garching F. Seidel, BfS), Salzgitter	**GERMANY**

11:20 - 11:50	**Digital Projects in the Near Past and their Consequences in Safety Regulations in Hungary** K.Hamar, HAEC	**HUNGARY**
TECHNICAL SESSION 3	**ANALYSIS AND ASSESSMENT OF DIGITAL I&C SYSTEMS**	**Chairmen:** **M.L. Järvinen** **M. Kersken**
13:30 - 14:00	**Preliminary Evaluation of Computerized Procedures From Safety Viewpoints** Yun H. Chung, Sung N. Choi, Bok R. Kim, KINS	**REP. OF KOREA**
14:00 - 14:30	**Modernization of the I&C System for ANP Dukovany by the Use of Computer-based Equipment** Jean Pierre Burel, Schneider El., F. Dalik, K. Wagner, M. Říš, ŠKODA Jean-Paul Mauduit, Framatome-ANP	**CZECH REPUBLIC/ FRANCE**
14:30 - 15:00	**FMEA Performed on the SPINLINE3 Operational System Software as Part of the TIHANGE 1 NIS Refurbishment Safety Case** L. Ristord, C.Esmenjaud, Schneider El. Industries	**FRANCE**
15:00-15:20	**Coffee Break**	
15:20 - 15:50	**Qualification of Pre-Developed Software for Safety-Critical I & C Application in NPP's** M. Kersken, ISTec Garching	**GERMANY**
15:50 - 16:20	**A Bayesian Approach to Risk Informed Performance Based Regulation for Digital I&C QA Programs** Swu Yih, Sun-Li Chyou Li-Sing Wang, AEC INER, Chin-Feng Fan, Yuan-Ze University	**CHINESE TAIPEI**
16:20 - 17.30	**Technical Discussion Sessions 2& 3**	

Thursday, 27 September 2001

TECHNICAL SESSION 4	**SOFTWARE LIFE CYCLE ACTIVITIES**	**Chairmen:** **G. Dahl** **F. Krizek**
09:00 - 09:30	**Implementation of Software Independent Verification Distributed Control and Information Systems and Validation for Lungmen** Jiin-Ming Lin, Jeen-Yee Lee, Taiwan Power Company	**CHINESE TAIPEI**
09:30 - 10:00	**Static Analysis of the Software Used in Safety Critical System of the NPP Temelin** Piroutek Z., Roubal S., Rubek J. I &C Energo a.s.,	**CZECH REPUBLIC**
10:00 - 10:30	**Assessment Methodology of the Temelin NPP Control System Performance and Quality** Ivan Petruzela, Karel Bednarík I &C Energo a.s.,	**CZECH REPUBLIC**
10:30-10:50	**Coffee Break**	
10:50 - 11:20	**Methodology of NPP I&C System Algorithms and Software Expert Analysis** V.S. Kharchenko, L.M. Lyubchik M.A., Yastrebenetsky State Scientific Technical Center on Nuclear and Radiation Safety	**UKRAINE**

TECHNICAL SESSION 5	**EXPERIENCE WITH APPLICATIONS SYSTEM ASPECTS, POTENTIAL LIMITS AND FUTURE TRENDS AND NEEDS**	**Chairmen: B. Liwång M. Hrehor**
11:20 - 11:50	**Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No. 6 and 7** Makino Shigenori Tokyo Electric Power Company,	**JAPAN**
11:50 - 12:20	**Technical Requirements on Maintenance of Digital I&C Systems Important to Safety** G. Schnürer, ISTec, Garching F. Seidel, BfS, Salzgitter	**GERMANY**
13:30 - 14:00	**Requirements Management of I & C System Refurbishment of NPP Dukovany** Jiri Pliska, I&C Energo a.s.,	**CZECH REPUBLIC**
14:00 - 14:30	**Licensing Process of the Digital Computer-based I&C Systems to be Implemented within the NPP Dukovany I&C Refurbishment Project,** Ceslav Karpeta, Scientech Inc. - CR Josef Rosol, CEZ a.s	**CZECH REPUBLIC**
14:30 - 15:00	**Temelin Nuclear Power Plant Westinghouse -I&C Change Process** Dennis M. Popp, John. L. Duryea	**USA**
15:00 - 16:00	**Technical Discussion Sessions 4 & 5**	
16.00 - 16.20	**Coffee Break**	

16:20 –17:20	**FINAL PLENARY SESSION/ Workshop Summary**	**Chairman: M. Chiramal**
	Conclusions by Session Chairmen	
17:20 - 17:30	**Concluding Remarks & Adjourn**	**P. Krs (SÚJB)**

19:00 - 21:00 **Meeting of the Session Chairmen to summarize conclusions and recommendations**

Friday, 28 September 2001

09:00 - 12:00 **Visit of NPP Temelin**

OPENING SESSION:
ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I & C SYSTEMS
Chairmen: M. Chiramal, P. Krs

EDF experience in computerized instrumentation/control

F. POIZAT, EDF Industry/Basic Design Department,
12-14 avenue Dutrievoz, 69628 Villeurbanne Cedex, France
Tel.: +33 4 72 82 74 79, Fax: +33 4 72 82 77 04, e-mail/francois.poizat@edf.fr

Summary

EDF gradually swapped from electromagnetic relay based I&C systems, used on the 900Mwe NPP series (exclusive use, if we put aside the operator and maintenance aids), to fully computerised and integrated I&C systems, on the new French 1450MWe NPP series (including all the protection systems, control systems and MMI systems).

This change, directly induced by the pervasive growing use of computerised systems in all the domains, raises new problems for their use in nuclear industry : Verification and Validation, as well as timelessness. For those matters, end 1999, a new Basic Safety Rule dedicated to the use of software in NPP safety classified systems was published by the French Safety Authorities.

Our presentation will trace back those changes, considering the problems faced, some of them having been unveiled during the recent refurbishment of the Fessenheim 900MWe plant Nuclear Instrumentation System based on the SPINLINE 3 product line, developed by Schneider Electric and Framatome.

It's now clear that the current trend to use COTS to develop NPP safety systems shall take into account in a cost effective way the absolute safety requirement, not to degrade the dependability of systems aimed at assuring the NPP safety.

Introduction

The second half of the century which just ended was marked, on the scientific and industrial fronts, by the coming to maturity of two new technologies: nuclear energy and information technology (IT). The nuclear power industry was obviously closely affected by the fantastic technological development represented by the post-war advent of the first computers and, afterwards, by the proliferation of digital systems in all human activities: plant design, equipment production, automatic controls and safety features for industrial processes, communications, project management and plant operation. Nothing is done today without IT.

Seventies: from Fessenheim 1 to Chinon B4 (900 MW CP0, CP1 and CP2 plant series [1])

All the same, the first nuclear power plants did not adopt digital technology from the outset. EDF, it should be said, had a few unhappy experiences, particularly the attempt to install static relay circuitry in the fossil-fired power plant of Montereau in the sixties, or the many innovations (probably premature) at the solar power plant of Targasone in the seventies [2].
Accordingly, the first French PWR units were not computerized, at least for the control of the physical process (fission and conversion into electricity) provided by levels 0 to 2 [3]. As a result:

- The process instrumentation ("level 0") uses standard-technology sensors (measurements and monitoring) and actuators (pumps and solenoids) ;
- "Level 1" is divided between automatic control by On-Off actions (and, first of all, the reactor protection circuits and the Turbine Generator Set), on the one hand, and the reactor control systems and the turbine (to ensure power output matches grid power demand) on the other: automatic control is provided by the electromagnetic relay circuitry, while the control cabinets feature ANAlog technology (Control-Bailey modules 8720 or 9020, Alsthom REC 70 in particular);
- the control room ("level 2") makes available to the operators strip recorders and galvanometric indicators for tracking, flashing windows and horns for alarms, selector keys, pushbuttons (the well-known backlighted pushbutton switches) and potentiometers (Auto-Manual Control Stations, Setpoint Stations) for controls, all on standard consoles.

The only breakthrough, the former "status recorder", an indispensable tool for retroactive analysis of any operating incident, made its control room appearance in the computerized and improved form[4] of centralized data processing (CDP). Supplied by software service companies specializing in the energy field, this CDP only participates in real-time plant control by differentiating between the alarms grouped in the same window. As it consists of a plant control aid, it is on the boundary with "level 3" [5].

[1] The 900 MW **C**ontract **P**rogramme was made up of three plant series:

- the 6 units of **CP0**: Fessenheim 1-2 and Bugey 2-5 ;
- the 18 units of **CP1** : Tricastin 1-4, Gravelines 1-6, Dampierre 1-4, and Blayais 1-4 ;
- and the 10 units of **CP2** : St Laurent B1-2, Chinon B1-4 and Cruas 1-4.

For the 1300 MW power plants, a distinction is made between two PWR **4**-loop plant series:

- the 8 units of **P4** : Paluel 1-4, St Alban 1-2 and Flamanville 1-2 ;
- and the 12 units of **P'4**: Cattenom 1-4, Belleville 1-2, Nogent 1-2, Penly 1-2 and Golfech 1-2.

The 1450 MW series (or N4, as in **N**ew **4**-loop) is made up of Chooz B1-2 and Civaux 1-2.

[2] But the "UNGG" units (Natural Uranium, Graphite and Gas) were nevertheless given plant control computers ...

[3] Bear in mind that the Westinghouse PWR license originally left only a small share for automatic controls.

[4] The histories, diagrams etc did not exist in the status recorders.

[5] As a result, some classify it as level 2.

The latter level[6], which groups together "constraint time" data processing systems, is not subject to the operating and safety requirements which govern real time. This is probably why these systems were favorable for computerization experiments (Tagging System, Event Counting, grid follow, environmental monitoring, ...) from the very first 900 MW units.

Emergence of programmable controllers in the process: SPIN, Controbloc, ... , KIC/N4

The flexibility offered by IT soon attracted the attention of French I/C system designers (including CEA and Framatome), for two reasons:

- the need to improve knowledge of physical parameters, and therefore the operating conditions (particularly for increasing reactor operation margins). This led to the development, by Merlin-Gerin (the future Schneider-Electric), of the first Digital Integrated Protection System (SPIN), based on Motorola 6800 microprocessors. However, emphasis should be laid on the boldness of the manufacturers, who gradually developed by themselves the whole array of digital I/C systems required by their processes, both for the logic of the so-called auxiliary systems (CGEE-Alsthom created the range of Controbloc programmable controllers for this purpose) and for the control channels (Micro-Z and µREC in the 1300 MW plant series).
- the Three Mile Island accident, which highlighted the safety and human factor aspects, was the catalyst for the program baptised S3C (Control Room and I/C combined with simulator) leading to the N4 concept: its total computerization, including plant control procedures, makes Chooz B and Civaux the flagships of the computerized units.

The attached table briefly summarizes and illustrates this trend, from two "time-based" standpoints: history (plant series) and data processing speed (corresponding to the I/C levels).

[6] A field which must be distinguished from the huge field of office automation: there are several hundred applications, most local, but all disconnected from the process ("level 4" ?).

Plant series:	**CP0 / CP1 / CP2**	**P4**	**P'4**	**N4**
Levels :	34 **900 MW** units	20 **1300 MW** units		4 **1450 MW** units
Level 0: instrumentation	Standard technology	Standard technology		Standard technology
Level 1:				
Automatic controls	Electromagnetic relays	Controbloc (CGEE-Alsthom)		Contronic-E (Hartmann & Braun)
Reactor protection circuits	Electromagnetic relays	SPIN (Merlin-Gerin)		SPIN (Schneider-Electric)
Reactor control systems	Analog electronics	Analog elect.	Micro-Z	Contronic-E (Hartmann & Braun)
Turbine protection/control	REC-70 (Alsthom)	REC-70	µREC	µREC (Alsthom)
Level 2:	Standard control room	Standard control room		"KIC" (Sema-Group) :
Tracking	recorders/indicators/windows	recorders/indicators/windows		Screen images
Controls	keys, backlighted pushbutton, auto-manual control station ...	keys, backlighted pushbutton, auto-manual control station		Interactive images
Procedures	manual	manual		computerized
Level 3:				*Functionalities incorporated*
Status recorder	"KIT-KPS" (Sema-Group)	"TCI" (Sema-Group)		*in KIC above*
Other systems	Many digital monitoring, maintenance, management applications ...			

Current trends

Revamping

The first I/C revamping operations are all aimed at computerization, at least partial. Such projects abound, right across the world. Some systems which have become obsolescent have to be replaced by digital systems. As a result, this topic is giving rise to intense standard-related activity (followed up by the IAEA and the International Electrotechnical Commission).
In France, two projects focussed thinking on possible I/C revamping of units prior to N4:

- The project baptised R2C and centering on the second ten-year inspection programs (VD2) of the 900 MW units (from 1998-1999) only led to two modifications, limited to the oldest units of Fessenheim and Bugey (CP0). It involves the steam generator level control (revamp based on Alstom's P320), and the flux measurement and nuclear protection system (RPN system), which inaugurated Schneider-Electric's new product line SPINLINE 3. It can be seen that technical and economic caution has, until now (the first units of the CP0 and CP1 plant series have just experienced their VD2), won out over innovation as long as the durability of the "old" relay-based systems is not threatened.
- The ACCORD program, aimed at the VD2 of 1300 MW plants, did not lead to spectacular decisions either. At the most, consideration is being given, on the eve of the second ten-year inspection program, to identifying spare (or repair) solutions for a given board thought fragile in Contrôbloc, or replacing the CDP, whose maintenance is becoming costly, by a commercially available supervision system.

EDF's comparative caution towards large-scale revamping is due in particular to its specific situation as sole operator of a pool of 58 units, characterized by a strong plant series effect (similarities and even absolute identities between units). Owing to its specific position, it very early (the R2C delivered its first verdict in 1995) reviewed equipment and system ageing and obsolescence issues and deduced coherent, industrial-scale action programs. Regarding I/C, the main focus is on the building of strategic storage areas, the contracting of durability agreements with the main suppliers of critical, difficult-to-interchange systems, the developing of any necessary repair methods as necessary and the setting-up of an I/C Ageing Observatory (recently reactivated with a view to making a new status report to prepare the future VD3s (third ten year outage program: the first will take place around 2008-2009).

Keeping in operational conditions

Other changes are nevertheless perceptible, which may be difficult to dodge for utilities like EDF. Most of the equipment items are now provided, from the outset, with digital components whose functionalities benefit other customers. This is especially the case with smart sensors, for which a supplement is paid to equip them with a 4-20 mA analog output [7]. This is already true for circuit breaker cells or switchboard contactors, likewise recorders, indicators, etc. Mass-market computing is also continuing to expand and threatening the preserve of top-of-the-range computers like workstations under UNIX : the result is that computing applications (will) rely increasingly on commercial "black boxes", the well-known *COTS* (*commercial off-the-shelf*) of the Anglo-Saxons.

[7] It is clear that the electronic component era is coming to a close, while that of relays (needed for power amplification and galvanic isolation) is not threatened in the short term: it can be observed that, despite the massive computerization of N4, there are more relays in a 1450 MW unit than in a 900 MW unit!

Moreover, the evidence shows that the more a plant is computerized, the more it relies on digital components whose industrial life cycles are short and on difficult-to-maintain software skills. As a result, this type of I/C is threatened with fast obsolescence. This general observation is backed up by our experience in both 1300 MW and N4 plants. This is only one (tempting) step away from the reverse proposition ("to ensure long unit life, keep standard technology"), which is worth debating.

The search for profitability ...

... from which nuclear cannot escape forces EDF to look for non-specific solutions. This option is irreversible. But it conceals a formidable, near-structural contradiction: as IT is by far the most opaque and the least durable industry, how, with the products on the market, can safety requirements (and therefore dependability demonstration, which means free access to all documentation) and lifetime (which is the basis for return on investment but assumes the retention of skills, particularly in software) be reconciled? These two requirements are inherent in the nuclear process and therefore in its associated instrumentation/control.
The forthcoming major choices will depend on the resolution of this contradiction, as it is difficult to imagine fitting a new unit (for example EPR) with instrumentation/control of a technology which is not in the industrial mainstream.

French PWR units

giving :

- **the breakdown by plant series ...**
- **and the connection dates of the first unit of each site.**

900 MW *			1300 MW ***		1450 MW
CP0 *	**CP1 ****	**CP2 ****	**P4**	**P'4**	**N4**
6 units	**18 units**	**10 units**	**8 units**	**12 units**	**4 units**
Fessenheim 1-2 Apr. 77	Tricastin 1-4 May 80	St Laurent B1-2 Jan. 81	Paluel 1-4 June 84	Cattenom 1-4 Nov. 86	Chooz B1-2 Apr. 77
Bugey 2-5 May 78	Gravelines 1-6 March 80	Chinon B1-4 Nov. 82	St Alban 1-2 Aug 85	Belleville 1-2 Oct. 87	Civaux 1-2 Apr. 77
	Dampierre 1-4 March 80	Cruas 1-4 Apr. 83	Flamanville 1-2 Dec. 85	Nogent 1-2 Oct. 87	
	Blayais 1-4 June 81			Penly 1-2 May 90	
				Golfech 1-2 June 90	

* The 6 units of Fessenheim and Bugey do not form a true plant series

** The nuclear islands of CP1 and CP2 are strictly identical. Only the turbine halls are different (respectively "transverse" and "radial").

*** P'4 is a "slimmed-down" of P4 (civil works and layout savings).

The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan

Yoichi Mito [1], Masafumi Utsumi [2.]

[1] *The Kansai Electric Power Co., Inc. Nuclear Power Division*
3-3-22, Nakanoshima Kita-ku OSAKA 530-8270 Japan
Tel.: +81-70-5938-2709, Fax: +81-6-6444-6279, e-mail: K576277@kepco.co.jp.

[2] *Mitsubishi Heavy Industries Ltd. Nuclear Energy Systems Engineering Center*
1-1-1, Wadasaki Hyogo-ku KOBE 652-8585 Japan
Tel.: +81-78-672-3305, Fax: +81-78-672-3268, e-mail: utsumi@atom.hq.mhi.co.jp

Summary

To resolve the aging and obsolescence issues for instrumentation and control (I&C) systems at nuclear power plants, it is necessary to form a long-range maintenance and replacement plan for them systematically. To plan to replace the non-safety I&C system, the digital I&C system would be the most powerful choice from the view of maintainability and reliability because it has already been applied to our latest PWR plants. For the safety I&C system, even though digital safety system has already developed for the next PWR plants, it has never yet been applied to our plants. Therefore, how to apply digital safety systems to existing plants has been carefully studied. At first, the differences on safety functions, redundant architecture, and system interface between the next PWR plants and the existing plants have been studied. Then, the best replacement plan for safety I&C systems has been studied to obtain as much benefits as possible that are expected for the next plants, such as high reliability, availability, operability, maintainability and cost reduction.

1. Introduction

Aging and obsolescence issue of I&C system in Japanese PWR plants has become a potential major problem, though the system has been showing excellent operating results for many years. Also, conventional non-digital I&C system contains a lot of components which need to be adjusted and maintained. So, many man-hours have been consumed for testing and maintenance during plant shutdown.

In addition, the nuclear power plants are required safety operation and higher availabilities, I&C system upgrading program from the conventional system to the latest digital system will contribute to improve system reliability, testability, and maintainability.

To upgrade I&C system in the near future also contribute to conduce plant life extension, short maintenance outage, and periodical safety review.

To apply the digital technology into the safety system, it should meet various licensing requirements. So, a joint study with utilities and venders was started to establish digital upgrading program for the safety system of the operating plants.

This upgrading program will be applied commonly to various plants that have different numbers of primary loops or different historical design backgrounds. Therefore, it is important to standardize the planning process, the applicable system architecture, and the upgrading procedure in order to ensure successful design and modification activities, and simplify operation and maintenance. In this standardization, some options will remain such as the type of the main control board (conventional type or fully computerized type) to satisfy various needs of utilities.

This paper reports status of the on going joint study to establish the most suitable system architecture and upgrading procedure to upgrade the safety system of operating plants with the digital system. The major points of this paper are;

- Selection of the model cases of system architecture
- Evaluation for each model case.

2. Digital application at Japanese PWR plants

There are sufficient successful experiences in the digital application to various non-safety control and monitoring systems. From the historical view, digital system was applied to the Radiation Waste Processing System at first. For the latest plants, digital technology was applied to all non-safety systems such as reactor/turbine control system and plant monitoring system.

Application of the digital technology into the non-safety systems is one of the steps of the plant wide digitalization plan. So, the platform hardware and software has been developed and verified in view of further their application to the safety system. For the next plants currently under licensing stage, digital system will be applied all I&C systems including safety system.

For the next plants, the operabilities and maintainabilities of digital I&C systems are improved based on various operating experiences and state of the art digital technology. And, its development and verification has finished.

3. Applicability of the system for the next plants to operating plants

To replace the safety system of operating plant with digital system, the first option will be applying the next plant system. But, it is difficult to apply the next plant system directly to operating plants because of some differences in system configuration and interfaces.(Fig.1) The issues are as follows.

(a) Difference in redundancy
Redundancy of the safety system in operating plants basically consists of three channels and two trains. On the other hand, the redundancy of the next plant consists of four channels and four trains.

(b) Difference in system interfaces
For operating plants, safety system interface with many dedicated controls, indicators and instrumentation modules via metal cables. On the other hand, for the next plant, communication network system is used as interface means between systems.

According to above differences, system architecture of the digital safety system for operating plants should be carefully examined from various points of views. Not only the differences in redundancy and system interface, but also items shown in the next section should be considered in the case study of the digital safety system for operating plants.

4. Case study of the digital safety system architecture for operating plants

Approach to establishing the suitable system architecture of the digital safety system for operating plants is going on based on evaluation of model cases.(Fig.2) In this section, preconditions to establish model cases and evaluation points for these model cases are described.

4.1 Preconditions to establish model cases

(1) Conformance to the latest licensing requirements

Some of the licensing requirements have been changed since it was issued for the current operating plants. These changes has been enforced plant safety and has clarified the design basis requirement. These latest licensing requirement updates are fully considered to develop model cases for digital upgrading for the safety system in operating plants.

(2) Functionality of the safety system

There are differences by plant in functional design and redundancy of the safety systems in operating plants. All these designs satisfy safety acceptance criteria through the safety evaluation in licensing process. But there are some points to be modified from the point of plant availability and operability improvement. For example, in the latest plants, four-channel system configuration and elimination of steam generator flow mismatch reactor trip improved plant operability. In the next plant, variable setpoint for the delta-T reactor trip will also improve plant operability.

To introduce these design into operating plant, safety re-evaluation is needed and additional equipment installation should be considered. Therefore, economical analisys have to be done to decide the re-modification on the safety system.

(3) Scope of digital application

It is important to study which system or function should be digitalized in the actual system architecture. In the next plant design, digital technology will be applied to all the safety system. On the other hand, for the operating plant upgrading, we are studying which system or function should be replaced by the digital system from the point of the interface with other systems. In this study, we are considering to include solid state logic circuit to the renewed safety system.

To examine the scope of digital application, reliability, testability and maintainability are also considered. Furthermore, countermeasures for common mode failure in the digital safety system will be included.

(4) Type of the main control board

Type of the control board is one of the major concerns to examine plant wide digital upgrading program. Conventional type control board of the operating plant is consists of dedicated instrumentation modules and controls. Instead, new type control board will be applied to next plants that is fully computerized with soft controls.

Basically, two types are considered. One is the replacement to the conventional type control board with individual indicators and controls such as used in the latest plants. The other one is the replacement to the fully software based control board for the next plants. Therefore, digital safety system must be fit to both of them.

Major Difference in interface between the safety system and the control board is the use of individual cables and communication network. Especially, component of control circuit configuration is quite different between the analog system and the digital system. In analog system, each electrical contact of controls at the control board, magnetic relays in controllers, and local switchgears are connected by individual cables to form control logic. On the other hand, in the digital system, all these data is put into the digital system to form control logic.

4.2 Evaluation points

Comparison on possible model cases based on above-mentioned preconditions are going on from many points of view including reliability, availability, test and maintenance, installation work and economy. Special considerations to be evaluated are summarized bellow from the point of upgrading of the existing system.

(1) Cabinet layout

In the planning about the layout of the cabinet, spatial separation requirements and required space due to the change of system architecture should be considered. Design basis about spatial separation in some old operating plants could be quite different from the latest design. So it will be possible to reconfigure cabinet layout referenced to the latest design at the same time with the replacement work of the cabinets.

On the other hand, due to the difference of system architecture between newly introduced digital safety system and the existing system, it may be difficult to install new cabinets in the same area of corresponding existing cabinet.

So it is important to examine possible layout changes including modification of the layout space considering spatial separation criteria for the safety system and the supporting system design such as heating and ventilation system. It might be needed to prepare new instrumentation rack room other than the existing room with some rearrangement of the layout within the building.

(2) Reuse of existing cables

Network interface between digital systems will be able to widely introduce instead of the existing interface using huge amount of cables. Especially, in the interface with the main control room and the plant computers, many cables and individual interface components such as isolation amplifier will be able to be eliminated. But, there will still remain many individual cable interfaces between non-digital equipment such as local cabinets and sensors. So it is important to reuse existing cables to minimize amount of replacement work.

Because it is difficult to extend existing cables, possible termination layout design within each cabinet and installation of some additional termination cabinets are considered in our examination. If it will needed, new termination cabinets may be installed in the cabling room under the instrumentation rack room, and some multi conductor cables may connect the new termination cabinets and the digital safety cabinets. These concerns are depend on the system architecture design and cabinet configuration of the digital safety system.

In addition to these planning, detailed investigation of the existing cables will be needed to identify each cable and to confirm route of cables and spare space in cable tray in the implementation design phases.

(3) Testing and maintenance procedure

Digital system will be able to improve testability and maintenability by many features such as elimination of components tend to drift, automatic test, automatic calibration, and self diagnostics depend on the platform and system design. These new features will change items and processes of the test and maintenance work drastically compared with conventional system. To effectively apply these features, test and maintenance procedure during plant refueling outage should be reviewed and revised. Also, equipment test requirements such as technical specification will be reviewed to achieve appropriate test procedure and interval.

(4) Effect on supporting systems

Introduction of the digital system into the safety I&C system may cause increase of power consumption and non-linear load effect on the vital instrumentation power supply system. In some cases, additional batteries or replacement to more large inverter will be needed.

Also increase of the heat source depend on the system architecture should be evaluated from the point of the heating and ventilation system design.

These examination about effects on the supporting systems should include adequate margin from the point of plant wide long-term I&C upgrading.

5. Approach to realization of digital safety system

The optimum facility compositions for the operating plant is due to be determined from the evaluation points. It is necessary to continue the following examination, in order to actually apply them to the existing I&C system.

(1) Determination of suitable upgrading time in I&C system

First of all, the facility renewal is necessary because of the deterioration of the apparatus and unavailability of electronic parts. Considering the life of the plant, I&C system needs to be replaced at the most optimum time.

(2) Consistency with plant wide I&C upgrading program

As stated at the beginning of this paper, digital upgrading of the safety system should be planned in accordance with the renewal of whole I&C system. And to realize the plan, the future design of the whole I&C system is indispensable. This future plan must include the upgrading of the main control board.

Therefore, in parallel to this examination, the future design of the main control board is being considered.

(3) Upgrading procedure of I&C system

In a case of realizing the future design of the whole I&C system, it is not so practical to replace all the I&C system at the same time because it will require too much long-term plant shutdown. So, it is feasible to perform replacement work by each through some plant refueling outages. In this situation, not only the examination on the plant wide final system architecture, but also the examination on the feasibility of the temporary system configuration is important.

As the digital systems already replaced and the conventional systems mixed in the temporary configuration, interface between systems will change along with the upgrading schedule. Though this situation itself is an inevitable process, it is important to establish the upgrading program that minimizes the changes in design of the interface portions of already replaced system.

From this point of view, the order of the system replacement is under examination to minimize the cost and to realize easier work process aiming at plant wide long-term upgrading program.

6. Conclusion

Systematic examination on plant wide I&C digital upgrading program into the Japanese operating PWR plants has been started. Especially, utility and vender joint study about the safety system upgrading is going on considering various items including licensing issue. Coupled with the examination about the type of main control board, an standardized upgrading program for operating plants will be established that include the system architecture and the order of implementation.

Fig.1 Operating Plants – Next Plants System Configuration

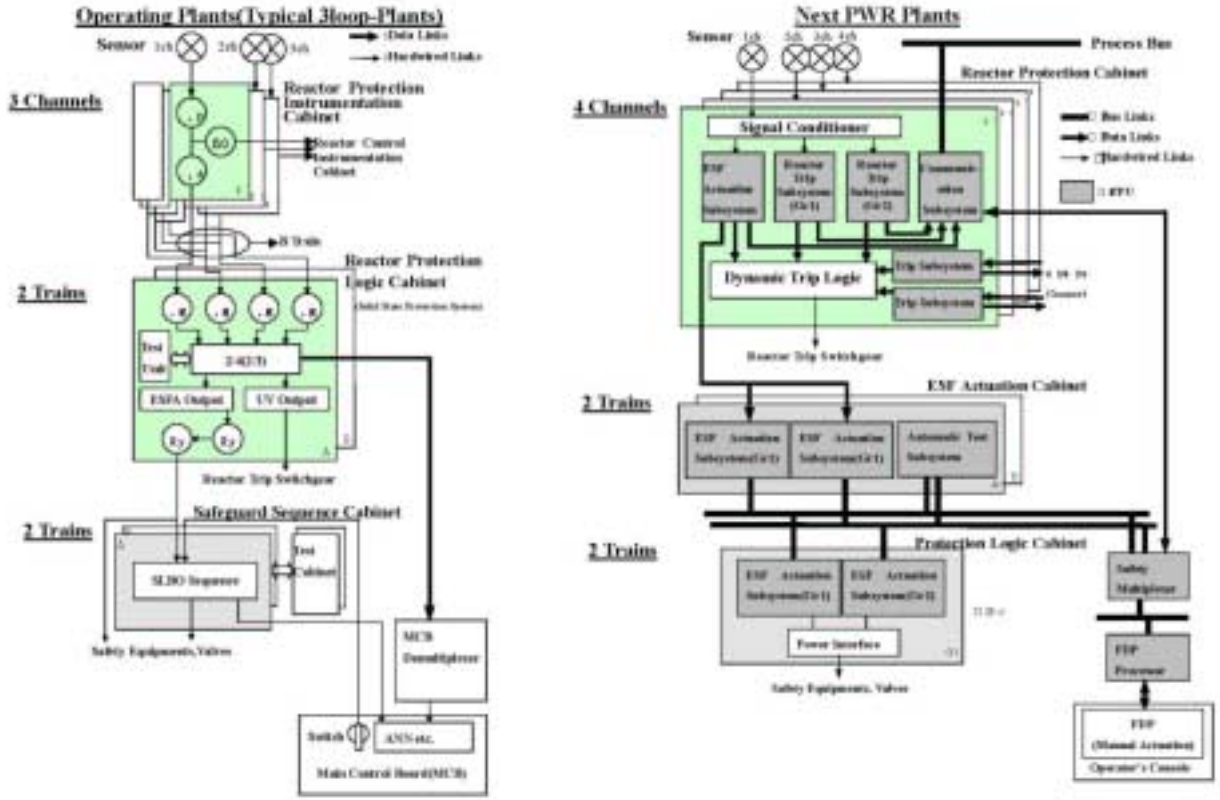
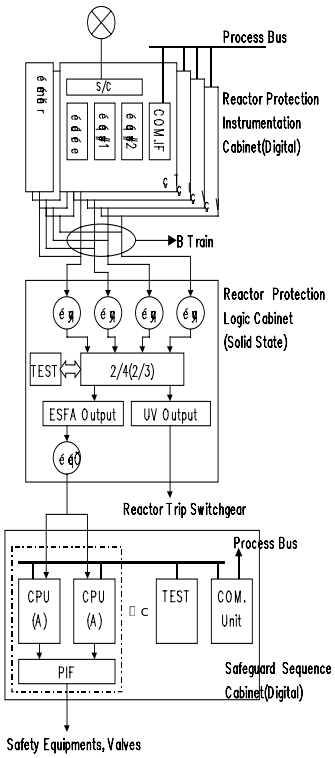
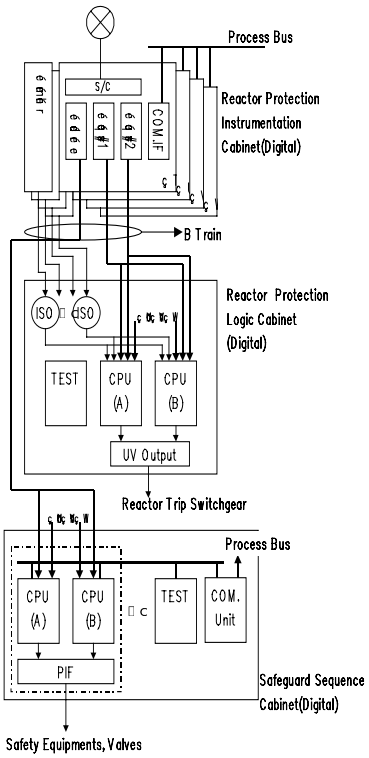
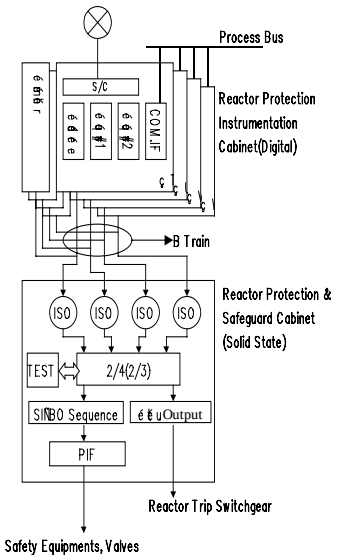


Fig.2 Typical Case of Safety System Composition (Application of the Digital System)

CASE1	CASE2	CASE3
		
Applying digital system to the reactor protection instrumentation cabinet and the safeguard sequence cabinet	Applying digital system to the reactor protection instrumentation cabinet, the reactor protection logic cabinet and the safeguard sequence cabinet	1. Applying digital system to the reactor protection instrumentation cabinet 2. Integrating the safeguard cabinet into the reactor protection cabinet

Independent Assessment of the Temelín Safety System Software

Petr Závodský
ČEZ, a. s., Division of Construction of NPP Temelín
Tel: +420 334 78 2151, Fax: +420 334 78 3815, E-mail: Zavodsky_Petr@mail.cez.cz

Summary

The Instrumentation and Control (I&C) System for the Temelín Nuclear Power Plant has been designed and supplied by Westinghouse Electric Company under contract to ČEZ and Škoda Praha. Under this contract, Westinghouse have performed independent verification and validation of the software for the safety related portion of the I&C system. In addition, a programme of Independent Assessment (IA) has been carried out to provide additional confidence in the integrity of the safety system software.

Data Systems and Solutions LLC (DSAS) have carried out the IA activities under contract to ČEZ. These activities were independent of Westinghouse. They were designed to confirm that the software production processes complied with the specified standards and to assess the software for each system. These activities were designed to be diverse from the V&V activities of Westinghouse. The scope of the IA activities was originally defined by the Czech Regulator SÚJB.

Introduction

ČEZ, a. s. Nuclear Power Plant Temelín is currently in the process of start up, commissioning and constructing two nuclear power units, based on the VVER 1000 Russian designed reactors. The Instrumentation and Control (I&C) system is being upgraded by a modern Westinghouse supplied I&C system, which meets requirements imposed on current NPP designs.

Safety Systems and Their Safety Roles

There are four safety systems of which two are automatic protection systems and two are reactor monitoring systems.

- PRPS and DPS are diverse automatic protection systems.
- PAMS and DMS are diverse reactor monitoring systems.

The automatic protection systems contribute most to plant safety as these perform automatic actions to maintain the plant in a safe state. The monitoring systems perform a significant but smaller safety role as they provide the operator with post-accident information on the reactor.

Primary Reactor Protection System

The Primary Reactor Protection System (PRPS) measures key plant parameters and performs automatic actions to maintain the reactor in a safe state including reactor trip and initiation of plant to maintain the reactor in a safe state after trip. The functions of the PRPS are:

- To provide an automatic reactor trip in all credible reactor faults that require reactor trip as part of the reactor protection requirements;
- To actuate engineered safety features (ESF) to maintain reactor safety, including post-trip cooling and containment isolation, in all credible reactor faults.

The PRPS is divided into three redundant Divisions that each comprise safety grade field sensors, Nuclear Instrumentation System (NIS) ex-core flux monitoring detectors and equipment, Integrated Protection Cabinets (IPC) and associated Reactor Trip Switchgear, and ESF actuation logic cabinets. A reactor trip condition in one Division is communicated to the other two Divisions where voting takes place which, if satisfied, results in initiation of reactor trip. Similarly, ESF actuation demands are communicated to other Divisions where voting takes place which, if satisfied, initiates the appropriate ESF plant systems depending on the initiating conditions.

The PRPS uses Westinghouse Eagle family hardware, utilising Intel 80X86 microprocessors. Each subsystem incorporates a 'host' processor board, in combination with a number of slave processor boards that provide input, output and communications functions. This general architecture is identical to that used on the Sizewell 'B' Primary Protection System (PPS), but some upgrades to the technology have been made in the Temelín PRPS. The PRPS software is mostly written in PL/M 86 but contains some modules that are written in ASM86 assembly language.

Diverse Protection System

The Diverse Protection System (DPS) is a secondary means of achieving reactor trip and initiation of post-trip cooling and provides automatic protection against all frequent reactor faults. The functions of the DPS are:

- To provide an automatic reactor trip in all frequent reactor faults that require reactor trip as part of the reactor protection requirements;
- To actuate engineered safety features (ESF) to maintain reactor safety, including post-trip cooling and containment isolation, in all frequent reactor faults.

The system therefore provides diverse reactor protection against reactor faults. As with the PRPS, the DPS comprises three redundant reactor trip and ESF actuation Divisions (Divisions I, II and III). DPS uses a different hardware platform (Motorola-based) and software language (Ada, with some 68000 assembler) to that of the PRPS. The DPS software is split into two main layers – Platform code and Application code. The Platform code provides the generic operating environment whilst the application code performs the safety tasks. As with the PRPS, the DPS uses configuration and calibration data to configure the application and provide tuneable constants.

Post Accident Monitoring System

The Post Accident Monitoring System (PAMS) is the primary means of acquiring and displaying reactor plant parameter indications to the operator that are important for accident mitigation. The functions of the PAMS are:

- Post-accident data acquisition;
- The display of plant variables important to accident mitigation.

The PAMS uses the same type of hardware, the same programming languages and the same software structure as the PRPS. The PAMS comprises two redundant divisions, each of which displays the post-accident information required by the operator, including redundant and diverse channels. The redundancy assures that loss of one power division along with the affected Post Accident Monitoring System division and input channels, is accommodated by the remaining Post-Accident Monitoring System division, without loss of required information and without creating information ambiguity.

Diverse Monitoring System

The Diverse Monitoring System (DMS) is a secondary and largely diverse means of acquiring and displaying all reactor plant parameter indications to the control rooms that are important for accident mitigation. The functions of the DMS are:

- Post-accident data acquisition;
- The display of plant variables important to accident mitigation.

The DMS uses the same type of hardware and the same programming languages as the DPS. The DMS can be considered to be an extension of the DPS that performs functions associated with displaying plant information to the operator. There are two divisions of DMS – one for the Main Control Room (MDMS) and one for the Emergency Control Room (EDMS).

Software Development Processes at Westinghouse

Implementation diversity between PRPS/PAMS and DPS/DMS is maintained by using different development teams, development processes, development platforms and tools for the two sets of systems. Associated with each of the development teams (Design Groups) is a management-independent group responsible for software V&V (V&V Group). The Design Groups are responsible for system and software specification, design and implementation. Members of the design team also perform review activities such as Design Review and second party review. A separate team within each Design Group is also responsible for subsystem and system level factory testing. The V&V Groups are responsible for verifying the software against its specifications through review, static analysis and module test activities. For DPS the V&V Group also performs V&V of higher level system documentation.

Acceptance Criteria

In 1994 SÚJB set up a clear licensing requirements, which are being used for evaluation and acceptance of the safety systems software. The acceptance criteria have been set as follows:

- The SW manufacturing including its verification at the manufacturer's factory (FAT) as well as on site (SAT) and check of the accepted SW (so called pre-existing SW) is in accordance with currently recognised recommended procedures for attainment of high quality end product (IEC-880/1986, ASME NQA-2a/1990 part 2.7, IEEE 7-4.3.2/1993),
- Independent verification and confirmation that the mentioned procedures have been really met,
- A positive outcome (meaning that no substantial deficiency has been detected which might endanger meeting the requirements of the corresponding safety function) of a Independent review of the SW end product which involved:
  - Check of system requirements and of the from them derived requirements on SW;
  - Static analyses of selected SW parts /related to PRPS and DPS/;
  - Dynamic tests of the SW as a system /related to PRPS only/.

Programme of Independent Assessment

The fulfilment of item 1) under acceptance criteria falls in responsibility of the I&C Supplier Westinghouse. To fulfil the items 2) & 3) a separate Independent Assessment (IA) programme was prepared and conducted. It must be noted that Westinghouse's program of Testing and Verification and Validation of software satisfies the requirements of standards on Testing and V&V. The IA program was in addition to the requirements in the standards. Similar program was conducted on the software of the safety system at Sizewell B. These activities were independent and diverse from the V&V activities of Westinghouse and they were designed to confirm that the software production processes complied with the specified standards and to assess the software for each system.

Organisation

The Independent Assessment of the Temelín safety system software was contracted by ČEZ, to the prime contractor Data Systems & Solutions (DSAS). The Independent Assessment team consisted of DSAS and two major subcontractors, British Energy (BE) and Fluor Global Services (FGS) formerly known as TA Group (TAG). BE and FGS had additional subcontractors to assist in the work. ČEZ have had the responsibility for communication with SÚJB as well as ensuring provision and/or access to the information and documents from the supplier, Westinghouse.

The IA comprised the following tasks and was allocated among the particular sub-suppliers as given in brackets (see Figure 4 for IA tasks example):

- Independent audit of software development processes (conducted by DSAS);
- System Software Assessment (conducted by BE);
- System and Software Requirements Verification (conducted by DSAS);
- Software Design Verification (conducted by DSAS);
- Static Source Code Verification (conducted by FGS);
- Dynamic Testing (conducted by DSAS with assistance of BE);
- Common Mode Failure Assessment (conducted by DSAS);
- Data Verification and Validation (conducted by BE).

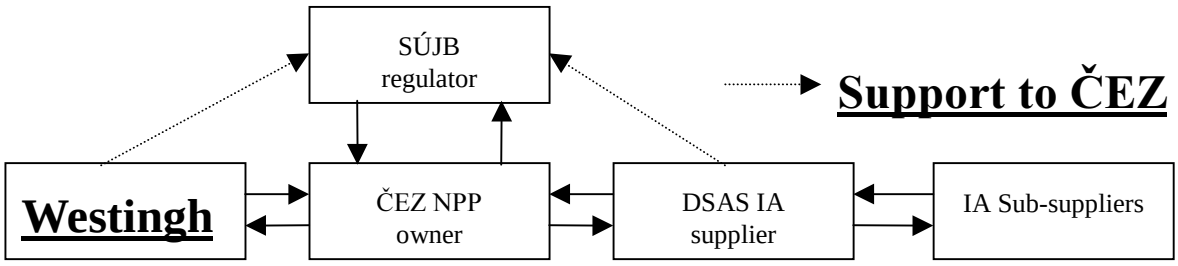


Figure 1 – Organisation of the Project

Independent Audit

Independent audits were performed on the Westinghouse software development processes for compliance with the following international standards:

- IEC 880
- IEEE 7-4.3.2
- ASME NQA – 2a, Part 2.7

The audits covered all (four) safety systems and were targeted at particular aspects of the development cycle. The audits also included an appraisal of the software development processes against certain good software development practices documented in the first supplement to IEC 880. Guidance given in NUREG/CR-6101 & NUREG/CR-6421 was used in the audit process, where appropriate.

The five audits were to audit the development processes against requirements and guidance that relates to plans and procedures and design implementation; the qualification of tools used in the development of software against requirements and guidance relating to the use of tools; the incorporation of features such as self-supervision, surveillance testing and return to service in PRPS and PAMS against requirements and guidance. Also appraised the development process against relevant industry good practice.

System Software (Tools) Assessment

System software was the term used to embrace the development system software tools that are used to develop the software of the safety systems. It includes compilers, linkers, locators, data table generation and other software tools. Some were commercial software tools and others were software tools produced by or for Westinghouse.

The overall objective of the system software assessment was to generate sufficient evidence to provide confidence in the integrity of the software tools used to produce the software. Particular attention was paid to those tools that perform complex transformations, such as compilers, which transform source code to object code. These tools have the greatest influence on the final executable code. The system software tasks set out to:

- Provide evidence that the system software has been developed in accordance with recognised good software development processes;
- Provide valid and objective evidence of operating experience of the system software;
- Provide evidence that the system software has been adequately verified, either through analysis or extensive testing for use in safety systems;
- Provide, where evidence is missing or is inadequate especially for commercially available products, further evidence that the tool performs correctly either through analysis, extensive testing (DPS) or by reverse engineering (PRPS source/code comparison) of a sample of the code.

System and Software Requirements Verification

The system and software requirements verification tasks cover the functional, performance, safety and integrity requirements. The purpose of these tasks was to confirm that:

- The system requirements satisfied all applicable codes, standards and regulatory requirements;
- The system requirements were a complete, consistent, unambiguous and accurate representation of the reactor protection functions;
- The high-level I&C system design was a complete and accurate representation of the system requirements with no unintended design elements;
- The software requirements were correctly derived from the system requirements;
- The software requirements were a complete, correct, accurate, clear, consistent and unambiguous representation of the software portion of the system requirements and design.

The scope of the task included all functionality except for subsystems not directly involved in performing the protection function such as the autotester, maintenance consoles and communication systems. To facilitate the verification of system and software requirements and to promote consistency, a traceability tool was used. The tool selected was DOORS.

Software Design Verification

This task took as its input the software requirements list generated by the System and Software Requirements Verification task. The task covered functional, performance, safety and integrity requirements in the software requirements. The purpose of the task was to confirm that the software design requirements had been correctly derived from the software requirements. The task comprised three sub-tasks:

- A software design traceability analysis that identified all software design elements from the Westinghouse documentation, which were then recorded in a software design elements list. The analysis traced the software design elements forwards and backwards to confirm that they are correctly derived from the software requirements list. It identified software requirements that are not adequately addressed in the software design, and software design elements not derived from the software requirements;
- A software design review that evaluated the software design for accuracy, completeness, consistency and correctness;
- A software design interface analysis that determined whether all external interfaces to the software and internal interfaces within the software are complete and that they are consistent with the software requirements. Each data flow item was evaluated for correctness by verifying that the name, format, content and syntax is correctly defined in all locations in the design and that each item is specified both as an input and output of interfacing modules.

For the PRPS, the scope of the task included all functionality covered in the software requirements task except for communications subsystems. For the DPS the scope was limited to the functions within the defined vertical slice.

Static Source Code Verification

Static source code verification was performed on all safety critical parts of the PRPS (defined by the PRPS hazard analysis task). Static source code verification was performed on a sample of the safety critical software for the DPS. The safety critical software was defined by the DPS hazard analysis task. The scope of the DPS sample was defined by the DPS software vertical slice analysis. This task was not performed on PAMS and DMS.

The task was a rigorous static analysis, involving a high degree of formality, to show conformance between source code and the software design. The analysis involved a tool-supported verification of the semantics of the code against the definition of the required operation of the code. It showed whether each source module implemented its corresponding module design specification and gave a high degree of confidence that the operation of each software subsystem met its requirements. This static analysis generally conformed to the requirements of IEC 880. The static analysis was carried out using software tool that was different from that used by Westinghouse. The source code was analysed using a suite of static program analysis tools known collectively as MALPAS. Static analysis comprises a set of techniques for examining the structure and the likely behaviour of the software without execution. The MALPAS analysis enabled the assessment to complete the analysis loop between the specification and the source code.

Data Verification and Validation

Data verification was achieved through verification of the data against the software specification documentation and the protection system requirements. The task included the configuration and calibration data for both the PRPS and the DPS but was limited to the safety critical sub-systems as defined for the Static Analysis task. The evidence provided by the task provides the main support for the assertions in the safety case regarding adequate data integrity.

Configuration data was verified as follows:

- Data used to configure the common functions employed by the application was checked for consistency with the Westinghouse standard template;
- Data used to configure local databases and the hardware interface used by the application was checked for compliance with the rules for the relevant data structure;
- Data was checked for correct cross-references, indexing, pointers to tables and correct buffer layout;

All data that determines functionality and architecture was checked for completeness against system requirements and functional requirements.

Calibration data was verified as follows:

- Functions that manipulate and use calibration data were checked to ensure that adequate range checking and error reporting exists;
- Data was checked to ensure the presence of all calibration data required by each function described in software documentation;
- Each calibration data item required by each function was checked to ensure that its value is in accordance with the system requirements.

Common Mode Failure Analysis

The objective of this task was to confirm that adequate defences against common mode failures exist in the design and implementation of the PRPS and DPS software and similarly, for the PAMS and DMS software. The CMF analysis task consisted of a number of activities including a review of Westinghouse documentation for CMF potential, discussions with Westinghouse personnel to determine the degree of independence between the primary and backup systems and analysis of inputs from the other IA tasks.

The analysis was performed in the following manner:

- Identification of potential CMF mechanisms through:
  - Review and comparison of development processes;
  - Comparison of development tools utilised and documented;
  - Review of identified sources in Section 4.1 of the First Supplement to IEC 880;

- Discussions with IA team members performing other tasks and review of products of other IA tasks as applicable.
- Documentation of CMF Issues - a CMF Issue was declared where any potential CMF mechanism was found to exist.
- Evaluation of each CMF Issue to determine the relative probability of occurrence - CMF Issues that were not determined to have a sufficiently low probability of occurrence were raised as Findings.

Dynamic Testing

The Dynamic Testing task was performed for the PRPS only. It was based on the same concept as the dynamic testing performed on the Sizewell B PPS. The scope of the testing was designed to maximise the coverage of the PRPS software safety functionality, therefore non-safety functions were excluded from the test coverage. The basis for exclusions from the testing was justified in a test boundary definition document.

The testing consisted of 5000 individual tests based on 10 selected accident scenarios. For each of the 10 scenarios, 500 unique combinations of PRPS input values were generated from reactor transient analysis. The tests were applied automatically to the Test Division and also to the Logical Model. The Test Division was a replica of PRPS Division 1 with simulated interactions with Divisions 2 and 3. The Logical Model was a software simulation of the PRPS requirements. Test results were recorded automatically and then compared to identify discrepancies between the predicted results from the Logical Model and the actual results from the Test Division. Discrepancies were recorded and resolved, with unresolved discrepancies being submitted as task findings.

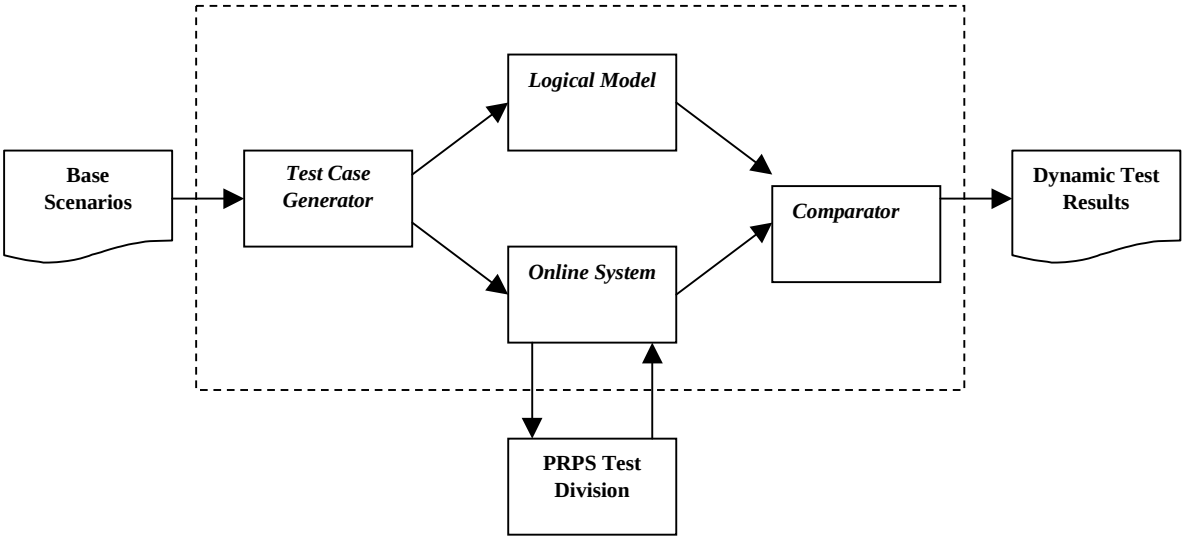


Figure 2 – Dynamic Testing Process Overview

CONCLUSION

Resolution of Findings

Each IA task had the potential to identify anomalies in the Westinghouse software processes, software and documentation. These anomalies were raised as Findings, in compliance with the Project Procedure "IA Findings Reporting and Resolution". This procedure defined the process that was used for generating, reviewing, sentencing to resolution and subsequent closure of Findings that had arisen. This process is represented in a simplified form in Figure 3.

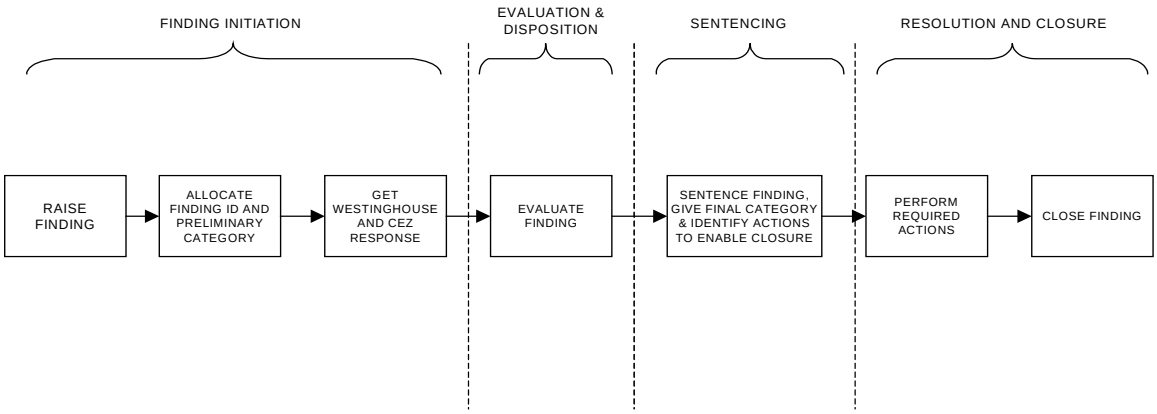


Figure 3 – Process of Resolution of Findings

Findings were sentenced by the sentencing team to agree on a final categorisation and resolution for each Finding, including the corrective action and corrective timescale categories. The sentencing team comprised a minimum of one member from the DSAS Project Management Team, one member from the organisation, which raised the Finding, a representative of ČEZ and a representative of Westinghouse. A category was assigned to each finding.

Severity/Safety Significance

Category 1: Impacts safety.
Category 2: No safety impact but is significant to the software development process or plant operation (e.g., could affect plant operation, provide misinformation to the operator or another system, or affect system testing).
Category 3: No safety impact, affects documentation, software, software development process, or conformance to defined requirements only.
Category 4: No safety impact, no effect on operations and no requirement to change documentation or software development process.
Other categories were Category 5: Invalid, Category 6: Duplicate and Category 7: Document baseline mismatch.

Corrective Actions

Category A: Design Change it is intended to align with Westinghouse's own Request for Engineering Change (REC) process.
Category B: Executable Code Change (does not include change to a code comment).
Category C: Design Document Change.
Category D: Development Process Impact.
Category E: Process Document Change.
Category F: No Action Required.
Category G: Complete the Development Process.
Category H: Provide Additional Evidence.
Category J: Add to "fix file" for consideration at the next revision of the item.
Category K: Confirm existence in "fix file" from Sizewell application.
Category L: Flag as operational issue.
Category M: Already addressed in later revision.

Statistic of Findings from IA program is following:

1	Impacts Safety	0.0%
2	Significant	0.5%
3	Not Significant	45.4%
4	No Effect	34.4%
5	Invalid	14.6%
6	Duplicate	1.3%
7	Baseline mismatch	3.8%

A	Design Change	0.0%
B	Executable Code Change	2.1%
C	Design Document Change	11.3%
D	Development Process Impact	1.2%
E	Process Document Change	1.8%
F	No Action	52.9%
G	Complete Development Process	1.3%
H	Provide Additional Evidence	0.2%
J	Add to Fix file	15.7%
K	Confirm in SXB Fix File	5.4%
L	Flag as Operational Issue	0.1%
M	Already addressed in later Rev	8.0%

Lessons Learned

Successful IA depends upon:

- Development process amenable to IA;
- Timing of work in relation to development phase;
- Adequate documentation;
- Cooperation of developers, assessors & customer.

Benefit of IA tasks can be maximised by timely and scope performance:

- Early tasks, focussed on development process;
  - Audits of development processes, to include some requirements IA;
  - Assessment of development tools.
- Later tasks focussed on verified products;
  - Static Analysis;
  - Dynamic Testing;
  - Data verification.
- Sample-based approach is acceptable, where justified;
- Consider relevancy of best practices from modern standards.

Lessons learned from particular tasks:

- Static analysis:
  - Need to define SA requirements early;
  - Make development process amenable to Static Analysis;
  - Need to match analysis to documentation quality;
  - Address code integrity and functionality separately;
  - Opportunity for significant automation.
- CMF task - Need for, and scope of, diversity between systems needs to be clearly defined prior to design activities;
- Dynamic Testing - It is the only IA task to validate end to end functionality;
- Source Code Comparison
  - Sample approach for SCC was deemed to be acceptable;
  - The SCC task should be started early to allow early tool development and to minimise the impact of findings
  - Feedback from tools suppliers is limited and difficult to obtain - effectiveness of this part of the task limited
- Audits:
  - They are effective, particularly when the audit scope is appropriate to the current lifecycle stage.
  - Elements of requirements IA tasks can be incorporated in the scope of audits.
- Data verification was effective in identifying a number of significant findings.
- Early involvement with the designers could help to automate the process and make it more effective.

Conclusions from IA program are following:

- Nothing was found that undermines confidence in the quality of either the software production processes or the software for the systems.
- The Westinghouse processes were shown to be generally compliant with the requirements of the relevant standards.

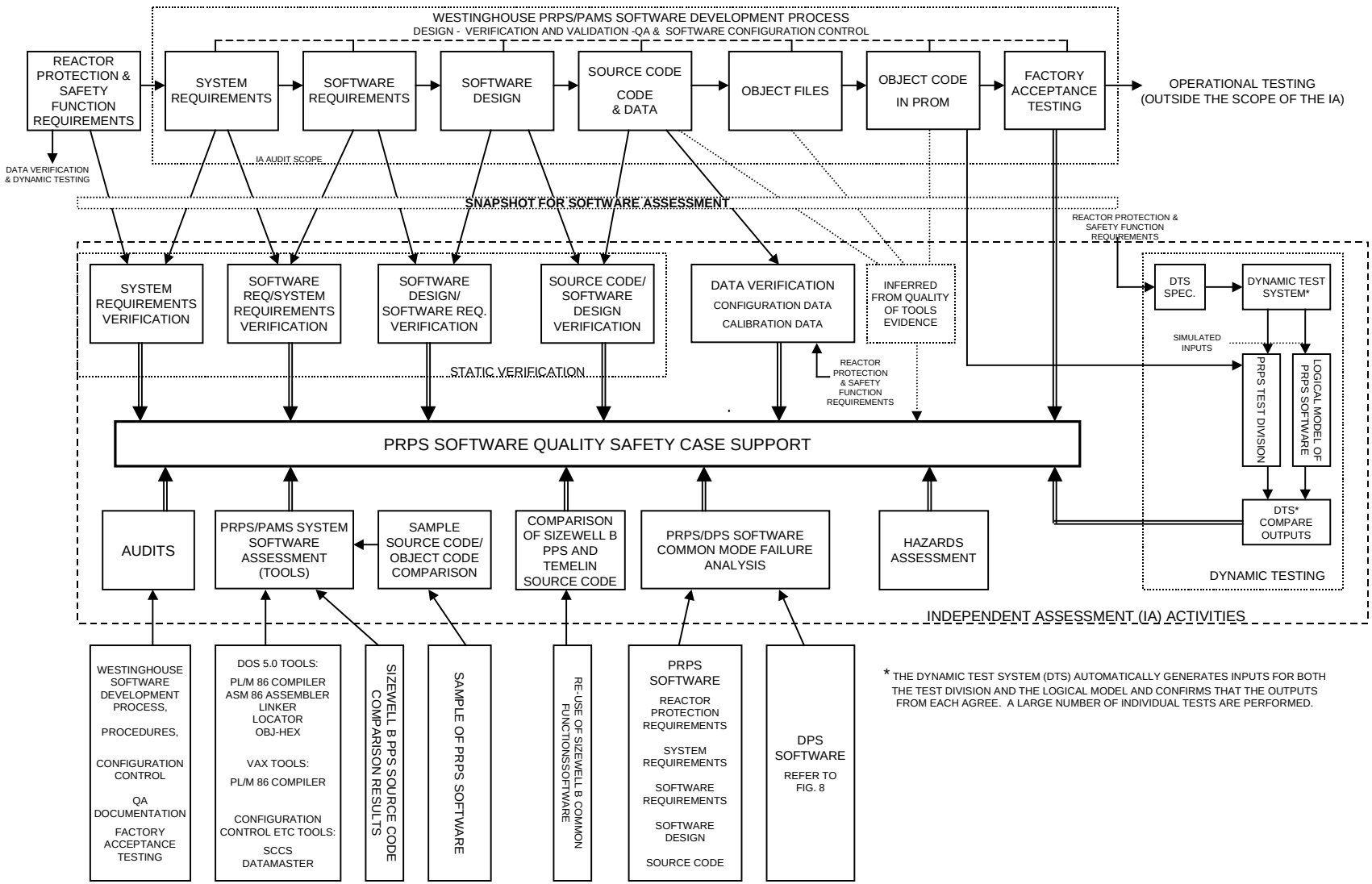


Figure 4 - IA Tasks for PRPS

Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor

DAI. I. Kim[1], B. R. Kim[1] and S. H. Oh[1]

[1] *Dept. of Instrumentation and Control, Korea Institute of Nuclear Safety,*
Ku Sung Dong 19, Yusung Ku, Daejeon City, 305-600, South Korea
Tel: +82-42-868-0246, Fax:+82-42-861-2535, Email:dikim@kins.re.kr

Summary

This paper presents the interim evaluation result and the regulatory approach of digital plant protection system (DPPS) for Korea Next Generation Reactor (KNGR: APR-1400). Firstly, we discuss the issue associated with the integration of bistable processor (BP) and local coincidence logic processor (LCLP) as one of design changes over digital plant protection system. Secondly, regulatory approach is presented on the safety classification and the independence of the soft controller to be installed in digital engineered safety features actuation system (DESFAS). Finally, hardwired back up systems against common mode failure of a digital system are described.

I. Introduction

In Korea, sixteen (16) nuclear power plants are being currently operated and four (4) units are under construction. The instrumentation and control (I&C) system of nuclear power plant has been partially upgraded or designed by a digital based system at the operating plant [1],[2]. However, recently, it is being designed as a totally computerized digital system in the instrumentation and control system important to safety. Whilst digital technology has the capability to improve both operational performance and safety, there might be some difficulties to evaluate it on the safety sense because evaluation methodologies have not been established systematically for a digital system and some portions of digital system can not but to apply implicit requirements applicable to an analog system.

This paper describes regulatory activities associated with the review of standard safety analysis report (SSAR) on Korea Next Generation Reactor (KNGR: APR-1400) submitted to the Korean regulatory body to attain the Design Certification (DC). The purpose of this paper is to present the regulatory approach for the safety assessment of a digital plant protection system (DPPS) of KNGR which has evolutionary design features and may result in key issues in regulatory review, thereby improving the safety of the plants and reducing unnecessary regulation burden.

The issues raised during the safety review are especially the system structure of DPPS related to bistable processor (BP) and local coincidence logic processor (LCLP), the safety classification of soft controller applied newly in the DPPS, and the defense-in-depth (DID) against common mode failure.

Firstly, we discuss the issue associated with the integration of BP and LCLP as one of design changes over previous digital plant protection system. Basically, these processors are separated physically since they have inherent functions to generate a trip signal and coincidence logic signal, respectively. However, licensee proposed the structure integrated bistable function with coincidence logic one to be controlled by a single processor. This integrated structure may cause the side-effects in the reliability of software due to the complexity of software, the functional diversity by the integration of processor, and the design consistency with analog protection system, even though the proposed structure is more reliable than the

separated one in view of simplicity of hardware. Therefore, it is required that bistable and local coincidence logic processors to have a distinctive function be separated to preserve the functional distribution and to accomplish software validation/verification (V/V) facilely.

Secondly, we discuss issues about the safety classification and the independence of the soft controller to be installed in DESFAS. The I&C systems of KNGR are designed using digital technologies like multiplexer/demultiplexer in safety systems to process data efficiently and to design optimum, compact and efficient system, whereby a huge number of manual switches dedicated spatially are replaced with soft controller which is mediated by software. This drastic design change makes it more difficult to ensure the independence between safety and non-safety signals and to perform software V/V [3].

Pursuant to requirements of codes and standards, manual switches used to control the safety-related components are classified into safety system. Therefore, the regulatory position is that soft controller functionally equivalent to manual switches shall be also classified into safety system including both software and hardware. In addition, the electrical isolation and physical separation among channels shall be maintained. Finally, regulatory approach is presented on the hardwired backup system against common mode failure for the DPPS in Section IV.

II. The integration of bistable and LCL processor

1. Background

The function of BP generates a command signal to actuate a reactor trip or an ESFAS when underlying process variable exceeds a trip setpoint comparing process variable with a trip setpoint. The LCLP performs the 2/4 logic function for every trip parameter to prevent spurious reactor trip signal. The BP and LCLP are inherent functions to accomplish the function of reactor protection. As shown in Table 1, it is designed such that the function of BP is independent upon that of LCLP in DPPS. However, the function of BP and LCLP of KNGR is controlled by one processor. We describe the regulatory approach on the structure of processor in the following subsections.

Table 1: Comparison of the number of processor in Digital Plant Protection System.

Processor	Wolsong (PDC)	Ulchin 5&6	ABB-CE System 80+	WH AP-600	KNGR
Bistable Processor (BP)	2/Ch -PDC1 -PDC2	2/Ch with forward and reverse direction	2/Ch (Assignment by diversity)	2/Ch (Rx trip) 2/Ch (ESFAS)	Unification of BP/LCLP 1/Ch
Local Coincidence Logic Processor (LCLP)	Relay 2/3 Logic	4/Ch forward(2) reverse (2)	2/Ch (Assignment by diversity	2/Ch (Rx trip) 2/Ch (ESFAS)	
Comm. between BP/LCLP	Hardwired	CCC-Hi-speed Serial Link	CCC-Processors (3/Ch)	Parallel I/O Comm. Processor	CCC-Processors (3/Ch)

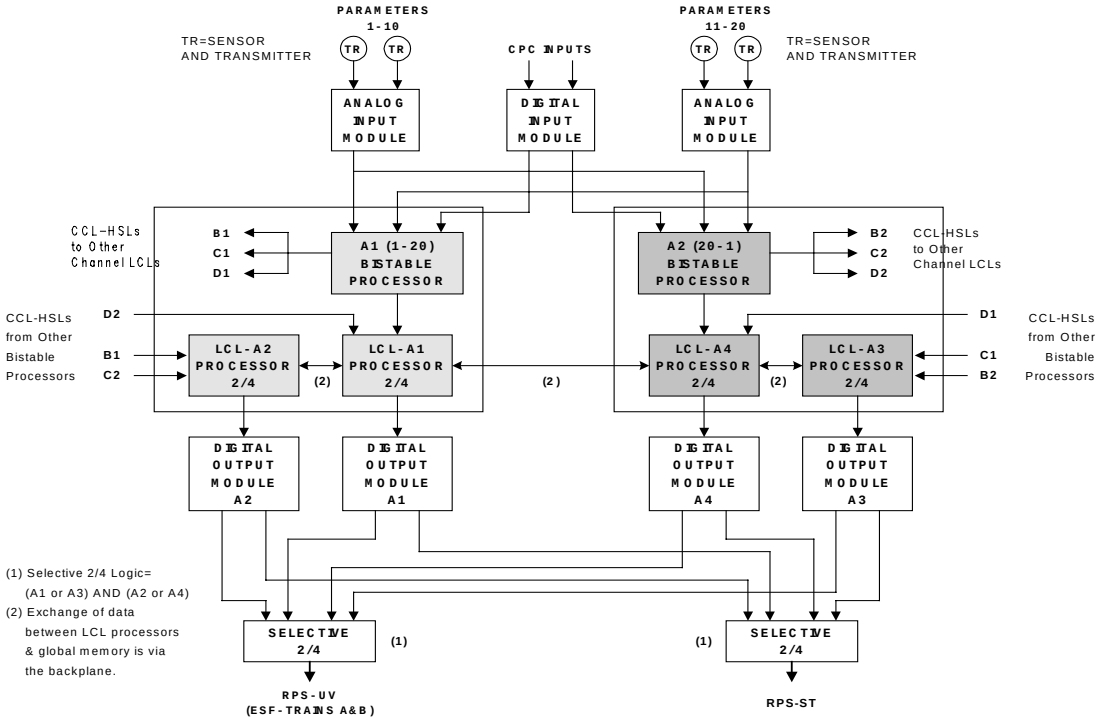


Figure 1 : Channel Block Diagram of DPPS (Ulchin units 5&6)

2. Diversity

In general, the design of digital system is distributing its function to accomplish the simplicity and to enhance the reliability due to the simplicity of software V/V. It is a current trend to design digital systems based on functional diversity. The protection system of Wolsung has two plant digital computers (PDCs) assigned by different trip parameters, therefore, even though one of PDC fails, the other PDC assigned as different trip parameters performs safety function. The protection of System 80+ is designed by principle of diversity similar to that of Wolsong plant. In case of Ulchin units 5&6, Korea, there are two BPs and four LCLPs per channel, they operate in reverse direction each other to implement the functional diversity. AP-600 system of Westinghouse has four BPs and four LCLPs, two BPs is for reactor trip and the other is for ESF. Different trip parameters are also assigned to two BPs and two LCLPs to implement the diversity. In this context, it is required that the DPPS of KNGR should be designed according to the principle of diversity.

3. Time Response and Performance

The distribution of function of BP and LCLP over the integration of them simplifies the design and enhances the system response time which may be used as a measurement of system performance. The integrated system controlled by one processor may increase the system response time and make more complex software compared with the separated processor (see Figure 1). Besides, even though the integrated system meets required response time, it may not be flexible to modify and expand its function because there is no sufficient margin after commercial operating. In general, it is practice to be designed with 40 % margin for the worst case. Multitasking and interrupting issues to design software may be also caused as opposed for deterministic processing.

4. Reliability of Software

Distribution of function of BP and LCLP may enhance the reliability by simplification of software and testability. As shown in Table 1, the functions of BP and LCLP are separated except that of KNGR. Besides, the distribution of function of BP and LCLP is to make software V/V easily and to minimize the fault of software. V/V effort needs a prohibitive amount of resource if design is too complex. Therefore, it is required that the design of software shall be simplified if possible.

III. Regulatory Approach of Soft Controller

1. Background

In the design of main control room (MCR) or remote shutdown panel (RSP), existing manual switches are replaced with soft controller on the flat panel display[5]. Soft controller controls safety related components as well as non-safety components as shown in Figure 2. As shown in Figure 2, the manual switches replaced with soft controller using a multiplexer can cut down the cost and optimize the operational sense. However, the safety classification of soft controller should be considered carefully since it controls directly components related to safety systems during and following the design bases events (DBEs). We describe the regulatory approach on the soft controller in the following subsections.

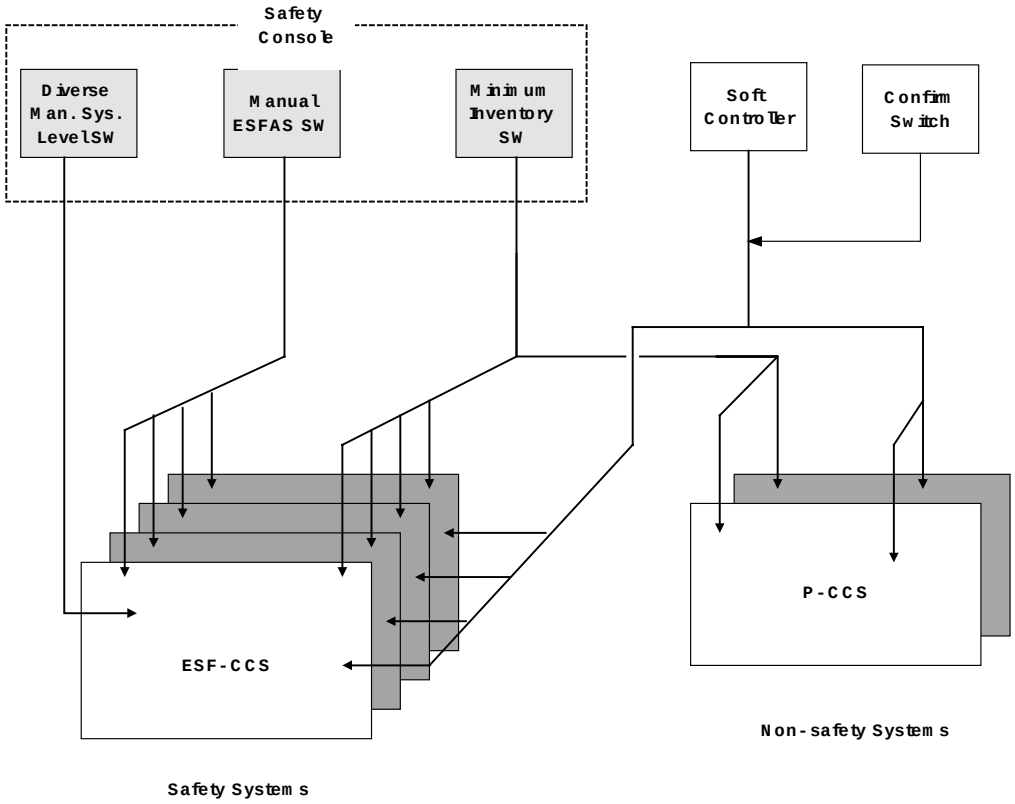


Figure 2: Soft Controller

2. Safety Classification of Soft Controller

As shown in Figure 2, diverse manual switches/controls for system level and minimum inventory switches classified into safety class are provided in safety console against the common mode failure of DPPS and DESFAS. Manual control switches on safety console are designed on the purpose of controlling safety-related systems during and following the design bases events (DBEs) using the hardwire-based control.

In accordance with requirement of IEEE Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Sections 6.2, and 7.2, "Manual Control" [3],[4] , soft controller shall be designed as a safety system because soft controller is utilized to perform the safety functions and corresponding protective actions of the execute features for each design basis event. However, only if the safety function can be completed using the manual controllers on the safety console such as manual ESFAS switch and minimum inventory switches excluding the soft controller, in the end, plant condition is capable of reaching at cold shutdown during and following the DBEs, soft controller may be classified into non-safety system.

As shown in Figure 2, soft controller is used in controlling both safety system and non-safety system. In relation with this, the existing regulations, regulatory guidelines and industrial standards require that equipment and circuit used in all of both safety and non-safety systems shall be classified into safety class and designed such that they meet requirements comparable with safety system.

Regarding capability of manual control by soft controller, the issues of man machine interface may be caused because soft controller is means replacing conventional control switches. Thereby, the performance of soft controller should be verified through dynamic simulation if it can assist the behavior of operator timely and appropriately under all anticipated situation.

3. Independence of Soft Controller

The control of component of conventional ESFAS is designed by dedicated control using the individual hand switches designed as a safety system and the physical separation among channels is maintained. Independence among channels is maintained in the view point of signal transmission by conform switch even though they are not separated physically. However, the design of soft controller in KNGR may not meet the channel independence and physical separation by using a multiplexer. Therefore, channel separation shall be maintained in accordance with relevant requirements.

IV. Regulatory Approach on the Defense-in-Depth and Diversity (D-in-D&D)

All protection systems of KNGR including a reactor trip system, ESFAS, and the plant control system (PCS) are designed on the basis of digital technology. Therefore, the postulated common mode failure of DPPS and DESFAS designed as a software-based digital system may have an adverse effect on the function of PPS and ESFAS. Diverse manual controls (e.g., backup systems) to comply with requirements on defense-in-depth and diversity (D-in-D&D) are implemented in the KNGR [1], [6]. These diverse controls are to be independent and diverse from the safety computer system, and to be located in the main control room (MCR) for manual system level actuation of critical safety functions.

The system-level circuitry is diverse from the component-level one under the assumption of different technologies and vendors. Therefore, we are able to assume that there is no chance of occurring common mode failures between these two levels. However, two kinds of backup panels have to be installed at the Main Control Room (MCR) or at the vicinity of MCR against common mode failures of each level. Firstly, the backup system at the system-level are added against loss of the DPPS due to common mode failures

and are totally diverse from the DPPS and the Alternative Protection System (APS) provided against ATWS events as shown in Figure 3. Thus, there are three layers of defense-in-depth at the system-level which are independent and diverse from among them. Secondly, the backup panel at the component-level is independent, diverse from that of the system-level and the PCS, so there are two layers of defense-in-depth. As described above, the regulatory approach for the hardwired backup systems provided against common mode failure of digitalized protection system is the same as those of Ulchin units 5&6 preceded by KNGR.

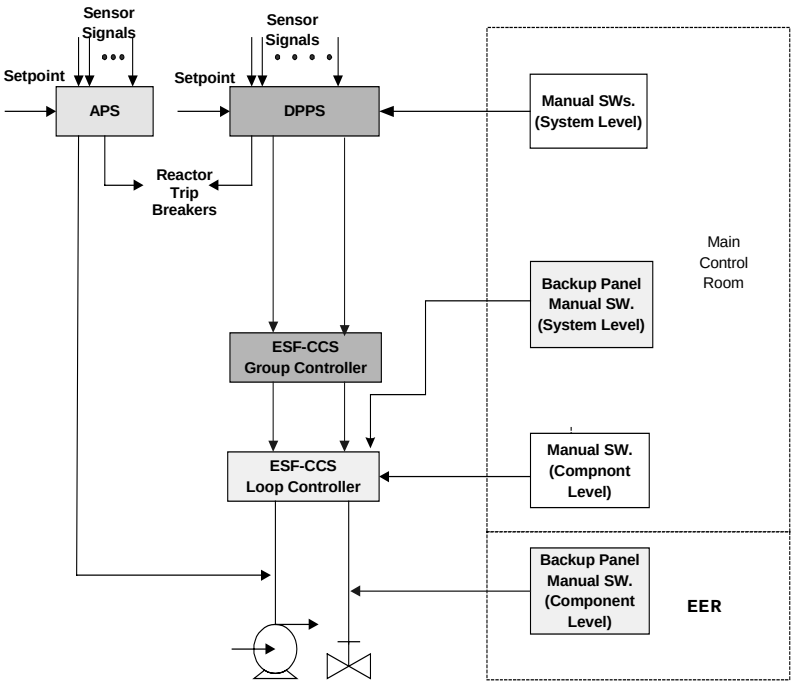


Figure 3: Backup Systems for DPPS

V. Conclusions

We have presented critical issues raised during reviewing the SSAR of KNGR (APR-1400), i.e., the integration of function of BP and LCLP, safety classification of soft controller and hardwired backup system against the common mode failure of digital system. Firstly, regarding the integration of BP and LCLP, we required utility to separate them to preserve their inherent functions to generate a trip signal and coincidence logic signal, respectively and the consistency with an analog system. Secondly, it was required that the safety classification of soft controller shall be classified into safety system in accordance with relevant requirements. Regarding the hardwired backup system, we required utility that two kinds of backup panels have to be installed at the MCR or at the vicinity of MCR, i.e., Electrical and Equipment Room (EER) against common mode failures of each level.

VI. References

[1] KINS/AR-622, “Preliminary Evaluation Report for Ulchin Nuclear Power Plant units 5 and 6,” Korea Institute of Nuclear Safety, March, 1999.
[2] B. R. KIM, “Current Status and Licensing Experience of Digital Instrumentation and Control Systems Important to Safety in Korean Power Plants,” IAEA Consultancy Meeting, Mar 13-16, 2001, Vienna.
[3] NUREG-0800, “Standard Review Plan,” Revision 4, Office of Nuclear Reactor Regulation, U.S. NRC, June 1997.
[4] P. J. Hughes and et al., “Instrumentation and Control Systems Important to Safety: A new IAEA Safety Guide,” Int. Topical Meeting on Nuclear Plant I&C, NPIC&HMIT 2000, WA. DC Nov, 2000
[5] John M. O’Hara and W. F. Stubler, “Soft Controls: Designing for Error Tolerance,” Int. Topical Meeting on Nuclear Plant I&C, NPIC&HMIT 2000, WA. DC Nov, 2000
[6] SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced-Light-Water (ALWR) Designs,” April 2, 1993

Decision Support for Approval of Safety Critical Programmable Systems.

Gustav Dahll[1], *Bjørn Axel Gran*[1] *and Bo Liwång*[2]

[1]*OECD Halden Reactor Project, P.O.Box 173, N-1751 Halden, Norway,*
Tel: +47 69 21 22 00, Fax: +47 69 21 24 40, E-mail (dahll,bjornag)@hrp.no
[2] *Swedish Nuclear Power Inspectorate,S-106 58 Stockholm, Sweden,*
Tel: +46 (0)8 698 84 92, Fax: +46 (0)8 661 90 86, E-mail bo.liwang@ski.se

Summary

One can distinguish between three principles for licensing: rule based, consensus based, and risk based. The paper discusses these three principles, and how they in practice are applied to software based systems. The Swedish nuclear regulatory body is drafting a new Inspection Handbook, where these principles are used in a lifecycle oriented framework. A methodology to combine these three principles in a systematic way, viz. Bayesian Belief Nets (BBNs) is described. An experimental study was performed to investigate the possibility to combine the BBN method with a software safety standard for safety assessment of software based systems. This was done by applying the approach on a real safety related program system.

Introduction

Due to the increasing use of programmable digital equipment in safety critical systems, the regulating bodies (in the nuclear power area as well as many others) faces the problem of licensing of such systems, in particular of the embedded software. There is therefore a clear need for methods and tools for assisting the licensing of safety critical programmable systems.

One can distinguish between three principles for licensing: *rule based, risk based and consensus based on expert judgement*. These three principles are discussed in section 2 with emphasis on how different information sources influence the decision for approval of safety critical software based systems.

The introduction in Sweden of programmable equipment in safety systems of nuclear power plants has been done successively. Along with this there has been a gradual development of the principles applied by the nuclear regulatory body in Sweden, SKI, for the approval of such systems. Section 3 describes the background and the preparation of a draft Inspection Handbook. This handbook is lifecycle oriented, i.e. the regulatory review should be made during the whole development of the system, and for each lifecycle phase it will be based on a combination of disparate evidences. A systematic way to combine such evidences is to use Bayesian Belief Nets (BBNs). This principle is discussed in section 4.

An experiment was made to investigate the possibility to combine the BBN method with a software safety standard for safety assessment of software based systems, by applying the method, on a test case, a real, safety related program system. This is described in section 5.

Principles for System Safety Assessment

Rule Based Safety Assessment

Rule based (also called deterministic) safety assessment means that the system must fulfill a certain set of rules to be approved for safety critical applications. The rules are easy to follow for the developer and easy to check for the assessor. On the other side, this method easily gets very rigid and inadequate to handle new technology.

Furthermore, the rules must be based on certain principles. Such principles may be based on laws of physics, be of probabilistic nature, or they can be of general nature, as e.g. the 'single failure criterion'. It is, however, difficult to establish such simple principles for software based systems. The rules for safe software are therefore rather based on consensus among experts of what is required for safety critical software. This is expressed through standards and guidelines.

Risk Based Assessment

There is a certain trend to change from rule based to risk based principles for licensing. This means to identify potential hazards from implementing a system in e.g. a nuclear power plant, and demonstrate that the probabilities of these hazards are kept under a certain safety integrity level. Probabilistic Safety Assessment (PSA) is therefore often required by the authorities, at least in the nuclear power area. The purpose of using PSA in nuclear power plants is to give an overall view on plant safety by identifying the initiating events of accidents, describe the event sequences, beginning from initiating events and leading to various plant damage states and radioactive releases. Further, PSA evaluates the plant risk quantitatively in probabilistic terms.

The PSA methodology comprises a variety of techniques which are partly complementary and partly overlapping. This means that in an actual analysis one will use a selection of PSA techniques. These techniques can be divided into two main categories: qualitative analysis and quantitative risk estimation. Qualitative analysis aims at identifying potential risks and their possible causes, and include methods like Fault Tree Analysis (FTA), Failure Mode, Effect and Criticality Analysis (FMECA), and Hazard and Operability (HazOp) analysis (IEC-812). The quantitative methods aim at giving probabilistic estimates of quantities related to risk, as e.g. probability of major accident, expected number of lost lives, etc. The results from the qualitative analysis are combined with probability figures associated with the different potential causes. These probabilities may be found by statistical analysis of actual events, or on the basis of engineering judgement or belief.

The PSA techniques has been applied in many decades, and was developed before programmable systems were used for safety related purposes. They are therefore best suited for conventional systems, and problems arise when programmable systems shall be analyzed, primarily due to their embedded software. There have, however, during the recent years been made several proposals to apply PSA techniques also to software systems, although they are not widely used in real safety cases.

Consensus on Safety Based on Expert Judgement

In practice, however, licensing authorities are often faced with the problem of approving systems for which there are no clear rules, and for which it is difficult to apply probabilistic methods. This is particularly a problem in software based systems. The rules given in standards and guidelines are often imprecise, or they are not directly applicable for an actual system. The practice seems to have been based on the opinion

of experts in various fields, including process knowledge, reliability engineering, human factors etc. The combined judgement of the different evidences about the system and its environment constitutes the basis for approval or not.

The acceptance process of a programmable safety critical system is based on a combination of disparate sources of information. This is illustrated in Figure 1 in the form of an 'influence net' where each node represents an aspect in the total assessment process. The top nodes in the graph represent the basic information sources which are used in the acceptance process. This information is penetrated through the net down to the bottom node, which represents the final acceptance of the system.

The latter is mainly influenced by the safety assessment of the system, although there may also be other acceptance criteria. The safety assessment is influenced by a reliability assessment of the system, as well as by an evaluation of whether a failure in the system will jeopardize safety. The latter can be achieved through a hazard analysis of potential risks to plant and environment. Safety defenses (both against hardware and software failures) may be implemented as additional barriers against consequences of failures. A commonly used principle in this respect is diversity, i.e. to obtain the same functional goal through different means.

The reliability of the system can be seen as an expression of the confidence one can have that the system contains no faults. There is also a possibility to make a reliability estimate based on test data and experience data using statistical models (e.g. reliability growth models). The confidence in fault freeness is based upon how well the system is made to avoid faults in the system, how the internal structure of the system makes it vulnerable to programming errors, and how complete the testing and other validation activities are performed. The basic information sources are:

Information about producer. The 'producer' in this context comprises both the company which develops the actual system which shall be approved for safety-related application, and vendors of COTS (Commercial Off The Shell software) modules which are applied. This information includes reputation and experience of the producer, quality assurance procedures, quality of staff, etc.

Information about production. A high production quality enhances this confidence in a system. This implies that the system is developed according to guidelines for good software engineering, that all phases are well documented, and that the documentation shows that the system at all development phases possesses desirable quality attributes as completeness, consistency, traceability etc.

Information about previous usage. The producers of COTS often use 'proven design' as an argument for high reliability. This means that the system has been used by a wide range of users over a long period, with no, or few, reported faults. The idea behind the claim of proven design is that long user experience should reveal all inherent faults, if they exist. So if no faults have been reported over a long period, this should be a strong indication on error freeness. It is questionable, however, whether this is sufficient. A COTS based system has often a quite general purpose, and may consist of many standard modules, each of which has many modes of operation. To claim general high reliability of the system based on user experience, it is necessary to show the experience with all modes of operation of all software modules. This requires information about all installations of the system.

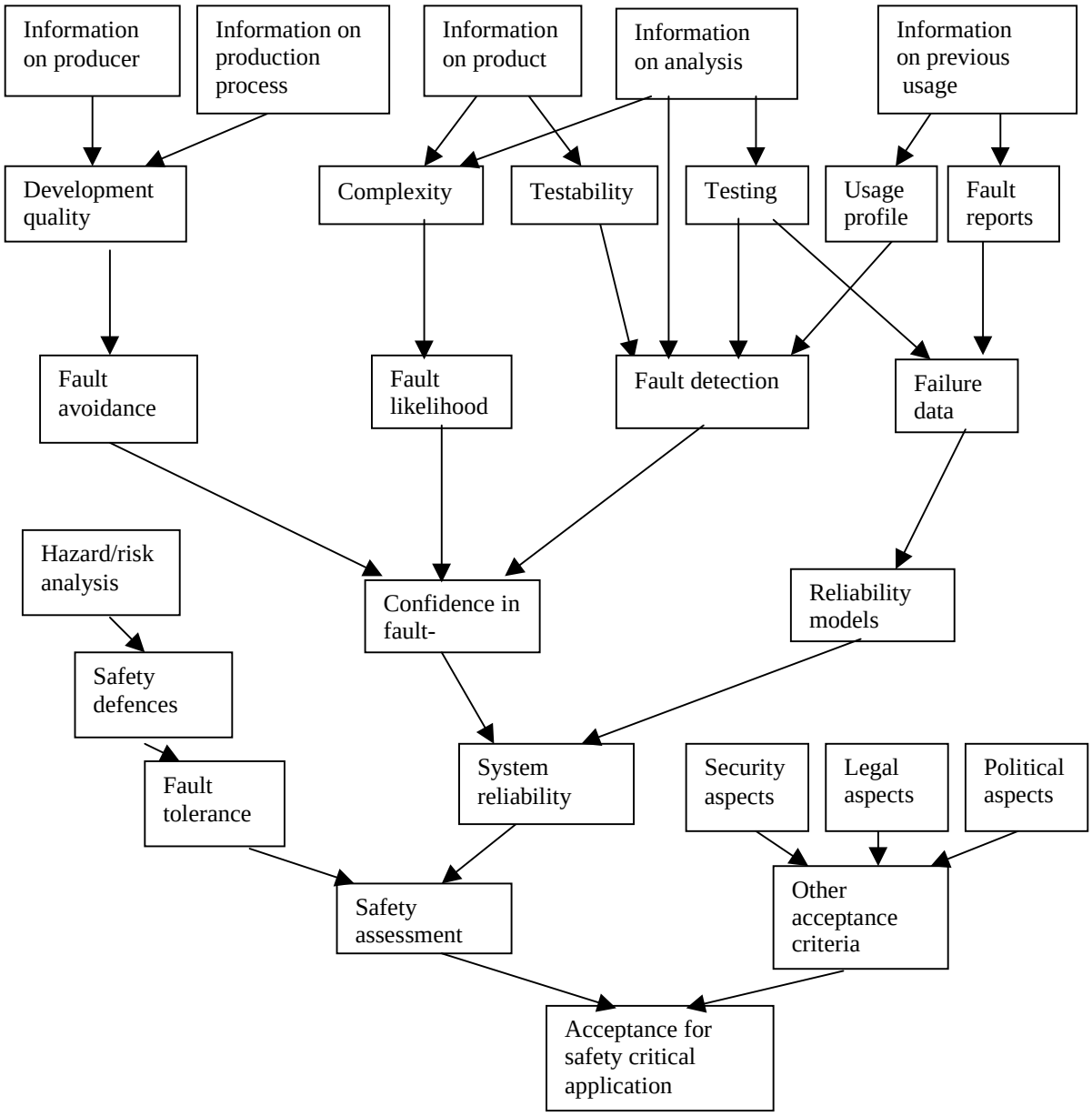


Figure 1 Influence graph of a safety acceptance and acceptance process

Information about the product. Even if a high quality production process presumably leads to a high quality product, there are certain quality attributes the final product should have, as reliability, simplicity, verifiability etc. This yields both the application software and COTS components. However, there is often a limited amount of available information about COTS at code level, so alternative information sources must be used. A main source of information about a software module is found in the specification. A complete, consistent, formal etc. specification is not always available for COTS module, but a functional specification should at least be deducible from the user manual.

Information about the analysis. This includes all activities performed to verify the correctness of the system. The analysis should be performed at the module level, and on the program as a whole. Ideally this activity should be made during all stages of the system development, as e.g. model checking of the

specifications, inspections and walkthroughs of the documentation, static analysis of code and testing of the system.

Development of ”draft Inspection Handbook” at SKI.

The nuclear regulatory body in Sweden, SKI, has not the possibility to perform a detailed technical review of a proposed new digital safety system; it has not the manpower or detailed technical expertise to do that. According to the legislation in Sweden the utility has the full responsibility for the safety of the NPP. SKI shall review that the licensee takes this responsibility in a proper way.

From 1995 SKI participates in ”Task force on safety critical software” within the EC. The purpose is to present a consensus view and recommended practices for selected issues. Both generic issues and life cycle phase licensing issues are selected. Reports has been released in 1998 and in 2000 (EC, 2000).

In Sweden a strategy for the regulatory work has been developed where an ”Inspection Handbook” is one of the tools. The strategy is to perform a review of the different types of information in the design process at the utility in what is called a Safety Demonstration and a Safety Plan. In the EC document EUR 19265 (EC, 2000) it is stated:

”Evidence to support the safety demonstration of a computer based digital system is produced throughout the system life cycle, and evolves in nature and substance with the project. A number of distinguishable types of evidence exist on which the demonstration can be constructed. The task force has adopted the view that three basic independent types of evidence can and must be produced:

- evidence related to the quality of the development process;
- evidence related to the adequacy of the product;
- evidence of the competence and qualifications of the staff involved in all of the system life cycle phases.

In addition, convincing operating experience may be needed to support the safety demonstration of pre-existing software.”

The report gives also a definition of the Safety Plan: ”A safety plan shall be agreed upon at the beginning of the project between the licensor and the licensee. This plan shall identify how the safety demonstration will be achieved. More precisely, the plan shall identify the types of evidence that will be used, and how and when this evidence shall be produced.”

As seen it is the utility that has the responsibility to give the evidence that all safety aspects has been taken care of, but the regulatory body must also know, based on the safety importance of the system, what aspects that is needed to review.

The Framework.

As the Safety Demonstration and the Safety Plan covers the total lifecycle of a project from the first concept to decommissioning, it is necessary to get knowledge of what impact on safety the different activities in the development process has. Several of the issues of interest are not directly observable, for example the quality in the design process.

To get a better structure of the review work at SKI, discussions started with IFE/Halden to develop a theoretical framework on the safety impact from different activities, or ”how to get information on issues

that are not directly observable" (Dahll and Liwång 1999). As a model of the different steps in a development process the structure in the IEC 61508 "Functional safety of electrical/ electronic/ programmable electronic safety-related systems" was used. For each of the phases in the model the framework associates a corresponding set of milestones. At each milestone there should be a check that the intended safety goal is preserved. This check could be rule based but this may become a rigid procedure. Instead an alternative was used where these checks are made on a measure of combined evidences from different information sources available about the system at the milestone. The set of milestones and corresponding milestone goals are shown in table 1.

Milestone	**Milestone goal**
Concept	Preparedness
Overall requirements	Completeness
Hazard and risk Analysis	Safety of concept
Requirement specifications	Dependable specifications
Project planning	Quality of plans
Overall System Design	Dependable design methodology
System realisation (Detailed design, programming and system integration)	Dependable system
System validation	Validated system
System installation	A safe system put in operation
Maintenance and modification procedures	Safety preserved during operation.

Table 1. The set of milestones and corresponding milestone goals.

For each of the milestones and corresponding goal there is a discussion of the set of evidence that influence the goal. As the intention is that it shall be easy to follow and understand during the development process, each milestone is illustrated with a graphical influence net model. This shows the observation and corresponding documentation, which are of importance, and how they influence the attainment of the safety goal at each milestone.

To facilitate the practical use in the regulatory review process a set of questions, with comments, are developed which reflects the structure of the influence net for each milestone. An example of the influence net for milestone goal "preparedness" in the milestone Concept can be seen in figure 2.

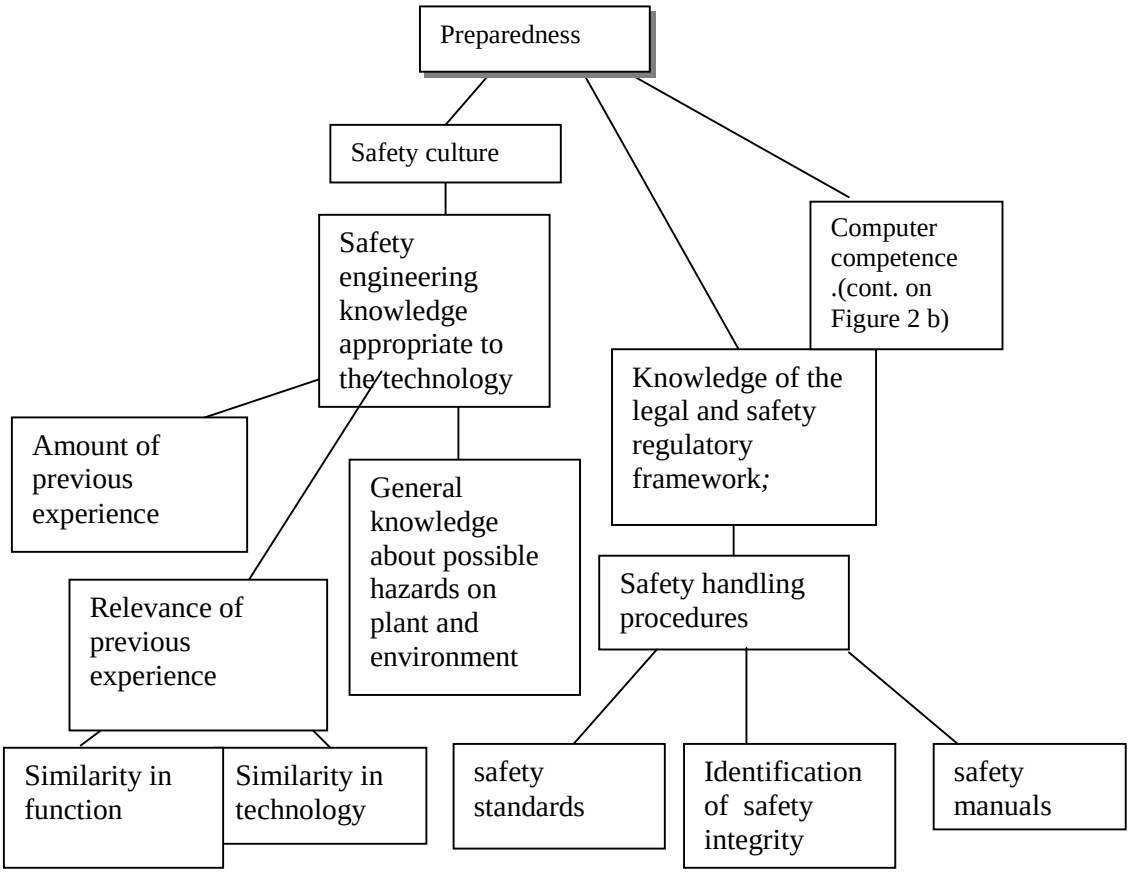


Figure 2a Influence net for milestone *Concept*

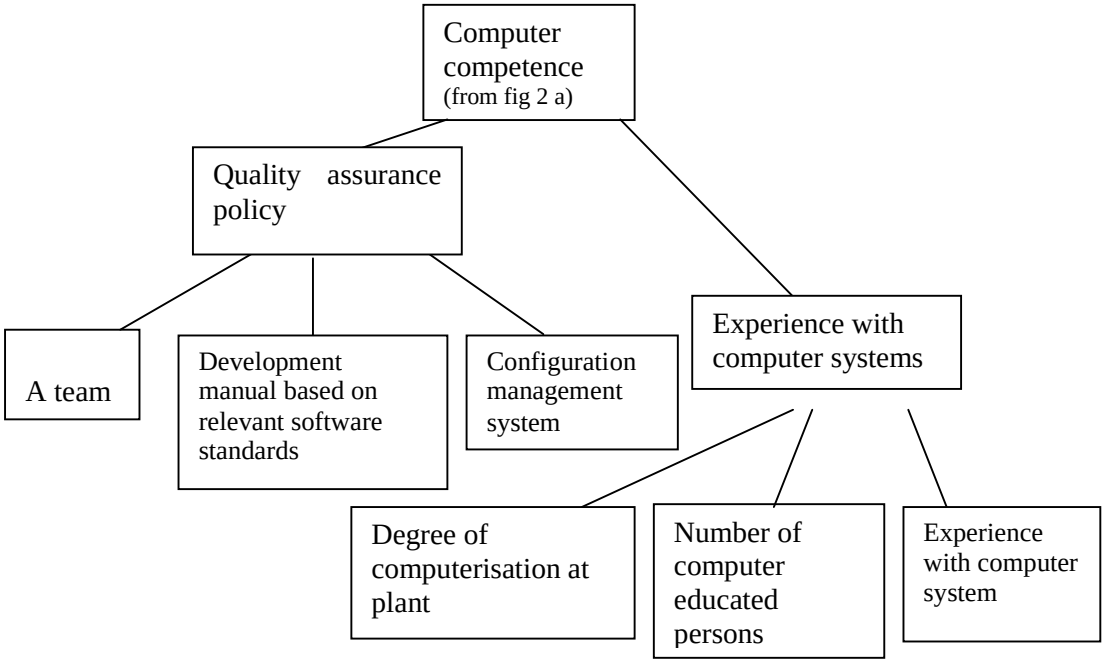


Figure 2b Influence net for milestone Concept (cont.)

The Handbook

The last step in the development of the ”Regulatory Inspection Handbook” is integration of information, criteria and issues from other activities into the influence net framework from the IFE/Halden work. This work was performed by Norman Wainwright, a former NII inspector, in Cupertino with SKI (Wainwright 2000). Most additional material comes from the EC document EUR 19265, presented above, and guides from International Atomic Energy Agency but also from relevant IEC guides.

The structure, milestones and influence net was unchanged from the previous framework but the questions and in particular the corresponding discussion and comments were expanded. The purpose is not to present exact criteria, more to be a background information for an overall safety evaluation and an evaluation of the presented evidence in the safety demonstration.

As a further development the draft inspection handbook will be used and evaluated in the review process for the new safety I&C system for Oskarshamn 1. A handbook like this is not a one time activity, it is a ongoing process to evaluate the technical development and research results to take necessary decisions on modification of regulatory review strategies and the supporting documents.

Bayesian Belief Nets

The use of Bayesian Belief Nets (BBN) has been proposed to combine evidences from different information sources in quantitative assessment of the confidence in a software based system. This methodology has mainly been developed and applied in the AI society. More recently, however, it has also been applied to software safety assessment. Work in this area has been performed in two ESPRIT projects: SERENE (SERENE 1999) and DeVa, and at the Centre for Software Reliability at City University in London (Fenton et. al. 1998) and at the Halden Project (Dahll and Gran 2000).

A Bayesian Belief Net is a directed graph consisting of a set of nodes connected by a set of edges. Both events and singular propositions are associated to each node, where the uncertainty is expressed by a probability density. The probability density expresses our belief about (or confidence to) the various variables. This probability depends conditionally on the status of other nodes at the incoming edges to the node. Some nodes are denoted as ‘observables’, and they represent the different observable properties about the software system and its development. The network edges model relations between adjacent nodes. The strength of these relations is represented as conditional probability distributions. The computation of our belief about a specific node (target node) is based on the rules for probability calculations using Bayes’ formula.

Application of the BBN method consists of three tasks:

Construction of BBN topology: This is made by combining the target node(s) with the observable nodes and the intermediate nodes. The aim is to combine all available relevant information into the net. One way to do this is to start from a target node and draw edges to nodes influencing this. Then from these nodes one can draw edges to new nodes, and in this way gradually build up a large BBN. One problem, however, is to decide when to stop, i.e. how much details one wants to have in the BBN. The practical procedure is to start with constructing a BBN, containing nodes representing high level information. The diagram in Figure 1 is not itself a BBN, but quite similar, so it is fairly straight forward to construct a high level BBN for safety assessment based on this.

Elicitation of probabilities to nodes and edges: The next step is the elicitation of probability distribution functions (pdfs) to the nodes and edges. To begin with one gives prior pdfs to variables to the top nodes (and optionally some others), and conditional pdfs for the influences represented by the edges. These pdfs may be either continuous functions or they may be in the form of conditional probability tables. The latter means that the ranges of the variables are divided into finite numbers of states.

Making computations: The computation method is to insert observations in the observable nodes, and then use the rules for probability calculation backward and forward along the edges, from the observable nodes, through the intermediate nodes to the target node (which again can be an intermediate node in a BBN at a higher level). To make computations with BBNs of a certain size and complexity computer tools are necessary. One description of a computational method is given in (Jensen 1993) with reference to the associated tool HUGIN (Aldenryd et al. 1993).

Combining BBN with the Rules of a Standard.

As a way to combine rule-, risk- and judgement based methods in licensing, an attempt has been made to combine the BBN technology with the rules of a standard for safety critical software. This was done in an experimental project carried out by a consortium composed of the OECD Halden Reactor Project, Kongsberg Defence & Aerospace AS and Det Norske Veritas. This project emphasizes the practical evaluation of the proposed methodology by trying it out on a realistic test case: a computerized system for geographical localization of helicopters. The main purpose of this system is to aid in a rescue operation if the helicopter has made an emergency landing on the sea. A correct localisation is necessary for a successful rescue operation, and the system is therefore safety critical. The system had to be approved by the Norwegian Civil Aviation Authority, and the standard for safety critical software in civil aviation, DO-178B (RTCA/DO-178B, 1992), was applied.

The project consisted of several tasks. The first was to construct BBNs on the basis of DO-178B. Even if this standard is branch specific, conclusions from this project will be of general value, since the different standards for safety critical software have similar structures. The BBN was constructed in two levels. The higher level (see Figure 3) shows how nodes representing four quality aspects, viz. *quality of the producer, quality of the production process, quality of the product*, and *quality of the analysis*, are combined with other nodes in the net, and lead to nodes representing the reliability and safety of the system.

The lower level BBNs were constructed by identifying the quality aspects with top-nodes in four BBNs. Each top node is linked to intermediate nodes representing the 10 lifecycle processes represented by the tables A1 to A10 of DO-178B. Each of these nodes was again linked to other intermediate nodes, representing the objectives of the tables (see Figure 4).

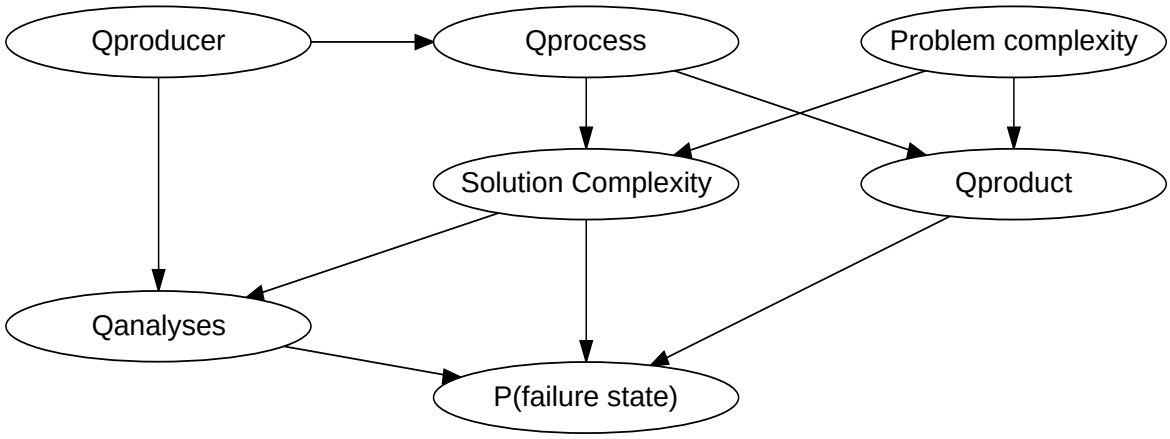


Figure 3. The BBN for the higher level

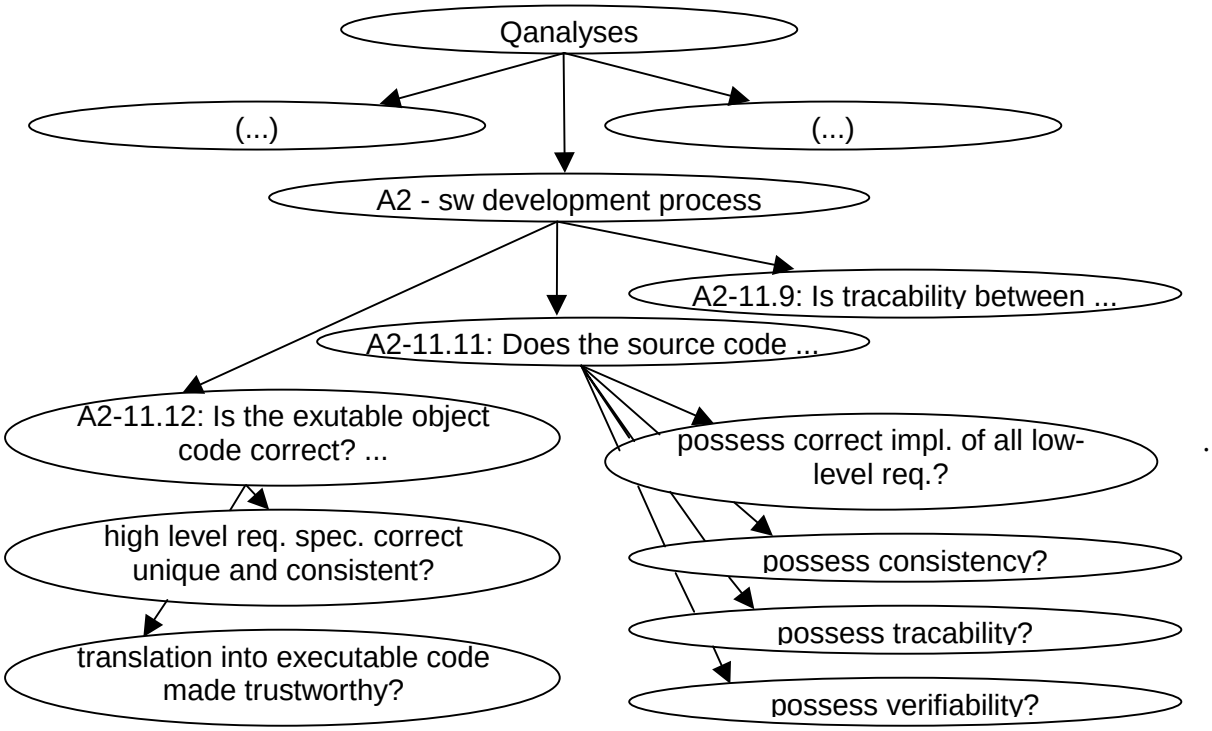


Figure 4. A part of the BBN for the '*Quality of the analysis*'

The further step was to identify a list of questions to each objective. These questions are based of the understanding of the text in the main part of DO-178B, and they are in general formulated so that the answer can be given by a 'yes' or a 'no', or a number between 0 and 1 as an expression of the strength in the belief that the answer is 'yes' (1) or 'no' (0). These questions were answered by the developer of the software, based on their experience from the system development. The elicitation of pdfs to the nodes and edges, in terms of conditional probability tables, was done as a 'brain storming' exercise by all project participants, based on general knowledge and experience in software development and evaluation. Finally

all this information was fed into the HUGIN and SERENE tools, to make a variety of computations, with the aim to investigate different aspects of the methodology (Gran 2000):

- What is the effect of observations during only one lifecycle process?
- How does the result change by subsequent inclusion of observations from the lifecycle processes?
- How sensitive is the result to changes in individual observations?

Summary and Conclusions.

The objective of this paper has been to describe ways to decision support for approval of safety critical software. Such decisions are made by rule- and risk- as well as consensus based principles combining, information from a variety of disparate evidences. The approval process should not only be made on the basis of the completed system, but should closely follow the development process. This is reflected in the draft Inspection Handbook prepared by SKI.

Software safety standards typically contain a variety of recommendations or requirements to be fulfilled during the development and validation of a system. The degree to which each of these is fulfilled constitutes a set of evidences, and these form the basis for the decision on approval. Bayesian Belief Nets has been proposed as a systematic way of combining disparate evidences.

A methodology to combine this with expert judgements and observations related to the rules/recommendations of a software safety standard was experimentally applied on a real safety related system. The experiences from this experiment led to the conclusion that the BBN methodology offers a systematic way to combine quantitative and qualitative evidences of relevance for the safety assessment of programmable systems. The most difficult activity was to perform the expert judgement, in particular in the assignment of values to the conditional pdfs. The establishment of the BBNs and prior pdfs was rather time consuming. However, the process of building up the network, e.g. by making questionnaires, and the elicitation of the prior pdfs were related to DO-178B, and not to the actual system. This implies that these have a general nature, and can be reused in many applications

Acknowledgement

The project team that performed the referred experimental project was, in addition to the authors Dahll and Gran, Siegfried Eisinger from Det Norske Veritas, and Eivind J. Lund, Jan Gerhard Norstrøm, Peter Strocka, and Britt J. Ystanes from Kongsberg Defence & Aerospace AS.

References

Aldenryd S.H., Jensen K.B., Nielsen L.B., 1993. "Hugin Runtime for MS-Windows". Tool made by Hugin Expert a/s, Aalborg.

Dahll, G. and Gran, B.A., 2000. "The Use of Bayesian Belief Nets in Safety Assessment of Software Based Systems." *Int. J. General Systems*, 29 (2), 205-229.

Dahll, G and Liwång, B, 1999 "Lifecycle model oriented safety assessment of programmable systems." Presented at OECD Halden Reactor Project EHPG Meeting, Loen, Norway, 24-29 May, 1999

EC, 2000 "Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors". EC – Nuclear safety and the environment, May 2000, EUR 19265 EN

Fenton N., Littlewood B., Neil M., Strigini L., Sutcliffe A. and Wright D., 1998. "Assessing Dependability of Safety Critical Systems Using Diverse Evidence." *IEEE Proc. on Software Engineering*, 145 (1), 35-39.

Gran. B.A. et. al., 2000. "Estimating Dependability of Programmable Systems Using BBNs." SAFECOMP'2000, Rotterdam, Oct.25th. – 27th.

IEC-publication 812, "Analysis Techniques for Systems Reliability - Procedures for Failure Mode and Effects (FMEA)." 1985.

Jensen F., 1993. *An introduction to Bayesian Networks.* UCL Press, University College London.

RTCA/DO-178B. "Software Considerations in Airborne Systems and Equipment Certifications." , 1992

SERENE, 1999. The SERENE Project. http://www.hugin.dk/serene/.

Wainwright, N., 2000 Guidelines for the assessment and approval of software based safety systems Final draft for SKI (unpublished) July 2000.

TECHNICAL SESSION 1:
NATIONAL AND INTERNATIONAL COMPUTER-BASED STANDARDS AND GUIDES FOR SAFETY SYSTEMS
Chairmen: J.-P. Bouard, Z. Ogiso

International Standardisation in Nuclear I&C Engineering

Jean-Paul BOUARD

IEC Sub-Committee 45A Secretary

SYNOPSIS There is a temptation to treat standards work as boring, tedious and not value-added! As explained in this paper, however, standardisation usually leads to economic development and increased sales. This and other reasons for international standardisation are presented, together with a brief outline of the history and operation of the International Electrotechnical Commission (IEC), which, together with the International Standards Organisation (ISO) is responsible for the preparation and maintenance of many of the world's International Standards. The paper then focuses on standardisation in the nuclear instrumentation and control sector and highlights current work being done within IEC Technical Committee TC45, and more particularly SC45A.

1 INTRODUCTION

Standardisation has been important since the industrial revolution and is normally driven by demands for:

- The interchangeability of products and
- Standard methods of measuring and assessing quality and performance.

Looking back over the decades, the most common result of national and international standardisation has been increased trade, although of course, some products are squeezed out of the market by standardisation; the story of the Betamax video recorder is the best known example of this. It may not be surprising to learn therefore, that one of the primary objectives of both the ISO and IEC is to foster trade and commerce.

Standardisation in nuclear engineering is important for the same reasons, but in addition there are other more specialised but equally valid justifications for standardisation. Most stem from the capital intensive nature of the work and from the need to promote safety on a world wide scale. In such respects there are analogies with the aircraft industry. Some other factors are worth noting here since nuclear engineering is by definition a specialised business employing a unique combination of engineering disciplines and skills.

- Firstly the need to share experience. Different countries are at different stages of nuclear development and, in some cases at least, progress and safety depend on the availability of appropriate codes of practice. Documents such as the IAEA Safety Guides are very useful in this regard but they tend to concentrate on principles whilst guidance is also needed on practical design matters. Although many countries have their own National Standards, the trend towards the adoption and use of International Standards is supported by many Nations, and one could argue that international standards represent the best codification of good practice.

- Secondly, standardisation also helps to promote a common technical language together with strong, technical infrastructures on which economies and indeed, safety depend. This is a feature of nuclear power development which has been emphasised by the IAEA.

- Thirdly there is the issue of continuity of both skills and the supporting industrial base. In many countries nuclear programmes are stagnating and fundamental and background development work is being curtailed. Such restrictions reduce the training of future generations and one way of minimising the impact of this - admittedly not the best - is by standardisation.

- Finally, then, in the nuclear industry, standardisation is a route to improved safety. This is particularly important in an environment in which the perception by the public of nuclear power is poor and based predominantly upon non-scientific judgements.

This paper describes some of the work which is being done to meet these needs through the International Electrotechnical Commission (IEC). The purpose of this paper is to remind readers of the existence of this well integrated, international standard organisation; to demonstrate its experience and to indicate how people and organisations can use it to help standardise needs. It also concentrates on IEC Technical Committee 45 (Nuclear Instrumentation) and the Sub-Committee 45A because of their relevance.

2 THE STRUCTURE AND PARTNERS OF THE IEC

The IEC was founded in 1906 and is the oldest independent International Standards organisation. The membership consists of more than 50 participating countries, including all the world's major trading nations and a growing number of industrializing countries. Together they represent more than 80% of the world's population and produce more that 95% of the world's electrical energy. A survey several years ago indicated that around 50% of the world's trade is with goods which complied with international standards.

2.1 Partners

International Partners

ISO and ITU

The IEC works closely with its international standardization partners, the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), other regional standardization organizations and international organizations, including the World Health Organization (WHO), the International Labour Office (ILO) and the United Nations Economic Commission for Europe (UNECE). An initial agreement was signed with ISO in 1976 and ten years later the two bodies established Joint Technical Committee 1 (JTC 1) to cover the vast and expanding field of information technology.

Governmental Agencies

One of the IEC's principal partners is the World Trade Organization (WTO), whose 100-plus central government members explicitly recognize, through their Agreement on Technical Barriers to Trade (TBT), that international standards play a critical role in improving industrial efficiency

and developing world trade. These relations at government level are of particular importance in heavily regulated areas like safety, health and the environment.The number of standardization bodies which have accepted the Code of Good Practice for the Preparation, Adoption and Application of Standards presented in Annex 3 to the WTO's Agreement on Technical Barriers to Trade underlines the global importance and reach of this accord.

The IEC encourages industrializing nations to share in the benefits of joining in its work and liaises closely with the International Monetary Fund (IMF), the European Bank for Reconstruction and Development (EBRD), the World Bank, and the United Nations Development Programme (UNDP).

Regional Partners

At the regional level, the IEC works to achieve harmonization of standards among regional standardization organizations, such as CANENA, CENELEC, COPANT, EASC, ETSI and PASC. A joint working agreement exists with the European Committee for Electrotechnical Standardization (CENELEC), comprising some 20 IEC National Committees. In addition, the IEC has agreements with COPANT, EASC and ETSI (IEC/ETSI agreement), based on the exchange of information.

Co-operation between the IEC and CANENA

The co-operation agreement between the IEC and CANENA (Council for Harmonization of Electrotechnical Standards of the Nations of the Americas) signed in September 2000 relates to:

- promoting the use of IEC standards with CANENA members and
- enhancing technical cooperation in standards development.

This agreement is expected to be instrumental in ensuring a rational use of available resources in standardization activities and transparency of the standards process, thus facilitating world trade. It will also accelerate the standardization process and promote the development and implementation of IEC standards in response to market demand.

Co-operation between the IEC and CENELEC

The co-operation agreement between the IEC and CENELEC (European Committee for Electrotechnical Standardization) ratified in September 1996, and commonly known as the Dresden Agreement, relates to:

- common planning of new work
- parallel IEC/CENELEC voting

The object of this agreement is to avoid duplication of efforts, speed up the preparation of standards and to ensure the best use of the resources available and particularly of experts' time. If the results of parallel voting are positive in both the IEC and CENELEC, the IEC will publish the international standard, while the CENELEC Technical Board will ratify the European standard.

2.2 IEC Structure

The IEC carries out its business in three official languages - English, French and Russian. Almost all of the working meetings are conducted in English but the Standards are published as bilingual documents in French as well as English. They are also translated into Russian.

Each member country interfaces with the IEC through its own, internal, national committee and the IEC is, in effect, governed by these national committees through a Council and a Committee of Action to which a number of Advisory Committees report. These bodies control the work of more than 100 Technical Committees (normally abbreviated to TC's) and more than 80 technical Sub-Committees (SC's) each of which is responsible for a precise, technical field. Also, there are also 10 technical specialist committees such as those associated with the International Special Committee on Radio Interference (CISPR).

Sub-Committees can be established by any technical committee, although not all TC's chose to do so. It depends primarily upon the workload and the availability of expertise. However, both types of committee operate in much the same way. The Technical Committees, of course, have to report to the Committee of Action.

The work can be classified under five main headings:

- The development of common means of expression, vocabulary, graphical symbols, units (plus their associated letter symbols).

- The generation of standard methods of test or of declaring equipment performance. Such methods permit the ready comparison of claims regarding quality or performance. These tests are not specified as the minimum mandatory requirements although purchasers and suppliers often agree to interpret them as such.

- Agreeing levels of quality or performance arrived at by such standard test methods.

- The agreement of design features, either mechanical or electrical, which enhance interchangeability and encourage common usage throughout the world.

- Increasing safety to personnel, something which is very pertinent to the nuclear community.

All of these, even the first, are important to the nuclear industry. It is sometimes argued that communication is not a serious problem in science based technologies because of the widespread use of mathematics and of only one or two languages. However, those active in the international field quickly learn that there as many concepts of, say, English as there are people to speak them and that misunderstandings easily occur. Vocabulary, often thought of as a Cinderella subject, is therefore much more important than might be perceived.

Based on these five headings, the working scope of every Technical Committee falls into one of two distinct classes; those concerned with the enabling technologies and those writing detailed Standards on applications within specific industrial sectors. This means that Technical Committees exist which are devoted to, for example,

- terminology and related matters;

- materials and basic technology;

- electronic components such as lamps, fuses, cables etc;

And on the other hand, there are Committees devoted to:

- power generation, or

- the performance, safety and/or reliability of electrical systems and equipment in different industrial sectors (telecommunications, nuclear, aerospace).

TC45 is responsible for International Standards in the field of Nuclear Instrumentation, with Sub-Committee 45A covering Reactor Instrumentation and Sub-Committee 45B looking after Radiation Protection Instrumentation.

The IEC Council and the Committee of Action control the way in which Committees work by means of Directives (1) and Administrative Circulars. These seldom, if ever, mention detailed technical subjects. They are much more concerned with the programme and progress of the work, the interfaces with other Technical Committees and the working process since the technical content is the prerogative of national committees. Naturally, the Committee of Action is concerned with the coordination and the prevention of overlap and actively encourages liaison between the TC's. For this reason each Technical Committee is obliged to prepare a "Strategic Policy Statement" clarifying its domain, the current work and the predicted future trends.

In a body which has been active for nearly 90 years one might expect a degree of ossification but this is not so and the directives evolve continually. For example, a matter of recent concern has been the time taken for some documents to emerge and the latest edition of the Directives specifies a 3 year target duration for the issue of a new International Standard. Another important change in recent years has been the harmonisation of the IEC and ISO directives into the same document.

3 THE ROLE OF NATIONAL COMMITTEES

The main work of the TC's and SC's is carried out by working groups, comprising of experts from member Nations who do the detailed drafting of Standards. A national committee which wishes to participate in a particular field or piece of work nominates national delegates to the relevant TC or SC and may also send experts to the associated working groups. In most cases, of course, the same individuals are involved but they operate, or should operate, in different ways in the two environments. In the working group experts discuss drafts as individuals with, it is hoped, no insuperable national bias. They may generate any number of drafts (within the time limit) but their work remains amongst themselves and is sometimes the subject of very frank discussion! When they are satisfied, the resultant document is submitted to the parent committee for distribution to the National Committees who then express a considered national view.

This structure can be confusing but it also has the great advantage of permitting any individual in any member country to propose and more importantly, to contribute personally to the work. If anybody wishes to participate in this work, he can offer his services to the appropriate committee. At the very least, since draft documents are published for public comment, anyone can write to the secretary of the specialist committee.

4 THE METHOD OF WORKING WITHIN A TECHNICAL COMMITTEE OR SUB-COMMITTEE

The secretariat of each TC and SC is held on a voluntary basis by one of the national committees. This national committee is appointed by the Committee of Action and is in turn responsible for appointing a secretary. He (or she) must always act in an international way, divesting himself of any national point of view. The Chairman is nominated by the national committee holding the secretariat but is appointed directly by the Committee of Action on personal merit after views of the Nations have been sought. Thus, chairmanship is entrusted to an individual whilst national committees undertake secretariat duties and appoint a secretary. Both are supported by a relatively small Central Office organisation in Geneva.

Topics for standardisation work are decided by the national committees. Proposals for new work are set out in a formal way - preferably complete with a first draft - and circulated to the rest of the Nations by Central Office. Comments are made and majority voting decides whether the project is to go ahead. A feature of this procedure is that work does not start unless an adequate number of national committees agree to take an active part. In addition, a target completion date is agreed for the new Standard.

Working groups develop the document and in due course the TC or SC decides that the draft is good enough to be formally submitted, as a so called Committee Draft (or CD), to all national committees for written comment. As noted already, this provides an opportunity for input from a wide range of people and organisations. The resulting comments are usually resolved in the appropriate Working Group and, if necessary, further editions of the CD are circulated. The next stage is to circulate the document as a Committee Draft for Voting. The vote is to approve the issue of the document as a Final Draft International Standard (or FDIS). Further formal voting then leads, hopefully, to its being accepted, edited and published. Overall, then, there are three stages of formal voting from the first proposal for new work through to publication. The rules which control this process appear in the IEC Directives and, although apparently complex, are close to the minimum necessary to guarantee high quality standards which command international consensus and at the same time are acceptable by each nation.

5 RELATIONSHIPS BETWEEN TC45 AND THE IAEA

In 1974, the IAEA started the Nuclear Safety Standards (NUSS) programme to provide member states with internationally agreed recommendations on the safety of land based thermal neutron power reactors. This programme covers areas of governmental organisation (for the regulation of nuclear power), siting, design and operation as well as quality assurance. The Code of Practice on design sets out the basic safety principles while fourteen Guides enlarge on the more important principles. In particular, three guides are concerned with instrumentation and control:

- 50-SG-D3 on Protection and Related Features in Nuclear Power
- 50-SG-D7 on Emergency Electrical Systems at Nuclear Power Plant
- 50-SG-D8 on Safety Related Instrumentation and Control Systems in Nuclear Power Plants.

These three guides address the subject matter from the safety philosophy viewpoint and are not technical standards. They do, however, overlap the earlier IEC 231 series.

As a result of this potential for duplication and even contradiction between IAEA Documents and IEC technical standards, a formal agreement of co-operation was reached in 1981 between the IAEA and the IEC/Technical Committee 45.

The Agreement states that:

- the IAEA is responsible for the development of safety principles for instrumentation, control and electrical systems in Nuclear Power Plants,
- IEC/Technical Committee 45 is responsible for the design requirements that realise these safety principles
- TC 45 is invited to participate in the development of the relevant IAEA Safety Guides and
- the IAEA is invited to participate in TC45 Meetings.

Close co-operation has continued since then with the common goal of preparing Safety Guides and Standards for the design of instrumentation and control systems which significantly add to the safety and operability of nuclear power plants.

6 IEC/TC45 - NUCLEAR INSTRUMENTATION

TC45 is the only true nuclear technical committee of the IEC. It was set up in 1960 at the IEC General Meeting in New Delhi and the current scope is "To prepare International Standards relating to the electrical and electronic equipment and systems for instrumentation, specific to nuclear applications."

The present chairman of TC45 is Mr Richard Schomberg from France and the secretariat is currently held by the Russian Federation (Mr Youri Seldiakov).

TC45 has 6 Working Groups (WG) dealing with:

- WG 1: Classification - Terminology
- WG 3: Interchangeability
- WG 6: Electrical measuring instruments utilizing radioactive sources
- WG 9: Radiation detectors
- WG 10: Multichannel analyzers and systems based on them
- WG 14: Nuclear instrumentation for geophysical applications

There are also two Sub-Committees.

SC45A Reactor Instrumentation:

- Was formed in 1963 and is concerned with "Electronic and electrical functions and associated systems and equipment used in the instrumentation and control systems important to safety of nuclear power plants. This includes the radiation monitoring instruments used directly for plant control or safety actuation. A major consideration is the application of emerging electronic techniques to nuclear requirements, particularly computer systems and advances in information processing and control, including artificial intelligence. Part of its strategic task is to review IAEA safety codes in order to identify detail technical aspects for which standards are appropriate."

- The chairman, Mr E. Corte, is from the USA and the secretariat is held by France (Mr Jean-Paul Bouard),

- Seven Working Groups report to SC45A:

    - WG A2: Nuclear reactor measurement, control and safety instrumentation

    - WG A3: Application of digital processors to safety in nuclear power plant

    - WG A5: Special process measurements

    - WG A7: Reliability of electrical equipment in reactor safety systems

    - WG A8: Control rooms

    - WG A9: Instrumentation systems

    - WG A10: Upgrading and modernization of instrumentation and control (I&C) systems in nuclear power plants (NPP)

SC45B Radioprotection Instrumentation:

- has the current scope "To prepare standards covering all the fields of radiation protection instrumentation. That is, for the measurement under both : normal and accident conditions of external and internal individual exposure, workplace, environment (including foodstuffs)"

- The chairman is Mr I. Thompson from the UK and the secretariat is France (Mr Jean-Claude Thévenin).

- Seven Working Groups report to SC45B:

    - WG B5: Radiation protection instrumentation for environmental monitoring

    - WG B7: Equipment for the monitoring of external contamination on the body, extremities and clothing of personnel

    - WG B8: Pocket active electronic dose equivalent, and dose equivalent rate monitors

    - WG B9: Installed equipment for radiation and activity monitoring in nuclear facilities

    - WG B10: Radon and radon daughter measuring instruments

- WG B12: Instrument for radioactive contamination measurement of foodstuff
- WG B13: Revision of IEC 761 series

In total approximately 160 experts from 19 different countries contribute to the work of TC45, with most active participation from the European countries, the USA, Canada and Japan.

All three committees have been, and are very active. They have, between them, generated over 130 agreed Standards, the work covers fundamental technology as well as the specification and design and development of complete systems.

The current work programme is large, consisting of 30 items as well as the review and amendment of older Standards. As you might expect the use of software in safety systems is a major topic in one of the SC45A Working Groups and this is the salient connection with the work of TC65 Working Groups A9 and A10 which have produced IEC 61508.

I would like to focus on a few of the more significant documents being developed by the various SC45A Working Groups.

- **IEC 60880 Software for Computers Important to Safety in Nuclear Power Plants.** The original Standard, the first part, was published in 1987 and was the first International Standard to give recommendations for the use of software in nuclear safety systems. The second part, just published, provides recommendations on several key areas of using software in nuclear safety systems, namely

  - the avoidance of common cause failure
  - the selection and use of automated tools
  - the re-use of pre-existing software.

  The revision of the original 1987 IEC 60880 started in 2000 is currently going on. The new edition of the IEC 60880, taking into account the last trends of the information technology relevant for nuclear important for safety systems and corresponding to a global consistent frame should be available in 2003.

- **IEC 61226 Classification of I&C Functions.** The original Standard, published in 1993, is currently revised. It deals with the difficult and often controversial subject of classification and graded requirements for I&C functions based upon their importance to safety. The safety principles for the Standard were taken from IAEA Safety Guide D8 where three categories of importance are defined in addition to a category which has no defined safety role. The Standard establishes a method of classifying the information and control functions for nuclear power plants and the I&C systems and equipment that provide those functions. The categorisation method is based on a qualitative (i.e. a deterministic) approach.

  The new version of the IEC 61226 should be available in 2004.

- **IEC 61513 General Requirements for Computer Based Systems.** This Standard will provide requirements for the design of computer based systems which are important to nuclear safety. This is a significant document in two senses; firstly, it will be the only Standard which deals with the difficult area of designing nuclear I&C safety systems using computer based solutions. Secondly, and probably

more important, it flows down the principles, and format of IEC 61508. Consequently, this IEC Standard represents the application of IEC 61508 in the nuclear sector.

The IEC 61513 is at final vote stage and should be available mid-2001.

- **IEC 62096 Instrument and Control Systems (I&C) of interim storage and final repository of nuclear fuel and waste**. This technical report will support owners of an NPP in the decision- making process and preparation of partial or complete modernization of the I&C. For this it will deal with:
  - motivating factors for I&C modernization,
  - principal options for the elaboration of different scenarios for I&C modernization,
  - technical and economic criteria for the selection of a long term I&C strategy,
  - principal aspects to be taken into account for a detailed technical feasibility study.

  Special attention will be paid to the improvement of the reactor safety and of the human machine interface.

- **IEC 62138 Computer-based systems important for safety software aspects for I&C systems of class 2 and 3.** This International Standard will provide requirements and recommendations for the software aspects of computer-based I&C systems of safety classes 2 and 3, as defined by IEC 61513. These I&C systems may be used for category B or C FSEs (Functions, and associated Systems and Equipment), as defined by IEC 61226. Its scope can be compared to the combined scopes of IEC 60880 parts 1 and 2, the difference being that these two documents address the software aspects of I&C systems of safety class 1. It is consistent with, and complementary to, IEC 61513.

  This standard should be available in 2002

- **IEC 62235 Instrument and Control Systems (I&C) of interim storage and final repository of nuclear fuel and waste .** This Technical Report gives guidelines for the Instrument and Control Systems of interim storage and final repository of nuclear fuel and waste, regardless the origin of the stored material. This Technical Report covers storage at all types of facilities such as; fuel fabrication plants, nuclear power plants, reprocessing facilities, interim storage facilities, encapsulation facilities and final repositories for operational waste and spent nuclear fuel. The Technical Report also covers storage during transportation. All these facilities contain different nuclear materials such as new fuel, used fuel, operational waste and other miscellaneous radioactive substances and objects.

These are just a few of the 30 documents which are part of the current work programme. Although nuclear power is not a growth industry in American and European countries, there is considerable interest in other parts of the world and international standards work helps to spread competence and expertise to all nations. In the USA and Western Europe the major work is retro-fitting of modern I&C systems. In Eastern Europe the work is dominated by the pressure to bring plant design and instrumentation up to western standards. Again international standardisation has a key role to play here since they provide common ground for discussion between utilities, suppliers and Safety Authorities.

7 CONCLUSION

This paper has underlined the existence of flourishing and effective international collaboration, on standards in general, and on nuclear standards in particular. It has indicated the route by which an individual person or organisation can introduce and, subsequently, influence the work. The use of harmonised standards has to be the correct approach when set against the background of increasing international trade. Overall, therefore, it is important that each country contributes to international standardisation work otherwise their voice will not be heard. This means taking part in meetings, listening to other experts talk about their ways of working and build the international consensus.

In the field of nuclear engineering, the hope is that standardisation promotes and enhances nuclear safety. Based on some earlier research it has been estimated that about half of the countries engaged in nuclear energy do use IEC nuclear standards as they are, quoting them in purchase contracts, whilst the other half prefer national ones.

A separate, and not insignificant, benefit which helps to offset some of the effort which individuals put into this work arises from the regular meetings between practising engineers with everyday involvement in manufacturing, research, development and regulation. Formal and informal exchange of professional knowledge at a detailed level stimulates cross fertilisation of ideas and generates value far beyond immediate standardisation needs. Those who attend and participate in the working meetings learn much from each other and come to accept that other people and other countries have good reasons for having different ideas on techniques and standardisation. Examination of the technical basis of differences then brings out aspects which had not previously been fully considered by any of the parties. The greater the difference, the longer it may take to arrive at an agreed standard and occasionally progress seems very slow - particularly in harmonising techniques which have been long established, but at the end of the day, there are clear commercial benefits from participating in standards work.

REFERENCES

1. ISO/IEC Directives. Parts 1,2 & 3 Second Edition 1995 Amdt. 1997

2. Some Aspects of International Standardisation in the IEC and Related Bodies. Dr A Goodings. 1993

3 The Role of International Standards in the Design of Modern I&C Systems for Nuclear Power Plants. J M Gallagher. 1993.

4 International Standardisation in Nuclear Engineering. D.L. Curtis. 1998.

ACKNOWLEDGEMENTS

This paper is based upon three previous papers written by Mr D.L. Curtis (4), Dr A Goodings (2) and Mr J Gallagher (3). Material has been extracted from the first paper and supplemented with up to date information concerning the IEC and its committees which could be found on the IEC server (www.iec.ch). The author would like to express his thanks to Mr Curtis, Dr Goodings and Mr Gallagher for their permission to use material from their papers.

Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety

Gary Johnson[8]

Summary

Many organizations worldwide develop standards that affect nuclear instrumentation and control (I&C). Two of the primary standards organizations that affect nuclear power are US IEEE's Nuclear Power Engineering, and IEC SC45A. Today, nuclear power is very much an international industry. In this environment is vital that the activities of these standards organizations be in harmony.

The harmony between IEEE and IEC standards is currently not adequate. This paper surveys the contents of the two sets of standards. Opportunities to improve consistency between the two sets of standards will be identified. It is hoped that this paper will excite a discussion of what might practically be done to improve the harmony between IEEE and IEC standards.

1 Introduction

The collections of IEEE and IEC standards have some overlap, but in many cases cover significantly different topics. For example, IEEE standards go to great depth covering environmental qualification of many specific types of components, while IEC covers the topic only at the general level. Conversely, certain IEC standards deal with specific instrumentation and control functions, a topic area where IEEE standards are largely mute. This raises several questions. Why do two bodies that are writing standards for the same purpose arrive at such a different collection of standards? Does this diversity offer opportunities for the two bodies to build on each other's standards to efficiently improve upon the coverage of their sets of standards?

This situation poses a problem for the developers of systems for plant upgrades who must try to address both sets of standards to avail themselves of a sufficiently broad market. Additionally, the IEEE and IEC standards together form a more comprehensive set of guidance than either set alone provides. If the interfaces between the standard sets were smoother plant staff and system designers would have a better set of tools to help in the design and specification of I&C upgrades.

To understand the similarities and differences between IEC and IEEE nuclear power standards layer diagrams were developed for each set of standards.

[8] *Lawrence Livermore National Laboratory, P.O. Box 808, L-632, Livermore, CA, USA 94550. Tel: +1-925-423-8834, Fax: +1-925-422-9913, e-mail: johnson27@llnl.gov*

Layer Diagrams

Layer diagrams show the structure of a set of documents from the most general to the most specific.

Used previously in the analysis of software engineering standards (ref Jim Moore book)

Five layers: terminology, overall guidance, principles, element standards, application guides, and techniques. (Give definition from Jim Moore book) All five layers are always needed.

For nuclear power standards regulatory requirements provide the overall guidance. For IEEE this is NRC's 10CFR50. For IEC this is IAEA 50-C-D. To the extent these are different the differences will drive irreconcilable inconsistencies between the sets of standards.

Figures 1 through 4 give the layer diagrams constructed. These represent one view of the standards. Other organizations are possible - it is not possible to produce a perfect one. It is hoped that the organization here is a useful one.

3 Analysis

The standards of each set may be categorized into three groups: system standards, human machine interface standards, standards for specific functions.

The greatest overlap is in system standards. The standards in the other groups mostly cover different specific topics even though the general topics are the same.

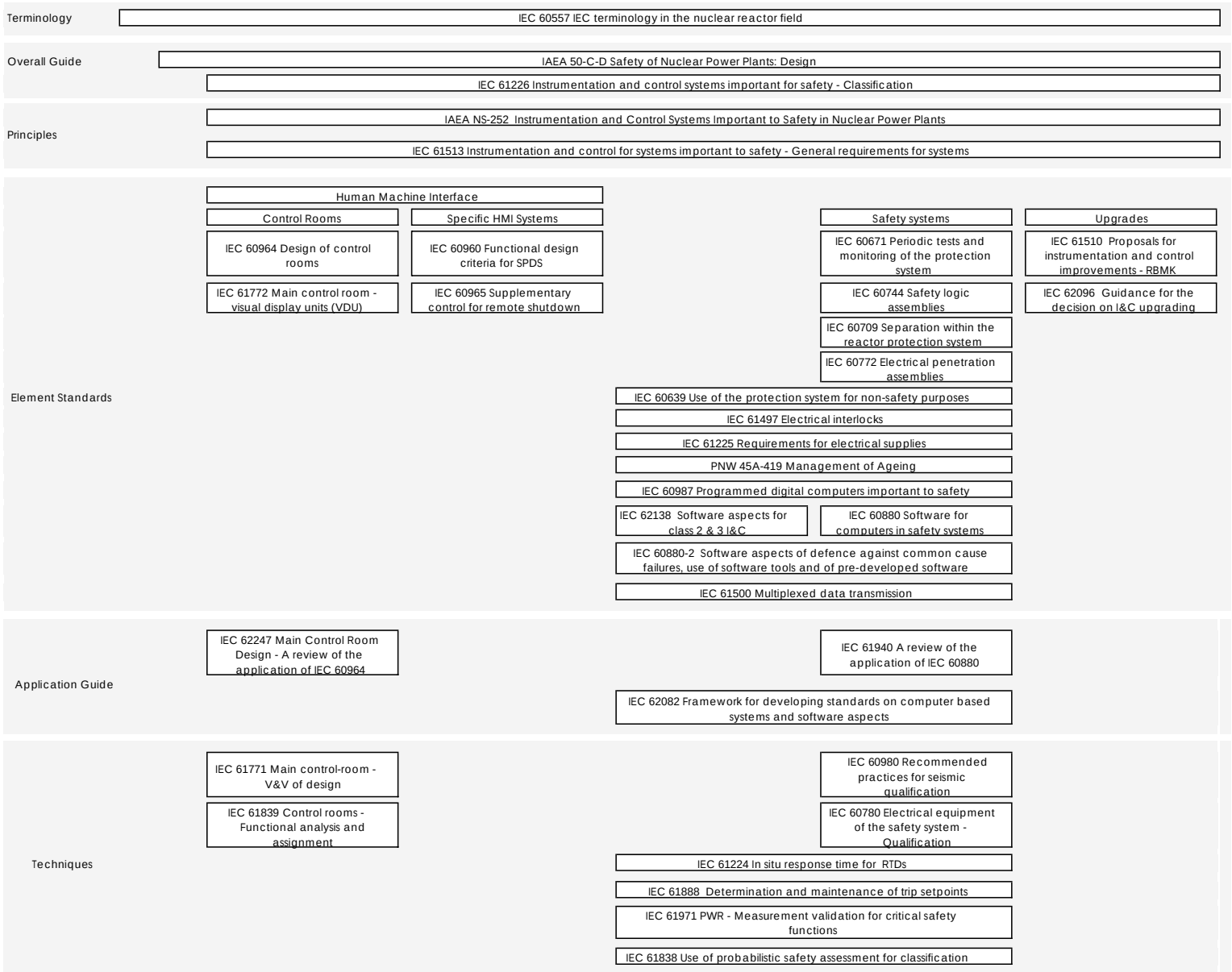
The IEEE standard set includes several general industry standards that cover relevant topics. These were explicitly included in the nuclear set by the IEEE management board, NPEC. Certain software engineering and EMI standards may be included in the set of applicable general industry standards because of their endorsement by NRC. There is no similar practice in IEC to "endorse" general industry standards for nuclear use.

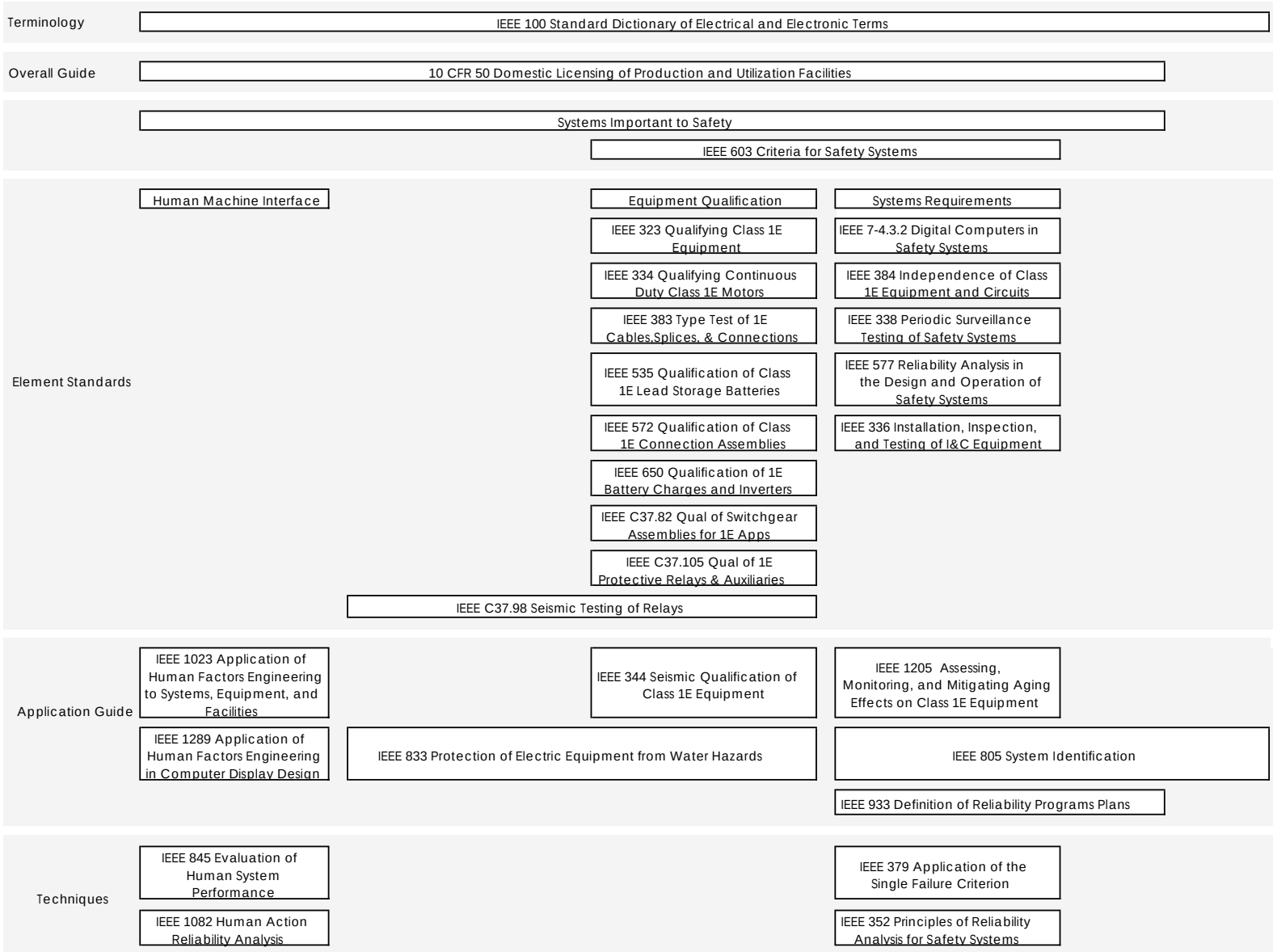
The IEC standards are considered industry specific standards under a general industry systems standard, IEC 61508. This is a relatively new development and the relationship between 61508 and the nuclear standards has not yet matured. No comparable relationship exists in the IEEE sphere.

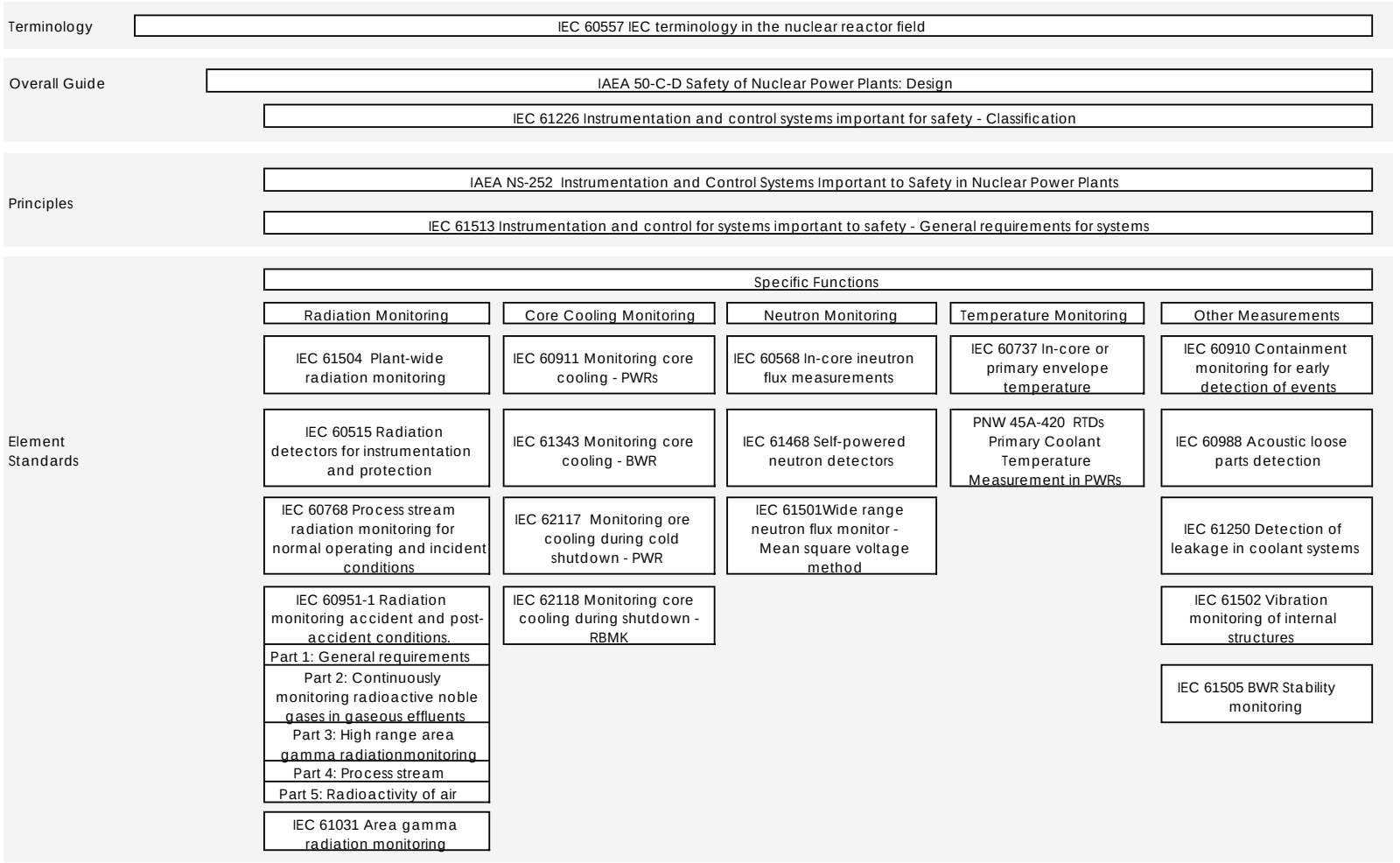
System Standards

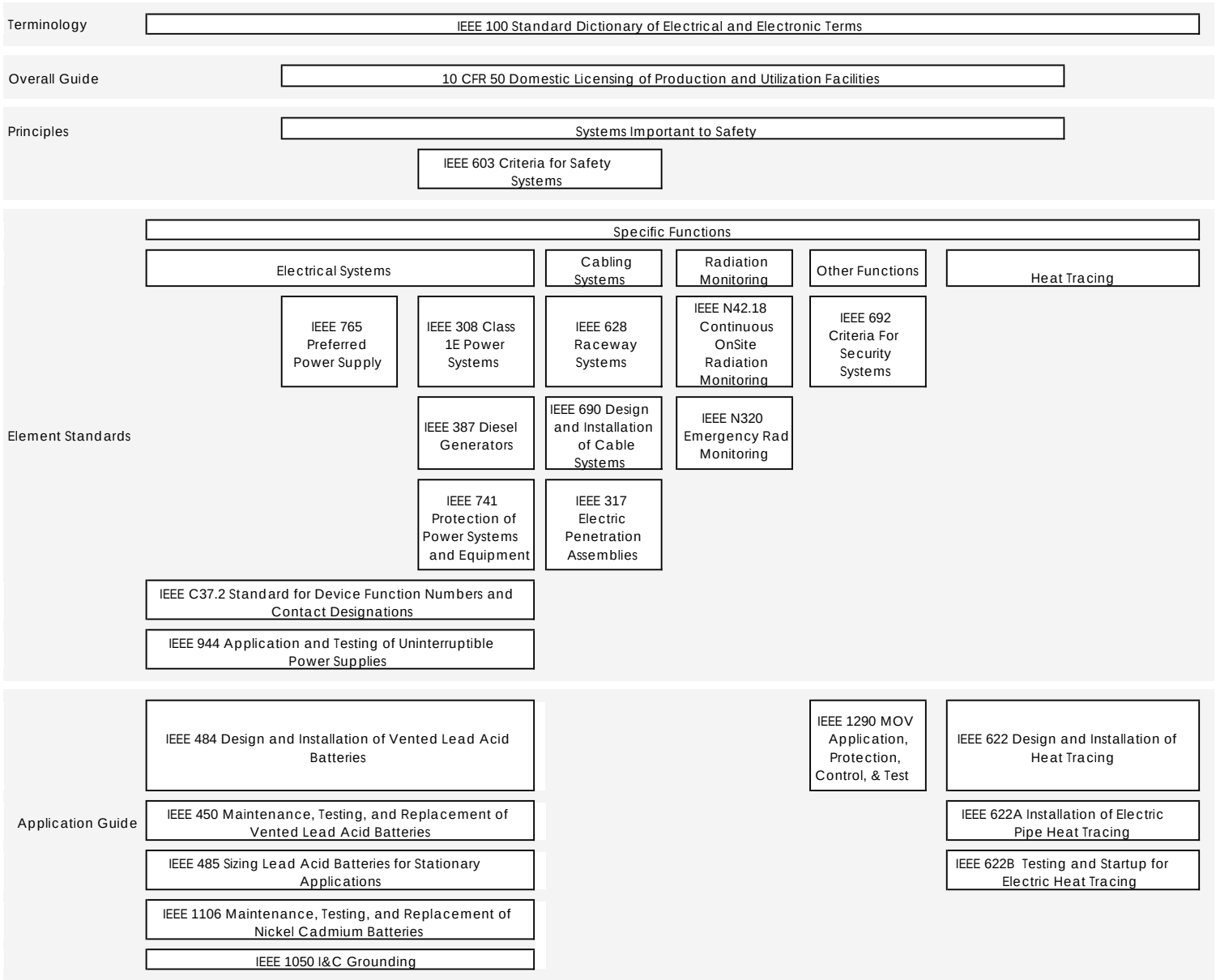
IEEE focuses on safety systems; IEC focuses on systems-important to safety. IEC gives guidance on classification. This topic is not addressed in the IEEE group. The IEC standards may offer useful tools for US risked-based regulation.

IEEE 603 overlaps with IAEA NS-252 and IEC 61513. IEEE 7-4.3.2 overlaps with IEC 60880. The highest priority should be given to working these towards harmony.


Terminology
IEC 60557 IEC terminology in the nuclear reactor field
Overall Guide
IAEA 50-C-D Safety of Nuclear Power Plants: Design
IEC 61226 Instrumentation and control systems important for safety - Classification
Principles
IAEA NS-252 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
IEC 61513 Instrumentation and control for systems important to safety - General requirements for systems
Element Standards
Human Machine Interface
Control Rooms
Specific HMI Systems
Safety systems
Upgrades
IEC 60964 Design of control rooms
IEC 60960 Functional design criteria for SPDS
IEC 60671 Periodic tests and monitoring of the protection system
IEC 61510 Proposals for instrumentation and control improvements - RBMK
IEC 61772 Main control room - visual display units (VDU)
IEC 60965 Supplementary control for remote shutdown
IEC 60744 Safety logic assemblies
IEC 62096 Guidance for the decision on I&C upgrading
IEC 60709 Separation within the reactor protection system
IEC 60772 Electrical penetration assemblies
IEC 60639 Use of the protection system for non-safety purposes
IEC 61497 Electrical interlocks
IEC 61225 Requirements for electrical supplies
PNW 45A-419 Management of Ageing
IEC 60987 Programmed digital computers important to safety
IEC 62138 Software aspects for class 2 & 3 I&C
IEC 60880 Software for computers in safety systems
IEC 60880-2 Software aspects of defence against common cause failures, use of software tools and of pre-developed software
IEC 61500 Multiplexed data transmission
Application Guide
IEC 62247 Main Control Room Design - A review of the application of IEC 60964
IEC 61940 A review of the application of IEC 60880
IEC 62082 Framework for developing standards on computer based systems and software aspects
Techniques
IEC 61771 Main control-room - V&V of design
IEC 60980 Recommended practices for seismic qualification
IEC 61839 Control rooms - Functional analysis and assignment
IEC 60780 Electrical equipment of the safety system - Qualification
IEC 61224 In situ response time for RTDs
IEC 61888 Determination and maintenance of trip setpoints
IEC 61971 PWR - Measurement validation for critical safety functions
IEC 61838 Use of probabilistic safety assessment for classification


Terminology
IEEE 100 Standard Dictionary of Electrical and Electronic Terms
Overall Guide
10 CFR 50 Domestic Licensing of Production and Utilization Facilities
Systems Important to Safety
IEEE 603 Criteria for Safety Systems
Element Standards
Human Machine Interface
Equipment Qualification
Systems Requirements
IEEE 323 Qualifying Class 1E Equipment
IEEE 7-4.3.2 Digital Computers in Safety Systems
IEEE 334 Qualifying Continuous Duty Class 1E Motors
IEEE 384 Independence of Class 1E Equipment and Circuits
IEEE 383 Type Test of 1E Cables,Splices, & Connections
IEEE 338 Periodic Surveillance Testing of Safety Systems
IEEE 535 Qualification of Class 1E Lead Storage Batteries
IEEE 577 Reliability Analysis in the Design and Operation of Safety Systems
IEEE 572 Qualification of Class 1E Connection Assemblies
IEEE 336 Installation, Inspection, and Testing of I&C Equipment
IEEE 650 Qualification of 1E Battery Charges and Inverters
IEEE C37.82 Qual of Switchgear Assemblies for 1E Apps
IEEE C37.105 Qual of 1E Protective Relays & Auxiliaries
IEEE C37.98 Seismic Testing of Relays
Application Guide
IEEE 1023 Application of Human Factors Engineering to Systems, Equipment, and Facilities
IEEE 344 Seismic Qualification of Class 1E Equipment
IEEE 1205 Assessing, Monitoring, and Mitigating Aging Effects on Class 1E Equipment
IEEE 1289 Application of Human Factors Engineering in Computer Display Design
IEEE 833 Protection of Electric Equipment from Water Hazards
IEEE 805 System Identification
IEEE 933 Definition of Reliability Programs Plans
Techniques
IEEE 845 Evaluation of Human System Performance
IEEE 379 Application of the Single Failure Criterion
IEEE 1082 Human Action Reliability Analysis
IEEE 352 Principles of Reliability Analysis for Safety Systems


Terminology
IEC 60557 IEC terminology in the nuclear reactor field
Overall Guide
IAEA 50-C-D Safety of Nuclear Power Plants: Design
IEC 61226 Instrumentation and control systems important for safety - Classification
Principles
IAEA NS-252 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
IEC 61513 Instrumentation and control for systems important to safety - General requirements for systems
Element Standards
Specific Functions
Radiation Monitoring
Core Cooling Monitoring
Neutron Monitoring
Temperature Monitoring
Other Measurements
IEC 61504 Plant-wide radiation monitoring
IEC 60911 Monitoring core cooling - PWRs
IEC 60568 In-core ineutron flux measurements
IEC 60737 In-core or primary envelope temperature
IEC 60910 Containment monitoring for early detection of events
IEC 60515 Radiation detectors for instrumentation and protection
IEC 61343 Monitoring core cooling - BWR
IEC 61468 Self-powered neutron detectors
PNW 45A-420 RTDs Primary Coolant Temperature Measurement in PWRs
IEC 60988 Acoustic loose parts detection
IEC 60768 Process stream radiation monitoring for normal operating and incident conditions
IEC 62117 Monitoring ore cooling during cold shutdown - PWR
IEC 61501Wide range neutron flux monitor - Mean square voltage method
IEC 61250 Detection of leakage in coolant systems
IEC 60951-1 Radiation monitoring accident and post-accident conditions.
IEC 62118 Monitoring core cooling during shutdown - RBMK
IEC 61502 Vibration monitoring of internal structures
Part 1: General requirements
Part 2: Continuously monitoring radioactive noble gases in gaseous effluents
IEC 61505 BWR Stability monitoring
Part 3: High range area gamma radiationmonitoring
Part 4: Process stream
Part 5: Radioactivity of air
IEC 61031 Area gamma radiation monitoring


Terminology
IEEE 100 Standard Dictionary of Electrical and Electronic Terms
Overall Guide
10 CFR 50 Domestic Licensing of Production and Utilization Facilities
Principles
Systems Important to Safety
IEEE 603 Criteria for Safety Systems
Element Standards
Specific Functions
Electrical Systems
Cabling Systems
Radiation Monitoring
Other Functions
Heat Tracing
IEEE 765 Preferred Power Supply
IEEE 308 Class 1E Power Systems
IEEE 628 Raceway Systems
IEEE N42.18 Continuous OnSite Radiation Monitoring
IEEE 692 Criteria For Security Systems
IEEE 387 Diesel Generators
IEEE 690 Design and Installation of Cable Systems
IEEE N320 Emergency Rad Monitoring
IEEE 741 Protection of Power Systems and Equipment
IEEE 317 Electric Penetration Assemblies
IEEE C37.2 Standard for Device Function Numbers and Contact Designations
IEEE 944 Application and Testing of Uninterruptible Power Supplies
Application Guide
IEEE 484 Design and Installation of Vented Lead Acid Batteries
IEEE 1290 MOV Application, Protection, Control, & Test
IEEE 622 Design and Installation of Heat Tracing
IEEE 450 Maintenance, Testing, and Replacement of Vented Lead Acid Batteries
IEEE 622A Installation of Electric Pipe Heat Tracing
IEEE 485 Sizing Lead Acid Batteries for Stationary Applications
IEEE 622B Testing and Startup for Electric Heat Tracing
IEEE 1106 Maintenance, Testing, and Replacement of Nickel Cadmium Batteries
IEEE 1050 I&C Grounding

IEEE 603 is supported by a suite of detailed standards on specific topics discussed in 603. With specific exceptions a similar set of daughter standards in the IEC sphere does not exist. Harmonization of the 603/7-4.3.2 and the NS-252/61513/60880 sets need to consider the influence of these detailed standards. Consideration might be given to bringing the detailed IEEE standards under the IEC umbrella.

Both IEEE and IEC have very general guidance on equipment qualification. IEEE has a set of very detailed standards describing the application of the detailed guidance to certain specific types of components. Ideally, these detailed standards would support both the IEEE and IEC general guidance.

Human-Machine Interface

IEC emphasizes HMI design for functions - main control room, SPDS, Remote shutdown. There is no equivalent in the IEEE set.

IEEE emphasizes HMI techniques. There is some overlap with IEC standards here. There should be a move towards common coverage and harmonization.

Discuss overlap in more detail - Later.

Standards for Specific I&C Functions

Both IEC and IEEE produce standards that impose requirements on specific I&C functions. Strangely, they mostly cover completely different sets of functions. The exception is radiation monitoring.

Ideally, both sets of standards could be used together. To do this they must be consistent with both the IEEE 603 and the NS252/IEC6153 sets.

Software Important to Safety:

The New IAEA Safety Guide and

The Common Position of European Nuclear Regulators

Courtois Pierre-Jacques,

Association Vincotte Nuclear (AVN), Brussels

Abstract: An overview of some distinctive aspects of two international documents which provide guidance on the design and the licensing of computer based systems important to safety prepared by a contributor to both documents. The paper takes a look at their coherence and complementarities, at their strong and original points, and at the issues they leave open.

1. Introduction

In September 2000, two documents were published simultaneously:

the International Atomic Energy Agency (IAEA) Safety Guide " *Software for Computer based Systems important to Safety in Nuclear power Plants*", Safety Guide NS-G-1.1,

and the report EUR 19265 EN of the Nuclear safety, regulation and radioactive waste management unit of the European Directorate General for the Environment[9] "Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors", categorized as a consensus document..

For practical reasons, we will refer to the first document as **SG**, and to the second as **REG**.

These two documents are important, each in its own way. **SG** is a *new* safety guide of the Agency, the first of its kind to focus specifically on software. **REG** is a first consensus document from nuclear regulators on licensing practices specifically addressing safety critical software and produced under the auspices of an international institution. Both documents have taken some innovative viewpoints, sometimes on thorny issues.

[9]This unit activities are now within the Directorate General for Energy and Transport

2. Background

Both documents have been the object of intensive work by experts and consultants, and the result of a long process of meetings and revisions.

The work on the **SG** was initiated as early as April 1991, when a group of distinguished international experts in software engineering – including Professors D.L. Parnas and N. Leveson - met in Vienna. They alerted the Agency that its current guidance did not address software issues –already considered as quite critical at the time - and they drew a list of topics for future technical reports. Their recommendations resulted in the publication, in 1994, of the technical report 367 [2]:" Software Important to safety in Nuclear power Plants" to which about fifteen experts actively contributed with papers and during lively meetings.
In April 1995, a group of four experts met again in Vienna to identify – on the basis of the technical report – the possible contents of a future safety guide. Their report advised the Agency to focus (i) on software issues, (ii) on the interface between the regulator and the licensee and (iii) on guidelines not on how to design but on what is needed to demonstrate adequacy of the design.
Then followed a series of alternate advisory group meetings, technical group and consultant meetings: October 95 and in particular November 1996, when 24 experts from 17 countries met for a week to review, comment and debate the current version of a safety guide. A fourth version of the document was submitted to the Agency Nuclear Safety Standards Advisory Committee (NUSSAC[10]) in October 1997 and accepted as a draft for a safety guide project. A subsequent version was then sent to Member States for comments. Fourteen Member States sent 465 comments which were dealt with in two consultant meetings. Two final consultant meetings took care of these comments, most very positive and constructive.
The version 7 of the guide was endorsed by the NUSSAC in its meeting of October 1999, by the Advisory Commission on Safety Standards (ACSS[11]) in December 1999, and published less than one year later.

The genesis of the **REG** document in many ways followed a similar pattern, albeit within the smaller community of the European nuclear regulators.
The 1995-2000 activity programmes of the Nuclear Regulator Working Group (NRWG) and of the Reactor Safety Working Group (RSWG) of the European Commission Directorate General XI (Environment, Nuclear safety and Civil Protection) were set up within the framework of the 1975 and 1992 resolutions of the Council of Ministers on the technological problems of nuclear safety.
In 1994, the NRWG and RSWG working groups launched a task force of experts from nuclear safety institutes with the mandate of "reaching a consensus among its members on software licensing issues having important practical aspects". From October 1994 to June 1997, the task force met three times a year. The task force selected a set of key issues, produced 64 contributions and made 7 revisions of a draft document which was eventually accepted by the NRWG/RSWG as a EC report [3] publicly available and open to comments (the report was also sent by the commission for comments to 30 prominent international experts). In March 1998, the project ARMONIA (**A**ction by **R**egulators to Har**mon**ize Digital **I**nstrumentation **A**ssessment) was launched with the mission to prepare a new version of the document which would integrate the comments received and would deal with a few software issues not yet covered. In May 1999, after 5 residential meetings of ARMONIA and 25 paper contributions, a revision 10 was submitted to the Task Force for comment and approval. Eventually, in May 2000, after two additional meetings, a revision 11 was presented

[10] now NUSSC, which stands for Nuclear Safety Standards Committee

[11] now CSS, which stands for the Commission on safety Standards

and approved by the NRWG[12], provisionally classified under the category "consensus document". It was made available through the europa server:
http://www.europa.eu.int/comm/energy/en/nuclearsafety/reports.htm - Nuclear installation safety
and published as report EUR 19265 EN in September.

3. Why this guidance is useful

SG and **REG** are guidance documents that aim to meet specific needs, not met by other standards.

The eighties left the nuclear I&C community somewhat traumatized by several modernization projects involving safety critical software that had experienced abnormal delays and costs. The lack of experience, of practical methods and of interactions between the nuclear and other industrial and software engineering communities were probably some of the causes of these problems.

Two observations emerged from these experiences.
If guidance was available to *design* software based safety systems, little or none was available to address the specific issues raised by the *licensing* of highly critical software. As far as software was concerned, regulators and licensees were abandoned to improvisation.
The second observation – somewhat antinomic but salutary – was that software is not per se safe or unsafe. Software is only one component of the system. Checking the software is (i) not sufficient and (ii) is dependent on the environment. The notions of *computer safety case* and of *computer safety demonstration* resulted from this observation and received increased attention.

The section on background already pointed out that the former of these two observations was an essential motivation for launching the **SG** and the **REG** projects.
The second observation was also instrumental. Paragraph 1.5 of the **SG** states: "*The objective of this Safety Guide is to provide guidance on the collection of evidence and preparation of documentation to be used in the safety demonstration of the software of computer based systems important to safety in nuclear power plants*." The **REG** document also has an introductory section which addresses the safety plan, the safety strategy and demonstration: "*…All the subsequent recommendations contained in this report are founded on the premise that (such) a safety plan exists and has been agreed upon by all parties involved. The intent herein is to give guidance on how to produce the evidence and the documentation for the safety demonstration and for the contents for the safety plan."*

This intent to focus on the evidence required by the safety demonstration of software - makes **SG** and **REG** documents complementary to other guidance which – like the IEC 60880 - focuses on requirements for each stage of the software design, development, and V&V processes.

To sum up, in some of its more distinctive aspects, this guidance:
- Addresses regulator and assessor concerns, potential sources of conflict in licensor/licensee negotiations, and identifies grounds for mutual agreement,
- Addresses the safety demonstration (safety case) rather than the system design,
- Emphasizes the need for documentation (**SG**) and identifies sources of evidence (**REG**).

[12]. The RSWG was discontinued in 1999. The NRWG is now made up of Nuclear Safety Authorities from the European Union countries as well as from candidate countries to the EU from Central and Eastern Europe.

4. A same Scope…

Both documents address the software of systems important to safety as the IAEA guides define them, but focus on safety systems. Both documents recognize the difficulty of defining possible relaxations on requirements for safety related software based systems. However, whenever possible, both documents explicitly specify recommendations which apply only to safety systems and thus indirectly admit possible relaxations for safety related system software:

SG: in paragraphs 1.6, 3.15, 4.17, 5.19, 5.21, 5.35, 6.7,

REG: the clauses (more than 30) that apply to safety system software only are mentioned in a specific section (section 1.10), together with specific clauses for safety related systems and examples of relaxations for new and preexisting software.

The **SG** relaxations essentially concern security requirements against the external world, the nature of the independence required from the V&V teams, requirements on the specification of functional and non-functional safety requirements, requirements for statistically valid tests commensurate with the required reliability, and the dedication of safety systems to safety functions.
Moreover, **REG** admits additional relaxations on requirements for the assessment of pre-existing software (PSW), on dependability and documentation requirements for tools, on requirements for software produced by tools, on the required safety culture, on staffing levels, on computer system design (isolation, data protection,…), on programming and coding directives, on statistical testing, on software change control and maintenance, on calibration and testing requirements in operations.

5… But Different Structures and Contents.

While the scopes of the documents are identical, their structures differ.
Their different structures reflect the fact that the **SG** is an emanation of designers, operators and regulators, while the **REG** gives a more focused regulator's common viewpoint.

The **SG** is organized in 15 sections (see appendix 1). The first four sections provide recommendations on preconditions of a software based system development project, on the management of safety, and on the planning of the project.
Sections 5 to 15 are dedicated to the individual phases of the development life cycle, up to post-delivery modifications. Each section is generally structured in the following pattern. In each section, under the heading "RECOMMENDATIONS" there is a set of recommended principles or concerns that should be addressed in this phase. Under the heading 'DOCUMENTS', there is a list of documents to be produced as an output from the phase and advice is provided concerning the contents of these documents. Also, some general recommendations are given concerning the attributes and presentation of the products of the phase. In all parts, the intent is not to provide an exhaustive description of all the material that will be needed for development purposes; instead, the intent is to summarize the principles, material and its attributes that are most important for the safety demonstration.

The **REG** document is organized around a selected set of technical issues which were considered difficult by the task force of regulators and of utmost importance to the licensing process. These issues cover a consistent set of licensing aspects right from the inception of the life cycle up to and including commissioning.
These issues were partitioned into two sets: "Generic Licensing Issues" and "Life Cycle Phase Licensing Issues". Issues in the second set are related to a specific stage of design and development process, while those of the former have more general implications and apply to several stages or to the whole system lifecycle. Each issue area is dealt with in a separate chapter of the report (see appendix 2).

Why two documents within the same scope?
The two documents have one part in common: the annex on preexisting software of the **SG** reproduces a section of the **REG**. Otherwise the contents are quite different. The **SG** is an inclusive account of all the aspects involved in the safety demonstration of a software based system, from the very initial phase before the start of a project up to and including the post-delivery modifications. The requirements and recommendations result from an agreement between experts representing different stakeholders (designers, utilities, regulators) and aim at completeness. They seek to establish an essential and comprehensive basis for the safety demonstration, assuming that more detailed requirements may need to be incorporated according to national practices, or on a case-by-case basis. In contrast, the REG focuses on a set of technical licensing issues only, for which it gives the common viewpoint of regulator's experts. The emphasis is on technical requirements, recommendations, and acceptance criteria, at a detailed level whenever necessary and possible.

6. Non - Prescriptiveness

None of these documents is of course legally binding.
Every IAEA guide foreword clearly states: *"The IAEA standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities."*

The **REG** executive summary is no less clear: " *While the Common Positions are intended to convey the unanimous views of the Task Force members on the guidance that the licensees need to follow as part of an adequate safety demonstration, it should be remembered that this guidance is non-prescriptive. Therefore, its specific application depends on each national regulatory authority. Throughout the document these common positions are expressed with the auxiliary verb "shall". The use of this verb for common positions is intended to convey the unanimous desire felt by the Task Force Members for the licensees to satisfy the requirements expressed in the clause. The Common Position requirements can be regarded as a common denominator of practices in the member states represented in the task force*."

It is the IAEA usage to use the verb "should" to express all recommendations in a safety guide, with the understanding that it is necessary to take the measures recommended or equivalent alternatives to comply with the requirements stated in the Safety Requirements publications. In the preparation of the **REG**, it was found useful to use, like the IEC standards, "shall" and "should" statements. "shall" statements are used in **REG** for expressing the common positions (as defined above), and "should" statements for *recommended practices.* Recommended practices are recommendations supported by most, but which may not be systematically implemented by all of the members states represented in the task force. In contrast, the set of requirements of a *common position* was – I believe -regarded as being "technically necessary" (the same technical necessity that would leave no choice to a railway safety guide but to require that the gates "shall" be closed before the train is on the railway crossing).

7. Some salient points

Both documents make steps forward by showing consensus on certain prevention or precaution measures to deal with software issues that either always proved difficult, or are new because they are engendered by new software practices. Below are a few examples, with no intent of being complete.

On automatic code generation
As far as licensing is concerned, there has always been much debate between proponents of systems generating code from application specifications and those more familiar with the classical development cycle. Here is the position of the **SG:**

Code can be produced from the system specifications in various ways that are essentially combinations of two distinct approaches: the classical development process through stages of specifications and design…, or the use of code generating tools which receive as input a high level language application-oriented description of the system. The choice between these two approaches depends on the tools and resources available to the parties involved in the project, and should, in particular, take into account trade-offs between design and the demonstration of the dependability of tools. The recommendations of this Section (i.e. the section on software implementation) *apply to all possible combinations of the two approaches.(9.2)*

And on software requirements for code generated by tools (**SG**):
Software requirements are the subset of the computer system requirements that will ultimately be implemented as computer programs…The verification of the software requirements against the upper level requirements is an important step in the licensing process…(7.1)
If the computer system requirements are sufficiently detailed and their documentation is sufficiently formal, and if parts of the computer system design and of the code are generated by tools, then a separate software requirement document may be unnecessary for those parts. However, those parts of such computer system requirements from which code is generated or reused should be regarded as a statement of software requirements against which subsequent code should be verified. Also any separately compiled modules that are included by the code generator should be supported by separate documents for the software requirements (7.4).

On software and code hazard analysis
The application of hazard analysis to software is still barely dealt with by international guidance. The **SG** has several recommendations, e. g.:
…the computer based system and its interfaces to the plant should be evaluated at various phases of the development for potential contribution to hazards at plant level. (possible techniques are outlined in TRS 367 - Section 8.3.9). When such potential critical behaviours are identified, they should be traced into the Computer System Design, the Software Design and the code in order to identify parts of the design and of the software that require special design features. In addition, these hazards should be traced back into the requirements and should be incorporated into the plant safety analysis as appropriate(10.27).

…A documented demonstration should be provided that the Software Design addresses the hazards identified in previous analyses and the requirements that have been identified as important to safety.(8.14)

On pre-existing software (PSW)

The **SG** addresses the use of pre-existing or COTS (Commercial-Off-The-Shelf) software for safety functions (paragraphs 1.9, 2.11, 6.1, 6.40, 10.1, and annex).
The **REG** recognizes that licensees may wish to make use of such software given that appropriate assessment has been undertaken. Two of its sections deal with the issue: a specific one also reproduced as an annex in the **SG**, and another devoted to safety related systems. For safety systems, the **REG** is clear: *For safety systems (category one), the PSW shall be subjected to the same assessment (analysis and review) of the final product (not of the production process) as new software developed for the application. If necessary, reverse engineering shall be performed to enable the full specification of the PSW to be evaluated. (1.3.3.5)*

For safety related software, the **REG** recognizes that several possible sources of evidence may be exploited: : *Simplicity is required for safety systems. Safety related systems can be more complex. For these latter systems less information may be available on the development process and on the product. In certain cases, it might be possible to compensate for this lack of information - typical for pre-existing software (PSW) of category 2 - by using evidence provided by functional testing and adequate operational feedback. (1.10.1.3)*

Another source of evidence is suggested for safety related software: *In order to evaluate the possibility of relaxing certain requirements of the safety demonstration, as a minimum, the consequences of the potential modes of failures of the computer based system shall be evaluated. For instance, a failure mode analysis may show that certain relaxations are possible, when failures of the system can be anticipated and their effects can be detected and corrected in time by other means. (1.10.3.3)*

On independent assessment

This is a difficult issue. In human societies, which draw their strength from interrelations and interdependencies, independence is somehow against nature, and often difficult to achieve. Besides, there are several types of independence, all of which are susceptible to make access to relevant information more difficult, and thereby affect assessors' competence. So, it is important to clarify what sort of independence is required and for what purpose.

The **SG** makes the following distinction**: …** *Independence includes:*

- *Technical independence: done by different people, preferably using different techniques and tools;*
- *Management independence: led and motivated by different people. The V&V team and the development team should have different management lines. Official communication between independent teams should be recorded;*
- *Financial independence: there should be a separate budget with restrictions on transfer of financial resources between development and V&V.(4.17)*

The **SG** also allows some relaxations:. *The amount and type of independent V&V should be justified with respect to the safety class of the system, e.g. financial independence may not be required for safety related systems.*

The **REG** emphasizes competence but does not go as far as strictly requiring (shall) financial independence: *The system and its safety demonstration shall be subjected to a documented review by persons who are*:

(a) Competent;

(b) Organizationally independent of the supplier(s) of the system (and of its safety demonstration), and

(c) Not responsible for or in the development, procurement and production chain of the system.(1.9.3.1)

The **REG** also suggests that for safety related systems, independent validation only might be needed, in contrast to the requirements for independent verification (section 2.5), validation (section 2.6) and assessment (section 1.9) defined for safety systems.

On formal methods

The **REG** has 9 common positions on this difficult topic and 6 recommended practices. One of the key principles on which the common positions were founded is:

No credit can be taken in a safety demonstration for the use "per se" of a formal method without due consideration being given to the specific evidence brought in by this use, and to its contribution to the safety demonstration of the system. (1.8.3.1)

On documentation

The **SG** emphasizes documentation, and has a set of requirements on the documents to be produced in each section dealing with a stage of the development process. One general requirement is: *The set of documents should ensure the traceability of design decisions… Appropriate documents should*

be produced at each step of the development process. It is essential that documentation be updated throughout the iterative development including commissioning and ongoing maintenance processes. The documents available to the regulator should be identical to those used by the designers. The designer should be informed of this requirement early in the project.(3.35)

On determinism and interrupts

Both documents are not always fully aligned, but it is difficult to catch them out in blatant incoherence. For instance, the **SG** states: *The architecture chosen should be deterministic. A design should be selected that makes the operation of the software predictable in terms of response to inputs and the time to produce a response. A fixed, repeated sequence of operations (e.g. polling) may generally be used rather than interrupts. Communication protocols should be deterministic and should not depend on the correct operation of other, external systems (8.10).*

The **REG** is somewhat less conservative**:** *…the code shall - as much as possible - run in a direct and fixed sequence pattern…Interrupts shall be avoided unless they lead to a significant simplification. Where interrupts are used, their usage and masking during time and data critical operations shall be proven correct and shall be well documented. The use of high-level synchronisation programming primitives shall preferably be used to deal with interrupts. The hardware and software shall be designed so that every interrupt is either serviced or explicitly masked. (2.4.3.3.2)*

On software reliability and demonstrable dependability

Here, both documents are more cautious than other international standards.

The **SG** emphasizes the issue of dependability, but avoids that of software reliability**:** *The system must not only be dependable, it must also be possible to demonstrate to the regulator that it is dependable. This safety guide is intended to guide licensees in how to achieve demonstrable dependability through design and qualification methods that improve traceability and through the production of adequate documents.(3.19)*

And later, in the section on software requirements, it explains why: *An overall software reliability target may be stated, but it should be understood that the achievement of such a target will be less demonstrable than the fulfillment of other types of requirements. It is extremely difficult to demonstrate that quantitative reliability requirements for software have been met. Currently available methods do not provide results in which confidence can be placed at the level required for systems of the highest importance to safety, and therefore this Safety Guide does not provide guidance on the use of software reliability models. If applicants propose the use of software reliability models for certification or commissioning, a rationale for the model should be included in the certification or commissioning plan and agreed with the regulatory authority. (7.11)*

The **REG** is clearly uncompromising. *It is recognised that the reliability of a computer-based safety system cannot be demonstrated by testing. Therefore, the demonstration of safety has to depend to some degree on the quality of the processes involved….(1.6.2.1).*

However, at the same time, it recommends that the level of reliability that would be required from the software be not left ignored: *The level of reliability required from the software should be explicitly stated, with the understanding that the achievement of a reliability level is less demonstrable than other requirements (2.3.4.1.4).* Retrospectively, one might wonder why this is a recommended practice, and not a common position (shall).

8. Recommendations for further work

Documents of this kind are never complete. Because they result from a consensus, they mark an important step forward, but need to be revised as knowledge and technology progress. When the **REG** neared completion, early in 2000, the members of the task force identified a few important areas where they agreed that more knowledge or experience was needed to establish useful guidance:

1. Diversity/Redundancy
   - Regulator positions requirements for diversity at architecture level;
   - Regulator positions on software diversity

2. Software Reliability
   - Methods to obtain quantitative estimations (numbers).
   - Regulator position to cope with situations where numbers cannot be obtained although quantitative objectives exist for plant operations.

3. Structure of Safety demonstration
   - Contents of a safety demonstration (safety case).
   - Organisation and structure (framework) for claims, sub-claims, arguments, proofs, ...

4. Criteria to rank software based systems in safety categories.
   - Criteria such as existence of redundant back-up, pure informative output or direct action, consequences of failure,..

5. Explicit requirements and acceptance criteria for distinct sorts of software:
   - Code produced by application oriented code generation tools (issues of validation).
   - Libraries,
   - Input/output drivers.
   - Run time and System software (operating systems), etc…

By way of independent confirmation, is was interesting to note a posteriori, that most of these topics were also included as research targets in the NRC proposed five year research plan for digital I&C technology, introduced by Steven Arndt at the Embedded Topical Meeting on Nuclear Instrumentation, Control and Human-Machine Interface Technologies, at the 2000 ANS/ENS International Meeting in Washington, D.C. [1]

9. Conclusions

The forceful value of the two documents lies in the consensus they achieve. Whatever the auspices are, consensus and common positions are always obtained at a given time, in a given context and on certain issues. They never dispense from adaptations and revisions. They are, however, the only way to make progress, especially in those cases where there is uncertainty or where some knowledge or operational experience is missing and a precautionary approach must be followed.

The work discussed above already proved useful in different respects:

- To share technical expertise among those who contributed,
- To support regulators in their national policies,
- To assist licensees in dealing with foreign manufacturers and suppliers
- To help designers produce systems that anticipate licensing requirements and are portable.

10. Acknowledgements

This paper gives a sketchy and personal viewpoint and is not an exegesis of the two guidance documents. As such, it does not do justice to the impressive work of the two teams of dedicated experts who produced them.
Thanks are due to J. Pachner, International Atomic Energy Agency, Vienna, J. Gomez, DG for Energy and Transports of the European Commission, Pierre Govaerts, AVN, and to Manfred Kersken, ISTec, Germany and Bob Yates, NII, UK, former members of those teams, for their useful comments on a previous version of this paper.
The European Commission Research Project "Cost Effective Modernisation of Systems Important to Safety (CEMSIS)" (project FIKS-CT-2000-00109) in part supported this work.

11. References

1. Licensing issues for advanced I&C technologies. Nuclear News, January 2001, 57-58.

2. Software Important to Safety in Nuclear Power Plants. IAEA Technical Reports Series 1994.. TRS N°367, 1994.

3. European nuclear regulators' current requirements and practices for the licensing of safety critical software for nuclear reactors. European Commission, DG Environment, Nuclear safety and Civil Protection, Report EUR18158 (revision 8), 1998.

Appendix 1: Contents of Safety guide NS-G-1.1

1. INTRODUCTION
2. TECHNICAL CONSIDERATIONS FOR COMPUTER BASED SYSTEMS
   Characteristics of computer based systems
   The development process
   Safety and reliability issues
   Organizational and legal issues
3. APPLICATION OF REQUIREMENTS FOR MANAGEMENT OF SAFETY TO COMPUTER BASED SYSTEMS
   Requirements for management of safety
   Design and development activities
   Management and quality assurance
   Documentation
4. PROJECT PLANNING
   Development plan
   Quality assurance programme
   Verification and validation plan
   Configuration management plan
   Installation and commissioning plan
5. COMPUTER SYSTEM REQUIREMENTS
   Recommendations
   Documents
6. COMPUTER SYSTEM DESIGN
   Recommendations
   Documents
7. SOFTWARE REQUIREMENTS
   Recommendations
   Documents
8. SOFTWARE DESIGN
   Recommendations
   Documents
9. SOFTWARE IMPLEMENTATION
   Recommendations
   Documents
10. VERIFICATION AND ANALYSIS
   Recommendations
   Documents
11. COMPUTER SYSTEM INTEGRATION
   Recommendations
   Documents
12. VALIDATION OF THE COMPUTER SYSTEM
   Recommendations
   Documents
13. INSTALLATION AND COMMISSIONING
   Recommendations
   Documents
14. OPERATION
   Recommendations
   Documents
15. POST-DELIVERY MODIFICATIONS
   Recommendations
   Documents

ANNEX: USE AND VALIDATION OF PRE_EXISTING SOFTWARE

Appendix 2:
Contents of Consensus Report EUR 19265 EN

Introduction
Background
Scope, Objectives and Implications
Safety Plan
Generic and Life Cycle Phase
Licensing Issues
Recommendations

Part 1: Generic Licensing Issues

1.1 **Categorisation and Classification**
Rationale
Issues Involved
Common Position
Recommended Practices

1.2 **Applicable Standards**
Rationale
Issues Involved
Common Position
Recommended Practices

1.3 **Use and validation of Pre-existing Software**
Rationale
Issues Involved
Common Position
Recommended Practices

1.4 **Tools**
Rationale
Issues Involved
Common Position
Recommended Practices

1.5 **Organisational Requirements**
Rationale
Issues Involved
Common Position
Recommended Practices

1.6 **Software Quality Assurance Programme and Plan**
Rationale
Issues Involved
Common Position
Recommended Practices

1.7 **Security**
Rationale
Issues Involved
Common Position
Recommended Practices

1.8 **Formal methods**
Rationale
Issues Involved
Common Position
Recommended Practices

1.9 **Independent Assessment**
Rationale
Issues Involved
Common Position
Recommended Practices

1.10 **Requirements for New and Pre-existing Software (PSW) of Safety Related Systems**
Rationale
Issues Involved
Common Position
Recommended Practices

Part 2: Life Cycle Phase Licensing Issues

2.1 **Computer Based System Requirements**
Rationale
Issues Involved
Common Position
Recommended Practices

2.2 **Computer System Design**
Rationale
Issues Involved
Common Position
Recommended Practices

2.3 **Software Design and Structure**
Rationale
Issues Involved
Common Position
Recommended Practices

2.4 **Coding and Programming Directives**
Rationale
Issues Involved
Common Position
Recommended Practices

2.5 **Verification**
Rationale
Issues Involved
Common Position
Recommended Practices

2.6 **Validation**
Rationale
Issues Involved
Common Position
Recommended Practices

2.7 **Change Control and Configuration Management**
Rationale
Issues Involved
Common Position
Recommended Practices

2.8 **Operational requirements**
Rationale
Issues Involved
Common Position
Recommended Practices

Approach to the Application of the State Regulatory Requirements, Legislation and Standards in Modernization of I&C systems, Concerning Especially the Digital Computer-Based Systems

Ing. Jan Zatloukal,
RNDr. Petr Krákora,
both ÚJV Rez a.s.

1. INTRODUCTION

This paper summarizes the experience with the specification and application of the licensing base for the modernization of I&C systems, especially with respect to the digital computer-based systems. It is based on the current project´s development state and licensing phase. The authors base their approach on the actual conditions and experience with suppliers, with whom they cooperate in the area of licensing (Ing. Zatloukal with Škoda, Nuclear Engineering, RNDr. Krákora with Framatome). By the date of the paper submission the phase 2 (which should be rounded off by the SÚJB approval of the upgrade according to §9 paragraph (1) letter f) of the Atomic Act) has not been yet completed and therefore the complete feedback, represented by the licensing documentation review and remarks by the state regulatory body, cannot be included into this version of the paper. The up-to-date experience will be therefore presented only at the seminar.

2. HISTORY

If we review the application of the digital computer-based protection and control systems and their compliance with requirements, it is necessary to recollect the history of the evolution of nuclear energy and simultaneously also the evolution of relevant legislation. The decisive period of the development of nuclear energy is the second half of the 1970s, when the government of Czechoslovakia decided to start construction of nuclear power plant based on licensed VVER-440 design. The design documentation was of Soviet origin and the construction, assembly and start-up were supervised by the authorized bodies of the Soviet Union. During continued construction of NPPs, the industry of the Czech Republic took over the increasing share of the technology supplies. However, the instrumentation and control system remained to be supplied by the former U.S.S.R. Together with the license was taken over also the safety approach based on Soviet standards. Czech legislation and standards in the area of the peaceful utilisation of the nuclear energy were significantly widened during the license appropriation. Among the most important legislative activities rank the approval of the **Act on the state supervision over the nuclear safety** and **decrees of the Czechoslovak Atomic Energy Commission No. 2, 4, 5 and 6. The Decree No. 2** specified requirements on the assurance of nuclear safety of nuclear power facilities during their design and construction, the **Decree No. 4** specified requirements on their siting. **Decree No. 5** specified basic requirements on the development, approval, implementation and control of the quality assurance programs and related measures and activities in planning, preparation, design, manufacture, assembly, commissioning and operation of selected nuclear power facilities from the viewpoint of nuclear safety. **The Decree No. 6** specified safety requirements on the nuclear power facilities during their commissioning and operation and determined the obligatory approach for bodies, organizations and their employees ensuring commissioning (including its preparation) and operation of such facilities. The decrees were subsequently applied even in the stage of the detailed design and during construction. According to these decrees, the

safety of the power plant was evaluated in the Final Safety Analyses Report before its start-up and the plant was commissioned.

Comparing the above mentioned decrees with current requirements, it can be stated that the Czechoslovak legislation (and in principle also then existing Soviet standards) were on very good level and covered all the areas of the today´s the nuclear safety policy and original principles and criteria are, to the large extent, identical with current ones. New regulations differ only in deeper explanation or in the concrete way of the realizing of the compliance with standards. The then created Czechoslovak legislation had also built on the experience of US NRC and took over some of its elements as the Technical Specifications and others, not used in Soviet approach. In licensed manufacture of the technology or in domestic supplies during assembly and tests the Soviet regulations and standards were modified to be in compliance with domestic ones or, if Soviet regulations and standards were not applicable or were missing, Czechoslovak regulations and standards were applied. In this way, the fully satisfactory system was created, completely ensuring requirements on nuclear safety as formulated in the document "Provisions on the application of regulations and standards in the design of Czechoslovak nuclear power plants with units VVER-440 with reactors V-213", issued by the Federal ministry of fuels and energetics of the ČSSR in 1980. In the 1980s nuclear power plants with VVER-440 reactors were successfully operated in the ČSSR and the construction of the Temelín NPP with VVER-100 reactors was being prepared. At the same time, the IAEA was developing the current standards of the nuclear safety goals and criteria. These are distinctly summarized in the report of the International Nuclear Safety Advisory Group (INSAG) Safety Series № 75-INSAG-3, "Basic Safety Principles for Nuclear Power Plants", and elaborated in detail in the IAEA Safety Guides (Safety Series №. 50-SG-xx).

3. NPP TEMELÍN

At the beginning of the 1990s, during construction, it was decided that the NPP Temelín has to comply with international nuclear safety criteria. Among others, it was decided about the replacement of the control system. Westinghouse Electric Corporation, the winner of the bid, incorporated into its design the digital computer-based systems, which up to then had not been used in the NPPs of the former Eastern bloc. These systems won the recognition for their indisputable advantages in other industries (including classical power plants).

Original legislation framework valid for construction and licensing of the NPP Temelín was determined by then valid acts of the CSSR, mainly the Act No. 28/84 Coll. and related regulations and decrees of the CSKAE and Soviet standards. Requirements on protection and control systems were on the legislation level formulated only vaguely and special regulations and technical standards took into account only the then used analog technology. SÚJB therefore accepted the principle of licensibility in the country of origin. The principles, guides and standards valid in the U.S.A. were therefore accepted for assessment of safety and reliability of the Temelín I&C system.

During the NPP Temelín construction, as a consequence of the split of Czechoslovakia and establishment of the SÚJB, so called "Atomic Act" – the Act No. 18/1997 Coll. – was developed and approved together with realization regulations, among others Regulations No. 195/97 Coll. and No.214/97 Coll. Therefore, it was necessary to prove the compliance with their requirements. The process of comparison of the new Czech legislation with the U.S. regulations was chosen as the most suitable.

The requirements on the safety important systems and components for the commercial nuclear reactors in the U.S.A. are codified in the Volume 10, Code of Federal Regulations, Section 50 (10 CFR 50), Appendix A, "General Design Criteria for Nuclear Power Plants". Guidelines, how to comply with the specified requirements, are in the Regulatory Requirements, Part 1, issued by the U.S. Nuclear Regulatory Commission (NRC). Generally, the Regulatory Guides in themselves do not provide all the details necessary to comply with individual requirements, but they refer to standards issued by the relevant

professional organizations. The Regulatory Guides provide the instructions about methods that are acceptable to the Nuclear Regulatory Commission. However, these methods are not the only ones acceptable by the Nuclear Regulatory Commission. The supplier in the Final Safety Analysis Report proved, that requirements of Regulation No. 195/1999 Coll. are identical to those of the NRC General Design Criteria (GDC) from Appendix A, 10 CFR Section 50, and therefore can be used without any limitations.

The basic U.S. standard for I&C systems is the IEEE Standard 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations". This standard specifies the minimum functional design criteria for the power supply and I&C of NPP safety systems and is used together with other standards that in more detail specify for instance the equipment requirements, criteria on separation, reliability analysis, human factors influence, etc. The list of all the used guides, standards, codes and regulations, their use and requested compliance was proved by the supplier in Chapter 7.1 of the NPP Temelín FSAR. In the review process of the submitted documentation, the SÚJB found such evidence as satisfactory.

4. NPP DUKOVANY

In the second half of the 1990´s, in compliance with requirements on the improvement of nuclear safety and operational reliability of the NPP, works have been initiated on the preparation of modernization of the NPP Dukovany I&C system. On April 9, 1999, on the request of the utility – CEZ a.s., NPP Dukovany, SÚJB issued its Decision No. 79/99, in which it summarizes the requirements that has to be complied with during the I&C modernization. In this way, SÚJB took from the very beginning the active approach in specification of legislation and standard requirements base (unlike at the NPP Temelín, where the process of specification of these requirements was in the introductory phases covered by the general principle of the licensibility in the country of origin). SÚJB employed its experience gained in the licensing process of the NPP Temelín and, taking into account the absence of more detailed Czech regulations and guides especially in the area of digital I&C systems, it decided to specify in advance the unified framework for the enforcement of the requirements of the Czech legislation and Czech and international standards by the issue of the document "Set of SÚJB Positions to Selected Aspects of the I&C Renovation of the Dukovany NPP" (further only the “Set of SÚJB Positions”). In this way it established the set of requirements, which allows to unify the evaluation of digital computer-based I&C systems of NPPs. This set is based on Czech and international legislation and standards in the following hierarchy (according to the priority of their application):

- Legislation of the CR (Act No.18/97 Coll., Regulation • 195/97 Coll., Regulation No. 214/97 Coll.)
- SÚJB Decision No. 97/99 and the "Set of SÚJB Positions" (appendix to letter No. 11987/3.2/00)
- IAEA Recommendations: Safety Series No.. 50-C-D/Rev.1, 50-C-D1/Rev.1, 50-SG-D3, 50-SG-D8; IEC and ISO standards (or their Czech equivalents), especially CSN IEC 643, 880, 987, 1226, IEC 61513; CSN EN ISO 9000-3; CSN ISO-IEC 12207.
- US NRC Codes and Regulations: 10CFR50, Appendix A; NUREG-0800/1997; selected Regulatory Guides, especially RG 1.152, 1.168 ÷ RG 1.173; IEEE standards, especially IEEE Std 603-1991, 7-4.3.2-1993, IEEE Standards Collection – Software Engineering (1994 edition).
- Other Czech technical standards

The set of requirements on the application of standards and regulations was included also in the tendering documentation for the Dukovany I&C modernization and subsequently it became a part of the contractual conditions.

The tender was won by the SKODA Nuclear Engineering with the principal supplier – consortium Framatome-ANP/Schneider Electric. Their solution is based on the integrated digital system SPINLINE 3, used also in EDF NPPs in France.

The proofs of compliance with the requirements are submitted to SÚJB in individual licensing stages in the form of documentation required by the Act No. 18/97 Coll., completed by others, more detailed technical reports. This documentation contains updates of the "SÚJB-approved" documentation (PSAR, Technical specifications, List of selected equipment and Program of operational controls), completed by Topical Reports both for the individual I&C systems and to the general aspects and requirements of the I&C system as a whole. These so-called Transverse Topical Reports are subdivided into the following thematic groups (as the "Set of SÚJB Positions"):

- I&C SYSTEMS CLASSIFICATION
- ACCEPTABILITY OF THE DIGITAL SOFTWARE I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY
- REQUIREMENTS ON THE SOFTWARE DEVELOPMENT PROCESS OF I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY
- REQUIREMENTS ON THE V&V OF THE SAFETY I&C SYSTEMS SOFTWARE
- REQUIREMENTS ON THE PROTECTION AGAINST CMF IN THE SAFETY I&C SYSTEMS SOFTWARE
- REQUIREMENTS ON THE COMMUNICATION BETWEEN SUBSYSTEMS OF THE SAFETY I&C SYSTEMS
- REQUIREMENTS ON THE TESTABILITY UNDER OPERATING CONDITIONS
- REQUIREMENTS ON MEETING THE SINGLE FAILURE CRITERION AND ON THE REDUNDANCY
- REQUIREMENTS ON THE EQUIPMENT QUALIFICATION AND THE ISSUE OF ITS VERIFICATION
- REQUIREMENTS ON THE RELIABILITY

The topical reports prepared by the supplier to individual topics are listed in the following table (corresponding Westinghouse reports for the NPP Temelín are given for the purpose of comparison):

ASPECT	NPP Temelín	NPP Dukovany
I&C SYSTEMS CLASSIFICATION		TTR 1 – Classification, NCD DC 13
ACCEPTABILITY OF THE DIGITAL SOFTWARE I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY		TTR 2 – Acceptability of Digital Computer- Based I&C, NCD DC 11
REQUIREMENTS ON THE SOFTWARE DEVELOPMENT PROCESS OF I&C SYSTEMS IMPORTANT FOR NUCLEAR SAFETY		TTR 3 – Software Development, NCD DC 6; Software Quality Assurance Plan, NCD DC 8, SEI 1 208 718; Software Configuration Management Plan, NCD DC 10, SEI 1 208 720; Software Life Cycle Process, NCD DC 10; Software Life Cycle Process, NCD DC 10;
REQUIREMENTS ON THE V&V OF THE SAFETY I&C SYSTEMS SOFTWARE	TEM-I&C-LICEN-005 "Verification and Validation Topical Report"	TTR 4 – Software V&V, NCD DC 7
REQUIREMENTS ON THE PROTECTION AGAINST CMF IN THE SAFETY I&C SYSTEMS SOFTWARE		TTR 5 – Software Common Cause Failure, NCD DC 12
REQUIREMENTS ON THE COMMUNICATION BETWEEN SUBSYSTEMS OF THE SAFETY I&C SYSTEMS		TTR 6 – Communication, NCD DC 17
REQUIREMENTS ON THE TESTABILITY UNDER OPERATING CONDITIONS	TEM-DOC-PRJ-026, "Temelín Test Strategy Document	– TTR 7 – Testability, NCD DC 14
REQUIREMENTS ON MEETING THE SINGLE FAILURE CRITERION AND ON THE REDUNDANCY	TEM-I&C-LICEN-025 "Functional Block Analyses and Failure Modes and Effect Analyses	TTR 8 – Single Failure Criterion, NCD DC 4
REQUIREMENTS ON THE EQUIPMENT QUALIFICATION AND THE ISSUE OF ITS VERIFICATION	TEM-I&C-LICEN-020, "Methodology for Qualifying Westinghouse-Supplied Safety-Related Electrical Equipment for the NPP Temelín Instrumentation and Control Program	TTR 9 – Qualification, NCD DC 19
REQUIREMENTS ON THE RELIABILITY	TEM- I&C-LICEN -027 "Topical Report - I&C Reliability Analysis	TTR 10 – Reliability, NCD DC 20

At the time of writing of this paper, the upgrade of the NPP Dukovany I&C system was in the stage of preparation of the Basic Design and from the required license documentation the Topical Reports, Appendix to the PSAR, revision 2, version 1, the draft of the List of Selected Equipment, the draft of the Limits and Conditions and the draft of the Program of Operational Inspections were prepared and submitted to SÚJB for evaluation. The compliance with the above mentioned requirements was proved by the supplier – Framatome-ANP/Schneider Electric for the designed equipment in corresponding Topical Reports. The supplier accepted all SÚJB requirements without exception and adapted oneself to the required standard and legislation base.

Some key aspects of the I&C modernization are discussed in more detail in the following paragraphs.

5. CLASSIFICATION

Equipment classification follows the standard IEC 61226/1993, in compliance with the SÚJB requirement in the "Set of SÚJB Positions". According to it, the systems are classified into individual classes and according to their ranking they are subject to other requirements, e.g. on qualification or inclusion into the Limits and Conditions. The classification according to IEC 61226/1993 and the Regulation № 214/97 Coll. is very similar, the requirements on classified equipment of both the standard and the valid regulation shall be met. The List of selected equipment, whose draft was submitted within the phase 2 of the licensing process, uses consistently the classification according to the Decree № 214/97 Coll.

6. ACCEPTABILITY OF DIGITAL SOFTWARE I&C

As the replacement of the NPP Temelín I&C by the digital system was approved and this system was subsequently licensed, the digital software systems can be considered as generally acceptable. The "Set of SÚJB Positions" quotes only the basic legal documents mentioned previously (the Act № 18/1997 Coll., the SÚJB Regulations № 195/1997 Coll., № 214/1997 Coll., № 106/1998 Coll.) and the requirements on the new system for the NPP Dukovany are generally specified in the „Resolution № 79/99“ independently on the fact if the system is digital or not. The volume 7 of the FSAR Update under acceptability understands the extent and requirements of IEC 61513, which further states, that the requirements on SW of digital computer-based systems to be applied in I&C category A systems are specified for SW in standards IEC 60880 and 60880-2 and on HW in IEC 60987.

Transverse Topical Report 2 was elaborated to this topics by the supplier to be transmitted to SÚJB.

7. SOFTWARE DEVELOPMENT PROCESS, SOFTWARE V&V

For modernized digital computer-based I&C systems, classified as IEC 61226 category A, the SW development process shall be (according to the "Set of SÚJB positions" a complex process containing:

- planning activities,
- life cycle process activities, and
- some transverse activities of the SW life cycle process implementation.

An appropriate set of SW life cycle activities is provided for instance in Regulatory Guide 1.173 "Developing SW Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants", which endorses IEEE Std 1074 "Standard for Developing Life Cycle Processes".

Planning activities shall result in a set of planning documents, containing

- SW Project Management Plan
- SW Quality Assurance Plan
- SW Verification & Validation Plan
- SW Configuration Management Plan
- SW Safety Plan, and
- SW Life Cycle Plan, which can be divided according to individual steps of the SW life cycle process into:
  - SW Development Plan
  - SW Integration Plan
  - SW Installation Plan
  - SW Training Plan
  - SW Operations Plan
  - SW Maintenance Plan.

In licensing process, phase 2, the supplier carried out required planning documentation as parts of Transverse Topical Reports 3 and 4 (see the table above).

The required outputs of the **life cycle process activities** are following design documents (only documents listed, worked out in phase of basic design):

- SW Requirements Specifications (SRS)
- SW Design Specifications

In the scope of basic design the supplier provided a set of documents containing input data for SW requirements specifications and several documents concerning the design specifications (functional diagrams, equipment specifications).

Other documentation (as Operation, Maintenance and Training manual) will be completed in later design phases.

Other **"transverse" activities of the SW life cycle process implementation** contain V&V (the required output is the set of V&V reports), configuration management (CM reports) and Safety analyses.
SÚJB requires for the V&V Process to meet the requirements of IEC 880, but does not insist on performing the V&V by a third independent organization assuming that the group carrying out the activities at the manufacturer's is in no way interested in the development process of the verified SW.

8. PROTECTION AGAINST COMMON MODE FAILURE, IMPLEMENTATION OF DIVERSITY AND DEFENSE IN DEPTH

The assurance of robustness against the common mode failures in performance of the safety important I&C functions and implementation of diversity is not required by the Czech legislation (there are only general requirements). The SÚJB Resolution № 79/99 specifies the requirements on diversity (items 11,B.3.a and 11,B.3.b), Czech legislation solves only separation of protection and control systems (Regulation № 195/99 Coll.).

The "Set of SÚJB positions" prefers the approach of US NRC and recommends as an example the Westinghouse document TEM-I&C-LICEN-017, which elaborates the design criteria for the diversity implementation. In relation to the Dukovany I&C modernization the document further develops the requirements on diversity.

The requirement on implementation of diverse line of protection in the U.S. legislation is on the general level stated in GDC 22 as the measure against the loss of the protective function and is specified in §50.62 of 10CFR50 for the purposes of ATWS (Anticipated Transient Without Scram). This requirement was later on extended in the US NRC Staff Requirements Memorandum on SECY 93-087 into so called four-point position, concerning the issues of the diversity and defense-in-depth implementation in safety important digital computer-based I&C systems. Good presentation of the methodology gives NUREG/CR-6303.

SÚJB requires implementation of diversity in protection against PIE solved in the safety analyses with occurrence frequencies above 10^{-3}/year (ANSI condition II, III). It is possible to limit the CMF postulation only to SW of the programmable parts of systems performing safety functions. It is also admissible not to consider the SW CMF in SW modules for which a 100% reliability will be declared (error-free SW). The diversity can be implemented as functional diversity or equipment diversity. The analysis of implemented diversity is required.

These requirements were taken into account by the supplier in the Basic Design and the topics was evaluated in the Licensing documentation: Transverse Topical Report 5 - Software Common Cause Failure, and the FSAR Update, vol. 7, rev.1, version 1). The supplier also took into account the newest IEC 60880-2 standard. Implemented CMF is based on means of functional and signal diversity. Transverse Topical Report 5 presents also the preliminary analysis of SW CMFs, the required detailed analysis will be submitted during next licensing phase.

9. single failure criterion (SFC), redundancy

SÚJB in the "Set of SÚJB positions" specifies for the case of EDU I&C modernization the definition of the single (random) failure criterion, including all operation states/conditions, during which the SFC shall be considered. SÚJB does not exclude the possibility of acceptance of extraordinary cases, in which the protection system will not be resistant against the single failure, but requires an exact specification of such conditions and their strict limitation, individual discussions and a demonstration, that the refusal of the exception would cause very significant and hardly feasible design modifications.

In the interpretation of the requirement on redundancy, at least threefold redundancy of all parts of protection systems is recommended (to express it in a simplified way). There shall be a deterministic evidence of meeting the SFC, probabilistic analysis will not be accepted.

During phase 2 of the licensing process the supplier carried out the Transverse Topical Report 8 - Single Failure Criterion, discussing the implementation of SFC and redundancy and containing also the deterministic analyses for the protection system.

10. CONCLUSIONS

The active SÚJB approach, consisting in early definition of the requirements beyond the Czech legislation and standards (especially for the digital computer-based systems), allowed CEZ to implement the specified requirements into contract documents. In this way priorities in application of legislation, guides, standards and other requirements together with their applicability status were set.

The application of the requirements, especially in several key aspects specified in the Set of SÚJB positions, express in all levels of the project: in contract provisions, design specifications (requirements on the system architecture, operational and performance requirements) as well as in design and licensing (safety) documentation.

The present state of the project (Basic Design, Licensing Phase 2) shows, that the used approach of early requirements specification serves well. Contemporary Czech legislation based on the Atomic Act and executive regulations together with clearly specified SÚJB positions establish an appropriate frame for application of other both Czech and international codes and standards without the need of further legislative codification of additional principles and requirements.

Standard Base for Regulatory Activity in NPP I&C Area

M. Yastrebenetsky, V. Goldrin, Yu. Rozen, S. Vinogradskaya

State Scientific Technical Center on Nuclear and Radiation Safety,
17 Artema str., Kharkov 61002, Ukraine

Tel.: +38 0572 471 700, Fax: +38 0572 471 700

e-mail: yastreb@reliable.kharkov.ua, rel@online.kharkiv.com

Summary

Ukrainian standard base for regulatory activity in the area of NPP I&C systems now includes 3 documents:

- *"Requirements on Nuclear and Radiation Safety to NPP I&C Systems Important to Safety" [1, 2]*
- *"Methodic of Assessment of Compliance of NPP I&C Systems to Safety Requirements" [3, 4]*
- *"Requirements to Order and Contents of Life Extension of Instruments which are included into Safety Important Systems" [5, 6]*

The methods of selection of regulatory requirements for I&C systems (status, criteria of selection, systematization of initial date, procedure of establishing, main peculiarities, etc.) were examined.

1. Introduction

Under establishment of standard base for regulatory activity in NPP instrumentation and control (I&C) systems area in Ukraine, different methods are possible in principle:

- to adopt as standard base the requirements of normative documents on safety that are currently in force in any other country (for example USA, Germany, Russia);

- to adopt as standard base the requirements of international standards and guides on safety developed by IAEA, IEC, ISO not creating own ones;

- to work out the own standard base taking into consideration home and international experience on regulation and safety evaluation as well as available scientific-technical and economical potentials for NPP safety assurance in Ukraine.

The last version was adopted, as:

- the Ukraine already has her own formed system of normative documents on nuclear safety and new documents shall fit the structure of this system.
- at Ukrainian NPP are implemented the I&C systems, designed not only by Ukraine but by great number of foreign companies (for example USA, Germany, Czech Republic, Russia), each of them uses the standard base of their own country. The Ukrainian standard base shall be unified for all these systems;
- the countries with different economic development have non-similar means to provide and confirm safety of their NPP that considerably influence the level of standard bases of these countries.

The standard base:
- applies to I&C systems important to safety and their components:
  - software-hardware complexes (SHC);
  - hardware (HW);
  - software (SW);
- not contrary to laws and basic normative documents on nuclear safety that are currently in force in Ukraine ;
- harmonized to a maximal possible extent with the requirements of international safety standards and guides [7-9, etc.] that are not included in Ukrainian normative documents;
- use the experience of safety regulation available in national standards of the leading countries.

Let us dwell on the development methods of the first of three indicated documents. These methods provide the following:
- determination of a status of developed documents (their category, rank and connections in the system of normative documents on nuclear safety that are currently in force in Ukraine;
- establishment of criteria for selection of regulatory requirements;
- systematization of initial data used for safety regulation of I&C systems and their components;
- standardization of regulation procedure (establishment of regulatory requirements)

The status of developed documents

In the system of documents on nuclear safety that are in force in Ukraine it is possible to separate out three hierarchy levels.

The upper hierarchy level is the documents of government bodies (Ukrainian legislation, decrees of Ministry Councils) determining the order of state safety regulation in the scope of nuclear power use.

Normative documents developed and/or put in force by Regulatory Body of Ukraine, containing the basic provisions on assurance of NPP safety including the fundamental regulatory requirements to their systems and components (including I&C systems) are considered as the second hierarchy level.

The third hierarchy level is represented by normative documents of Regulatory Body of Ukraine, which establish the general regulatory requirements with regard to determined tasks, system classes or kinds of NPP equipment.

The connections between these hierarchy levels provide the following:
- requirements established in documents of upper hierarchy level are detailized in documents of downstream adjacent hierarchy;
- documents of more low hierarchy level can in case of necessity establish the additional regulatory requirements;

- in documents of lower hierarchy level the requirements contradictory to requirements established in documents of any upper hierarchy level shall not be laid down.

On the grounds of stated above it is determined that documents being developed on I&C systems regulation and safety evaluation should:

- be positioned on the third hierarchy level;
- establish the general regulatory requirements with regard to I&C systems important to safety of NPP and their components that ad and/or detailize the basic requirements of normative documents of the second hierarchy level;
- be binding under elaboration of normative, project, design and other documents and carrying out of works on creation, reconstruction or modernization particular I&C systems and their components;
- be used as basis for evaluation of I&C systems safety, both acting at Ukraine NPP and new (reconstructed, modernized) ones.

Selection criteria of regulatory requirements

An important aspect of safety regulation methods is the establishment of guideline criteria for determination of composition and contents of regulatory requirements on I&C systems and their components. Such criteria were elaborated as result of analyses and summarizing of domestic and foreign normative documents, recommendations of international organizations on safety as well as other sources.

Under elaboration of normative documents the following criteria ("requirements to regulatory requirements") are used:

- ***necessity*** – criteria according to which the using of I&C systems not meeting this regulatory requirements can result in violation of limits and/or conditions of NPP safe operation;
- ***completeness*** - criteria according to which the using of I&C systems meet all qualifying standards most likely does not result in violation of limits and/or conditions of NPP safe operation;
- ***sufficiency*** – completeness criteria attributed to separate regulatory requirement;
- ***unambiguous*** - criteria according to which the least rigid requirement of possible versions meeting the sufficiency criteria are adopted as the regulatory requirements;
- ***correctness*** – correspondence of regulatory requirement with respect to similar requirements that are regulated in normative documents of the same and/or more upper hierarchy level;
- ***progressiveness*** – meeting of the regulatory requirement the achieved level of science, engineering and technology;
- ***testability*** – the possibility of evaluation of I&C systems meeting to the regulatory requirements, which are based upon the facts, test results and/or analyses results;
- ***traceability*** – testability criteria attributed to different stages of object life cycle;
- ***clarity*** – quality criteria of regulatory requirement statement providing its understanding by specialists without additional explanations;
- ***uniqueness (single meaning)*** - quality criteria of statement which makes it impossible to interpret differently the same regulatory requirement;
- ***categoricity*** - criteria according to which each I&C systems shall meet all relevant regulatory requirements.

During safety regulations the necessity, completeness and sufficiency criteria were taken into account when determining the list of the regulatory requirements; the correctness, progressiveness, testability and traceability criteria – when establishing the concept contents of each requirement; the clarity and uniqueness criteria – when stating the regulatory requirements in the developed normative document. The testability, traceability, clarity, uniqueness criteria as well as categoricity of regulatory requirements are essential from the point of view of safety evaluation.

Initial date systematization

The normative base foundation used under elaboration of regulatory requirements of I&C systems and their components is as following:

- Ukrainian Legislations concerning nuclear power use and nuclear safety;
- Norms and Rules on Nuclear Safety;
- Standards of former USSR that are currently in force in Ukraine;
- Ukrainian Standards;
- Safety Standards and Guides developed by international organizations – IAEA, IEC, ISO;
- National Standards of USA, Germany, France, Russia.

The documents of two last groups are not formally adopted in Ukraine; therefore, the requirements, norms and rules included into them cannot be regarded as per definition as regulatory requirements for Ukraine. However, they are of exclusively great importance for our county, as they reflect the international experience that «outrunning the limits of purely national bounds tends to definite harmony in practice of safety assurance at the European and even the world level" [11].

In accordance with the adopted methods, all abovementioned normative documents (ND) are structured as per two classification characteristics.

Depending on the subject of normative regulation the following classes are marked out:

- ND on NPP safety containing requirements to NPP systems and elements, that apply also to I&C systems and/or their components (class A: "NPP Safety");
- ND establishing the requirements to I&C systems and their components used in different industrial branches including NPP (class B: "Industrial systems");
- ND that are concerned directly and only to NPP I&C systems and their components (class C: "NPP I&C systems");
- ND of general technical nature establishing requirements related to NPP I&C systems (class D: "General Technical ND").

Depending on the scope of activity ND are divided into the following types:

- Ukrainian Legislations, Standards, Normative Decrees of Ukrainian Regulation Body (type 1: "Ukrainian ones");
- Norms and rules on nuclear safety and standards of former USSR that are currently in force in Ukraine (type 2: Interstate ND);
- Safety Standards and Guides of International Organization (type 3: "International ones");
- National Standards of other countries (type 4: "National ones").

Crossings of rows (classes) and columns (types) generate the groups of ND, each of which was analyzed during the development.

Procedure of establishment of regulatory requirements

Proposed procedure provides the following order of initial data analyses and establishment of regulatory requirements to I&C systems [1,2]:

- in accordance with the adopted structure of normative base for each group of ND the lists of normative documents that include the requirements to I&C systems and their components are worked out;

- the complete lists of such requirements regulated in each of analyzed normative documents are worked out;

- on the ground of necessity criteria the requirements important from the point of view of nuclear safety assurance are generated;

- for each of such requirement the essential analyses are carried out using method of comparison its statements within different normative documents, probably, with involvement of other sources (publications, reports, etc.);

- carrying out the evaluation if each requirement meets the criteria of completeness, unambiguous, correctness, progressiveness, testability and traceability;

- according to analyses results the statements of regulatory requirements are offered;

- each statement is evaluated as per clarity and completeness criteria;

- in accordance with the necessity, completeness and sufficiency criteria the complete lists of requirements to I&C systems are determined as well as the degree of their binding (depending on safety class, functional destination and other peculiarities of subject of regulation).

Table 1 – 3 present the proposed lists of the regulatory requirements to I&C systems, hardware (HW) and software (SW).

Table 1. Regulatory requirements to I&C systems

Group of requirements
Meeting single failure principle
Meeting independence principle
Meeting redundancy principle
Meeting diversity principle
Requirements to protection against common cause failures
Requirements to reliability
Requirements to accuracy
Requirements to response rate
Requirements to human-machine interface
Requirements to protection against unauthorized access
Requirements to technical diagnostics
Requirements to prevention from staff errors
Requirements to resistance against environmental impact
Requirements to resistance against changing parameters of supplied power
Requirements to quality
Requirements to testing and acceptance

Table 2. Regulatory requirements to HW

Group of requirements
Requirements to stability against the environmental impact
Requirements to stability against mechanical impacts
Requirements to stability against electrical fields
Requirements to stability against impact of special media
Requirements to stability against changing parameters of supplied power
Requirements to accuracy
Requirements to electrical insulation
Requirements to electromagnetic compatibility
Requirements to reliability
Requirements to testability
Requirements to protection against unauthorized access
Requirements to fire safety
Requirements to qualification

Table 3. Regulatory requirements to SW

Group of requirements
Requirements to structure and elements of SW
Requirements connected with diagnostics and self-inspection
Requirements connected with provision for reliability
Requirements connected with protection of data
Requirements to process of SW development
Requirements to used SW
Requirements to documenting of SW development
Requirements to procedures of SW verification
Requirements to documents on SW verification

The main peculiarities of regulation "Methodic of Assessment of Compliance of I&C systems to Safety Requirements"

- Maximum usage of existing in Ukraine types of documents. Expert review of each document is performed immediately after preparation of this document – almost in "on-line" mode. Safety Analysis Report is important but is not the only document in the complete set of documents for safety assessment. The designer and NPP can analyze the remarks of experts and make appropriate changes without long delay.

- Typical steps of I&C systems expert review:

    - expert review of NPP technical decision on modernization (with conception of modernization);

    - expert review of specification;

    - expert review of design documentation;

    - expert review of software V&V plan and report;

    - expert review of Safety Analysis Report;

    - expert review of methodic and results of site acception test.

- Safety assessment includes:

    - software and hardware analysis along with analysis of systems as a whole;

    - analysis of the interface between I&C modernized and unchanged parts;

- analysis of the system quality assurance program.

- Each expert review contains a set of expert cards. Each card contains:
    - the requirements according to standards, rules, guides;
    - brief description (summary) of this requirements realization in system documentation;
    - expert evaluation;
    - conclusion and recommendations.

Regulatory requirements was used in licensing of computer information systems, SPDS, automatic regulators, refueling machine control systems, protection systems, etc. (designers of these systems were the companies of USA, France, Germany, Czechia, Russia, Ukraine) for Ukrainian NPP. These requirements will be used under licensing process of I&C systems for new units – Rovno 4 and Khmelnitsky 2.

References

1. NP306.5.02/3.035-2000. Requirements of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety on NPP/ M.A. Yastrebenetsky (ed.), Y.V. Rozen, V.S. Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

2. M. Yastrebenetsky, Y. Rozen, V. Vasilchenko, S.Vilkomir. Elaboration of common regulatory requirement on modernized NPP instrumentation and control system important to safety. Foresight and precaution. Proceedings of ESREL 2000, SARS and SRA-Europe annual conference.A.A.Balkema, Rotterdam, 2000,p.813-817.

3. NP 306.7.02/2.041-2000. Methodic of Assessment of Compliance of NPP I&C Systems to Safety Requirements/ M.A. Yastrebenetsky (ed.), S. V. Vinogradskaya, V.S. Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

4. M. Yastrebenetsky. Safety assessment of NPP instrumentation and control systems. Nuclear plant instrumentation , control and human-machine interface technologies (NPIC & HMIT 2000).American Nuclear Society. 2000. Washington, DC. ISBN : 0-89448-6446.

5. ND 306.711-96. Life extension of hardware included into safety important I&C Systems. General requirements to order and content of works/ M.A. Yastrebenetsky (ed.), V.M. Goldrin. Ukrainian Ministry of environment protection and nuclear safety. Kiev, 1996.

6. M.A. Yastrebenetsky, L.N. Garagulya, etc. Reliability analysis of VVER-1000 information and control system. The 3rd JSME/ASME Joint International Conference on Nuclear Engineering. Kyoto, Japan. 1995, Vol. 3, p. 1295-1298.

7. IAEA 50-Sg –D3. Protection System and Related Features in Nuclear Power Plants.

9. IAEA 50-Sg-D8. Safety-Related Instrumentation and Control Systems for Nuclear Power Plants.
10. IAEA Safety Standards Series. Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Draft safety guide.
11. IEC 880. Software for Computers in the Safety Systems of Nuclear Power Plants.

12. Libmann, J., Elements of Nuclear Safety, EDP, France, 1996

TECHNICAL SESSION 2
REGULATORY ASPECTS

Chairmen: K. Hamar, A. Lindner

EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Regulatory Commission

C. Antonescu[1], P. D. Ewing[2]

[1]U.S. NRC, Office of Nuclear Regulatory Research, ERAB, MS T-10E33, 2 White Flint North, 11545 Rockville Pike, Rockville, Maryland 20852, USA
Tel.: +011 1 301 415 6792, Fax: +011 1 301 415 5160, e-mail: cea1@nrc.gov

[2]Oak Ridge National Laboratory, P.O. Box 2008, MS 6006, Oak Ridge, Tennessee 37831 USA
Tel.: +011 1 865 576 5019, Fax:+011 1 865 576 2813, e-mail: ewingpd@ornl.gov

Summary

This paper discusses the regulatory guidance implemented by U.S. NRC for minimizing malfunctions and upsets in safety-related instrumentation and control (I&C) systems in nuclear power plants caused by electromagnetic interference (EMI), radio-frequency interference (RFI), and power surges. The engineering design, installation, and testing practices deemed acceptable to U.S. NRC are described in Regulatory Guide (RG) 1.180, "Guidelines for Evaluating Electromagnetic and Radio-Frequency in Safety-Related Instrumentation and Control Systems" (January 2000) and in a Safety Evaluation Report (SER) endorsing EPRI TR-102323, "Guidelines for Electromagnetic Interference Testing in Power Plants," (April 1996). These engineering practices provide a well-established, systematic approach for ensuring electromagnetic compatibility (EMC) and surge withstand capability (SWC).

Introduction

The typical environment in a nuclear power plant includes many sources of electromagnetic interference (EMI), radio-frequency interference (RFI), and power surges, e.g., hand-held two-way radios, arc welders, switching of large inductive loads, high fault currents, and high-energy fast transients associated with switching at the generator or transmission voltage levels. The increasing use of advanced analog- and microprocessor-based instrumentation and control (I&C) systems in reactor protection and other safety-related plant systems has introduced concerns with respect to the susceptibility of this equipment to EMI/RFI and power surges, as well as the creation of additional noise sources.

Digital technology is constantly evolving, and manufacturers of digital systems are incorporating increasingly higher clock frequencies and lower logic level voltages into their designs. However, these performance advancements may have an adverse impact on the operation of digital systems with respect to EMI/RFI and power surges because of the increased likelihood of extraneous noise being misinterpreted as legitimate logic signals and of surge potentials causing equipment/parts damage. With recent advances in analog electronics, many of the functions presently being performed by several analog circuit boards could be combined into a single analog circuit board operating at reduced voltage levels, thereby making analog circuitry more susceptible to EMI/RFI and power surges, as well. Hence, operational and functional guidance related to safety in the nuclear power plant environment is necessary to address the possibility of upsets and malfunctions in I&C systems caused by EMI/RFI and power surges.

Regulatory Guide (RG) 1.180, *Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems*, was issued in January 2000 to address EMI/RFI and power surge issues for safety-related digital I&C systems in nuclear power plants. The technical basis behind the practices in RG-1.180 is given in NUREG/CR-5941, *Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems*, and NUREG/CR-6431, *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C Systems in Nuclear Power Plants*. Prior to the issuance of RG-1.180, NRC staff had accepted the Electric Power Research Institute (EPRI) topical report TR-102323, *Guidelines for Electromagnetic Interference Testing in Power Plants*, in a Safety Evaluation Report (SER) by letter dated April 17, 1996 as one method for addressing electromagnetic compatibility (EMC) issues in safety-related digital I&C systems. RG-1.180 complements the position set forth in the SER by improving the technical basis for evaluating EMI/RFI immunity and power surge withstand capability (SWC).

RG-1.180 and the EPRI TR-102323 SER adhere to the same overall approach and are generally in agreement. Each recommends EMI/RFI-limiting practices based on IEEE Std 1050, endorses emissions and susceptibility test criteria and test methods to evaluate safety-related I&C systems, and identifies appropriate operating envelopes for equipment and systems intended for selected locations in nuclear power plants. Each document presents acceptable means for demonstrating EMC and they are consistent in their respective approaches. The licensee has the freedom to choose the method best suited to the situation.

Design and Installation Practices

RG-1.180 endorses the design and installation practices described in IEEE Std 1050-1996, *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, as suitable for limiting the generation and effects of EMI/RFI and power surges. IEEE Std 1050-1996 was developed primarily to provide guidance on the design and installation of grounding systems for I&C equipment specific to power generating stations. Further purposes of the standard are to achieve both a suitable level of protection for personnel and equipment, and suitable electrical noise immunity for signal ground references in power generating stations. IEEE Std 1050-1996 addresses grounding and noise-minimization techniques for I&C systems and recommends practices for the treatment of both analog and digital systems. The standard specifically addresses the grounding and shielding of electronic circuits on the basis of minimizing emissions and their susceptibility to EMI/RFI and power surges. The SER accepts the 1989 version of IEEE Std 1050. There are minor differences between the 1989 and 1996 versions of IEEE Std 1050, with some technical ambiguities from the 1989 version being cleared up in the 1996 version.

One exception was taken in RG-1.180 to the design and installation practices in IEEE Std 1050-1996. Section 4.3.7.4, "Radiative Coupling," of the standard maintains that the "field strength" of propagating electromagnetic waves is inversely proportional to the square of the distance from the source of radiation. This statement needs to be reevaluated because radiative coupling is a far-field effect. A distance, r, greater than the wavelength divided by 2π ($r > \lambda/2\pi$) from the source of radiation is considered to be far field, which is the region where the wave impedance is equal to the characteristic impedance of the medium. Both the electric and magnetic "field strengths" fall off as $1/r$ in the far field, not as $1/r^2$. This concept is not to be confused with the propagation of electromagnetic waves in the near field ($r < \lambda/2\pi$) where the wave impedance is determined by the characteristics of the source and the distance from the source. In the near field, if the source impedance is high ($>377\Omega$), the electric and magnetic "field strengths" attenuate at rates of $1/r^3$ and $1/r^2$, respectively. If the source impedance is low ($<377\Omega$), the rates of attenuation are reversed: the electric "field strength" will fall off at a rate of l/r^2 and the magnetic "field strength" at a rate of $1/r^3$. The significance of this exception lies in the appropriate application of the design and installation practices in IEEE Std 1050-1996. For example, the strength of magnetic fields

from a low-impedance source is typically substantially much reduced within a short distance and simply moving equipment away from strong sources of magnetic fields can prevent interference problems.

IEEE Std 1050-1996 references other standards that contain complementary and supplementary information. In particular, IEEE Std 518-1982, *IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources*, and IEEE Std 665-1995, *IEEE Guide for Generating Station Grounding*, are referenced frequently. The portions of IEEE Std 518-1982 and IEEE Std 665-1995 referenced in IEEE Std 1050-1996 are endorsed by RG-1.180 and are to be used in a manner consistent with the practices in IEEE Std 1050-1996.

EMI/RFI Testing Practices

To verify the adequacy of safety-related I&C systems and equipment design, both RG-1.180 and the SER endorse applicable EMI/RFI test criteria in the U.S. Department of Defense's Military Standard (MIL-STD) 461, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*. Also endorsed are the associated test methods in MIL-STD 462, *Measurement of Electromagnetic Interference Characteristics*. EMI/RFI test criteria from both MIL-STD 461C and 461D, as well as their respective MIL-STD 462 and 462D test methods, are cited in RG-1.180 and the SER. The bases behind the selections are detailed in NUREG/CR-5941 for RG-1.180 and in EPRI TR-102323 for the SER. MIL-STDs 461 and 462 were developed as measures to ensure EMC. Applications of the MIL-STD test criteria and test methods are tailored for the intended function of the equipment and the characteristic environment (i.e., which tests and what levels are applied depend on the function to be performed and the location of operation).

The MIL-STD 461D test criteria acceptable to the U.S. NRC in RG-1.180 and the SER for susceptibility and emissions testing on safety-related I&C systems intended for nuclear power plants are listed in Table 1. These criteria cover conducted and radiated interference (emissions and susceptibility), exposure to electric and magnetic fields, and noise coupling through power and control leads. The criteria do not cover conducted interference on interconnecting signal lines because the MIL-STD test methods do not explicitly address signal line conducted susceptibility. Research covering this area is presently ongoing. MIL-STD 461D provided the latest revision of the test criteria at the time that RG-1.180 and the SER were issued, thus it represents current practice. However, guidance on the MIL-STD 461C counterparts to the MIL-STD 461D test criteria is also given to avoid placing an undue burden on the nuclear power industry by limiting the available test resources to those test laboratories with just the MIL-STD 462D test capability.

Table 1 MIL-STD 461D Test Criteria.

Criterion	Description
CE101	Conducted emissions, power leads, 30 Hz to 10 kHz
CE102	Conducted emissions, power leads, 10 kHz to 10 MHz
CS101	Conducted susceptibility, power leads, 30 Hz to 50 kHz
CS114	Conducted susceptibility, bulk cable injection, 10 kHz to 400 MHz
RE101	Radiated emissions, magnetic field, 30 Hz to 100 kHz
RE102	Radiated emissions, electric field, 10 kHz to 1 GHz
RS101	Radiated susceptibility, magnetic field, 30 Hz to 100 kHz
RS103	Radiated susceptibility, electric field, 10 kHz to 1 GHz

C = conducted, E = emissions, R = radiated, and S = susceptibility.

RG-1.180 provides two acceptable suites of EMI/RFI emissions and susceptibility criteria. It is intended that either set of test criteria be applied in its entirety, without selective application of individual criteria (i.e., no mixing and matching of test criteria). The reason for this is the avoidance of lapses in frequency coverage of the criteria, discontinuities in test phenomena coverage, miscalculations in test unit conversions, and unreasonable comparisons of operating envelope levels. The SER does allow mixing and matching, but exercising good engineering judgement in the performance of the EMI/RFI tests is recommended when doing so.

The MIL-STD 461 test criteria have associated operating envelopes that serve to establish test levels. The operating envelopes that are acceptable to the U.S. NRC are not given herein, but can be found in RG-1.180 and the SER. The operating envelopes in both documents are similar, with only minor differences. The detailed technical basis for the operating envelopes in RG-1.180 is presented in NUREG/CR-6431. The technical basis for the RG-1.180 operating envelopes begins with the MIL-STD envelopes corresponding to the electromagnetic environment for military ground facilities, which were judged to be comparable to that of nuclear power plants based on general layout and equipment type considerations. Plant emissions data measured at 14 nuclear units were used to confirm the adequacy of the operating envelopes. From the MIL-STD starting point, susceptibility envelopes were adjusted to account for the plant emissions measurement data collected at eight nuclear units in 1995 and reported in NUREG/CR-6436, *Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants*. In addition, emissions data collected at six nuclear units during a 1994 EPRI study were used as a basis for adjusting the susceptibility envelopes. Figure 1 illustrates the comparison of the power plant data and the operating envelope for radiated electric fields (RS103), while Figure 2 illustrates a similar comparison for radiated magnetic fields (RS101). The basis for adjustments to the equipment emissions envelopes included consideration of the primary intent of the MIL-STD envelopes and maintaining some margin with the susceptibility envelopes. Finally, when changes to the operating envelopes from the MIL-STD origin were motivated by technical considerations, consistency among the envelopes for comparable test criteria was promoted and commercial emissions limits for industrial

environments were factored into adjustments of the envelopes. The basis for the operating envelopes endorsed by the SER is detailed in EPRI TR-102323.

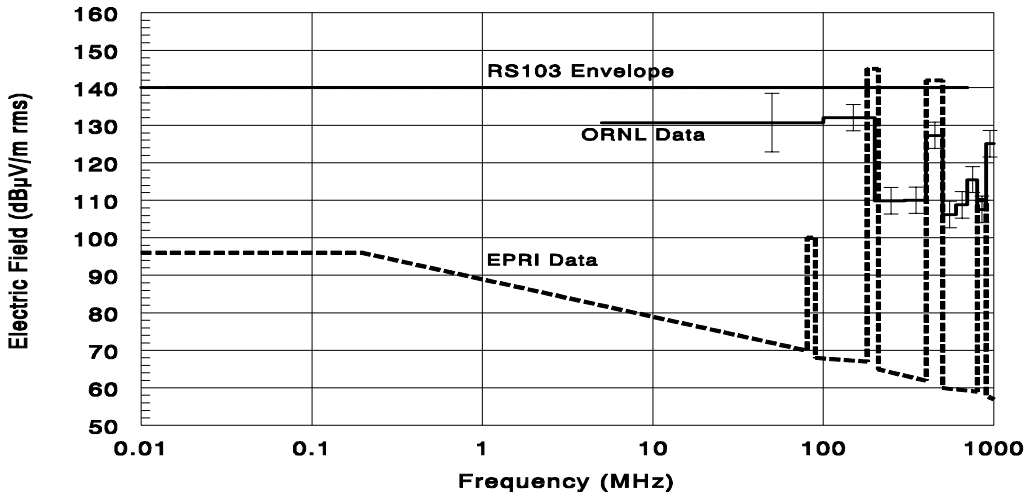


Figure 1 Plant Data vs Radiated Electric Fields Envelope

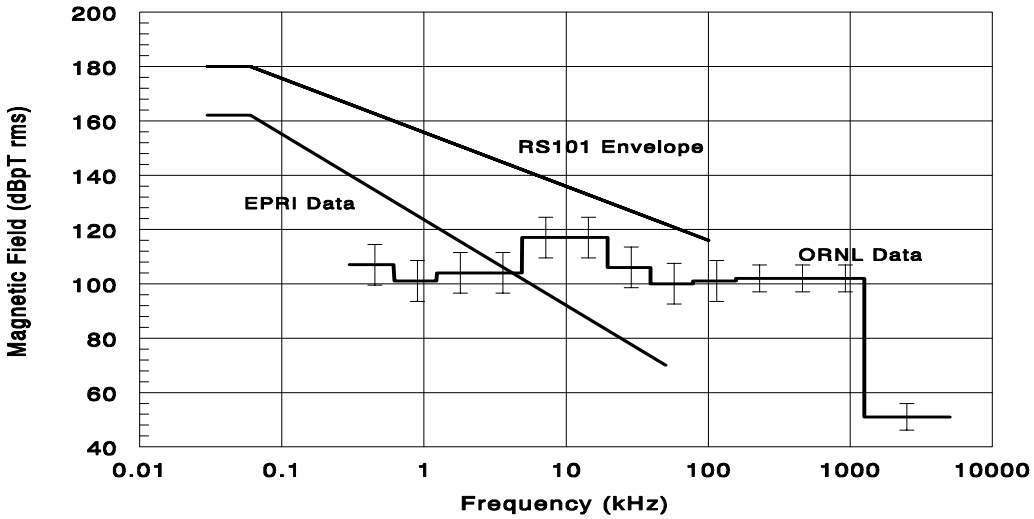


Figure 2: Plant Data vs Radiated Magnetic Fields Envelope

Surge Withstand Capability (SWC) Testing Practices

RG-1.180 endorses the SWC test criteria recommended in IEEE Std C62.41-1991, *IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits*, and the associated test methods recommended in IEEE Std C62.45-1992, *IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits*. IEEE Std C62.41-1991 provides guidance for the selection of voltage and current surge test criteria for evaluating the SWC of equipment connected to low-voltage ac power circuits. The standard defines a set of surge test waveforms that includes lightning-induced transients, oscillatory ring waves, and electrically fast transients (EFT) caused by load switching. The recommended test waveforms have manageable dimensions and represent a baseline surge environment. IEEE Std C62.45-1992 provides guidance on the test methods and equipment to be employed when performing the surge tests. The SER endorses the comparable surge testing practices in Parts 4 and 5 of the International Electrotechnical Commission (IEC) Standard 801, *Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment*. IEC 801 has been superseded by IEC 61000-4, *Electromagnetic Compatibility: Part 4, Testing and Measurement Techniques.* Typical environmental conditions for surges in a nuclear power plant can be represented by the waveforms given in Table 2.

Table 2 Representative Power Surge Waveforms.

Parameter	Ring Wave	Combination Wave		EFT
Waveform	Open-circuit voltage	Open-circuit voltage	Short-circuit current	Pulses in 15-ms bursts
Rise time	0.5 µs	1.2 µs	8 µs	5 ns
Duration	100 kHz ringing	50 µs	20 µs	50 ns
Peak value	3 kV	3 kV	1.5 kA	3 kV

Withstand levels that are acceptable to the U.S. NRC are given in RG-1.180 for each surge waveform. IEEE Std C62.41-1991 describes location categories and exposure levels that define applicable amplitudes for the surge waveforms that should provide an appropriate degree of SWC. Location categories depend on the proximity of equipment to the service entrance and the associated line impedance. Exposure levels relate to the rate of surge occurrence versus the voltage level (e.g., surge crest) to which equipment is exposed. Withstand levels are presented in NUREG/CR-6431 and based on *Category B* locations and *Low to Medium Exposure* levels. *Category B* covers feeders and short branch circuits less than 10 meters from the service entrance. *Low to Medium Exposure* levels encompass systems in areas known for little load or capacitor switching and low-power surge activity to areas known for significant switching transients or medium- to high-power surge activity. Comparable IEC 801 SWC levels, also acceptable to the U.S. NRC, are given in the SER.

Regulatory Positions

Table 3 lists the specific regulatory positions in RG-1.180 that have been set forth by the U.S. NRC. This guidance complements the position set forth in the SER by improving the technical basis for evaluating EMI/RFI and power surges. The RG-1.180 guidance is applicable for all new safety-related systems or modifications to existing safety-related systems that include analog, digital, or hybrid (i.e., combined analog and digital electronics) equipment. While nonsafety-related systems are not part of the

guidance, control of EMI/RFI from these systems is deemed necessary to ensure that safety-related I&C systems continue to perform properly.

The electromagnetic conditions at the point of installation for safety-related I&C systems should be assessed to identify EMI/RFI sources that may generate local interference. The EMI/RFI sources could include mobile, portable, and fixed equipment. Steps should be taken during installation to ensure that systems are not exposed to EMI/RFI levels from sources that are greater than 8 dB below the operating envelopes. When feasible, the emissions from nonsafety-related systems should be held to the same levels as safety-related systems.

The endorsed operating envelopes are acceptable for locations where safety-related I&C systems either are or are likely to be installed and include control rooms, remote shutdown panels, cable spreading rooms, equipment rooms, auxiliary instrument rooms, relay rooms, and other areas (e.g., the turbine deck) where safety-related I&C system installations are planned. To ensure that the operating envelopes are being used properly, equipment should be tested in the same physical configuration as that specified for its actual installation in the plant. In addition, the physical configuration of the safety-related I&C system should be maintained and all changes in the configuration controlled. The design specifications that should be controlled include cable separations, shielding techniques, enclosure integrity, apertures, gasketing, grounding techniques, and EMI/RFI filters. Also, the endorsed test methods for evaluating electromagnetic emissions, EMI/RFI susceptibility, and power SWC are intended to be applied to the safety-related I&C equipment in test facilities or laboratories prior to installation.

Any modifications to the electromagnetic operating envelopes (e.g., lower site-specific envelopes) should be based on technical evidence comparable to that presented in NUREG/CR-6431. Relaxation in the operating envelopes should be based on actual measurement data collected in accordance with IEEE Std 473-1985, *IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 GHz)*.

Exclusion zones should be established through administrative controls to prohibit the activation of mobile and portable emitters in areas where safety-related I&C systems have been installed. An exclusion zone is defined as the minimum distance permitted between the point of installation and where portable emitters are allowed to be activated. The size of the exclusion zones should be site-specific and depend on the effective radiated power and antenna gain of the portable emitters. The size of exclusion zones should also depend on the allowable emission levels designated for the installation area. Additional guidance on exclusion zones is provided in NUREG/CR-6431.

Table 3 Specific Regulatory Positions for EMC Guidance.

Regulatory Position	EMC Issue	Standards	Comments
2	EMI/RFI limiting practices	IEEE Std 1050-1996	Full standard endorsed with one exception taken.
		IEEE Std 518-1982 IEEE Std 665-1995	Endorsed as referenced by IEEE Std 1050-1996.
3, 4, 5	EMI/RFI emissions and immunity testing	MIL-STD 461D MIL-STD 462D	Selected MIL-STD 461 test criteria endorsed along with MIL-STD 462 test methods.
		MIL-STD 461C MIL-STD 462	Alternative test suites.
			Operating envelopes are included in Reg. Pos. 4 and 5.
6	Surge withstand capability testing	IEEE Std C62.41-1991 IEEE Std C62.45-1992	Selected IEEE Std C62.41 surge test waveforms endorsed with IEEE Std C62.45 test methods.
			Withstand levels for nuclear power plants are included in Reg. Pos. 6.

Conclusions

The issuance of RG-1.180 and the EPRI TR-102323 SER by U.S. NRC has resulted in clear guidance on the practices necessary for a comprehensive EMC program. Both documents represent guidance that is acceptable to U.S. NRC. These practices are presently being applied to analog, digital, and hybrid (i.e., combined analog and digital electronics) safety-related I&C equipment. The concurrence within the nuclear industry is that approval cycles have been significantly reduced, EMC awareness has been heightened, and the number of EMC-related occurrences has been reduced.

Adherence to the guidance in RG-1.180 and the SER for safety-related I&C systems has contributed to the assurance that structures, systems, and components important to safety are compatible with the environmental conditions associated with nuclear power plants. Consensus standards were endorsed that cover design, installation, EMI/RFI, and SWC practices. Test methods have been provided that contribute to a well established, systematic approach for ensuring EMC. Operating envelopes that have been confirmed with actual measurement data in nuclear power plants have been recommended.

References

EPRI TR-102323, *Guidelines for Electromagnetic Interference Testing in Power Plants*, Electric Power Research Institute, April 1996.

Ewing, P.D., Korsah, K., *Technical Basis for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related I&C Systems*, NUREG/CR-5941, Oak Ridge National Laboratory, April 1994.

Ewing, P.D., Wood, R.T., *Recommended Electromagnetic Operating Envelopes for Safety-Related I&C Systems in Nuclear Power Plants*, NUREG/CR-6431, Oak Ridge National Laboratory, January 2000.

IEC 801, *Part 4, Fast Electrical Transient/Burst Requirements*, International Electrotechnical Commission, Technical Committee No. 65, 1988.

IEC 801, *Part 5, Surge Immunity Requirements*, International Electrotechnical Commission, Technical Committee No. 65, 1990.

IEC 61000-4-4, *Part 4, Electrical Fast Transient/Burst Immunity Test*, International Electrotechnical Commission, 1995.

IEC 61000-4-5, *Part 5, Surge Immunity Test*, International Electrotechnical Commission, 1995.

IEEE Std 473-1985 (Reaff 1991), *IEEE Recommended Practice for an Electromagnetic Site Survey (10 kHz to 10 Ghz)*, Institute of Electrical and Electronics Engineers.

IEEE Std 518-1982 (Reaff 1990), *IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources*, Institute of Electrical and Electronics Engineers.

IEEE Std 665-1995, *IEEE Guide for Generating Station Grounding*, Institute of Electrical and Electronics Engineers.

IEEE Std 1050-1996, *IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations*, Institute of Electrical and Electronics Engineers.

IEEE Std C62.41-1991 (Reaff 1995), *IEEE Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits*, Institute of Electrical and Electronics Engineers.

IEEE Std C62.45-1992, *IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits*, Institute of Electrical and Electronics Engineers.

Kercel, S.W., Moore, M.R., *Survey of Ambient Electromagnetic and Radio-Frequency Interference Levels in Nuclear Power Plants*, NUREG/CR-6436, Oak Ridge National Laboratory, November 1996.

MIL-STD 461C, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*, U.S. Department of Defense, August 4, 1986.

MIL-STD 461D, *Electromagnetic Emission and Susceptibility Requirements for the Control of Electromagnetic Interference*, U.S. Department of Defense, January 11, 1993.

MIL-STD 462, *Measurement of Electromagnetic Interference Characteristics*, U.S. Department of Defense, July 31, 1967.

MIL-STD 462D, *Measurement of Electromagnetic Interference Characteristics*, U.S. Department of Defense, January 11, 1993.

Regulatory Guide 1.180, *Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems*, U.S. Nuclear Regulatory Commission, January 2000.

Pre-Qualification of Digital Platform - U.S. N RC Regulatory Review of The Common Q Platform

Keith Mortensen
Matthew Chiramal
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Washington DC 20555
E-mail address: WKM@NRC.GOV, MXC@NRC.GOV

ABSTRACT

CE Nuclear Power (CENP)(formerly ABB Nuclear Automation, presently Westinghouse Nuclear Automation) submitted Topical Report CEN PD-396-P, Rev.1,"Common Qualified Platform" to the NRC for review. The intent of the submittal is to obtain NRC acceptance of the pre-qualification of the CENP Common Q platform. The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. The Common Q platform was developed by CENP from the standard AC 160 computer system developed by ABB Automation Products, GmbH (ABB Products) of Europe. The Common Q platform is to be loaded with plant-specific application software to implement various nuclear plant safety system applications.

The basis of pre-qualification is compliance with the NRC-approved EPRI Topical report TR-106439, "Guideline o n Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications." [A copy of this document may be obtained from the NRC Public Document Room http://www.nrc.gov/NRC/PDR/pdr1.htm]. The pre-qualified Common Q would provide utilities and other users with a pre-qualified platform that could be used in future applications for upgrade or replacement of plant safety instrumentation and control (I&C) systems. The purpose of the NRC review is to determine whether the design and proposed use of equipment and other technical requirements provide reasonable assurance that the applicant or licensee will comply with the applicable regulatory requirements, and that public health and safety will be protected. The review, audit, and inspection n activities by the NRC staff are not intended to completely evaluate all aspects of the design and implementation of the digital I&C system. The review scope is sufficient to allow the reviewer to reach the conclusion of reasonable assurance described above.

To ensure that the CENP Common Q platform will perform its safety function as designed, the NRC staff reviewed the basic operation of the system, life cycle process and documentation associated with the Common Q hardware and software design implementation, the commercial grade dedication reports for the components and previously-developed software (PDS) for the ABB AC160 PLC modules and for the flat-panel display system (FPDS) and other non-AC100 support components, the programming specifications for the future development of application software, and generic design information far the systems described in the four appendices to the topical report. These activities involved the review of design implementation documentation, technical meetings with the vendor; and audits at the vendor's facilities.

The NRC staff used the guidance in NUREG 0800, the Standard Review Plan (SRP), Chapter 7, Rev.4 [http://www.nrc.gov/NRC/NUREGS/SR08OO/CH7/index.htm], in conducting the review. Based on this guidance, the NRC staff identified additional information needed by the staff to perform the safety evaluation of the Common Q platform. The staff, in its review of the CENP qualification program, focused on how the safety requirements are met according to the guidance in SRP Chapter 7, including the supporting Branch Technical Positions (BTPs) and referenced US Regulatory Guides, and in EPRI Topical Report TR-106439. The staff has completed the review of the qualification of nearly all of the AC160 PLC system components and the staff's evaluation of the completed activities has been documented in the safety

evaluation report (SER) issued on August 11, 2000. CENP has remaining qualification testing of some AC160 PLC modules and all of the qualification testing for the non-AC160 components. This testing is scheduled for August2001. The SER and this paper reflects the status of the review as completed. The SER also identifies generic open items and plant-specific action items.

INTRODUCTION

In March 1999,CEN P submitted topical report CENPD-396-P, Rev. 00, "Common Qualified Platform" and the associated software program manual, "Software Program Manual for Common Q Systems" (SPM). Later in1999, the following four appendices to the topical report were submitted

Appendix 1, "Common Qualified Platform Post-Accident Monitoring System"
Appendix 2, "Common Qualified Platform Core Protection Calculator System"
Appendix 3, "Common Qualified Platform Digital Plant Protection System"
Appendix 4. "Common Qualified Platform Integrated Solution"

In June 2000, CENP submitted Revision 1 of both the proprietary and non-proprietary versions of the topical report and the associated software program manual and the four appendices that considered the comments provided by the NR C staff o n the initial set of documents.

Revision 1 describes a nuclear safety-related instrumentation and controls (I&C) platform developed by CENP. CENP is proposing one common platform with a modular structure in which various components can be incorporated and applied to nuclear safety-related applications, including component replacements and complete system upgrades. The appendices describe design approaches for implementing the generic platform into I&C systems at nuclear power plants and provide additional information to support the review of the generic design details for the Common Q platform.

SYSTEM DESCRIPTION

The Common Q platform developed by CENP consists primarily of a set of digital hardware and software components from the standard AC 160 system, a product developed by ABB Automation Products, GmbH (ABB Products), in Europe The standard AC160 is a system of PLC products currently used for control systems in industries unrelated to nuclear power. To complete the Common Q platform, CENP combines the FPDS and other components with its set of AC160 system components The FPDS consists of the flat-panel display module, a microprocessor-based single-board computer module, and communication interfaces for communication with the AC160 and other components and systems. The display module is a color thin-film transistor flat-panel display readable under high ambient light. The display module provides a graphic-al user interface (GUI) with pull-down menus and touch-screen capability. The FPDS is the human-system interface system (HSIS) for the associated nuclear plant system.

For nuclear power plant applications, this platform consisting of a let of commercial-grade hardware and previously developed software components.is being dedicated and qualified and is to be loaded with plant-specific application software to implement various nuclear plant safety system -applications.

The hardware components of the platform are:

- Advant Controller 160(AC160) with P M646 or PM645C processor modules
- S600 input and output (S6001/O) modules
- Bus communication interface (C1631) modules

- Power supply modules
- Watchdog timer module
- Communication systems
- Flat-panel display system(FP D S)

The AC 160 software, residing on flash programmable read-only memory (PROM) in the processor module, consists of a real-time operating system, task scheduler, diagnostic functions, communication interfaces, and plant specific application programs. The application program will be created using the Asea Brown Boveri (ABB) Master Programming Language (AMPL) Control Configuration (ACC) software development environment that includes a function block library for creating specific logic for the application. The Common Q platform uses three types of data communication systems: the AF100 (Advant Field bus 100) network communication system; the high-speed link (HSL) serial communication system; and external communication systems such as Ethernet. The AF100is used for transferring process data and messages within the channel (e.g., between AC160s and the FPDS). The process data are used for monitoring and controlling a process, and the messages are used for program loading and for diagnostic purposes. The HSL is used to transmit data to other channels in a multichannel system. Fiber-optic modems and cables maintain isolation of redundant safety channels. The external communication system is used to transfer calculate data from the Common Q system to the external systems, such as the plant non-safety control system. Previously-developed software (PDS) embodies the .software that was developed to satisfy a general market need before being incorporated into the Common Q platform. PDS includes commercial software that is integral to the delivered system and software that supports the delivered system. Some PDS is used to develop the application software to implement the safety functions in the Common Q upgrades. The PDS for the Common Q platform is procured from two vendors: the vendor of the AC160 PLC system and the vendor of the FPDS operating system.

The PDS being used in the Common Q are as follows:

Operating systems
Compilers, linkers, and loaders
Database software
Communication drivers
Human-machine interface software
Display-building software

Some of the PDS resides in Common Q memory when the Common Q is performing its safety functions (i.e., at runtime). Other PDS used as development or support tools does not reside in Common Q memory at run time. That which resides in memory at run time is subjected to higher regulatory requirements. The run-time P DS for the Common Q platform include the real time operating systems, task schedulers, diagnostic functions, and communication functions, all of which reside in the PLC’s PROM. The AC160 operating system provides for the deterministic behavior of the Common Q platform.

CENP's S PM specifies the procedures for implementing a structured software life cycle process for the plant-specific software and provides guidance for configuration management of commercial-grade hardware and PDS. Since the application software has not yet been developed, the staff's evaluation does not include the review of the outputs of the life cycle process, but is limited to the evaluation of the specified process. The same is true of the FP DS software. Licensees using the Common Q platform for plant-specific applications will be required to implement the application software in accordance with CENP's SPM. The application program and its control modules in a n AC160 will coexist in PROM with the other system software programs, such as the diagnostic routines and communication interfaces.

QUALIFICATION

In evaluating the Common Q platform, the staff made several site visits to the CENP offices and inspected CENP procedures that are referenced in the topical report and audited reports of commercial-grade dedication activities. During the site visits, the staff inspected CENP procedures that are referenced in the topical report and audited reports of commercial-grade dedication activities.

CENP provided copies of selected reports of commercial-grade dedication activities for more detailed review by the staff at NRC headquarters. Based on these activities the staff requested that additional documents dealing with commercial-grade dedication activities be placed on the docket. In June 2000, CENP submitted the following six proprietary reports:

"Seismic Qualification Test Report for Common Q Applications"
"Environmental Test Report for Module Equipment Qualification for Common Q Applications"
"EMI Qualification Test Report for Module Equipment Qualification for Common Q Applications"
"Commercial Grade Dedication Report for the QNX Operating System for Common Q Applications"
"Generic Operating History Evaluation Report on Previously-Developed Software in ABB AC160, U0 Modules and Tool Software"
"Design and Life Cycle Evaluation Report on Previously-Developed Software in A BB AC160.U0 Modules and Tool Software"

Based on its review of these documentation and interaction with CENP staff, the NRC staff identified items that needed additional activities and related documents to complete its review. CENP committed to provide the needed details. The safety evaluation by the NRC staff issued on August 16, 2001, discusses these open items: Common Q input/output modules to be re-designed to meet specified performance requirements; complete dedication of power supplies: complete design and dedication of watchdog timer; complete electro-magnetic compatibility and environmental qualification activities of some hardware items; provide additional information on software module testing, independence aspects of communication buses, and human-machine interface design details

Based on its review of CENP's dedication of the commercial-grade AC 160 PLC system and FPDS GUI, the staff concluded that CENP had demonstrated in accordance with the guidance in EPRITR-106439 that the Common Q platform is acceptable as equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program.
The staff reviewed CENPs SPM, which specifies the procedures for implementing a software life cycle process for the yet-to-be-developed application software and provides guidance for configuration

management of commercial-grade hardware and previously developed software, against the guidance in SRP Branch Technical Position-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems." Based on the review of the SPM and the topical report and appendices, the staff concluded that the specified procedures for software development and software configuration management will provide a quality software life cycle process, and that these plans commit to documentation of life cycle activities that will permit the staff or others to evaluate the quality of the design features upon which the safety determination will be based. The staff, therefore, concludes that the software development plan for new plant-specific safety system application software for the Common Q platform safety systems meets the guidance of US Regulatory Guide 1.152 (http://www.nrc.gov/NRC/RG/01/01-152rl.html], and that the special characteristics of computer systems have been adequately addressed.
The design applications discussed in the four appendices of the topical report are considered by the staff as models that can be used in designing the plant-specific applications.

PLANT-SPECIFIC APPLICATION

The staff has .reviewed the commercial-grade dedication of the Common Q platform and has determined that the Common Q platform has the required quality upon the satisfactory resolution of the outstanding open items. The quality of the plant-specific Common Q system is dependent on the licensee's proper implementation of the CENP software program manual and the resolution of plant-specific items. Because this topical report is for a generic platform, licensees referencing the topical report must describe in detail how they propose to use the Common Q design in plant-specific applications and must address all plant-specific interface item s. including the following plant-specific action items:

assess and verify the compatibility of Common Q, I/O modules to plant l/O requirements HSIS review and implementation
verification of environmental qualification compatibility of generic Common Q to actual plant conditions
design implementation of plant-specific application software per the requirements of CENP's SPM
verification of plant-specific requirements of l&C systems such as accuracy and response times, functions, control of access to the system, failure modes analysis, and technical specification requirements.

CONCLUSION

CENP submitted the topical report to obtain NRC acceptance of the pre-qualification of the CENP Common Q platform. The Common Q platform is a computer system consisting of a set of commercial-grade hardware and previously developed software components dedicated and qualified for use in nuclear power plants. Based on the review of the topical report and other documents, and on the audits conducted and meetings with CENP, the NRC staff concludes that for the systems and component reviewed, the design of the Common Q platform meets the relevant NRC regulatory requirements and is acceptable for safety-related instrumentation and control (I&C) applications in nuclear power plants, subject to the satisfactory resolution of the generic and plant-specific open items.

Survey and Evaluation of Digital I&C Licensing Experiences

Swu Yih[1], Chin-Feng Fan[2] Chan-Fu Chuang[3]

[1] Institute of Nuclear Energy Research, PO Box 3-11, Lung Tang, Taiwan, ROC.
Tel: +3-4711400-6335, e-mail: syih@iner.gov.tw

[2] Dept. of Computer Science, Yuan-Ze University, Chung-Li, Taiwan, ROC
Tel:+3-4638800-360, e-mail: csfanc@saturn.yzu.edu.tw

[3] Nuclear Regulation Division, Atomic Energy Council, Taipei, Taiwan, ROC
Tel:+2-23634180-307, e-mail: chung@aec.gov.tw

Summary

Digital I&C licensing experiences showed significant performance variance among different cases, i.e., some were smooth and efficient while others were lengthy and problematic. In order to explain the causes of such variance and to develop more efficient licensing techniques, we conducted an in-depth survey and analysis of these licensing experiences. By viewing the licensing process as an evidence- confidence conversion process, a Licensing Performance Model has been developed and used as a framework to analyze the behavior characteristics of licensing activities. The model identified major factors and functions that dominate the performance of licensing process, among which the proficiency maturity and evidence profiles are the most critical factors that affect the licensing performance. During the evaluation step we were able to apply this model to explain why some previous licensing cases were successful and some were troublesome. This successful application shows the validity of the proposed model. Finally, we presented insights into the nature of licensing process gained form this study and recommended approaches for improving licensing performance .

Introduction and Motivations

This paper presents a survey and evaluation of efficiency-related issues of digital I&C licensing cases performed in the recent years. The process of digital I&C licensing in nuclear industry starts when the utility presents an I&C design and its associated quality evidence to the regulator; the regulator will then determine whether the presented I&C system meets mandatory safety requirements that prescribed in pre-issued regulations. Thus the scope of our concern covers both the applicant's preparation effort and the regulator's review effort. An inefficient licensing process may cause unnecessary delay of the commercial operation of nuclear plants. Due to the enormous investment of constructing a nuclear power plant, any delay implies huge social and economical loss. Therefore, in the nuclear industry, every stakeholder is working hard to pursue a smooth and efficient licensing process. The licensing practice in general is quite effective and smooth for most case; however, experiences showed that some digital I&C licensing cases were frustrating for each party involved. It is even not too exaggerated to claim that the licensing practice has hindered the progress of introducing digital I&C techniques to nuclear power plants. This makes the progress of I&C computerization process far behind that of the petrochemical industry, which does not have mandatory licensing requirements. Various efforts have been proposed to resolve this problem, such as developing better regulations, powerful license review tools, etc. We propose another approach to alleviating the I&C licensing problem by extracting useful lessons learned from previous experiences. The rationale is that since some licensing cases are successful and some are problematic, thus if we could conduct a comparative analysis of these cases, focusing on analyzing the reasons of their success and failure. Thus, we may identify the critical *efficiency shaping factors* affecting the licensing process efficiency, and then by managing these critical factors properly, we may be able to avoid repeating the same problems that were encountered by previous troublesome cases in the future.

Our strategy is to develop a licensing performance *evaluation framework* based on the information collected from previous digital I&C licensing experiences. This framework is then used to identify critical factors and their influence on licensing efficiency. The following part of this paper presents preliminary results of our study. Our paper consists of 5 sections, First, a brief survey of five digital I&C licensing cases will be presented. The survey focuses on licensing practice and the future trend is also revealed from these cases. We then describe an evaluation framework, which is used to investigate the cause-consequence relations among licensing efficiency shaping factors. The framework thus can be used to explain why some licensing case succeeded and others failed. Recommendations that may improve I&C licensing efficiency will then be presented, followed by conclusion and future work.

Survey of Digital I&C Licensing Experiences

Licensing process can be divided into two distinct sub-processes: evidence preparation process and evidence review process. The following discussion is presented in terms of these two categories.

Chooz B Nuclear Power Plant (Peyrouton,1993)

P20 was the major digital control system selected by EdF for its Chooz B nuclear power plant. It was designed by Cegelec Company, which is a major French I&C provider with abundant relevant I&C experiences. The system is a distributed microprocessor-based control system that resides on a redundant LAN network. A 32-bit Transputer (Guesnier,1989) is chosen as its primary microprocessor. Since Transputer is designed for parallel applications, this system basically is running as a parallel processing system.

This project was started in 1986. In 1990, the project was delayed for 2 years; it was finally given up by EdF because more delay (estimated 4-6 years) was expected. This failed project cost EdF 300 million Francs (MacLachlan, 1994a) and 4 years schedule delay (delay already made by P20 and delay by the new design). The major reason for the failure is that the software has become too complex to be verified effectively and confidently.

Contronic E is chosen by Edf to replace the failed P20 system (Appell,1992). The problem of software verification is alleviated because Contronic E has many years field experience in chemical and petrol plants. However, French regulatory agency still did not feel confident in this new design (MacLachlan,1994b), and all the safety issues were finally settled after a long negotiation between two sides.

Darlington Nuclear Power Plant (Craigen, 1994)

Darlington nuclear plant is a CANDU type nuclear power plant developed by AECL. CANDU is among the first nuclear plants to use computers to perform safety functions. The digital technique has evolved from Digital Comparators (PDCS) used in the CANDU 600 (early 1980s), to microprocessor based trip meter (Pickering Nuclear Generating Station), to the fully computerized shutdown system of Darlington SDS1 and SDS2. The latest design made improvements in increasing the functionality to support more comprehensive self testing, surveillance, diagnosis, and channeled displays to the operators.

In 1982, Ontario Hydro, with the concurrence of AECB, had decided to fully implement the decision-making logic of the shutdown system on computers. The development work began in early 1983. In early 1987, an AECB review uncovered discrepancies and raised doubts as to whether the software implemented

the requirements correctly. In mid 1987, AECB hired software safety expert Dr. David Parnas to help investigation and to recommend how to improve the software. Dr. Parnas identified the areas of concerns and proposed a formal mathematical inspection in Jan. 1989 to break the licensing impasse. The complete software requirements specifications have to be rewritten to provide the required and correct format documents for inspection. This whole process completed in Feb. 1990 when AECB finally issued a license for full power operation.

When AECB issued the license on Feb. 1990, AECB also made a statement, requesting that the software would have to be *redesigned* for long-term use (Craigen ,1994). As a consequence, Ontario Hydro, AECL, and AECB are designing a new set of software engineering standards for guiding software development (AECL,1995). The development and regulatory status for the redesign activities is reported in (Chun,2000).

Sizewell B Nuclear Power Plant (NEI,1993)

Sizewell B plant adopts a two level strategy to its reactor system, i.e., a digital primary protection system backed up with a conventional secondary protection system. PPS consists of four Eagle series redundant channels as its backbone structure; each channel consists of the digital equipment performing data acquisition, signal conditioning and conversion, signal processing, trip demand processing, and Engineering Safety Features actuation. In normal operation, trip signals come from any two of four channels will trigger the protection system.

The PPS was developed by Westinghouse as one of its Eagle 21 series product. According to the statistics (NEI,1993) published by Nuclear Electric (Owner of Sizewell B), Westinghouse invested 200 man-years for developing PPS and 50 man-years for carrying out independent verification and validation (IV&V) to assure that PPS met all related quality standards and requirements. However, due to lack of objective software quality and safety metrics, NE spent another 250 man-years to perform a comprehensive and complicated verification and validation to improve its confidence in PPS (Marshall, 1993).

On October 21 1993, Computer Weekly, a U.K. based magazine, published a short editorial message (CW,1993) saying that it had obtained a confidential NII (British nuclear regulatory agency) report consists of questions raised by NII for the reliability issues of Sizewell B PPS. The magazine will make this confidential report available to anyone who is interested in the topic; the purpose is to providing a "well informed discussion" in the subject. In early 1993, British Computer Society, an prestigious academic organization, published an open letter expressed concerns over the safety performance of Sizewell B Primary Protection System and recommended several improvements (Marshall, 1993).

Kashiwazaki-Kariwa 6 / 7 Nuclear Power Plants (Fukumoto,1998)

Kashiwazaki-Kariwa Unit 6 and unit 7 (KK6/7) is the first commercial Advanced Boiling Water Reactor (ABWR) design nuclear power plant. The basic design was jointly developed by Hitachi, Toshiba and GE Nuclear Energy. The digital I&C development process followed Japan’s regulation (JEAG 4609-Guidelines for Application of Digital Computer to Safety Protection System) which in general are less complex than USNRC regulations. The I&C design was based on Problem Oriented Language (POL) which helped to make the final system reliable and verifiable. The system validation testing was performed with the help of a PC-based automatic testing tool. This tool could carry out pre-defined validation testing procedures and generated testing reports automatically. The use of automatic testing tool effectively reduced the time and manpower required for the validation test. The validation testing covered dynamic transient tests in which simulated design base transients were generated for testing the behavior of digital I&C system. A very important feature of KK6/7 I&C project is that manufacturers have accumulated more

than 15 years experience in handling the digital I&C components for non-safety operations. Such experience paves the foundation for the success of the project.

During licensing process the regulator authority-MITI, asked Nuclear Power Engineering Corporation to perform a comprehensive qualification testing. The testing was efficient and successful; thus, the permit was issued without lengthy negotiation as that happened in most cases in the western countries. Due to its success in licensing process, KK6/7 has become a performance benchmark for other digital I&C licensing projects.

Load Sequencer of FP&L Turkey Point Plant (Kenndy,1994)

The Load Sequencer of unit 3,4 of Turkey Point Nuclear Power Plant was upgraded to digital design in late eighties. FP&L submitted application documents to USNRC for approval in June 1988. All review open items were finally closed and an approval was issued on Feb. 1992. The complete licensing process took 3 year and 8 months. During a NRC sponsored digital I&C technical workshop held in 1994, Mr. Larry Kennedy of FP&L reported this project and expressed complaints about the lengthy licensing process (Kenndy,1994).

Case Summary

Generally speaking, the above cases show that some digital I&C licensing cases suffered from high evidence preparation cost (P20, Darlington, Sizewell B), but still faced doubts about their potential safety performance (Darlington, Sizewell B); thus, these cases demonstrated poor licensing efficiency. On the other hand, KK6/7 showed quite good licensing efficiency. The remarkable point is that the result of licensing is not proportional to the invested effort. For example, KK6/7 spent relatively less quality-related effort than Sizewell B, Chooz B and Darlington, but still gained satisfactory review results from regulators. Such obvious performance difference implies the existence of techniques that can improve efficiency of current licensing practice. In the next section we will investigate what the critical efficiency shaping factors are and pursue methods that can manage these factors effectively.

Development of Evaluation Framework for Digital I&C Licensing Process

This section is to develop an evaluation framework that can investigate the underlying factors affecting the performance of licensing process.. First two subsections explain how to develop such a framework, followed by applying this framework to diagnose previous licensing experiences and propose solutions.

The Nature of Licensing Process

The purpose of licensing, according to Chapter 7 Standard Review Plan (SRP) (NRC,1997), is to "*determine whether the equipment, …process to be performed provide reasonable assurance that the licensee will comply with the regulations and public health and safety protected.*" The key word here is "*reasonable*" which apparently is quite subjective in nature, i.e., different regulators may have different acceptance standard about the quantity and quality of evidence that are considered to be "*reasonable"*. In another paragraph, SRP states that the reviewer need not to "*completely evaluate all aspects*" of the submitted documents. "*The review scope needs only to be sufficient to allow the reviewer to reach conclusion*." Here the word "*sufficient"* is also a subjective criterion. Based on these statements we can identify the mechanism of licensing process is to let the regulator to buildup a feeling of *assurance* or *confidence* based on submitted evidence. Therefore, the most important concepts in licensing process are: *sufficient evidence and assurance*. According to Webster Dictionary, assurance means: (1) something on which one can rely as a guarantee of truth. (2) Self-confidence. Now let's compare the difference before and after licensing process. Before the license process starts, it is reasonable to assume that the applicant should already have *reasonable assurance* in his mind that his design fully complies with regulations. Then after a successful licensing review process, a permit will be issued if and only if the regulator *also*

has reasonable assurance that the submitted design will comply with regulations. Therefore, the difference before and after licensing process is that, superficially, the evidence is presented to the regulator and accepted by the regulator; pragmatically, a state of *confidence* is built up in the regulator's mind based on the evidence. In other words, the major mechanism during licensing process is the conversion of the submitted evidence into the regulator's confidence. Thus, we may consider the essence of licensing process as an *evidence-confidence conversion* process.

There are many factors that can affect the efficiency of this evidence-confidence conversion process, Proper handling of these factors results in an efficient licensing process. The following sections will identify these factors and analyze their contributions to the efficiency of licensing process.

Licensing Process Evaluation Framework: An Evidence-Confidence Conversion Process

Figure 2 shows a schematic view of a licensing process based on evidence-confidence conversion perspective. The complete licensing process covers evidence preparation process and evidence-confidence conversion process.

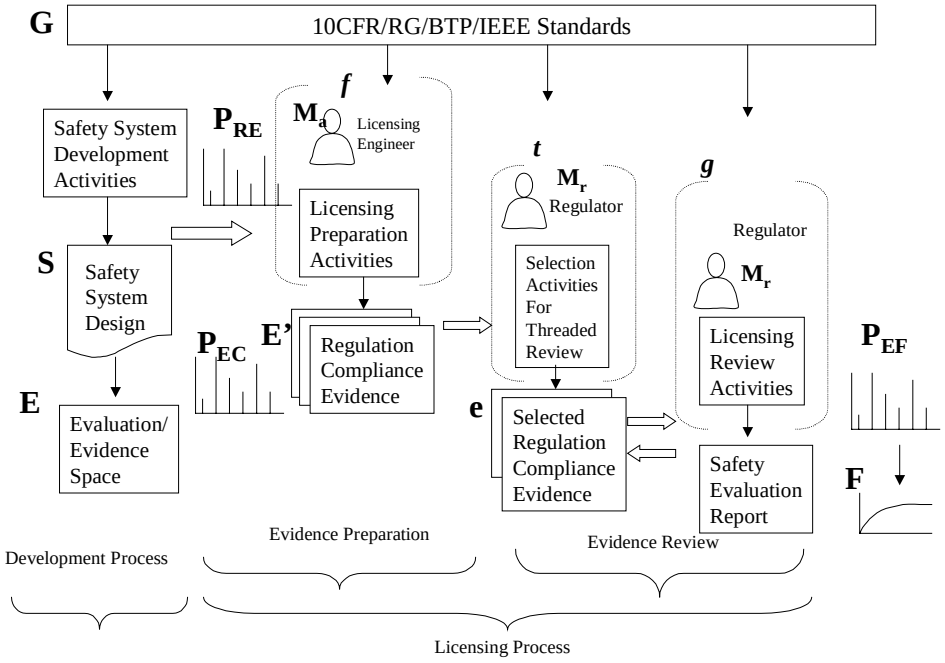


Figure 1: Licensing process model viewed as evidence-confidence conversion process

The licensing process can be defined as 9 tuples with 6 sets and 3 functions. Licensing Process $= (\mathbf{G}, \mathbf{S}, \mathbf{R}, \mathbf{E}, \mathbf{P}, \mathbf{M}, f, g, t)$

$f : \mathbf{G} \times \mathbf{S} \times \mathbf{M_A} \times \mathbf{P}_{\mathrm{RE}} \times \mathbf{P}_{\mathrm{EC}} \rightarrow \mathbf{E'}_{\mathrm{A}}$ .....Evidence preparation function

$t : (\mathbf{G} | \mathbf{S} | \mathbf{E}) \times \mathbf{M_R} \rightarrow (\mathbf{G'} | \mathbf{S'} | \mathbf{e'})$.....Thread auditing(selecting and slicing) function

$g : \mathbf{G'} \times \mathbf{S'} \times \mathbf{e'_A} \times \mathbf{P}_{\mathrm{EF}} \times \mathbf{M_R} \rightarrow \mathbf{F}_R$..... Confidence conversion fucntion

Definition of each term is explained as following:

G-Government regulations: As shown in Figure 1, they are 10CFR codes, regulatory guides, branch technical positions, technical reports, industry standards, etc.

S- I&C System design: complete I&C system design specification submitted by the applicant for licensing review.

R –Resource allocated for evidence processing effort. $\mathbf{R}_p$ represents evidence preparation effort, $\mathbf{R}_p$ represents evidence review effort.

E- Evidence space, **G** x **S** defines the state space needed to be evaluated, **E** is all the evidence needs to be generated for evaluating whether **S** complies with **G**. In reality, the applicant can only prepare a subset of **E**, i.e., **E'** and **E'** $\subseteq$**E** under a fixed **R**. The regulator can only select (thread auditing) a part of **E'**, i.e., **e**, **e**$\subseteq$**E'**, for review. Therefore, **e**$\subseteq$**E'** $\subseteq$**E.**

P- Various Profiles that shaping the performance of licensing activities.

$\mathbf{P}_{EF}$**-** Evidence-conFidence Profile: There are many different kinds of evidence and evidence owns different confidence conversion power, i.e., some evidence is more convincing than others.

$\mathbf{P}_{EC}$-Evidence Cost profile. The preparation cost for different evidence is not equal. $\mathbf{P}_{EC}$ represents the cost variance when one prepares different evidence.

$\mathbf{P}_{RE}$- Resource Evidence allocation profile. It represents how the total evidence preparation resource **R** is allocated for preparing different evidence.

M - Proficiency maturity level: it represents the degree of proficiency of staff members performing licensing activities. The proficiency can be roughly divided into three levels: novice, competent and expert. The level will affect the quality of evidence and resource consumption. $\mathbf{M}_A$ represents the applicant's and $\mathbf{M}_R$ represents the regulator's proficiency level respectively.

F – Confidence level achieved after reviewing evidence **e** during licensing process.

This model provides a framework such that further investigations can be conducted by analyzing relations among model components.

Conditions for Optimal Licensing Performance: Aligned Profiles

From the model we can define the optimal licensing performance as that achieving the maximal confidence under a fixed licensing resource. A qualitative discussion on the conditions that lead to the optimal licensing performance is given below.

1. Assume the total amount of resource for evidence preparation is **R**
2. Assume the resource allocation scheme is defined as resource allocation profile $\mathbf{P}_{RE}$ **;** then resource devoted to preparing each kind of evidence is determined.
3. The amount of evidence produced under such resource allocation scheme is decided by referring to evidence cost profile $\mathbf{P}_{EC.}$
4. When the evidence submitted to the regulator for review, the regulator's confidence will be converted from the evidence by referring to evidence-confidence profile $\mathbf{P}_{EF}$**.**

The process is shown in Figure 2. The confidence conversion process showed that conditions that lead to the optimal licensing performance are closely related to the alignment relation among three evidence profiles, i.e., $\mathbf{P}_{RA}$,$\mathbf{P}_{EC}$ and $\mathbf{P}_{EF}$**.** The exact optimal condition can be derived by mathematical techniques if the mathematical definition of each profile is known. Intuitively speaking, the more the confidence return generated by evidence, the more resources should be devoted to that evidence. Thus we may conclude that the key to an optimal licensing efficiency is the proper alignment of resource evidence profiles, Evidence-Cost Profile and Evidence-Confidence Profile. Figure 2a shows a good alignment case and Figure 2b shows a poor alignment case.

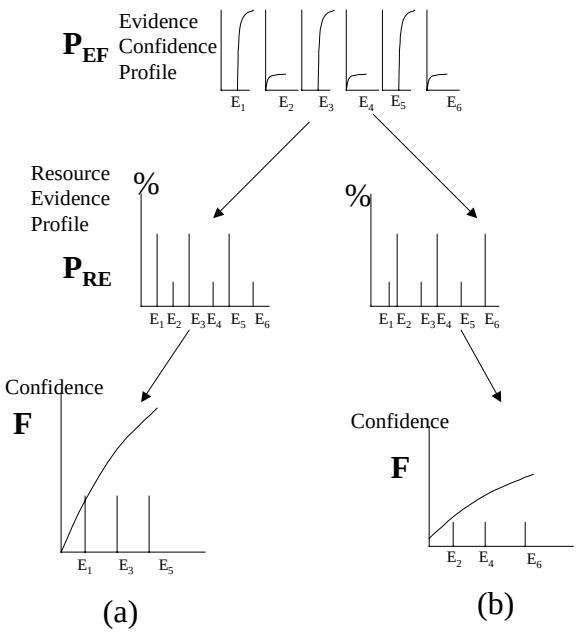


Figure 2: Licensing performance comparison for different profile alignment

Application of Licensing Process Model

The developed licensing process model represents a simplified model, but it captures essential features of real licensing practices. The advantage of having a model is that we can perform logical analysis and correlate results with real cases. Thus we can apply this model to explain previous licensing experiences and obtain insights into the characteristics of licensing process.

Diagnosis of Previous Digital I&C Licensing Cases

In this section we apply the developed model to explain those digital I&C experiences reported above. The result is also shown in Figure3.

Sizewell B: The major problem stems from the misalignment of three evidence profiles. The extra IV&V performed by EU did not contribute commensurate confidence return due to the fact that Westinghouse had already performed an effective internal V&V. The evidence-confidence return for EU IV&V effort became very low due to the saturation effect. The evidence preparation is an overkill activity due to the overlooking of the diminishing return effect of the evidence-confidence profile.

Chooz B: Chooz B's I&C project overlooked the severity of evaluation space explosion problem. The chose of Transputers as its computing platform resulted in a prohibitive workload for V&V task, i.e., the evaluation space is too huge to be evaluated. Unable to conduct complete V&V was the official statement for explaining why P20 project failed.

Darlington: Darlington Digital Shutdown System Project's problem came from the mismatch between the applicant's and the regulator's evidence-confidence profiles. Regulatory authorities adopt Dr. Parnas' position, which considered more rigid analysis as necessary evidence. The utility had to re-submit formal analysis information for review thus delayed the licensing process.

KK6/KK7: The major reason for KK6/7's success lies in the fact that KK6/KK7 I&C project adopted well-developed design that vendors have accumulated more than 10 years' experience. The cost for preparing evidence was low and knowledge was abundant and shared among stakeholders. Thus all evidence profiles were well aligned, and this resulted in an effective licensing process.

Load Sequencer/Turkey Point:

This project was performed in late eighties when both the utility and regulators were lacking of enough digital I&C experience. At beginning the evidence-confidence return was very low as showed in Figure 3. It took time for the regulator to establish a working evidence-confidence profile to support the reach of final conclusion.

Figure 3 shows the profile alignment situations for each case discussed above.

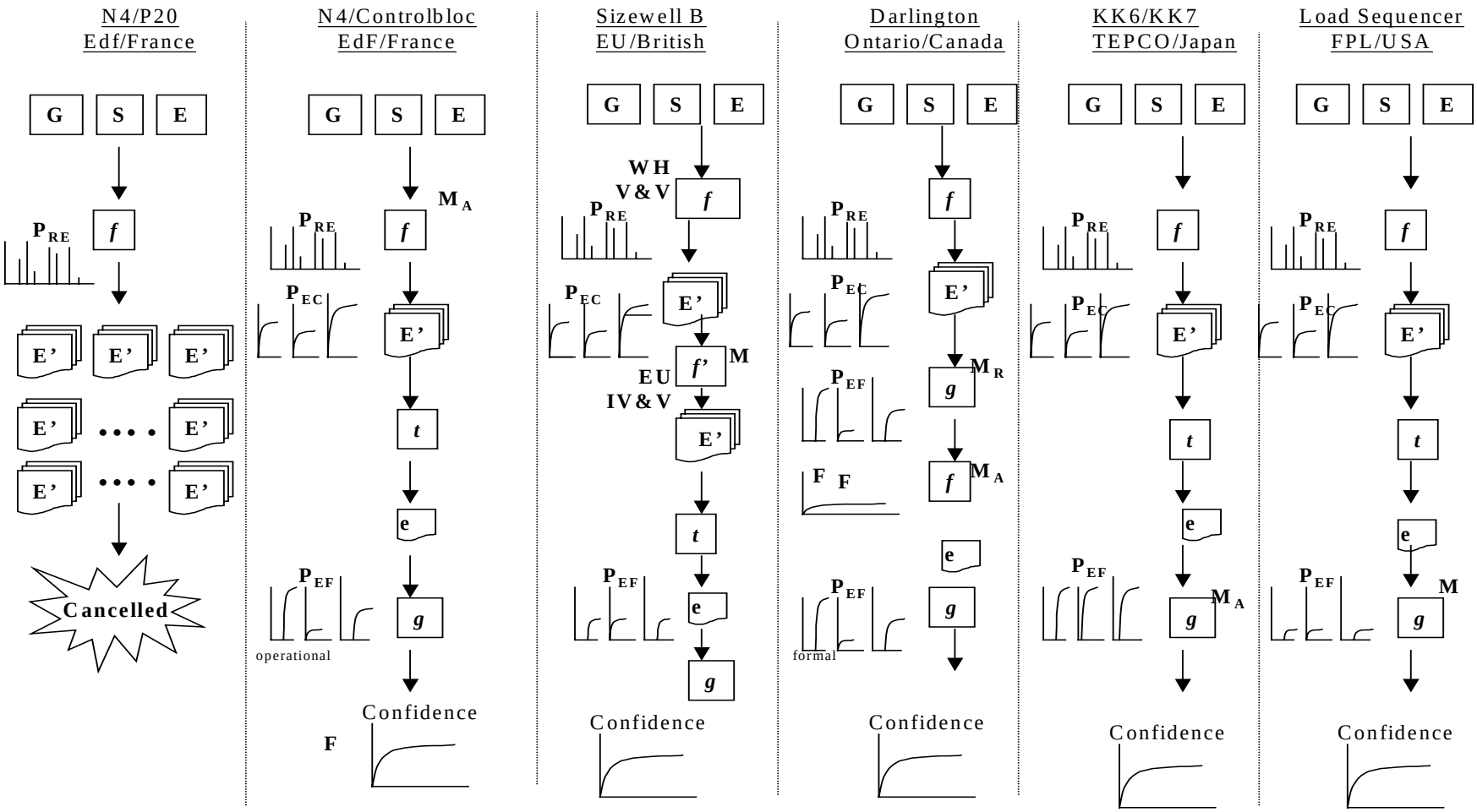


Figure 3: Diagnosis of Digital I&C Licensing Experiences

Insight Gained From Evaluation of Licensing Process Model

After applying the proposed licensing performance framework to evaluate the previous licensing experiences, we can obtain lessons learned and thus improve our understanding about the nature and limitations of licensing process.

- *Concept of Evaluation Space and Its Implications*

  Evaluation space is defined by regulations and system design, i.e., $G \times S$. This represents the scope to be worked with during licensing process. The larger and complex of the evaluation space, the more difficult the licensing will be. This feature implies that we shall choose simplified digital devices for safety systems in order to have a small and manageable evaluation space. This explains why PLC-based design is more popular than microprocessor-based design in digital I&C safety applications; a PLC-based design is much simpler than a microprocessor-based design for a same functionality. This observation coincides with Dr. Lawrence's recent research finding that promotes the use of "simple, but practical, computer-based instrumentation components for safety application." (Lawrence,2000)

- *Diminishing Return Behavior of Evidence Cost profile*:

  The evidence-confidence profile in general has a diminishing return characteristic. At beginning, the confidence level can increases as more evidence is collected. But the tendency of increment will saturate, i.e., up to a certain point, the confidence level gained will diminish even more evidence is collected. Thus, beyond the saturation point, invested resource will be wasted as what happened in Sizewell B PPS IV&V project. This feature can also be used as an argument for reducing some controversial regulations, such as independent requirements for V&V and safety analysis (NRC ,1997), as well as overwhelming documentation requirements, etc.

- *The Impacts of Human Factors in Licensing Process*

  This influence of human factors can be observed by examining the proposed model. For functions *f,g,t,* each process involves the proficiency maturity factor which is highly people-dependent and also can be highly subjective. Therefore, the performance of software licensing process is heavily affected by people's capability. This is quite different with hardware-oriented equipment licensing process. The ultimate goal of managing human factor for a licensing process is to maintain well consensus among all stakeholders. In a broader sense, consensus represents not only having similar interpretation of regulations but also having the same perception of evidence-confidence profiles. Without consensus the licensing process can be difficult and frustrating, as that happened in Sizewell B or Darlington projects. On the other hand, when all people reach consensus, then the licensing process can be smooth and efficient as that happened in KK6/7 project.

- *The Essence of Managing Licensing Process: Resource Management Under Uncertain Environment*

  The key words appeared in SRP include such as: *reasonable assurance* and *sufficient*. All of these key words heavily depend on personal judgment. The subjectivity invokes certain degree of flexibility and unpredictability for the performance of licensing process. In the model we represent such subjectivity judgment in form of evidence-confidence profile and evidence-cost profile and maturity proficiency. Figure 3 shows the typical distribution of these profiles. However, in reality, there is significant uncertainty associated with these profiles. The uncertainty comes from both stochastic nature (aleatory uncertainty) and lack of complete knowledge (epistemic uncertainty) about the behavior of evidence–confidence relation. Without accurate evidence-confidence and evidence-cost information, the managing of licensing process becomes a resource management process under highly uncertain environment.

- *Principle of Effective Digital I&C Licensing Process: Continuous Risk Management (CRM)*

  Experiences point out that within evidence-confidence conversion model two dominant performance influence factors are proficiency maturity and evidence-confidence profile. The inherent uncertainty associated with these factors makes any attempt for efficient licensing resource management very difficult. It is because our traditional regulation philosophy is founded on a deterministic environment such that safety can be assured by prescribing what the applicant must comply with. In other words, conventional compliance-based regulation is based on the assumption that the behavior of those activities or equipments under regulation is deterministic and predictable; confidence thus can be established thereafter. For digital I&C equipment, along with its related software development activities, the performance is neither stable nor predictable for most of the time. Thus, compliance-based regulation approach often results in resource waste due to the inaccurate estimation of the evidence-confidence profile and the evidence-cost profile. In principle, such an inherent uncertainty problem can be alleviated by Continuous Risk Management (CRM) technique. An accurate evidence profiles assessment is still difficult. However, the mismatched gap between various evidence profiles can be narrowed by continuously assessing and mitigating risk as the project goes on. Risk Informed Performance Based (RIPB) approach, recently promoted by USNRC, emphasizes the consideration of risk contribution of regulated equipment or activities in the decision-making process. RIPB practice can be viewed as a CRM technique. Thus, we consider RIPB practice a promising candidate for solving digital I&C licensing problems and worth further studying.

Conclusion and Future Work

In this paper we reported the preliminary result of our survey and evaluation of major digital I&C licensing experiences accumulated in the recent years. The motivation is that we noticed the performance variance among different digital I&C licensing cases, i.e., some were smooth and efficient while others were lengthy and problematic. In order to explain the causes of such variance and to develop techniques for improving the effectiveness of licensing process, we conducted an in-depth survey and analysis of these experiences. By viewing the licensing process as a confidence conversion process, a Licensing Performance Model is developed and used as a framework to analyze the behavior characteristics of licensing activities. The model identified major factors and functions that dominate the performance of licensing process, among which the proficiency maturity and evidence profiles are the most critical factors affecting the licensing process. During the evaluation step we were able to apply this model to explain why some licensing cases are successful and some are troublesome. This successful application shows the validity of the proposed model. Finally, we presented several insights into the nature of licensing process.

Our evaluation identified that inherent uncertainty associated with the various profiles dominates and limits the potential performance of licensing process. Based on our study we consider that Continuous Risk Management technique should be applied to cope with such uncertainty. Risk Informed Performance Based Regulation (RIPBR) currently promoted by US nuclear industry basically fits the definition of Continuous Risk Management technique. USNRC has issued relevant regulatory guidance for RIPBR and some of which could be applied to digital I&C licensing process. We believe that the development of a comprehensive RIPBR approach to digital I&C licensing process worth further in-depth studying.

References

(AECL,1995) Standard for Software Engineering of Safety Critical Software, (Electrical and Controls Engineering Department Standard), 982-C-H-69002-0001 Rev R0.

(Appell,1992) Appell, B., "Putting in a Replacement for Controbloc P20 at Chooz B," *Nuclear Engineering International*, July 1992, pp.45-48

(Chun,2000) Regulatory Assessment of the Darlington Shutdown System Trip Computer Software Redesign, C. Chun, L. Staples, A. J. Faya, NPIC&HMIT 2000, Washington DC, Nov. 2000.

(CW,1993) Editorial Message, *Computer Weekly*, October 21, 1993, UK.

(Fukumoto,1998) Fukumoto,A, et al**,** A verification and validation method and its application to digital safety systems in ABWR nuclear power plants, *Nuclear Engineering and Design*, V183N2, pp.117-132, July 1998.

(Craigen ,1994) Craigen, D., Gerhart, S. and T. Ralston, "Case Study: Darlington Nuclear Generating Station," *IEEE Software*, Jan. 1994, pp30-32.

(Guesnier,1989) Guesnier, G., Anglaret, M., Colling, J.M., and Raimondo, "C&I Systems for France's N4 NPPs", *Nuclear Europe*, Sept.-Oct., 1989, pp.17-18

(Hughes,1993) Hughes, G. and Boettcher, D.B., "Developments in Digital Instrumentation for Nuclear Electric's(UK) Power Plant", *Nuclear Energy*, Vol. 32, No.1, Feb. 1993, pp.41-52

(Lawrence,2000) Lawrence, J.D., "Software Qualification in Safety Applications," *Reliability Engineering and System Safety*, 70(2000)167-184.

(Kenndy,1994) Paper presented in Proceedings of Digital System Reliability and Nuclear Safety Workshop, Sept. 13-14, 1993, Rockville, Maryland, USA.

(MacLachlan,1994a) MacLachlan, A., "I&C Woes Behind It, EDF on Target for Startup of First N4 Reactor", *Nucleonics Week*, July 14, 1994, pp.3-4.

(MacLachlan,1994b) MacLachlan, A., "French Regulators 'Lost Hope' of Proving Chooz-B Digital I&C System," *Inside NRC*, May 30, 1994. pp.6-7.

(Marshall, 1993) Marshall,P and R. Silver, "Sizewell B Computer Controversy Looms Over Fuel Load Schedule," *Nucleonics Week*, Vol.34, No.42, Oct.21, 1993

(NEI,1993) "Sizewell B Reactor Protection Reliability: Nuclear Electric Presents its Case," *Nuclear Engineering International*, Mar. 1993, pp.28-33.

(NRC,1997) NUREG 0800, Chapter 7, Standard Review Plan, USNRC, Washington, DC.

(Peyrouton,1993) Peyrouton, M. and M. Pirus, "Progress on N4 I&C Architecture," *Proceedings of Topical Meeting on Nuclear Plant Instrumentation, Control and Man-machine Interface Technologies*, Apr. 18-21, 1993, Oak Tenn., pp.305-311.

Collecting Data from Operational Experience of Computer-Based I&C Systems - A Regulatory Perspective on Goals and Tasks

G. Schnürer[1], F. Seidel[2]

[1] Institute of Safety Technology (ISTec), Garching
Tel.: +49 89 32004-523, Fax: +49 89 3200-300, e-mail: sgu@grs.de

[2] Federal Office for Radiation Protection (BfS), Salzgitter
Tel.: +49 5341 885-863, Fax: +49 5341 885-865, e-mail: Fseidel@bfs.de

Abstract

Provided that the considered computer-based I&C systems are developed, qualified and maintained using an unique platform, the data from operational experience of the system's application at nuclear power plants can be collected under unified aspects. The main goal of the data collection is to contribute to the further qualification of these systems.

The following goals are of particular interest from the regulatory perspective:

- Evaluation and optimization of the qualification procedure,
- Demonstration of the achieved systems' dependability as well as
- Utilizing the experience of the system applications of lower safety significance within the licensing procedure for computer-based systems critical to safety

The content of the records and the evaluation methods for operational experience have to be identified carefully. As a good practice, the involved experts of the participants in this business, i.e., the licensees, manufacturers, technical support organizations and regulatory bodies should agree upon this identification. It should be noted, that not only the failures and the reported events are of interest, but also periods of operation without significant failures. Those should be considered as well in the frame of safety evaluation and qualification.

As a long-term goal of the collection of operational experience, the achieved performance of the system might be estimated in quantitative terms. To calculate the reliability, it is crucial to establish an evaluation model in order to identify the necessary parameters as early as possible and to collect them continuously during the operation.

Introduction

The safety-related application of software-based I&C systems is increasing also at nuclear power plants. Consequently there has been also a growing debate over the issues what data can be derived from test and operational experience.

The source of the uncertainty in software dependability is not of probabilistic nature. Rather, software failures may follow an erroneous data input or because of an inadequate requirements specification. Thus, software failures may occur in applications (distinct demand) or under environmental circumstances for which the system was not or not correctly designed; therefore in [1] the term "error-forcing context" is introduced. Because the input data configuration space as well as the configuration space of possible environmental data are very complex for real I&C systems the software behavior can not be tested completely. As an example, just consider the non-linear interaction between the hardware/software modules of a distributed I&C system during a real time application. Due to this quasi-probabilistic software failure behavior, probabilistic methods like fault and event tree analysis are applicable for quantitative reliability assessment.

Systematic approaches for quantitative software reliability assessment are still under investigation. Complementary, deterministic expressions about the software reliability can be derived from the software qualification procedure, particularly if the software and hardware of the I&C system are developed on a unique platform over the whole life cycle.

With this contribution the authors like to repeat and rearrange the facts on operational experience of computer-based I&C from the regulatory and expert's perspectives. They would like to stimulate the further collection of operational experience, particularly for software-based I&C developed on a unique platform. Especially, the principles and high-level requirements implied for platform development and qualification can be utilized to assess the operational experience.

Classification

Faults and failures

Because the possible design faults and erroneous input data will influence the software functionality in different manner, it is necessary to distinguish types of failures and faults, e.g. related to safety or reliability. The distinction between different types of software failures and faults should be consequently considered during the collection of operational experience by assessing the impact of the distinct occurrences on safety and reliability. For instance, a fault tolerant system operating in a cyclic deterministic mode will tolerate any erroneous input signal. On the other hand the system will react fail-safe if the erroneous input signal will get consolidated over some system cycles. Thus, this case is characterized by the transition from normal to abnormal but safe operation mode. Unlike, a system without fail-safe capabilities will react accidentally. Within the collection of operational experience both cases should be clearly distinguished from each other. Generally, faults and failures should be assessed and valued according to the importance to safety.

Collecting operational experience, following kinds of faults and failures should be considered:

- Hidden fault versus detected fault
- Systematic failure of the whole system versus systematic failure of only one subsystem
- Non-detected (passive) failure versus self-detected (active) failure
- System failure without fail-safe reaction versus failure after which the system is automatically transferred into a safe operating mode
- Input data error which will disturb the system's operation versus the case that the same input error is ignored or corrected by the system; i.e. the system's operating mode is robust against input errors
- Dependent versus independent failures

For instance, according to this scheme the following hypothetical scenario may have the deepest impact on safety:

- The software contains hidden faults.
- On a certain demand (by special combination of input data, or by a signal value outside the specification) a hidden fault will become active and will lead to a systematic failure of the safety I&C system.
- The I&C system will not react fail-safe, i.e. the I&C system is left in an accidental state or a plant safety system function will get activated to transfer the plant to a non-tolerable state.

Software types

Within the collection of operational experience software types should be distinguished, e.g. in the following manner:

- Application software: Non-application specific functional blocks or modules as well as function block diagrams, in which the modules are coupled to each other according to the application specific designed. The functional block diagrams may be developed on an unique platform
- Operational software: Like software for CPU operation, I/O actions, signal transmissions, exception handling, etc. Mostly this software can be treated only as black boxes. A re-qualification is useful to limit the functionality to the necessary extent.
- COTS (commercial off the shelf software): Pre-developed software, mostly developed on a platform different from the platform for the development of the application software. Normally the above mentioned operational software originally consists of COTS. Depending on the safety significance, COTS should be re-qualified to a certain extent. The assessment of operational experience – here in different application – might be helpful.
- Tool software: E.g. software used for the specification and coding of application software. This software should be qualified according to the safety significance of the target software. Particularly the software tools used for platform development and qualification are belonging to this category, in this application the software tools or distinct versions of the software are used during the whole life cycle, i.e. for specification, design, qualification (simulator and test software) and maintenance.

Collecting data of operational experience/ Goals of data collection

The most common objectives of the collection of operational experience for software-based systems are the in-depth analysis and assessment of new types of faults and failures including the recommendation of corrective actions as well as the derivation of learned lessons. Moreover to the authors understanding, the following aspects might be considered in more detail:

Demonstration that the applied I&C system meets the design principles (deterministic approach, root cause analysis)

After collection of operational experience over a certain period of time, the question should be answered from a deterministic point of view, whether the system has met the design principles and the top-level system requirements. The main design principles are e.g. deterministic cyclic behavior, functional independence of redundant system parts, diversity, fail-safe behavior, and robustness against environmental exposures. Top-level system requirements are established e.g. on the response time, signal and data flow.

As a basis for this assessment the findings of self-tests and periodical maintenance as well as all experiences where the system gave an abnormal response should be taken into account. For each of this case a certain list of design principles and system requirements should be analyzed item by item, whether this item is touched by the respective abnormal finding or not. Concerning top-level system requirements the above mentioned list might be established from the system requirements specification. The design principles can be taken from associated guidelines; e.g. [2]. In the frame of a BMU/BfS research project such principles are listed up specifically to a German I&C system [3].

This kind of systematic approach to the assessment of operational experience can be helpful to examine the I&C system requirement specification as a possible source of faults - implying also the potential to common cause failures. It will contribute to establish root cause analysis procedures to cover the high-level requirement specification.

Test coverage assessment

For concrete I&C systems a fully test coverage is practically not achievable. Nevertheless the designer and the V&V team are faced with the problem of performing and optimizing an appropriate test profile to meet the associated requirements of guidelines and standards. Therefore, it should be demonstrated that the chosen test file is appropriate or - if this cannot be achieved - this test file is to optimize. For this task the collection of operational experience can be very helpful, if the records of the I&C activities are available, unlike they are resulting in a system failure, in an abnormal system reaction or in the correct activation of the specified function. An operational profile can be derived and later compared to the test profile to demonstrate whether the profile was appropriately chosen for the qualification.

For further discussion we found two related main questions concerning the treatment of operational experience:

- Treatment for a high amount of data

The record of all occurred I&C activities may imply a great expense in the later assessment of the collected information. An appropriate record structure and schedule for condensing the recorded data might be helpful to reduce the effort. In this matter we would like to pick up proper recommendations and, if already available, the experience of the audience. The question can also be expressed as " What effort is appropriate to gain more detailed information to optimize the test strategy for further system application?" – always assuming, that the system is developed and qualified on the same platform.

- Treatment, if the data base is too low

This case concerns that during operation the number of I&C activities is too low to gain evidence for the test coverage. This case will particularly occur if the I&C system performs functions of high importance to safety with the result that the system function is very seldom activated, assuming that an appropriate defense in depth concept is applied in the I&C design. Even this case is the most interesting case from the safety point of view. Covering this, in Germany the following solution is applied:

Selected systems to perform safety-related functions like reactor power limitation and control were developed and qualified on the same platform as for safety-critical systems. That means, in comparison to safety-critical systems the same qualification requirements were applied for the qualification of the safety-related hardware and software. These systems were extensively tested, particularly during on-site operation in parallel to the original hard-wired I&C system. Due to the off-line mode chosen for parallel operation of the software-based system, additionally special test sequences were performed without affecting the plant operation. This leads to additional test experiences. After commissioning these systems now the performance of real I&C functions like reactor power control is much more frequently than any function of higher safety significance.

Of course, the concern is remaining that the safety related control functions are generally not comparable with any safety-critical function. According to the design the considered I&C systems are operating in a deterministic cyclic manner. Thus the system's operating mode is independent from any input signal. That means, from the aspect of operational experience the final purpose of signal processing and voting has no importance; again, provided that the compared systems are developed and qualified according to the same basic design and on the same platform. Therefore, the resulting higher amount of operational experience with the I&C system for reactor control and limitation may result in the first above mentioned problem. Note that the provision of the deterministic cyclic system behavior should be approved as a main postulate for this kind of collection and interpretation of operational experience. Robustness tests with any given input signals can be helpful. Within the later assessment of the collected operational experiences it should be further examined whether this postulate is met by the system. For instance, a system or component failure triggered by an input signal, gives evidence that the system does not fulfil the postulate, at least not in any case of demand.

Quantitative system reliability assessment

There are different approaches to analyze the software-based system's reliability quantitatively. Methods successfully applied in reliability analysis for hardwired I&C systems like fault tree analysis, event tree analysis, Markov analysis and failure mode and effect analysis will be analyzed to a certain extend according to their applicability to software-based systems. This paper cannot show the

state of the art of quantitative reliability assessment in detail. Recent results can be summarized as following [4-7]:

- For complex I&C systems there is no general approach, often the combination of different methods applied for certain software modules (distinguishing e.g. application specific software and COTS) will yield best results [4]
- Often there is a lack of data to feed the reliability models. In a first step the data will get conservatively estimated to estimate the lower limit of the reliability. Further investigations will show, whether more precise data can be derived from operational experience

In the case that the correct function as well as findings of the system are recorded following results can be derived:

- The systems' or sub-system's availability can be obtained with more evidence; that means under consideration of the test intervals.
- The ratio of cases in which the system reacts either abnormal or as specified can be estimated with more evidence.
- If dependent failures are occurred, their nature can be analyzed in more detail, using all the test data recorded between and after their occurrences.

Taking these facts into account, we suggest that the reliability experts should identify

- The reliability models, which are appropriate to estimate the reliability of the special I&C system, and
- All the data, which are necessary to feed these models.

The result might be discussed together with system specialists to confirm that the collection of all identified data will be feasible.

The Five-Steps-Concept – a proposal to collect and assess operational experience

In Table 1 a systematic approach following [8] is proposed for the acquisition of data to evaluate operational experience. The approach covers the following 5 steps:

1) Evaluation of data and information which have been collected by the utility and involved experts to identify and investigate distinct fault phenomena (incident reports)
2) Taking into account the related information about operational experience which the vendors gained from the operators (backward system)
3) Evaluation of the operational data which are collected by the utility covering the cases the digital system has responded on a operational or safety related demand correctly in the specified manner (experienced operational profile)
4) Consideration of the data concerning digital I&C related incidents in domestic plants
5) Consideration of the data concerning digital I&C related incidents in foreign plants.

To our present concept the first three steps are particularly directed in order to collect operational data of a equipment family which is developed and maintained on a distinct platform. So the

description of the distinct platform and the failed functionality should be of more interest than e.g. the place of application.

Complementary in the last both steps, the world-wide gained experience will be taken into account, including the information about the application of other I&C products. Therefore, to our understanding this concept represents not a different or separate program, but will be rather a special selective application of the very useful COMPSIS data library.

REGULATORY ASPECTS APPLYING THE RESULTS OF RELIABILITY ANALYSIS OR SOFTWARE-BASED SYSTEMS

Relation between quantitative and qualitative approaches

Within the German regulatory framework, qualitative reliability requirements are preferably established. Concerning the deterministic requirements, operational experience can be utilized and evaluated in order to show that the I&C design principles and top-level requirements are met during operation.

The German regulatory framework contains quantitative criteria only by relative terms. For instance, it is required that the safety I&C shall not determine (affect) the availability of the plant safety system, see KTA 3501. According to the state of the art, the availability of both, the plant safety system as well as the I&C hardware, can be estimated. However, as a new task the estimation of an upper limit for the software-based system availability is to cope with. The result might be of certain interest within the licensing procedure for a software-based system for safety-critical applications.

As a German requirement for licensing, any new system's functionality and quality should be demonstrated by operational experience. This stands of course beside the general requirement to prove the quality.

This paper refers particularly to software-based I&C systems developed on a unique platform. Such a unique platform ensures an adequate documentation. During qualification, the hardware and software modules can – at least partly - be treated as white boxes. Consequently, the platform development supports the qualitative reliability assessment. As a compliment, the quantitative assessment can be supported by operational experience which are collected from all systems qualified according to the same standard and using the same platform. This way, the platform development shows advantages also according to the quantitative reliability assessment.

Consensus between involved parties

Even the optimization might be possible, the collection of operational experience may imply a considerable effort for all participants over the long-term period of some years. The participants (licensee, vendor, regulatory body and technical support organizations) should therefore agree from beginning upon the effort (e.g. the record format, time period and the content of the data collection), as

well as upon the objectives of this collection. If quantitative reliability assessment is foreseen experts on reliability assessment should be involved to establish the record contents and format from the beginning.

Conclusion

Taking into account the effort of the operators and vendors to collect operational experience from applications of computer-based I&C, the authors see the chance that these information and data can be utilized to support in following fields:

- The demonstration of the required qualification of computer-based I&C is based on deterministic as well as probabilistic approaches. Operational experience is required to derive dependability data.

- In the case of comparable operational profiles and unique platforms operational data can be collected together within a unique data library. Consequently the derived dependability data should be applicable – case by case may be under special conditions - to other systems of the same platform and of a comparable operational profile.

- Already established qualification procedures can be additionally validated and optimized. For instance, the test procedure of systems of the next generation can be optimized on the basis of the – real experienced - operational profile of the previous generation.

- The procedure to license the safety critical application of computer-based I&C – e.g. in the case of upgrading of a hardwired safety I&C system - can be supported using the operational experience from applications of the equipment which is developed and maintained on the same (unique) platform.

Needed agreements for the treatment of operational experience:

- The parameters which are necessary to obtain dependability data after a certain period of operation should be established before the data collection is started.

- The parameter profile should be harmonized under participation of the involved parties.

- Conditions by means of familiarity and anonymity are prerequisites for the treatment and acquisition data of operational experience.

The project is supported by the German Ministry of Environment, Nature Conservation and Reactor Safety (BMU). As a first result the five step concept is now under discussion. The participation in the COMPSIS activities is important for our project which started last year.

References

[1] Garrett, Ch, Apostolakis, G., Context in the Risk Assessment of Digital Systems, Risk Analysis, Vol. 19, No. 1, 1999

[2] Instrumentation and Control Systems Important to Safety in NPPs, IAEA Safety Guide 252, Vienna,

[3] Laue, K.-D., et.al., “Werkzeuge (Tools) zur Überprüfung rechnergestützter Leittechniksysteme mit sicherheitstechnischer Bedeutung", BMU/BfS research project, excerpt is to be published

[4] NUREG/CR-6101, “Software Reliability and Safety in Nuclear Reactor Protection Systems”, Appendix “Technical Background”, June 1993, Livermore, CA

[5] Saglietti, F., “Verfahren zur quantitativen Abschätzung von Zuverlässigkeitskenngrößen für Softwareprodukte”, ISTec-A-320, Institut für Sicherheitstechnologie Garching, 1998

[6] American Nuclear Society, “Proceedings of the International Topical Meeting on Probabilistic Safety Assessment PSA ’96”, vol. III, chapter “Information and I&C Systems, p. 1453ff., October 1996, Park City, Utah

[7] American Nuclear Society, “Proceedings of the International Topical Meeting on Probabilistic Safety Assessment PSA ’99”, vol. 1, chapter “Reliability Analysis of Digital systems”, p. 499ff.; chapter “Software Reliability”, p.641 ff.; August 1999, Washington, DC

[8] Lindner, A., Makuschies, B., Hoffmann, E., “Entwicklung von Methoden zur Erfassung von Betriebserfahrung mit rechnerbasierter Sicherheitsleittechnik in Kernkraftwerken”, ISTec–A–566, Institut für Sicherheitstechnologie Garching, 2001

Tab. 1: 5 steps concept – a proposal to collect and assess operational experience

Step	Kind of operational data acquisition	Acting organizations / institutions	Area of application	Period of acquisition	Aim of the acquisition	Remarks
1	**INVESTIGATION OF ASSERTIONS WHICH DO NOT EFFECT THE FUNCTIONALITY IN A NON TOLERABLE MANNER**	**UTILITY**	Limited to the effected system	Limited period	Explanation of root causes, investigation of fault phenomenon	
2	Feedback experience of the manufacturer	Manufacturer	All specimen of a distinct type of equipment	Lifetime of the equipment	Conclusions concerning fault effects B (reliability data)	Backward system
3	Acquisition of the operational acting (correct initiation of protection e.g.)[1)]	Utility (manufacturer)	total system	Lifetime of the system	To gain confidentiality in the experienced operational profile; "positive operational experience" (reliability data)	[1)] Important because of activations are seldom
4	Acquisition of national incidents	Utility TSO manufacturer	Digital safety systems in German NPP	Lifetime of the system	Generic assessment of digital I&C systems and equipment, particularly regarding the detection of design faults	TSO: technical support organizations like TÜV and GRS/ISTec
5	Acquisition of international incidents (within the COMPSIS framework)	OECD/IAEA	Digital systems in NPP abroad	Duration of operation of nuclear power plants	Establishing an international database for generic operational experience	

Digital Projects in the Near Past and their Consequences in Safety Regulations in Hungary

K.Hamar
Hungarian Atomic Energy Authority H-1539 Budapest 114. Pob. 676 hamar@haea.gov.hu

Summary

With the licensing and operational experience, the Hungarian Authority intends to reformulate the safety regulations and guideline statements. We have to refine the design principle recommendations, and restructure the licensing from the aspect of procedural rules, in order to establish better licensing environment for the benefit of the licensees, and the regulatory staff. Experience discussed below covers first of all the cases of reactor protection system, core monitoring system and process computer. Some statistical data will be also presented.

Experience

Reactor protection system, Teleperm-XS

In 1993, evaluating a Simple Task Specification the Hungarian Atomic Energy Authority (HAEA) Nuclear Safety Directorate (NSD) formulated first time an opinion about I&C refurbishment, and has not refused the idea of installing digital system for reactor protection functions. This regulatory position resulted digital solutions for the Hungarian NPP units in the commercial bid.

In the reliability analyses about the Teleperm-XS system of the contracted Siemens Company it was assumed that, for every EP1 actuation, functional diversity is ensured by the use of two physical diverse measured initiation criteria dealt by two different computers (Ts-a and Ts-b) in each train. The list of these diverse initiation criteria were accepted by NSD in 1996.
This is the only diversity assumed in the system against common mode failures. Accordingly, the possibility that the first action initiation can be missed must therefore be considered.

From the viewpoint of software, the interesting result of the analyses was the demonstration, that the common software parts, common to both computers Ts-a and Ts-b, a reliability level of 1E-6 is achieved. The analyses take the challenge to demonstrate, these levels are guaranteed.
On the other hand, the international expert opinion assumes, such a level is impossible to demonstrate by statistical testing. While the quantified reliability gave the opportunity to go on with scientific and theoretical discussions on the subject, the practical necessity of licensing this system arose.

Fortunately, not only the probabilistic approach could prove the reliability and requirement fulfilling behavior of the T-XS system.

The regulatory approach rely very far on the institutional type testing results, which are certified by German state authority technical support organizations. Another important issue in the licensing procedure was the existence of manufacturer independent factory acceptance test. The FAT test field provides the possibilities for open loop tests. In the Hungarian project the closed loop tests were done with the full scope plant simulator on the site, with a representative RPS configuration. The role of the closed loop testing is mainly the validation of technological functions, while open loop tests are exercising the computer system functions more. The above mentioned testing targets were interpreted in the FAT Plan, as it is in the Appendix of this paper.

During the evaluation we could see, beyond the theoretical effort Siemens went into big depths citing all of the available operational experience to formulate statistical evidences. What is desirable from operational aspect, was bad from statistical aspect. However there are some hundreds of Teleperm-XS modules operated in the existing configurations, the number of modules of one or another specific type, and the number of error occurrence are not enough for a big statistical mass. According to the available figures, the theoretical error calculations on the different modules resulted much worse reliability, than the real life operation up to now. So the T-XS behaved better in operation than it was theoretically assumed in a conservative approach, for example, with that assumption, the self testing can discover only the 90% of random HW errors. This year the reactor refurbishment project is about installing the 3rd Teleperm-XS configuration in the Hungarian Paks site, between 20. July and 20. September 2001.

The loss of reactor scram actuation is a crucial potential system error, which can happen only as result of common cause failure in all of the redundant RPS trains, due to the design principles. In this case the operator has the opportunity to start manual action, at least, switching off the control rod drives electric power supply with handy push button, to drop the rods with gravity. Going further, we have to analyze the rod effects.

The consequences of control rod jam or sticking were analyzed on different ways, among them with SMARTA computer code. The calculation show, in the VVER440 reactor core the pressure and the temperature in relation with the dynamic reactivity effects are not challenging the primary circuit on dangerous level, boiling is not probable, while, of course, the safe and long term reactivity control needs the boron injection. As a comparison, unintended rod withdrawal may have worse consequences to local temperature and boiling probability, and to the fuel and control rods. In general the ATWS event group has ~1% contribution to the CDF, that is in the 10E-6/year range, while the CDF median value is in the range of 10E-5/year.

These facts are conveying that message regarding the system reliability qualification, an ALARA approach is acceptable, especially, if the most important serial element to the RPS, the control rod drives and mechanism, have a given, and in the best case constant reliability.

Another approach is a kind of cost-benefit comparison, where the assessment effort spent to exhaustive and statistical testing, should take into consideration that fact among others, the I&C and electrical systems are together contributing with 15% to the CDF value in a detailed PSA level-1 model. The resources for different assessments should be shared among the different systems.

After the above considerations about the RPS, the licensee and developer offered test strategy and extent were accepted. The number of the test cases is approximately 200, which are representing different unit transient scenarios, which result actuation of reactor protection. The tests were executed in FAT, and in simulator environment.

Because of the individual modifications in the application, these test cases were run several times in both environments, on the Unit 1 and Unit 2 configuration. The total number of the executed tests, including the closed-loop manual test performed on the simulator, is around 2000.

No failures were detected in the on-line software during these tests. Considering the 0.5/year value for the real actuation demand, we probably may have that estimation, that the time elapsing between the occurrence of two software failures, causing actuation masking, exceeds 4000 years. Taking into consideration the periodic tests of the RPS also, which are exercising the protective functions, while the unit is running with nominal load, we believe the unavailability due to SW reason, is better, than 1E-4/year. We have to keep in mind, during these tests, those input parameters which are not intentionally triggering the RPS, can de defined, random, or living, which introduce differences, even if one specific test case will be executed many times.

It can be assumed due to the fail-safe design, the residual SW errors, which hasn't been discovered yet, will initiate spurious actuation instead of actuation masking.

The total number of the test cases for the RPS and the representative configuration, connected to the plant simulator, on the four Units together, is expected to be 10 000, thus the SW reliability is hopefully growing to 1E-5, upon the completion of the Unit 4 system.

Core monitoring systems

Core monitoring system resides in IEC1226 "B" class, since it has been installed on all of the four units between 1992-1994. The system consists of two fold redundant micro-VAX, with the application named Verona 5.2 version, running in VMS environment. The application can be characterized with 50.000 line of Fortran and C source code. Data acquisition is running on 5 Motorola68000 computer cabinets, under OS9 system.
In August 2000 Authority refused operational license application due to many modifications during the implementation phase (coding, testing and pilot run) of the last version.
With the modification permit the Licensee had right to operate and test the modified system for three month. The modifications had been completed during this period aimed to correct algorithm and communication problems.
Asking the procedure, what the Licensee followed many cases, the Licensee argued with the citation of safety code paragraphs, which were formulated originally to distinguish the repair and modification regarding the mechanical components. Since the software hasn't been excluded in the paragraph text, this argumentation had a formal chance.
The SW error correction is naturally modification, deviates from the mechanic analogy, where the corrective action intends to restore the original technical conditions. The SW error correction intentionally wants to achieve new technical condition and behaviour.
The review of safety regulations in 2001 needs to handle software issues in a special manner, deviating from the presently existing general definition of error and repair. Our approach this time is that, in case of SW products, we try to define the terms of repair and modification against the functional specification, and the system specification.

Process computer re-classification due to increasing safety importance

The old system had been in "C" (IEC1226) safety class. The newly installed successor process computer system consists of four pairs of redundant Supervisory Control and Data Acquisition (SCADA) Intel platform servers, several additional computers and operator workstations. A WEB server provides information for a large number of remote users in their office computers. The application is running in Windows-NT environment.
The system has an important role to present and archive the RPS readings, and corresponding calculated values in the control room. Due to this fact, the system installation took place parallel to the Reactor protection system refurbishment.
The most significant function group comprises the implementation of a critical safety function monitoring system. This task is being carried out under the scope of a joint international agreement established by the OECD NEA. The project goal was to develop an operator support system to support the execution of new symptom-based Emergency Operating Procedures, for application in VVER reactors, with the Paks NPP as the target plant. EOP starts run in 2002.
Due to the increasing safety significance, the Regulator classified the process computer as "B" safety class system this year, but give dispensation from immediate qualification of the system, regarding the pilot project, and the good operational experience since 1999.

The system has many "commercial off the shelf" COTS software modules, that means any functional modification in the future requires qualified COTS, or qualified application. Both parties are facing problems to solve it.

Errors and problems of digital systems and related components 07.1999 – 07.2001

All of the below listed systems started their service in this period. The below data is based on licensee event reports (LER).

RPS and RPS related errors and problems were found during service time, FAT excluded. Cumulated service time in the period: 3 years. DFD is the graphic representation of the application, this is practically a data flow scheme, the symbols are I&C engineering and process control symbols. The DFD is compiled to running code.

Specification error (DFD correction needed)	**3**
Random HW error (power supplier errors: 4)	**10**
Recurrent HW error (first occurance random, DC power supplier error)	**3**
Systematic or CCF HW error	**1**
Application SW bug	**2**
High load on safety related (non safety) Ethernet bus	**1**
Measurement anomaly, no cause identified	**1**
Loss of telegram (due to assyncron behaviour)	**1**
Error log, but no cause identified	**1**
Non-recurrent phenomena, had no effect to log files	**1**
Sensor error	**17**
Human error caused value reading lead to actuation	**2**
Gateway and Service Unit (recurrent error is 1 error)	**3**

Diesel Generator Control System – Woodward PLC error during service time.
Cumulated service time in the period: 2 years.

Random HW error (power supplier error)	**1**

Uninterrupted 220VAC power supply, type Staro-Eta error during service time.
Cumulated service time in the period: 32 years

Random HW error (inverter ignition control board)	**1**

Other systems had no LERs during the same time, which doesn't mean necessarily, they had no errors. LER criteria is technical specification violation due to system unavailability.
In case of the RPS systems the above data covers only the new digital systems on the 1st and 2nd unit of Paks NPP. The old systems are not included. **Not only LERs, but all RPS error indications should be reported** due to occasional regulatory prescription in the permission of the RPS refurbishment.

Licensing

In the safety code we have only some statements about computers. These statements were formulated in 1996.

Where such a system or component is used, the reliability of which basically depends computer program, suitable techniques and standards should be used during the development and the entire lifetime of the computer program or the compliance with these techniques and standards should be set as an objective through the following:

a) during the development of the computer program, verifying the operation of the safety-related system and component, the application of ***latest design practice*** *commensurate with approved standards;*

b) quality assurance program and plan operated on the basis of ***appropriate quality assurance*** *standards****;***

c) complete and sufficiently ***diverse testing*** *of the latest validated program version by a group independent of the developer;*

d) execution of a ***wide-range and independently qualified test program****, which includes the test of all system functions and proves system reliability.*

The quality assurance played proper role in the RPS, and in the diesel controller project. The uninterrupted power supplier control function is very simple, and the PLC has mainly firmware. It is easy to report the QA worked.
In the core monitoring project, despite of the QA, the big mass of software, and the classic structured development characterized the situation. It took a big effort to finish the project.
The process computer and the object oriented SCADA has a very good reputation among the licensee staff, but the regulator had no opportunity to assess the quality and quality assurance measures, up to now.
We believe, the sufficient testing could be proved in all of the projects, but the divers testing can be mentioned surely in case of the RPS project, only. Diverse testing environment was not available in the other projects. The independently qualified test program is true from that aspect, they were independent to the developer, in every case.
We are in trouble with point a), with latest design practice. The above characterized projects followed totally different techniques in development: Complex PLC like graphic interpretation, simple conservative PLC program development, structured programming, and tendency to object oriented programming in the SCADA project.

Due to the appropriate standards the RPS introduced into the practice the most important safety requirements:

- Simplicity
- CCF protection: separation, cabling, earthquake resistance
- CMF protection: HW, SW, specification
- Fail-safe construction
- Reliability
- Testability

Since the appropriate standards could not be identified neither among the Hungarian standards, nor among the EU directives, we should like to address these system properties in the new safety code directly, in order to maintain the safety of class “A” systems. It is not possible to go into details from technical aspect, the safety code is governmental decree level document. On the other hand it is also not practical to do so, because there are many interested parties in a general legislative procedure, which can disturb technical

statements easily. The IEC and IAEA will represent the good practice, as it is intended originally, and they can be interpreted in the guideline series, however they are not obligatory.

The requirement of simplicity conflicts with almost all the other requirements, mainly the functional requirements (not representing the subject of the present article), testability and diversity.

Some other system properties should be underlined among the requirements for class "A" systems:

- Use of a strictly cyclical, controller-type program
- The input data should be processed only by the application software. The input data may have no impact on the behaviour of the operating system and the run-time environment.
- Changes in the input data do not cause interruption.
- Changes in the input data do not cause changes in the sequence of task implementation.
- The processors and the communication networks have a constant load, regardless of the status of the inputs and the equipment (HW failures).
- The status of the system does not depend on the status of the environment.
- The distribution of the system resources is static.
- The software modules and their interface are strictly defined.
- Software modules are thoroughly tested and qualified, independently to the application specific tests.
- The redundant trains operate asynchronously and do not use a synchronising mechanism, while the actual service time of the trains should be always different.

Analyzing the above projects and systems, we can see, the RPS system meets these requirements, the diesel generator controller also owns these properties, the uninterrupted power supplier control function is very simple, and the safety could be proved easily, even with no regard to the above requirements.
In case of the core monitoring, the sample readings and calculations has the cyclic and deterministic behaviour, the question is that, how it is running in the reality on a VMS system, together with the archive function. The archive is working on aperture principle, so it is event driven.
The process computer intentionally transient sensitive due to archive goals, the changing of input data may change the execution sequence, during plant transients the system load has very dynamic character.

Conclusion

That means in the reality, to give floor to the daily practice of assessment and other regulatory activities, not all of the above requirements should be followed in class "B" (class "C" is out of regulatory interest). This is beneficial to the Licensee operated existing systems, too.
But, it is interesting to see, the qualification of class "A" systems was much easier, than the cases of the "B" class core monitoring system, and, what we believe, the process computer. The reason is that, the safety is manifesting in a set of static and dynamic system properties, among them probably the most important is the deterministic behaviour. If this property is assured, the assessor has much easier job. Which is again a safety contributor. That conclusion will be surely addressed in the new safety regulations.

Appendix

A very short description of the Hungarian party executed FAT tests, excercising the Teleperm-XS system to be installed in Paks NPP for Reactor Protection System functions.

1. Identification of system components and test environment. The examination is based on the comparison to of the CRC sums in the downloaded code to the CRC of the compiled code, while some other identifiers are also taken to account. The identification of the SPACE system components running on the service unit is belong to this task also.

2. Function tests, status of readings handling. Verification of the functional behavior of the system against the functional specification. The task also combines input failures, and transient simulation is generated on the inputs. This test was done by the Siemens Co. also, finalizing the in-house tests.

3/1. Fault tolerant behavior. The system is divided into stand-alone units, while unit errors are simulated in different combinations. The testing staff is checking the impacts of the failures. Automatic system regeneration should follow the error situation.

3/2. Fail safe behaviour. Single, double and triple analog and binary signal failures are injected into the redundant inputs of the system. The effect is checked on the different data monitors and on the output to the actuators.

3/3-1. Self monitoring. The test covers basic hardware tests during start up, cyclic testing in operation, voter computer master-checker function, watchdog (time out), exception handler functions, cabinet alarm, individual signal monitoring, check back of output signals, error status and error message processing.

3/3-2. Periodic tests. This test covers the operator initiated test functions, the safety conditions of periodic test initition (only one train can be tested at the same time, etc),
returning of the tested train back to normal operation, while artificial errors still are in the data process.

3/3-3. Start–up tests. The extent and the content of these test differs from the periodic tests.
Anyway this test is due at power unit start-up after refueling and general overhaul.

3 /4. Man-machine interface. This test is exercising the human operations on the safety monitoring system, the service unit, the test machine, and the information subsystem.

3/5. Independence of the subsystems. This exercise should prove, he three redundant trains, the man-machne interface in the main and emergency control rooms, the service units and the gateway computers to the information subsystems are totally independent from each-other from physical, electrical and logical aspect. The test field is applicable only to prove the logical aspect, no information or lack of information can influence the proper operation of the subsystems. The electrical aspect is type tested, any further test can damage the system. Physical aspect is the function of on-site installation.

3/6. Deterministic behaviour. The test should provide that proof, the operation and collecting of analog and binary signals are really cyclic with the same time constant, with a given tolerance margin, in any external condition represented by values of inputs. The external conditions are simulated by redundant, nearly syncron, slowly slipping probe signals, while the safety function execution, in accordance with the momentary probe signal configuration, is expected. At the same time the availability of the data on different points of the system is checked.

3/7. Input accuracy check. This test doesn't need explanation. The test should cover all of the existing and physically different input channels and converters. The test machine is a requisite.

3/8. System reliability checks. Exercising the system with big number of negative random input sequences, which tests the potentiality of unintentional reactor trip. Success condition is the lack of reactor trip signal during any time extent.
The another test is random input test also, the input random patterns are mixed with trip combinations. Serves to test the loss of reactor trip potentiality.

3/9. Accessibility of system software. The user can assess the software on three ways: via the Service Unit on-line, via the Test Machine, and by manual actions. Authorised user is allowed to access on the Service Unit. Under defined system conditions or without administered permissions (turn key switches) the test machine operation is not allowed. If test has already started, the system should turn back to normal operation. Manual action like opening the cabinets must be indicated by alarm.

3/10. Information interface. In these tests the data connection to the gateway computers are tested. The completeness of the data tables and the cyclic refresh of the data items are verified.

Unclassified **NEA/CSNI/R(2002)1/VOL2**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

10-Jun-2002

English - Or. English

NUCLEAR ENERGY AGENCY
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

NEA/CSNI/R(2002)1/VOL2
Unclassified

CNRA/CSNI WORKSHOP ON LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS

WORKSHOP PROCEEDINGS

Hluboka nad Vltavou, Czech Republic
25th-27th September, 2001

English - Or. English

JT00127841

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of 27 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of scientists and engineers. It was set up in 1973 to develop and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety amongst the OECD Member countries.

CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of its programme of work. It also reviews the state of knowledge on selected topics of nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus in different projects and International Standard Problems, and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups and organisation of conferences and specialist meeting.

The greater part of CSNI's current programme of work is concerned with safety technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment and severe accidents. The Committee also studies the safety of the fuel cycle, conducts periodic surveys of reactor safety research programmes and operates an international mechanism for exchanging reports on nuclear power plant incidents.

In implementing its programme, CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also co-operates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

CNRA/CSNI WORKSHOP ON
LICENSING AND OPERATING EXPERIENCE OF COMPUTER-BASED I&C SYSTEMS
Hluboká nad Vltavou, Czech Republic

25th-27th September, 2001

A Contents

B Programme

C Summary and Conclusions

D Papers

E Participants

A TABLE OF CONTENTS

Page

Volume I

B Summary and Conclusions 11

C Programme 37

D Papers 45

OPENING SESSION:
ADVANCES MADE IN THE USE AND PLANNING OF COMPUTER-BASED I & C SYSTEMS
Chairmen: M. Chiramal - P. Krs

Electricité de France Experience of Computer-based I & C Systems 47
François Poizat, EdF, France

The Evaluation on Applying the Digital Safety System to Existing PWR Plants in Japan 55
Yoichi Mito, the Kansai EP Co., Inc.
Masafumi Utsumi, Mitsusbishi HI Ltd., Japan

Independent Assessment of the Temelin Software Safety System 63
Petr Zavodsky, CEZ a.s., Czech Republic

Regulatory Review of the Digital Plant Protection System for Korea Next Generation Reactor 75
D.I. Kim, B.R. Kim and S.H. Oh, Korea Institute of Nuclear Safety, Korea

Decision Support for Approval of Safety Critical Programmable Systems 83
Gustav Dahll, Bjørn Axel Gran, OECD Halden Reactor Project, Norway
Bo Liwång, Swedish Nuclear Power Inspectorate, Sweden

TECHNICAL SESSION 1:
NATIONAL AND INTERNATIONAL COMPUTER-BASED STANDARDS AND GUIDES FOR SAFETY SYSTEMS 95
Chairmen: J.P. Bouard, Z. Ogiso

International Standardisation in Nuclear I &C Engineering 97
Jean-Paul Bouard, EdF, France

Comparison of IEC and IEEE Standards for Computer-Based Control Systems Important to Safety 109
Gary Johnson, Lawrence Livermore National Laboratory, USA

The New IAEA Safety guide and the Common Position of European Regulators on Software for Systems Important to Safety 117
Pierre-Jacques Courtois, Association Vinçotte Nuclear, Brussels, Belgium

Approach to the Application of the State Regulatory Requirements, Legislation and Standards in Modernization of I &C Systems, Concerning Especially the Digital Computer-Based Systems **129**
J. Zatloukal, P. Krakora, NRI Rez, Czech Republic

Standard Base for Regulatory Activity in NPP I & C Systems Area **139**
V. Goldrin, M. Yastrebenetsky, Yu. Rozen, S. Vinogradskaya
State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

TECHNICAL SESSION 2: REGULATORY ASPECTS **147**
Chairmen: K. Hamar, A. Lindner,

EMI/RFI and Power Surge Withstand Guidance for the U.S. Nuclear Power Industry **149**
Christina Antonescu, USNRC,
Paul D. Ewing, Richard T. Wood, Oak Ridge National Laboratory, USA

Pre-Qualification of Digital Platform - U.S. NRC Regulatory Review of the Common Q Platform **159**
W. K. Mortensen, M. Chiramal

Survey and Evaluation of Digital I & C Licensing Experience **165**
Swu Yih, Chin-Feng Fan, Chan-Fu Chuang

Collecting Data from Operational Experience of Computer-Based I & C Systems - A Regulatory Perspective on Goals and Tasks **177**
G. Schnürer, ISTec, Garching, F. Seide, BfS, Salzgiter, Germany

Digital Projects in the Near Past and their Consequences in Safety Regulations in Hungary **187**
K. Hamar, HAEC, Hungary

Volume II

TECHNICAL SESSION 3
ANALYSIS AND ASSESSMENT OF DIGITAL I & C SYSTEMS
Chairmen: M. L. Järvinen, M. Kersken **11**

Preliminary Evaluation of Computerized Procedures from Safety Viewpoints **16**
Yun H. Chung, Sung N. Choi, Bok R. Kim, Korea Institute of Nuclear Safety, Korea

Modernization of the I & C System for ANP Dukovany by the Use of Computer-based Equipment **21**
F. Dalik, K. Wagner, M. Ris, SKODA, Czech Republic
Jean-Pierre Burel, Schneider Electric, Jean-Paul Mauduit, Framatome-ANP, France

FMEA Performed on the SPINLINE3 Operational System Software as Part of the TIHANGE1 NIS Refurbishment Safety Case **37**
L. Ristord, C. Esmenjaud, Schneider Electric Industries, France

Qualification of Pre-Developed Software for Safety-Critical I & C Application in NPPs **51**
M. Kersken, ISTec, Garching, Germany

A Bayesian Approach to Risk Informed Performance Based Regulation for Digital I & C QA Programs **69**
Swu Yih, Sun-Li Chyou, Li-Sing Wang, AEC INER
Chin-Feng Fan, Yuan-Ze University, Chinese Taipei

TECHNICAL SESSION 4
SOFTWARE LIFE CYCLE ACTIVITIES **81**
Chairmen: G. Dahll, F. Krizek

Implementation of Software Independent Verification Distributed Control and Information Systems and Validation for Lungmen **83**
Jiin-Ming Lin, Jeen-Yee Lee, Taiwan Power Company, Chinese Taipei

Static Analysis of the Software Used in Safety Critical System of the NPP Temelin **91**
Z. Piroutek, S. Roubal, J. Rubek, I & C Energo, a.s., Czech Republic

Assessment Methodology of the Temelin NPP Control System Performance and Quality **99**
Ivan Petruzela, Karel Bednarik, I & C Energo, a.s., Czech Republic

Methodology of NPP I & C System Algorithms and Software Expert Analysis **109**
V.S. Kharchenko, L.M. Lyubchik, M.A. Yastrebenetsky, State Scientific Technical Center on Nuclear and Radiation Safety, Ukraine

TECHNICAL SESSION 5
EXPERIENCE WITH APPLICATIONS SYSTEM ASPECTS, POTENTIAL LIMITS AND FUTURE TRENDS AND NEEDS **119**
Chairmen: B. Liwång - M. Hrehor

Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No. 6 and 7 **121**
Makino Shigenori, Tokyo Electric Power Company, Japan

Technical Requirements on Maintenance of Digital I & C Systems Important to Safety **131**
G. Schnürer, ISTec, Garching, F. Seidel, BfS, Salzgitter, Germany

Requirements Management of I & C System Refurbishment of NPP Dukovany **141**
Jiri Pliska, I & C Energo, a.s., Czech Republic

Licensing Process of the Digital Computer-based I & C Systems to be Implemented Within the NPP Dukovany I & C Refurbishment Project **151**
Ceslav Karpeta, Scientech Inc., Josef Rosol, CEZ, a.s., Czech Republic

Temelin Nuclear Power Plant Westinghouse - I & C Change Process (Paper not available)
Dennis M. Popp, John L. Duryea, USA

E. LIST OF PARTICIPANTS **169**

TECHNICAL SESSION 3:

ANALYSIS AND ASSESSMENT OF DIGITAL I & C SYSTEMS
Chairmen: M. L. Järvinen - M. Kersken

Preliminary Evaluation of Computerized Procedure From Safety Viewpoints

Yun H. Chung[1], Sung N. Choi[2], Bok R. Kim[3]

Korea Institute of Nuclear Safety, 19 Guseong-Dong Yusung-Gu, Taejon, 305-338, South Korea

[1]Tel: +82 42 868 0245, Fax: +82 42 861 9945, e-mail: yhchung@kins.re.kr
[2]Tel: +82 42 868 0241, Fax: +82 42 8612535, e-mail: choisen@kins.re.kr
[3]Tel: +82 42 868 0242, Fax: +82 42 861 1700, e-mail: kimbr@kins.re.kr

Summary

The KNGR is an evolutionary reactor and is under development. This paper briefly describes standard design license system and primary design features of the Computerized Procedure System (CPS) and compares the CPS of the KNGR with other computer-based procedure systems.
From a literature survey and an informal study, we firstly derive the review issues for safe plant operation – safety impact on operation personnel and shift performance, design for situation assessment and response planning, utilization during complex situations including the CPS failure, design for navigation and communication, and software quality. Then we present the preliminary evaluation results.

Introduction

Korean Next Generation Reactor(KNGR) is an evolutionary reactor, which has an official name as Advanced Power Reactor 1400 and is under development. The KNGR is now under preliminary safety review and has a plan of commercial operation in 2010.

The KNGR introduces a lot of brand-new human-machine interface (HMI) design features in nuclear industry of Korea, such as workstation-based control room; Large Display Panel which provides a bird's view of plant condition; the CPS which shows all operation procedures; Soft Controls using touch screen which can control both safety and non-safety components; advanced alarm system using prioritization and filtering.

The standard design license system for APR 1400 requires Standard Safety Analysis Report(SSAR), Standard Design Specification, Emergency Operation Procedure Writing Guidelines, and the design details of Standard Design is expected to the level of design certification documents of U.S. advanced light water reactor. The applicant of Standard Design should establish and submit a verification program to confirm that the as-built facilities of a nuclear power plant (NPP) satisfies both the design and applicable regulatory requirements, during the stage of design licensing review. And the program which is called as DCPVP(Design, Construction, and Performance Verification Program) shall be reviewed by the regulatory body and performed by an applicant to construction or operation license during the stage of construction or operation licensing review. The Certificate of Standard Design will be valid for 10 years (Lee et al., 2001). The KNGR is under the preliminary safety review.

The purpose of NPP procedure is to guide human actions when performing a task to increase the likelihood that the actions will safely achieve the task's goal. In contrast to decision aids, procedures define decisions to be made and actions to be taken (USNRC, 2000). The human factors goals of procedures do not generate an undue task overload and are easy to understand and follow (Niwa et al., 1996). That is the reason why Writer's Guide is an essential component of the Emergency Operation Procedure(EOP) Generation Packages.

Evaluation of Computerized Procedure System

Computerization of procedures in nuclear industry seems to be a design trend as shown in Table 1. Spurgin et al. (1993) described an overview of many computer-based procedure system. Now many nuclear power plants (e.g, Beznau, Chooz B, Civaux, Temelin) use various types of computer-based procedure(CBP) system. The driving forces include the limit of paper-based procedure(PBP) presentation ways, including lack of interactive capabilities between PBP and sophisticated systems, and the high volume and cost associated with paper manuals used in complex and technically demanding environments. (Wourms and Rankin, 1994)

Overview of Computerized Procedure System

The CPS is a computerized operator support system and covers all operation procedures. It provides information through workstation consoles using flowchart and tree structure and also has an automatic checking capability of step logic including continuously applied steps. The CPS however is a passive system. The CPS was developed upon the basis of Computerized Procedure Manual II (COPMA II), which was developed by the Halden Reactor Project.

Table 1. Comparison of Computer-based Procedures

System Name	KHNP CPS	EdF N4 Reactor	Westinghouse COMPRO[1]
Procedure Scope	All[2]	All	EOP
Active/Passive	Passive	Active[3]	Passive
On-line/Off-line	On-line	On-line	On-line
Operation/ Training	Both	Both	Both
User = SS or Operator	Operators with SS[4] overview	Operators with SS overview	SS
System falls?	Paper-based procedures	Paper-based procedures	Paper-based procedures
HMIs	2 CRTs Workstation	2 CRTs	2 CRTs Workstation
Basic structure of main page	Six parts[5]	Three parts[6]	Four parts[7]
Software grade	Non-safety	Non-safety	Non-safety
NPPs	APR 1400, Korea	Chooz B and Civaux, France	Beznau, Switzerland Temelin, Czech Rep.

Note:

1. COMPRO stands for Computerized Procedure
2. All means normal and abnormal procedures as well as emergency operation procedures.
3. Operator can override computerized monitoring. So the human operator must remain in final charge of plant unit operation at all times (Pirus et al., 1997).
4. SS stands for Shift Supervisor.
5. Six parts consist of Menu pane, Continuously Applied Step pane, Postponed pane, Multi-procedure Display pane, Procedure Overview pane, and Current Step pane.

6. Three parts consist of upper, middle, and lower panel. Upper part presents symbols of all the sub-procedures. Middle part presents the main parameter values and special plant system states. Lower part presents the same kind of presentation, but is reserved for support systems monitoring (Pirus and Chambon, 1997).
7. Four parts consist of Pull Down Menus, Parallel Information, Current Procedure Information, and User Prompts (Lipner and Kerch, 1996).

The CPS displays consist of a main screen and a support screen. The main screen has six panes. Those are menu pane, continuously applied step pane, postponed pane, multi-procedure display pane, procedure overview and current step pane, as shown in Figure 1. The support screen can show additional information for the current step on an adjacent screen.

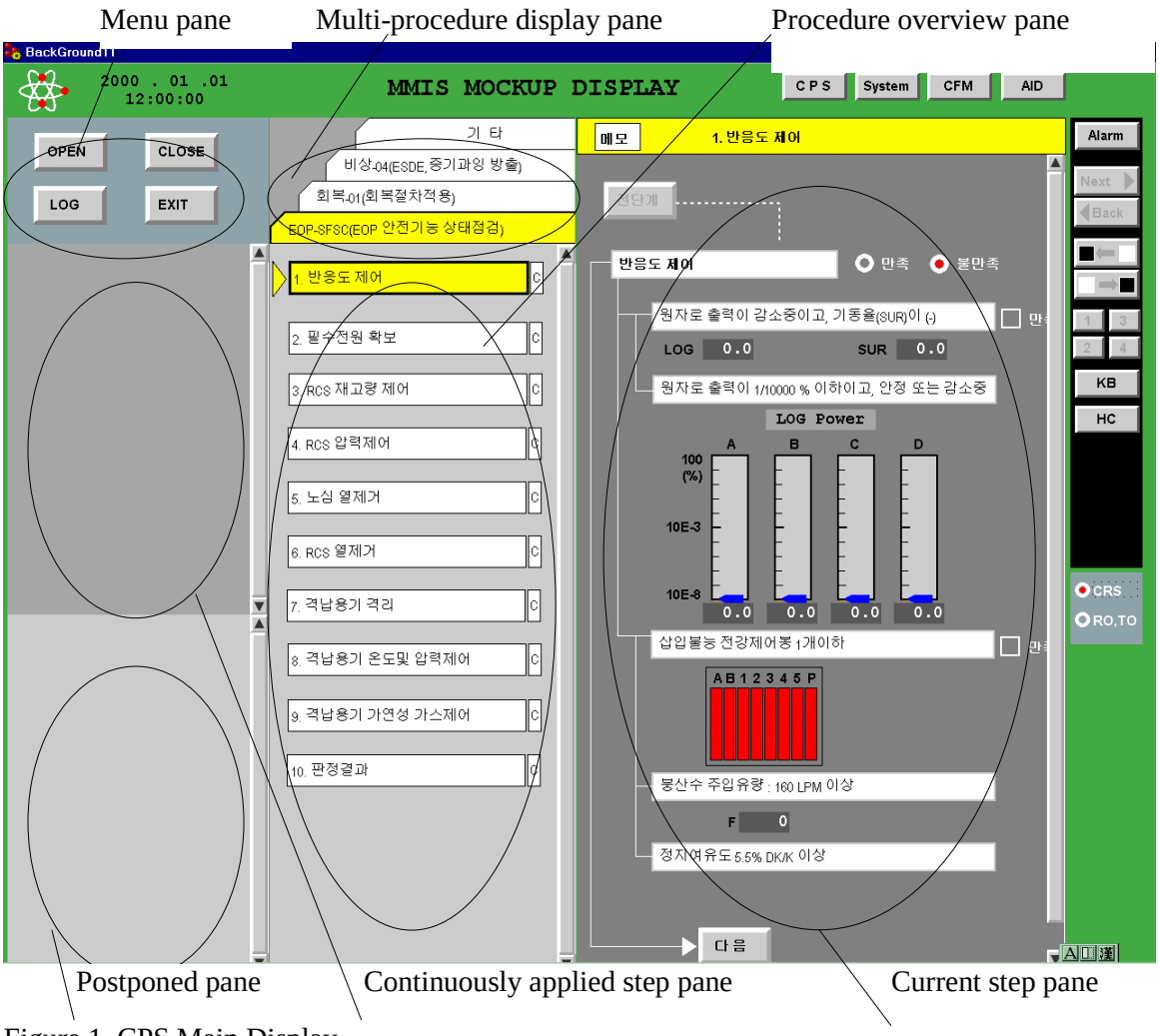


Figure 1. CPS Main Display

Operator (Reactor Operator or Turbine Operator) is able to accomplish plant operation by using only the main screen, but when he wants additional information (e.g., P-T curve, variable trends, etc) in relation to current step, he can use the support screen. The support screen is linked to the current step and appears automatically as the current step changes in the main screen.

All the process information and control components that are cross referenced in the instruction, are presented near the associated instructions so that an operator can easily evaluate the

instruction or confirm the computer's evaluation. The component symbols targets are used to call up the control components in the soft control HMI. All these process information are updated by plant data from Information Processing System. Control commands from the CPS are sent to soft control HMI to select the control component.

The entry condition of current step is evaluated by the computer based on process information. The result of evaluation is dynamically displayed on the instructions of current step pane. So the procedure is no longer static like paper procedures. Even though the CPS shows its evaluation dynamically, operator is able to override the computer's decision and change the procedure flow.

Expected impact of the CPS usage

In relation to expected impact of the CPS, Min et al. (2001) addressed one study that has examined the effect of using the CPS in 2000. One major finding was that there was a dramatic reduction in verbal communication between the supervisor and the two operators. In Korea, while executing an EOP with a PBP, the control room supervisor is supposed to read each procedure step aloud and the corresponding operator should echo the procedure step. The assumption the designers made was that the operators at the advanced MCR would follow the same guideline for verbal communication while executing the procedure with the CPS. Apparently participants did not fully abide by this guideline and the CPS seemingly eliminated inquiry-reply type of communication.

Another finding was about the scope of auto-checking features. Designers emphasized the benefit of providing auto-checking features and showed the tendency towards more auto-checking features. For example, the CPS can execute a procedure step by comparing the set point value with actual process values using the logical relationships specified in the step. This reduces the crew cognitive workload. However, although auto-checking features are a major advantage of the CPS, it creates serious concern. Roth and O'Hara(1998) reported that "on occasion the CPS could provide misleading information or direct the operators down the wrong procedural path." The supervisor put too much trust in the CPS, and called out the wrong actions suggested by the CPS without double-checking. This problem may occur with paper-based procedures, but the CPS aggravates the problem. The supervisor's passive mode of information processing may erode mental model.

Design and evaluation issues of the CBP system

Wourms and Rankin (1994) recommended the design approach from an integrated systems point-of-view which considers the combined influences of software, hardware, interface design, and available techniques on human-machine system performance, the thoughtful consideration of the relative strengths and weaknesses in human information processing, and a smooth transition from CBP to PBP during CBP failure.

Niwa et al. (1996) identified four concerns of using procedures, such as whether operators are able to use the current procedures in a sufficiently reliable way; whether the use of procedures creates additional tasks that deflect effort from main task; whether the procedure in their present form lead to damaging increases in workload; whether the specific format of the procedures constitutes a source or risk. And they suggested six aspects of procedure presentation that can have an impact on above concerns; navigation, formatting, progress in monitoring, help and explanation facilities, process linking, and procedure adaptation.

Roth and O'Hara (1999) described impacts of CBPs, such as team structure and dynamics; ability to monitor and redirect procedures. They specifically classified effect on team structure and

dynamics into the cognitive performance of individual crew members, the functioning of the crew as a team, the scope of responsibility of the different crew members, the communication pattern among crew members, the situation awareness of the different crew members.

O'Hara et al. (2000) suggested general considerations for near-term approaches to CBP systems: the pace control of the procedure and the transitions within and between procedures, support of the high-level awareness of procedure goals and the context, availability of variable levels of detail in procedure steps, automatic monitor of process variables, procedure step completion, and place keeping, careful support of step logic analysis, emphasis of training issues.

US NRC (2000) also raised several human performance issues associated with CBPs. The issues are as follows: methodological and criterion requirements for evaluating CBP effects, role of plant personnel in procedure management, team performance, situation awareness, response planning, and operator error; level of automation of procedure functions; keyhole effects and use of multiple CBP procedures; CBP failure in complex situations; hybrid procedure systems; and specific CBP design features.

From the above literature review and informal study of the CPS, we identified the review issues. Those are impact on operation personnel and shift performance, design for situation assessment and response planning, utilization during complex situations, including the CPS failure, design for navigation and communication, and software quality. The following section describes the preliminary results for each review issues respectively.

Preliminary Evaluation Results

Impact on operation personnel and shift performance

The CPS does not have a capability of automation for decision-making and manipulation to control plant according to operation procedures, but provides information for operator to handle (i.e., finish, delay, pass) each step. So responsibility of decision-making still remains to each operator. The designers took preliminary validation using some scenarios (e.g., LOCA, SGTR) during design phase. However, they did not suggest the evaluation measures for performance of operation personnel and shift. Although the CPS can make information search easy, it needs an appropriate performance measures and the evaluation results as per, which shows the acceptable impact on personal and shift performance.

Design for situation assessment and response planning

The CPS automates error-prone tasks, such as basic step logic determination; monitoring of continuously applied step and entry condition, that can minimize cognitive load on operators. The current step pane contains detailed information (e.g., variable value, component status, note and so forth) in order to accomplish each step. Basic structure for current step is flowchart and tree logic. Operator has to execute some actions to satisfy each instruction. Since the structure is very simple and intuitive, operators are able to understand it easily. It also provides additional information of plant system with Information Processing System (IPS) mimic CRT.

With the improvement of related information search, memory of plant condition, operation support information and recording of execution results, the CPS tries to support the situation assessment and response planning. In addition, the procedure overview pane displays the current step and executed steps using color coding. The design for situation assessment and response planning seems reasonable for

changing operation environment. However, the display method of automated processing, the display space and/or the large number of continuously applied steps remain as an open issue.

Utilization during complex situations, including the CPS failure

When the CPS failure takes place during its use, it does not any longer provide supporting information to operator any more. Then operator has to use the paper procedures, which looks similar to computerized procedures. Just in case, the computer system printed the executed steps when each step completed. It will give a chance to keep track of failed condition. After fast understanding with printed steps, operator can handle an unexpected situation with paper procedures. The design for smooth transition from CBP to PBP seems acceptable. However, there still exists the necessity of the usefulness validation about the design of transition.

Design for navigation and communication

In order to reduce the unnecessary navigation, the CPS has six panes and supporting screen as described before. Specifically for navigation among steps and/or procedures, it contains procedure overview pane, current step pane and multi-procedure display pane. Among these panes, the multi-procedure display pane holds the three most recent procedures which operator opened from the procedure lists. All the other procedures can be accessed by using ?Etc? button at the multi-procedure display pane. Comparing with the COMPRO of Beznau nuclear power plant, shift operators of main control room share the information of the CPS, which can provide an implicit communication tool among operators.

The design for navigation seems acceptable. As for communication issue, the very low level of communication among the crews raises serious concern in many aspects (Min et al., 2001). It may hinder crews from sharing situation awareness. In general, when a group of persons work together to accomplish a common goal, they need a common understanding for the given situation and each other's intentions and actions. In other words, a high performance team shares situation awareness so that a member may find other members error, or even prevent an error (Hutchins, 1995). The low level of communication also eliminates the chance of training on the job. Operators learn the supervisor's role by observing his action and by communicating one another. Therefore the CPS needs the more thoughtful way of communication.

Software quality

The CPS is a non-safety grade information system. That is, the software category of the CPS is "Important to Safety" among four categories (i.e., Safety Critical, Important to Safety, Important to Availability, General Purpose), and will take verification and validation process according to its grade. The "Important to Safety" software is a second grade software whose function is necessary to directly perform alternate protection system control actions or software that is relied on to monitor or test protection functions, or software that monitors plant critical safety functions. The software grade of the CPS is equivalent to that of AP-600 and N4 plants. The software grade and its corresponding V&V plan are acceptable.

Conclusion and Discussions

From the literature survey of design and evaluation documents and an informal study, we found that CBP is a design trend and can support and enhance operator performance effectively. However there exist a few open issues too. That is why the designers need to implement CBP system thoughtfully. This paper addressed five issues for the review of the CPS for safe plant operation, but we will not limit to the review issues that are listed here. This paper also described the preliminary evaluation results. That is, we are on the long way of safety review.

References

Hutchins, E. (1995), Cognition in the Wild, MIT Press, Cambridge, Massachusetts.

Lee, J., et al. (2001), Legislation of Safety Regulatory Requirements for Korean Next Generation Reactor (III-2), Korea Institute of Nuclear Safety (in Korean).

Lipner, M. and Kerch, S. (1996), Operational Benefits of an Advanced Computerized Procedures System, Westinghouse Electric Company

Min, D., Chung, Y. and Kim, B. (2001), An evaluation of computerized procedure system in nuclear power plant, Proceedings of IFAC Human-Machine Systems 2001 (in press).

Niwa, Y., Hollnagel, E. and Green, M. (1996), Guidelines for computerized presentation of emergency operating procedures, Nuclear Engineering and Design, 167, pp. 113-127

O'Hara, J., Higgins, J. and Kramer, J. (2000), Automation of emergency operating procedures: Finding the right balance, Proceedings of NPIC & HMIT 2000

Pirus, D. and Chambon Y. (1997), The Computerized Procedures for the French N4 Series, IEEE Sixth Annual Human Factors Meeting, pp. 6-3~6-9.

Requests for additional information (RAI) and Responses for Standard Safety Analysis Report of the KNGR (in Korean).

Roth, E. and O'Hara, J. (1998), Integrating Digital and Conventional Human System Interface System: Lessons Learned from a Control Room Modernization Program, BNL Report J6012-3-4-5/98, Upton, NY: Brookhaven National Laboratory.

Roth, E. and O'Hara, J. (1999), Exploring the Impact of Advanced Alarms, Displays, and Computerized Procedures on Teams, Proceedings of the Human Factors, and Ergonomics Society, 43rd Annual Meeting, pp. 158-162.

Spurgin, A. and Wachtel, J. (1993), The state of practice of computerized operating procedures in the commercial nuclear power industry, Proceedings of the Human Factors, and Ergonomics Society, 37th Annual Meeting, pp. 1014-1018.

Sung, C. and Jung, Y. (2000), Computerized Procedure System for Korean Next Generation Reactor, Proceedings of NPIC & HMIT 2000

USNRC (2000), Computer-Based Procedures Systems: Technical Basis and Human Factors Review Guidance, NUREG/CR-6634, U.S. Nuclear Regulatory Commission.

Wourms, D. and Rankin, W. (1994), Computer-based procedures, CSERIAC-RA-94-002, CSERIAC.

Modernisation of I&C system for ANP Dukovany by the use of computer-based equipment.

Author: Jean-Pierre BUREL (Schneider Electric)
Co-author: Frantisek DALIK, Karel WAGNER (Skoda-JS), Miroslav RIS (Škoda Energo), Jean-Paul MAUDUIT (Framatome-ANP)

Abstract

The original safety and control systems of Dukovany NNP will be replaced by new digital systems. For safety systems (category A according to CSN IEC 61226) the SPINLINE 3 Technology developed by Schneider Electric and Framatome ANP is used. For some systems important for safety (category B), the computer based system Škoda is used. Both technologies, already implemented on several reactors in different countries over the world, are well suited for modernisation projects and have been yet used for these ones. They give the opportunity to reach the latest safety requirements governed by international and national standards.
This paper describes these technologies, the architecture and the main features of the new I&C systems, especially safety systems. The consequences regarding safety and operability are considered.
The computer-based systems used for information systems (category C) are not mentioned in this paper.

Implementation of New Digital Safety Systems on Dukovany NPP

1. INTRODUCTION

The fundamental trend of the technology for automation has a high changing rate. The components on the market become more and more fast and complex. They allow better performances and a better efficiency in system operation. The use of computers to operate industrial plants and factories becomes general and Nuclear Power Plants have the same evolution.

Safety systems for Nuclear Power Plants are governed by strong requirements, which cannot be fulfilled by products designed for normal industrial applications. That's why in all countries, safety classified systems and non-safety classified systems for NPPs use different technologies even if the classification standards give several definitions and gradations for systems.

In co-operation with Framatome ANP, Schneider Electric has developed a technology dedicated to safety systems. This digital technology called SPINLINE 3 results from the experience obtained by Schneider Electric after more than 20 years on digital safety systems for Nuclear Reactors.

For the management of the Control Rod Drive Mechanism System for the reactors VVER-1000 operated in Czech Republic and in Ukraine, a computer-based system has been developed in Škoda and is in operation since 1996 on the South – Ukraine NPP and then in Chmelnická NPP and Temelín NPP.

The modernisation of I&C safety systems of the Dukovany NPP is based mainly on the SPINLINE 3 technology with the active participation of Czech companies like ŠKODA-JS and ŠKODA ENERGO, I&C ENERGO and •EZ. This project is now in progress. The first implementation of new safety systems is foreseen for the Unit No. 3 of the Dukovany NPP during the years 2002 - 2005.

2. CHARACTERISATION OF THE SAFETY SYSTEMS FOR NPPs

In the context of NPPs, the differences between „ Safety systems „ and „ Industrial systems " concern, for safety systems, the guaranty of operation in all circumstances, even in case of failure or after an accident like a limited fire or an earthquake.

An „ **Industrial system** " needs to be efficient in term of performances and in term of costs. The development has to be easy and the time for design and for implementation must be as short as possible. The consequences of a possible failure can be acceptable even if it is not desired.

A „ **Safety system** " has more or less the same requirements regarding performances and costs, but it has to be primarily capable to operate in any time and in any conditions. That is the fundamental difference and the main issue is to reach a reasonable proof of it. This guarantee of operation is of the highest importance. It is not acceptable to have a faulty system when a protective action is required.

3. TECHNOLOGY

3.1 SPINLINE 3 Technology

SPINLINE 3 is a digital and modular solution, which covers all safety functions and all functions important for safety, from measurement acquisition to actuator control, mainly:

- Reactor protection (reactor trip and associated engineered safety features, diesel load sequence),
- Reactor control and limitation,
- Nuclear instrumentation.

The main featuring objectives of the SPINLINE 3 technology are:

- A technology, which complies with safety requirements for NPPs (national and international standards).
- An efficient, fast and industrial development methodology
- A long term guarantee for maintenance and spare parts, more than 25 years
- Easy operation and maintenance,
- State of the art performances

The SPINLINE 3 technology can be described from a combination of three major components: The system, the hardware, and the software.

3.1.1 The System

A system built with the *SPINLINE 3* technologies is a combination of several units, which perform functions following strict safety performances. The achievement of these safety performances is obtained by following a development methodology, which includes the design of the architecture, the validation of probabilistic safety assessment, the qualification of the design with accuracy and response time.

With the *SPINLINE 3* it is possible to design small and large distributed safety systems, with an adequate redundant architecture.

A safety system has to comply with various criteria, some typical can be listed:

- Fail-safe architecture: *SPINLINE 3* assures that the outputs controls to actuators are always valid or in a safe position in case of failure.
- Fault-tolerance (including single failure criterion): *SPINLINE 3* can meet any redundancy requirements.
- Functional diversity: can be implemented to defend the system against common cause failures.
- Functional insulation: by avoiding propagation of failures between redundant divisions and individual system of different categories.
- Determinism: for all types of processing, the same inputs produce the same outputs with a guaranteed response time.
- Easiness of operation and maintenance.
- Flexibility for further evolution without any hardware modification.
- Modularity: *SPINLINE 3* can be delivered either as racks to be integrated into existing cabinets (for refurbishment purposes) or as whole cabinets.
- Scalability: *SPINLINE 3* fits various sizes of I&C systems. It can be used for highly distributed architectures such as a reactor protection system, distributed processing for acquisition, function processing and vote.

SPINLINE 3 meets international standards (IAEA, IEC) and various national standards for the design of nuclear safety I&C system.

3.1.2 The Hardware

The *SPINLINE 3* hardware is a set of modular components, designed, manufactured and qualified specifically for safety applications in nuclear reactors. These components are cabinets, racks, electronic boards or modules and cabling elements between components. They are designed, manufactured and qualified according to nuclear requirements and standards.

The wide range of I/O boards and their capacity allows *SPINLINE 3* to fit any safety nuclear application needs for control. The use of powerful CPU boards and high speed networks gives short response times even for complex functions and, above all, the response time is guaranteed by the deterministic features of the *SPINLINE 3* components.

The hardware components include:

- Cabinets and 19" 6U racks. Cabinets and racks are designed to withstand harsh conditions e.g. temperature, EMI, vibrations, earthquake as defined in relevant standards,
- A full range of input and output boards for binary and analogy data, neutron instrumentation, thermodynamic instrumentation, actuator control,
- A 25 MHz 68040 Motorola microprocessor CPU board, with 2 megabytes of secured read only flash, 2 megabytes of RAM and 64 kilobytes of non-volatile EEPROM memory. This board can provide up to 4 NERVIA interfaces,
- High speed deterministic 1E network: NERVIA is a 10 megabit/s, broadcast type, token ring network. The medium is either optical fibre or shielded cable with twisted pairs of wires. It is used for communications within the safety system or for communications with non-safety units. Both NERVIA hardware and software fully comply with class 1 E requirements,
- Actuator network: The 1E actuator network is based on a master/slave protocol and uses many of the NERVIA network components. It is dedicated to safety actuator control needed for example for the Engineered Safety Features,
- Interfaces to the PC world via the NERVIA network. *SPINLINE 3* may also interface with other analogy or digital systems using networks, serial data links or wire-to-wire links.
- The NERVIA network is the standard communication link within the safety system.
- It provides safe and efficient data exchange among units. It is based on a broadcast protocol i.e. any message sent by one unit is received simultaneously by all the other units of the network. Data is exchanged within consistency blocks and secured by CRC checksum.
- A processing unit can communicate with other units through one to ten NERVIA networks.
- One NERVIA network can link up to 30 different units.
- A PC NERVIA board, installed in PC, allows communication between 1E equipment and other equipment.
- Other data links.
- Gateways are available to Ethernet networks and can be developed to other networks if needed, either on a processing unit or on a standard PC.

Cabinets comply with the IEC 60529 standard: « Degrees of protection provided by enclosures (code IP) », protection index IP22 and are qualified under seismic stress. They receive power supply, racks, fans, input/output cabling interfaces, internal wiring and display devices.

3.1.3 The Software

The *SPINLINE 3* software of each digital unit is developed by using a set of tools and procedures dedicated to nuclear safety software developments. The software tools are based on a „ System and Software Development Environment (SSDE) “ named CLARISSE, which allows developing a complex multi-unit processing system. CLARISSE is standardised and is delivered as an independent software package. It provides the software tools a libraries needed to perform *SPINLINE 3* configuration and the application software development.

Any *SPINLINE 3* software is a combination of two parts:

- The **system software** is standard and comes as a software component to be used on the CPU boards of the processing units. It is ready for use after a simple configuration to fit the needs of the customer I&C systems. It provides basic functions like communication, data acquisition or services to be used by the application software.
- The **application software** is specific and may be developed either by Schneider Electric, by an engineering company or by the customer himself.

The **system software** is a software layer with a minimum complexity that mainly achieves the interface between the local and remote data delivered by the I/O and communication link boards and the application software.

It also tests continuously the hardware and provides services to the application software.

The system software has been developed and validated according to nuclear standards for software based 1E safety systems, mainly CSN IEC 60880, CSN IEC 60880-2.

The adaptation of the system software to the application needs is done, using the processing units and networks configuration tool of the CLARISSE System and Software Development Environment.

The **application software** performs the functions linked with the functional diagram and the operation of the system.

The main features of the application software are the following:

- *Dataflow organization*: the program is entered as a set of boxes connected by wires, flowing from the input data on the left to the outputs orders on the right. The wires convey data according to data types; the boxes transform data by means of Boolean operators, numeric operators or by means of functions. All loops in the layout are precisely controlled using the „previous„ operator.
- *Top/down design*: The application program starts with an upper level view and proceeds through refinement steps for both the functions and the data. Relevant details are added at the appropriate level (information hiding concept).
- *Single task*: the application program associated with the system software runs as a single continuous program loop. One loop execution is called a scan. Every scan, outputs are computed from a fixed image of the inputs and from relevant results of the previous scans. There is no processing done under interrupt and no multitasking. These avoid potential deadlocks, resources sharing and overload problems. It helps demonstrating the fulfilment of the response time requirements as well as the simplicity of the software design.

- *Synchronous approach*: the application program is designed to meet the synchronous hypothesis i.e. the program shall react instantaneously to input events. The hypothesis is fulfilled when the processing is always performed within the scan time allocated to the unit. The *SPINLINE 3* CPU board offers enough computing power to fit the processing needs of typical I&C protection functions in the nuclear field. Moreover, the dataflow organisation of the program makes the CPU load quite independent from the actual values of the inputs.

The development of the **application software** takes place in a classical lifecycle-based development process, starting with system requirements and ending with validation and commissioning tests.

The software design and coding phases are made easier and safer due to the use of CLARISSE SSDE.

The main *SPINLINE 3* application software development benefits:

- There is no longer software design and coding phases involving manual and error-prone activities. The software architecture comes with the product with all the properties needed for the intended type of application (i.e. safety protection I&C).
- As the SCADE language is close to automatism, process engineers can easily review the unit functional specifications and hence, they can help getting the right functional specification even at the detailed software specification level.
- In order to fulfil specific functional requirements, the development of elementary functions, using a high level programming language is possible. The development of elementary functions is performed, using a dedicated V development-cycle on the CLARISSE SSDE.

The CLARISSE System and Software Development Environment (CLARISSE SSDE) are available for the specification, design, coding, and validation of I&C systems. It runs on a UNIX based workstation (typically a Sun SPARC station under OS Solaris). The CLARISSE SSDE provides the followings functions:

- Description of the I&C architecture and processing units: This description is used to automatically configure the system software, the networks stations and the messages exchanged among the units.
- Input have the I&C functions: I&C functions are described, using The SCADE formal language. This language provides block diagram formalism with a rigorous graphical and textual syntax and a well defined semantic. It is easy to learn and to use by technical staff involved in I&C project. SCADE is user-friendly and does not require specialized programming skills: the I&C application is described in the same way as non-software based automatism. The verification and validation process does not require software skills and is therefore simpler.
- Simulation of SCADE specification: the simulation is possible since the early phases of the application design. It allows designers to check the actual behaviour of their specification. The simulation capability can also be useful during the test and validation phases, to perform additional functional tests on the final specification.
- Automated code generation: The SCADE specification is translated into understandable C code. This C code is then compiled, assembled and link-edited. The resulting binary code is either downloaded to the target CPU boards (development phases) or loaded into read-only memory components (for operation). For safety purpose, on line downloading or modification of software is not possible on the units, once in operation. The software is secured in write-protected memory with both physical and electronic identifiers. During operation, only user-defined parameters, which have been declared as modifiable, can be changed, either locally or through a NERVIA communication.

- Verification and validation of each steps of the software design using appropriates tools.
- Documentation production: Most of the documentation is automatically generated.
- Software configuration management.

3.2 The Skoda Technology

3.2.1 The System

This system is an industrial microcomputer-based system with an user program support SoFIC (Software for Industrial Controller) implementing control algorithms primarily of logical and regulation character. The use of efficient communications enables to build remote complexes ranging from middle to large control systems.

The special parts of the system are units executing functions connected directly with the VVER reactor technology.

The system technology is designed such to meet requirements for long-term reliable operation, permanent keeping all functional parameters, easy operation and maintenance.

Methodology of the system design is in compliance with normal industrial standards meeting simultaneously requirements for the safety- related systems in NPP.

3.2.2 The Hardware

The hardware components are cabinets, racks, electronics modules and cabling accessories. Cabinets and racks are designed to withstand environmental influences as defined in relevant standards (including seismic, EMC etc.). Group control level processor module is based on Intel 486 processor. The module is provided with 16 MB RAM, 512 kB Flash EPROM and 512 kB SRAM. Individual control processor modules are based on Intel 80C196 series microcontrollers. Basic system communication is the RDD (Remote Distributed Data) communication based on a RS485 serial bus with the transmission speed of 0,5 MBaud. The message transmission is based on the „flying master – token passing access„ with the synchronous SDLC message format (secured by CRC). The RDD is deterministic broadcast type communication with redundant arrangement in critical applications.

3.2.3. The Software

The basic system software integrates environment for loading, saving, initiation, debugging and operating user control algorithms. Due to its design, the system software directly supports modular programming and enables the user to utilize resident library containing functional elements, blocks and services for communications control. The operation history oriented system seems to be an advantageous instrument, which enables the storage and reviewing of selected system and user defined events.

The system basic tool of application program module development is a language PL/C (Programming Language for Controllers) having features of higher structured program language. The PL/C language describes all program and data objects at a symbolic level. The PL/C language together with the system software architecture support the following main principles:

- Transparency of programming through structuring of user control tasks to modules.
- Symbolical handling with objects by using large resident library of functional elements, blocks and services.
- Predefined names of variables and constants having global validity in a specific controller (at the RDD communication at a specific network).

- System reliability supported by a development policy of the application software, system support security and testing as well as Watchdog system for system run security.

The process of the application software development complies with requirements of relevant standards (primarily CSN IEC 60880).

4. THE SAFETY

4.1 The Safety Of SPINLINE 3 System

One of the major interests of a *SPINLINE 3* systems is the high level reached regarding the safety performances. The safety is built from several fundamental characteristics: the Deterministic behaviour, the Separation between safety parts and the fully Safety oriented design.

4.1.1 Deterministic behaviour

SPINLINE 3 deterministic behaviour is a key feature in order to meet response time requirements and to avoid overload situations.

It is based on the following characteristics:

- Software units run cyclically and sequentially

  A unit cycle (scan) is composed of the following steps:
  - Self-monitoring,
  - Cycle time management,
  - Data acquisition,
  - Application processing,
  - Data output,
  - Local terminal management.

  The steps are always executed in the same order. The scan time of each unit is fixed and monitored, and then the unit response time is bounded and guaranteed.
- Software units do not make use of interrupt driven tasks or algorithms based on dynamic memory allocation.
- NERVIA networks run cyclically and sequentially
- A network cycle (scan) consists in:
  - A token is circulated through all the network stations according to a pre-defined order,
  - A station is allowed to transmit its data on the network only when it owns the token and within a specified time window.

  The network response time is bounded and guaranteed The scan time of each network is fixed and monitored. The network stations are always scanned in the same order.

- Exchange of data among units through networks are pre-defined and systematic:
- All inter units data exchanges are configured in fixed tables.
- System response time. The maximum response time for a system is established using the max response time of each units and networks. The *SPINLINE 3* determinism guarantees that I&C outputs will always be delivered within the computed maximum response time limit.

4.1.2 Separation

The separation between redundant divisions or channels is achieved by separate locations for redundant parts of the equipment and electrical isolation for communications.

Using some specific features performs the functional separation between units regarding the communications:

- Inter-units communication through NERVIA networks, using optic fibres implements electrical separation and geographical separation within the plant.
- Asynchronous behaviour of units and networks neither at the hardware level nor at the protocol level. This avoids the risk of multiple units hangs due to the failure of a single unit or network. The operation management of redundant units is easier thanks to the fact that networks work independently of the status of the connected units and units work independently of the status of the connected networks.
- "1E units / non 1E units" are separated:
  - Non-1E units shall be clearly separated from 1E units. Nevertheless, non-1E units may have to exchange data with 1E units. *SPINLINE 3* makes it possible, thanks to the safety properties of the NERVIA network. These properties ensure that non-1E units can never prevent 1E units from performing their safety function.
  - Non-1E units may act as observers only: These units can only read the data available on the network but they cannot emit data on the network. They cannot interfere with the 1E functions.

4.1.3 Safety Oriented Design

SPINLINE 3 hardware and software components have been designed specifically to design safety I&C systems. They include appropriate features to defend (i.e. detect and act) against failures, which may occur inside the system, due to causes coming from inside or outside the system. *SPINLINE 3* safety-oriented features are given hereafter:

- Each data processed by SPINLINE 3 is associated with „validity„ information.
- Each unit monitors its related units and networks and takes appropriate actions in case of failure or error detection.
- Output controls from the system are set in a safe status in case of internal hardware failure detection, loss of power supply, or detection of IC scanning disruption,
- The CPU clock is monitored against possible frequency drift.
- The system software includes appropriate defensive programming to make sure that there are no inconsistencies in the control and data flows. The detection of any inconsistencies would result in a CPU stop.
- The application software can include consistency checks and properties assertions in order to defend against possible design or operation faults.

4.2 The Safety of Skoda Technology

The system design of the SKODA technology includes in principle the same characteristic as the SPINLINE 3 system.

The deterministic behaviour is the fundamental system characteristic and to be attained, basically the same means are used as with the system SPINLINE 3.

Though the system separation is not designed in such a range as required for safety systems, all I/O signals are galvanically separated inclusive redundant system communications. Signals representing connection links to the safety system are galvanically isolated even between each other.

Within the system design, also principles supporting achievement of maximum safety behaviour of the system in the event of detection of failure in input data or proper failures are incurred.

5. INTRODUCING THE NEW SAFETY SYSTEMS FOR DUKOVANY PROJECT

The main motivations for the replacement of safety I&C systems are the following:

- Availability of spare parts
- Improvement of safety by implementation of new functions
- Consistency with international standards
- Reduction of the costs of plant operation

The objectives of such a modernisation are the following:

- To guaranty performances in term of safety, reliability and technical performances. This implies the use of a qualified system with adequate features like redundancy and diversity.
- To reduce the number of sensors.
- To reduce the time between periodic tests.
- To minimise the costs for maintenance: powerful diagnostic functions to simplify the time to repair and a short time to perform the periodic tests.
- To be adaptable with the existing installation. It means to be compatible with the parts of the existing system, which are not modernised.

5.1 The existing systems to be modernised

The existing systems (important for safety, categories A and B) to be modernised are the following:

- EX-CORE: The Nuclear Instrumentation System corresponding to previous AKNT
- RTS: The Reactor Trip System corresponding to the HO-1
- ESFAS: The Emergency Safety Features Actuating System corresponding to the SOB
- RLS: The Reactor Limitation System corresponding to the HO-3 and ROM
- RCS: The Reactor Power Control System corresponding to the ARM
- RRCS: The Reactor Rod Control System corresponding to the control part of SORR
- ELS: The Emergency Load Shedding corresponding to the APS
- SAS: The Support Action System corresponding to the TOPG

Additionally, a new system PAMS, Post Accident Monitoring System will be introduced (as the category A) on the basis of the FRAMATOME/VME technology.

Also the systems of category C are modernised by computer – based technologies, but are not described in this paper. There are namely:

- SGPS: Steam Generating Protection System corresponding to the LOPG
- PCS: Process Computer System corresponding to the URAN
- IN-CORE: IN-CORE Measurement System corresponding to the SVRK (Hindukus)

5.2 The CONCEPT, main requirements

The design of the new system is based on fundamental requirements, which are the results of a safety analysis performed under the supervision of •EZ technical team. Some of the most important requirements are the following:

- Three divisions instead of two for the reactor trip
- Integration of trip and ESFAS
- Sharing the sensors between the different systems (RTS, ESFAS, PAMS etc.) and sharing digital outputs between the three divisions.
- Taking into account the need for diversity to reduce the risk of Common Mode Failure.
- The cabling to the actuators is kept, including the 220Vdc for control
- Installation to be executed during normal outages
- Parallel operation of new safety systems during one year
- All the safety sensors and their cables are replaced
- Limited number of modifications in control rooms and new procedures

5.3 Building the architecture of the new system

The new safety system is built by following a classic method, starting from the protection functions: These functions concern the trip and ESFAS. Two levels are considered:

- The acquisition and processing level
- The voting and actuation level

Acquisition and Processing level: Acquisition, digitalisation and processing the parameters in three independent divisions. The Digital Instrumentation System (DIS), which receives all the measurements, covers this level: The functions of the DIS are the following:

- Acquisition and digitalisation of signals from sensors: this includes:
  - Temperatures (TCs and RTDs)
  - Pressures, levels, flows
  - Neutron measurements (pulses and wide range current)
  - Binary inputs from switches
- Processing the signals to make calculations and comparison to setpoints
- Transmission and communication between the units by using NERVIA, a network designed to achieved the safety requirements in NPPs.
- Communication with external systems based on an open industrial network, typically Ethernet.

Voting Logic and Actuation level: Inside each division, equipment performs a 2oo3 voting logic and produces controls for all safety actuators and for the trip system. This level is covered by the Digital Reactor Protection System (DRPS). Actuator signals are treated with a high level of reliability by using a dual control concept to reduce the risk of spurious actuation and to allow the test during the operation.

Communication between safety units is based on three independent safety networks (NERVIA) based on a fibre optic technology, one for each division transmit the results of the comparison to the setpoints from the processing level to the actuation level. These networks are also used to send data to other systems, including to the PCS computer via two gateways: the Interface and Display Management System (IDMS).

To improve the resistance to the risk of Common Mode Failure, diversity is implemented.

- Each PIE is addressed by two parameters, each processed by two separate digital units, giving two Lines Of Protections (LOP A and LOP B). That is why inside each division, four digital units process all the parameters needed for TRIP and ESFAS.
- Each division of the DRPS is divided in two sets. Both sets control the ESFAS actuators of the division. Each set of a DRPS division controls respectively a set of TRIP breakers performing a 2oo3 voting logic from the three divisions. This structure provides a diverse protection system.

A specific NERVIA network connects the three DRPS divisions to the IDMS in order to transmit the internal parameters for diagnostics, supervision or transfer to the Process Computer System (PCS).
The role of the power supply to guarantee the ESFAS actuation is fundamental. To respect the original design, each division has an Emergency Load Shedding System (ELS) to start a diesel generator.
To limit the number of reactor trips, each division is equipped with a Digital Reactor Limitation System, separate from the DRPS but located in the same cabinets.
Two other systems are connected to the protection system: The technological protection of steam generators and its peripheral functions are included in the SAS function. The Reactor Control System (RCS) performs the regulating function to operate the reactor in a predefined diagram according the power of the reactor. This system replaces the existing ARM function.

Optimised structure of a new **Reactor Rod Control System** (RRCS) is a result of functional analysis and arrangement of the existing equipment. The RRCS is divided in two basic levels:

- The level connected with reactor drives consists of Motor control cabinets connected to motors (drives) of control rods and Position evaluation cabinets connected to LD-1 sensors. Also Position rough indication cabinets located on the main and emergency control rooms belong to the level.
- Control and information level consists of Group and individual control cabinets, Monitoring and diagnostics cabinets and equipment of Operator's console.

Cabinet arrangement and subsystems housed therein are performed in such a way that dimensions of the new cabinets comply with initial dimensions of cabinets and contain identical number of subsystems performing the same basic functions as the original systems providing, however, all advantages of the modern technology. Using this experienced approach when replacing the original system with new one provides for quick and safe implementation even during such short time as planned (only outages for refuelling).

Individual subsystems are interconnected by redundant communication links RDDCU ŠKODA (RS485 Interface). Communication system contains three independent redundant lines.

5.4 Operation of the new safety systems

The technology of **SPINLINE 3** offers various possibilities to support the operation of the system:

- **On-line diagnostics** to identify and locate all detected failures. This function allows a short time to repair the system.
- **Test without stopping the operation**: Due to the architecture of the system, the test of a unit inside a division is possible by keeping the division in operation.
- **The use of Automatic tester** gives a great advantage to reduce the costs for maintenance. The tester is based on a computer, which manages some specific interface components or modules to generate test signals, which replace the input signals of the tested unit.
- **First cause identification**, this function is important to address the time sequence of an accident for analysis. It is performed in the IDMS to select the first decision to start a protective action.

- **Display management.** The system is able to manage the displays in the Main Control Room and in the Emergency Control Room.

The **RRCS system** performs the following main functions during operations:

- **Control rods movement** (manual/automatic mode)
- **Control rods position** measurement and indication
- **Individual and group rods control**

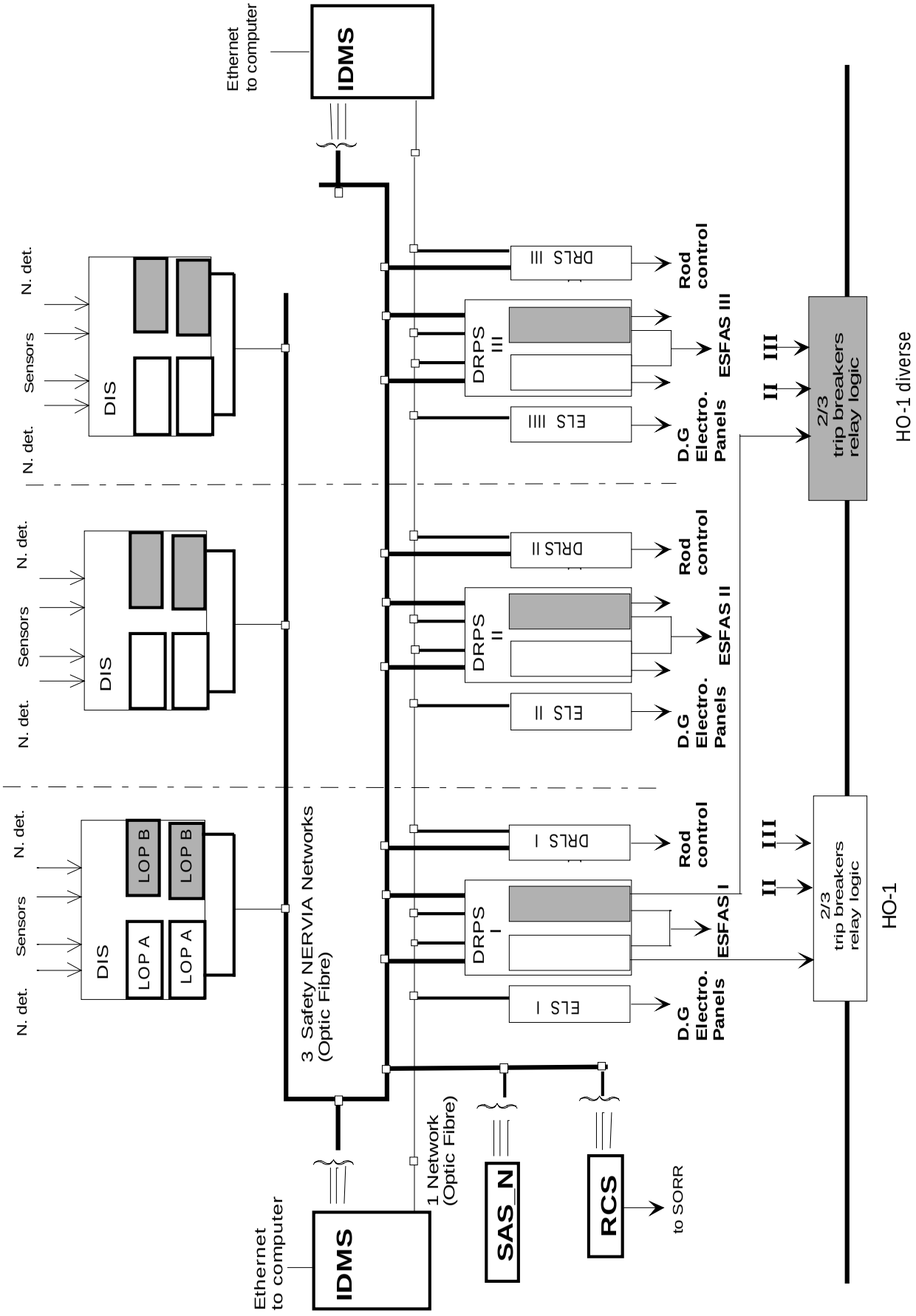
  One part of RRCS is dedicated to measure and monitor other important internal signals for diagnostic and maintenance purposes. In this case it possible to perform following additional functions:
- **Failure detection and its signalisation** occurred within the RRCS system and received either by means of binary inputs or via communication links from other parts
- **Collection, pre-processing and displaying** of measured data and control signals
- **Archiving of selected data** and failure reports
- **Display, evaluation and archiving** of important data while testing individual derives or driving groups on the reactor
- **Test report** printouts
- **Checking for functionality** of all microprocessor units of the RRCS system through data verification procedure
- **Sending failure** signals to MCR
- **Display of data tables** received from individual parts of the equipment as per operation personnel choice

6. CONCLUSION

The project of I&C modernisation in Dukovany NPP is in progress. The new safety systems are based on the latest technology developed by Schneider Electric in co-operation with Framatome ANP to produce any kind of safety systems for NNPs.

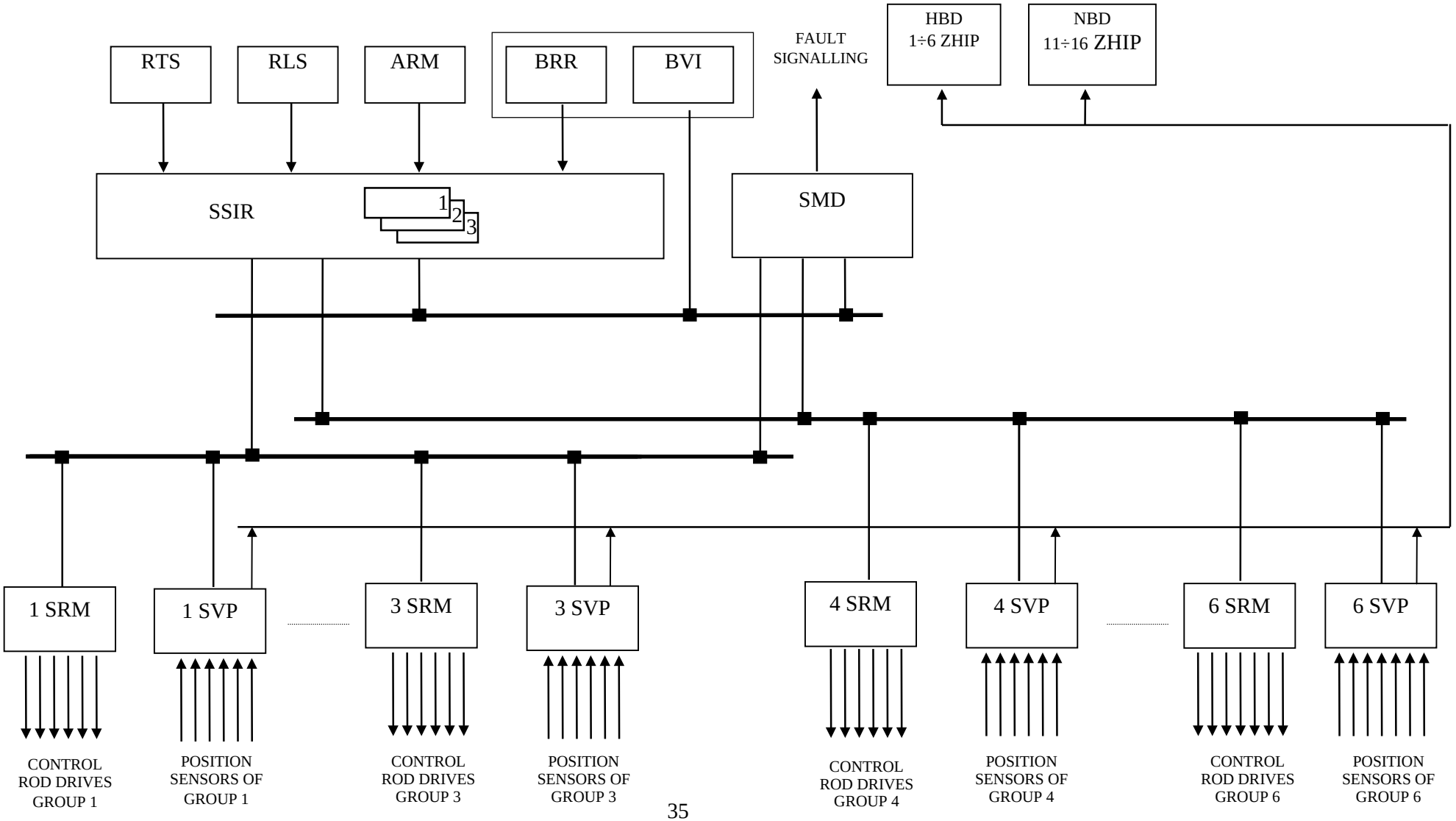
The RRCS as a system important for safety is based on the industrial state of the art system proven for five years on several Nuclear Power Plants of VVER type.

The detailed design is starting and the first system implementation on site is planned to be done in 2003.
The new system will be operated in parallel with the existing system between 2004 and 2005.
The final operation with the new system on the first unit will start in 2005.
The last unit will be modernised in 2009.



GENERAL ARCHITECTURE OF THE SPINLINE 3 SYSTEMS

GENERAL ARCHITECTURE OF RRCS system



FMEA Performed on the *SPINLINE3* Operational System Software as part of the TIHANGE 1 NIS Refurbishment Safety Case

L. Ristord [1], C. Esmenjaud [2]

[1] *Schneider Electric Industries M3 38050F Grenoble France*
Tel.: +33 476 606 827, Fax: +33 476 606 462, e-mail:laurent_ristord@mail.schneider.fr

[2] *Schneider Electric Industries M3 38050F Grenoble France*
Tel.: +33 476 605 860, Fax: +33 476 606 462, e-mail:claude_esmenjaud@mail.schneider.fr

Summary

This paper introduces the SPINLINE3 technology and TIHANGE 1 the NIS project.
It then focuses on the specificity of FMEA performed on software. It points out the benefits of this analysis and also some of the limitations and possible developments. It also gives characteristics that, if present in the software, help the analysis and the defenses.

It takes as an example the analysis performed on the Operational System Software of the Schneider Electric safety digital generic platform SPINLINE3.

Introduction

Schneider Electric has been designing and manufacturing I&C solutions dedicated to the implementation of safety and safety related functions in nuclear power plants for more than 25 years. The first solutions were non software-based. Since 1980, software-based safety solutions have been successfully developed and used.

Building on the I&C components developed for the EDF N4 1450MW PWRs, Schneider Electric and Framatome have developed a safety generic digital platform called *SPINLINE3*, dedicated to the implementation of safety I&C functions in new plants or for the refurbishment of safety equipment in existing plants. *SPINLINE3* has been available since 1997 and has been successfully used to implement category A safety functions on several projects for new reactors as QINSHAN phase II PWR plants in China and for refurbishment projects as KOZLODUY VVER plants in Bulgaria, and FESSENHEIM and BUGEY 900MW PWRs in France. *SPINLINE3* has been chosen to refurbish the TIHANGE 1 Nuclear Instrumentation System (NIS) and the safety I&Cs at the four DUKOVANY VVER 440/213 units.

The architecture of most of the safety systems implemented by Schneider Electric and Framatome includes a redundancy of identical I&C channels, i.e. using the same hardware and software design. When performing safety analyses on such architectures, software is identified as a potential source of Common Cause Failure (CCF).

Defense against CCF due to software within one system is usually based on diversity measures taken at plant or system level or on reliability of the software at system level. Where the “software reliability” argument is claimed, the demonstration shall provide sufficient evidences that the software is free of defects that could lead to CCF. The claim of “error free” software is generally not possible to demonstrate, due to impossibility of exhaustive testing and limitations within formal proof processes.

Performing a FMEA on the software is a mean to narrow the scope of the demonstration by finding out the software components that may, if faulty, lead to a CCF. It is then easier to show, either that those software components are error free or that the postulated component failure modes will be detected and will lead to a safe position. This analysis has been performed on the Operational System Software and on the Application Software for the new TIHANGE 1 Nuclear Instrumentation System (NIS).

Main features of the SPINLINE3 technology

Introduction

Nuclear safety I&C systems have to meet demanding functional and non-functional objectives. They need high reliability and quality of components as well as good properties of architectures such as deterministic behavior, fail-safe and fault tolerant features, functional diversity, and separation. Furthermore, these systems should avoid unnecessary complexity and prevent when possible, operator and maintenance errors. In addition, safety I&C systems shall meet the other customer expectations such as modularity, scalability, flexibility, ease of operation.

Th*e SPINLINE3* technology possesses the features essential to design and implement safety I&C systems fitted to the customer requirements and compliant with national and international nuclear standards and regulations.

SPINLINE3 concepts and design criteria

SPINLINE3 provides a set of mechanical, electronic and software components consistent with the following concepts and design criteria:

Deterministic behavior

SPINLINE3 architectures are designed using two kinds of basic components: Processing Units (PU) and data links. Theses basic components are combined to implement multi channel architectures with distribution of treatments and redundancy of data links where relevant in order to meet the functional and non-functional requirements. The properties of the processing units and data links ensure a deterministic system behavior with bounded response time for the functions under any load conditions.

*SPINLINE*3 architectures may be modeled as a set of synchronous (i.e. cyclic) components exchanging data through non synchronized interfaces. The European project CRISYS (CRitical Instrumentation and control SYStem) has shown that, for application functions such as those needed for reactor protection, a *SPINLINE*3 architecture has the same deterministic behavior as a single synchronous processing unit.

Failsafe and fault tolerant features

SPINLINE3 failsafe and fault-tolerant features allow the design of I&C systems compliant with the single failure criteria. Failsafe features are part of the component design. For instance, to control trip and ESFAS safety actuators, *SPINLINE3* provides actuators boards with 2oo2 votes between two processing units. Any detected failure within the board itself or in the related processing units will result in a predefined output toward the actuator. Fault tolerance features include both fault detection mechanisms within and outside the basic components, and the ability to design adequate redundancy in the system architectures.

Functional diversity

SPINLINE3 features ease the implementation of functional diversity, by allowing distribution of diverse treatments in separate processing units. The high quality of *SPINLINE3* hardware and software components makes other types of diversity non necessary, resulting in systems simpler to design, operate and maintain.

Physical and functional separation

SPINLINE3 data links are mainly implemented through safety networks: *NERVIA* networks and *ACTUATOR* networks. The use of optic fiber allows implementation of clear geographical and electrical equipment separation within one system and between systems. The *NERVIA* network can link 1E units and non-classified units implemented for instance in industrial PCs. The *NERVIA* protocol ensures that any unit on the network can read data from data areas of other units but can only write in its own data area. Therefore, a non-classified unit cannot do unintended changes in a classified one.

SPINLINE3 technology

SPINLINE3 is mainly based on microprocessor technology. The application functions are basically implemented by means of application software programs running on the microprocessors of the processing units. Microprocessor capabilities are also used within *SPINLINE3* components when relevant for acquisition and output of data, hardware self-testing, HMI and network protocols. *SPINLINE3* components include also non-microprocessor-based components like pulse and low current amplifiers for neutron detector input conditioning. It also includes a set of mechanical components such as cabinets, racks and cabling systems fitted to NPP's requirements. (See [4] for further details)

Software components

- A low complexity and standardized software component, the Operational System Software, comes with each processing unit and provides within an infinite single loop, the following functions: hardware tests, cycle time management, data acquisition, call to application software, data output, HMI management.

- The application software is dedicated to the customer needs. It is derived from the requirements and expressed as functional block diagrams, using the System and Software Development Environment. The application software may call pre-existing components from a qualified library.

System and Software Development Environment

The System and Software Development Environment (SSDE), named *CLARISSE*, include the following activities: (see [4] for a full list of features)

- description of the I&C architecture, processing units configuration, input/output with sensors and actuators, data exchanged between processing units,

- description of the I&C functions, using the *SCADE* tool. *SCADE* provides a functional block diagram language with a formally defined graphical and textual syntax and semantic. It is easy to learn and use by technical staff trained in I&C process. *SCADE* does not require specialized software programming skills and helps achieving the consistency and completeness of the descriptions,

- automated generation of the executable code. The *SCADE* diagrams are translated into high quality C code, then compiled and link-edited with relevant libraries. The resulting binary code is identified, and secured in read-only memory for operation,

Software qualification

The *SPINLINE3* software components intended to run within safety processing units or networks have all been developed and qualified according to IEC60880. They are fully documented and reviewable [5] by licensing bodies, under contractual agreement with confidentiality clauses. The re-usability of the Operational System Software component makes possible additional arguments based on feedback of experience.

The TIHANGE 1 NIS refurbishment project

Background

The non-digital TIHANGE 1 NIS I&C system has been replaced by a digital equipment which had to meet the same physical and functional requirements.

The NIS architecture

The TIHANGE 1 NIS is composed of four cabinets, one for each protection channel (See figure 1).

The Source, Intermediate and Power range functions are performed within separate processing units distributed in four physically and electrically independent cabinets.

Each cabinet hosts one power range processing unit and either a source range or an intermediate range processing unit as follow :

- cabinet L1 : Power + Source
- cabinet L2 : Power + Intermediate
- cabinet L3 : Power + Source + Reactivity unit (non 1E)
- cabinet L4 : Power + Intermediate + Monitoring unit (non 1E)

Two Nervia networks link units of cabinets 1 and 2, and units of cabinets 3 and 4 to the non 1E Reactivity and Monitoring units

A mobile automatic testing unit has been also provided. It can be plugged to only one processing unit at the same time and only for the periodic testing session of this unit.
As in the former non software-based NIS, Source range processing units, Intermediate range processing units and Power range processing units are redundant and identical.

The main benefit of this architecture is its simplicity and its low cost. A drawback is the sensitivity to software common mode failure and more generally to design common mode failure.

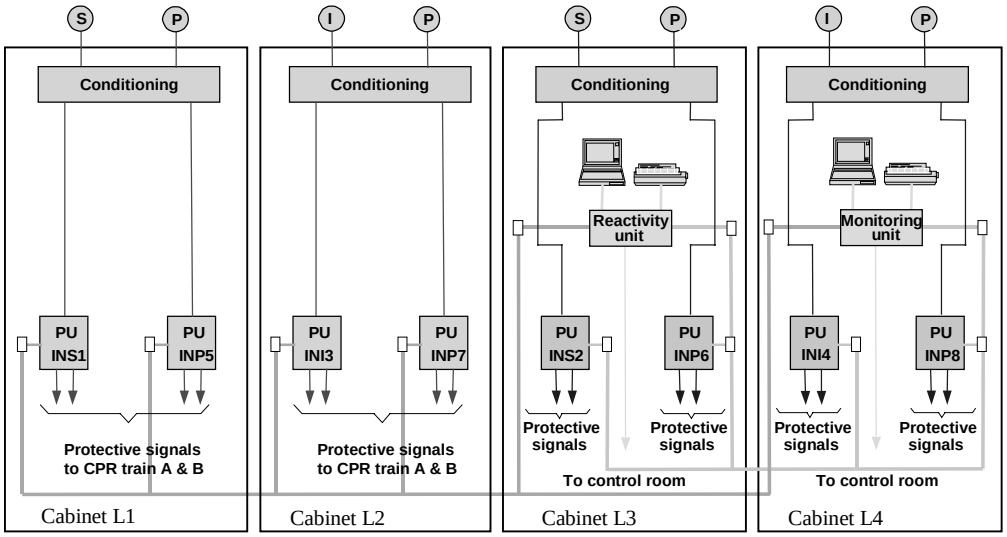


figure 1 : Tihange 1 NIS architecture

The Tihange 1 NIS software

Each 1E classified processing unit is composed of standard *SPINLINE3* hardware, the standard Operational System Software, parameterized according to the Source, Intermediate or Power Input/output requirements, and a dedicated application software.

The *SPINLINE3* Operational System Software has been developed and validated to IEC 60880 requirements previously to the Tihange 1 project. It is a standardized pre-existing software component of the *SPINLINE3* solution.

The application software for the Source, Intermediate and Power range processing units have been developed to meet the functional requirements of the Tihange 1 NPP. The requirements have been derived from the former Tihange 1 NIS and translated into Functional Block Diagrams (FBD) by Framatome. Then, the software have been developed and validated by Schneider Electric, using the CLARISSE System and Software Development Environment and the SCADE design language.

Requirement for software free from errors leading to SCCF

For the Tihange 1 project, we have been required to demonstrate that the software is free from errors which could lead to Significant Common Cause Failures (SCCF), i.e. common cause failures of the NIS that could lead to an unsafe situation of the plant.

It has been recognized that the methods and tools used for the software development and V&V, the respect of the requirements of IEC 60880, the experience of the software teams were suitable to produce software “as error free as possible”. This has been proven by the feedback of experience gained on similar projects that we have developed during the last 20 years. We have nevertheless been required to perform an additional analysis on the 1E software, using an FMEA technique, in order to identify those parts of the

software which, if faulty, could lead to SCCF and to provide additional evidences that theses parts are free from theses faults.

In the next section of this paper, we introduce the principle of the FMEA performed on the Tihange1 software and discuss some of the results found, using this technique.

Principles of the Software FMEA performed for the Tihange 1 project

Introduction

Definitions of « failure mode and effects analysis »

"The Failure Mode and Effects Analysis (FMEA) is a systematic, bottom-up method of identifying the failure modes of a system, item, function and determining the effects on the higher level. It may be performed at any level within the system (e.g., piece-part, function, blackbox, etc,). Software can also be analyzed qualitatively using a functional FMEA approach. Typically, a FMEA is used to address failure effects resulting from single failures" [1]

The Failure Mode and Effects Analysis (FMEA) is a "Qualitative method of reliability analysis which involves the study of the failure modes which can exist in every sub-item of the item and the determination of the effects of each failure mode on other sub-items of the item and on the required functions of the item." [2]

Particularities of FMEA performed on software

An FMEA may start from any level of design provided that it defines identified components with understandable failure modes. It is then possible to find the consequences of the failure of the components at system and/or plant level. It should be also possible to find out and understand the causes that may lead to these failure modes.

When performing an FMEA on mechanical, fluid or electrical system, failure modes of components such as pipes or resistors are generally understood, likely to happen and their consequences may be studied. A component is supposed to fail, due to some reason as wearing, aging or unanticipated stress. The analysis may not always be easy, but at least, the safety engineer can rely on data provided by the component manufacturer, results of tests and feedback of experience when available.

When performing an FMEA on software, very few information or support is available. The safety engineer has to apply his own knowledge of software to set up an FMEA approach, i.e.:

- to find out the appropriate starting point for the analyses,
- to set up a list of relevant failure modes,
- to understand what makes those failure modes possible or unlikely (the causes) and what are the consequences.

When Common Cause Failure is not a concern due to the use of diversity, the software failure modes can be considered at processing unit level only.

A list of five general purpose possible failure modes at this level has been given in [3] :

(a) - the operating system stops
(b) - the program stops with a clear message
(c) - the program stops without clear message
(d) - the program runs, producing obviously wrong results
(e) - the program runs, producing apparently correct but in fact wrong results

For a 1E I&C software such as the Tihange 1 software, developed with the *SPINLINE3* technology, failure modes (a), (b), (c) will lead to a safe state, whatever the causes could be, even if such failure mode should be avoided as far as possible.

Failure modes (d) and (e) may or may not lead to SCCF, depending on the cause :

- if the cause is a software fault, activated by a hardware failure, sensor failure, or human error within one channel, the failure mode is unlikely to be a CCF or a SCCF, due to the redundancy.
- if the cause is a software fault activated by an operational condition, the failure mode will be a CCF and could be a SCCF if it happens to prevent the performance of a required safety action.

Principles of software faults and software failure modes

A software component designed and coded either manually or with the help of tools may be subject to a wide variety of faults. The root cause of these faults is to be found in the specification, in the design or in the implementation. A software fault can be seen as a deviation in the content and/or in the order of instructions or data stored in memory causing the microprocessor not to behave as expected under some event or sequences of events. Trying to consider all possible faults that could affect even a simple software component is not practicable. Nevertheless, it is possible to consider the consequences of such faults, as they will lead to a few numbers of software failure modes

Differences between hardware and software FMEA

Hardware FMEA

- may be performed at functional level or part level
- applies to a system considered as free from failed components
- postulates failures of hardware components according to failure modes due to aging, wearing or stress
- analyses the consequences of theses failures at system level
- states the criticality and the measures taken to prevent or mitigate theses consequences

Software FMEA

- is only practicable at functional level
- applies to a system considered as containing software faults which may lead to failure under triggering conditions
- postulates failures of software components according to functional failure modes due to potential software faults
- analyses the consequences of theses failures at system level
- states the criticality and :
  - describes the measures taken to prevent or mitigate theses consequences,
  - or shows that a fault leading to the failure mode will be necessarily detected by the tests performed on the component,
  - or demonstrate that there is no credible cause leading to this failure mode, due to the software design and coding rules applied

Application to the Tihange1 software FMEA

SPINLINE3 software components relevant for FMEA

The *SPINLINE3* software is composed of Blocs of Instructions (BIs) executed sequentially.

- BIs are either "intermediate" – they are a sequence of smaller BIs – or "terminal" – they cannot be decomposed in smaller BIs.
- They have only one "exit" point. They produce output results from inputs and possibly memorized values. Some BIs have direct access to hardware registers.
- They have a bounded execution time (i.e. the execution time is always smaller than a fixed value).
- They exchange data through memory variables. A memory variable is most often written by only one BI and may be read by one or several BIs.

SPINLINE3 BIs do not implement dynamic resource allocation algorithms which could lead to dead-lock situations and Interrupts are not used

Figure 1 shows the first levels of decomposition of the software of a processing unit

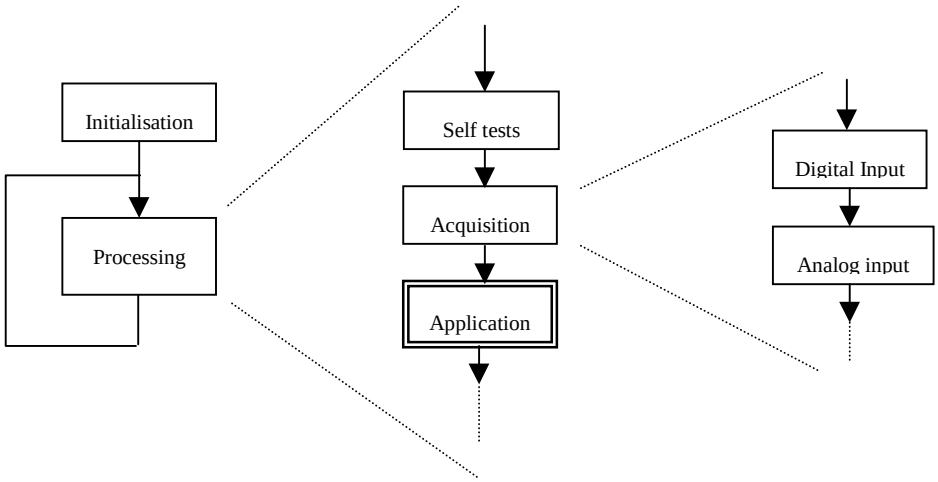


figure 1 : firsts levels of the BI decomposition of a *SPINLINE3*

The block of instruction "Application" is itself a sequence of BIs, derived from the application functional block diagrams or from the SCADE diagrams.

The other blocks of instructions belong to the *SPINLINE3* Operational System Software.

Definitions of software failure modes in the context of SPINLINE3 software

The BI is the basic component used for the software FMEA
The correct behavior of a BI is characterized by the following:

1. the BI execution ends at its "exit" point

2. the BI execution time is bounded. The execution time may be different from one execution to another, due to possible different control flow paths within the BI.

3. the BI performs the intended actions and does not perform unintended actions

   3.1 it provides the expected outputs

   3.2 it does not modify variables that it shall not modify

   3.3 it interacts as expected with I/O boards

   3.4 it interacts as expected with CPU resources

   3.5 it does not modify code memory and constants

The BI failure modes are derived from the definition of this correct behavior:

1. the BI execution does not ends through the “exit” point

2. the BI execution time does not meet time limits

3. the BI does not perform the intended actions or performs unintended actions

   3.1 it does not provide the expected outputs

   3.2 it modify variables that it shall not modify

   3.3 it does not interact as expected with I/O boards

   3.4 it does not interact as expected with CPU resources

   3.5 it modify code memory or constants

Software FMEA process

The following process has been chosen:

Generic analyses have been performed, considering software components of BI type and SPINLINE3 characteristics for all failures modes but 3.1

Dedicated analyses of the SPINLINE3 Operational System Software and of the Tihange 1 application software have been performed, at the functional level for failure modes 3.1 and some aspects of failure modes 3.3 and 3.4. The functional level has been found equivalent to the high level BI decomposition, and easier to analyze.

All failure mode found to be a CCF have been considered as potential SCCF (worst case).

Issues raised have been solved by complementary analyses, based on the detailed implementation of the software.

Examples of analysis and results obtained by the FMEA

Example 1: failure mode "bi execution does not meet time limit"

SPINLINE3 software is such that:
- output boards shall be periodically refreshed, otherwise a watchdog switches the outputs to a safe position
- the processing unit cycle time is regulated. If the associated timer is exceeded when the regulation test is executed, it causes the unit to stop and consequently, the output boards watchdogs to react.

The possible situations caused by the failure mode are :
- the execution time of the BI is "infinite" and causes the output boards watchdogs to react => safe position,
- the execution time of the BI is "infinite" and the output boards are still refreshed (i.e. there is an infinite loop involving an output module) => **potentially unsafe situation,**
- the execution time of the BI is not "infinite" and causes an overrun of the unit cycle time : the unit stops => safe position,
- the execution time of the BI is not "infinite" and does not cause an overrun of the cycle time : no consequences.

The second situation has led to a further analysis of the loops within the Operational System Software in order to show that this situation cannot happen. In addition, a list of the Technical and Quality Assurance measures taken to avoid or detect this failure mode has been established.

Example 2: failure mode 3.1."BI does not provide the expected outputs "

Introduction

The example is about the Acquisition Functional Block of the *SPINLINE3* Operational System Software.

The acquisition function accesses the input boards through hardware registers or shared memory. It delivers the values to the application software, with a validity bit set to "true" if the input values are "ok" and set to "false" if either a sensor or the input board itself is faulty

The analysis is reported in the following array

Failure Mode	Local effect	System effect	Criticality	SCCF	Prevention/comments
1	2	3	4	5	6

1. failure mode description
2. effect at first level
3. effect at NIS system level
4. criticality : C : high, CM : limited, NC : low
5. SCCF : Significant Common Cause Failure at NIS level
6. if SCCF, measures taken in order to be sure that the failure mode cannot happen (no software fault) or will be detected and lead to a safe position.

Sample of the analysis

Failure Mode	Local effect	System effect	Criticality	SCCF	Prevention/comments
1. - acquisition block provides values with invalid status when they are valid hardware is ok	correct values are transmitted to application software with invalid status	application software processes validity bit and take safe behavior	NC		
2. - acquisition block provides values with valid status when they are invalid hardware is not ok	invalid values are transmitted to application software with valid status	risk of unsafe outputs	C	no	This failure mode is activated by a random hardware failure in one unit. It is not considered as a SCCF
3. – acquisition block provides erroneous values when they are valid hardware is ok	erroneous values are transmitted to application software with valid status	risk of unsafe outputs	C	yes	Digital boards: software processing is independent from the input values. – test of each input with values 0 and 1 Analogue boards: software processing is independent from the input values. - test of each input with several values, checking that others inputs are not changed. Range checks performed by the application may detect this failure mode
4. - acquisition block provides erroneous values when they are invalid hardware is non ok	erroneous values are transmitted to application software with invalid status	application software processes validity bit and take safe behavior	NC		

figure 3 – sample of FMEA of the Acquisition Functional Bloc

Comments

The analysis is dedicated to software components. The postulated failures of these components are supposed to be caused by software faults present in the components, triggered by external conditions. In the example, the status of the input boards (hardware ok or non-ok) is one of these conditions. Other possible conditions may be sensors input values, operator interfaces, operating modes.

Comments on failure modes 1 and 3: hardware ok. The correct behavior of the acquisition function is to access the input board and to return correct data with a validity bit set to “true”. These failure modes state that the acquisition function acquires data from a non-faulty input board but because of software faults, provides erroneous output to the application software, resulting in situations 1 and 3. In situation 1 the validity bit is erroneously set to false; the application software assures the safe behavior of the unit In situation 3, the validity bit is correct but the data is erroneous. This situation is critical because the application software may behave in an unsafe way and is a SCCF because it may impact any units using this type of board, while in normal operation.

Comments on failure modes 2 and 4 : hardware non ok. The correct behavior of the acquisition function is to return a validity bit to “false”. These failure modes state that, because of software faults, the acquisition function provides an erroneous output to the application software, resulting in situations 2 and 4. Situation 2 is critical because invalid values are transmitted to the application software with valid status that may result in an unsafe behavior of the unit. It is not a SCCF because the software fault is triggered by a failure of the hardware that is unlikely to be simultaneously present on several units. Situation 4 is not critical because of the invalid status associated to the erroneous data.

Feedback of experience

Analyses oriented toward failure mode 3.1.“BI does not provide the expected outputs” performed on a software component are only functional for two main reasons: The first reason is the nature of software components, which are basically functions providing, outputs from inputs. The second reason is that all the possible functional failures shall be considered because, neither the possible failures of the underlying microprocessor and memories, nor the potential software faults can help restricting this analysis.

When the FMEA analysis is oriented toward the risk of SCCF, possible failures of the underlying hardware are taken into account by redundancies at system architecture and are not likely to cause SCCF, because of the random nature of theses failures.

Software faults may be SCCFs when the same software is used in identical redundant units in a system architecture as it is the case in the Tihange 1 NIS and when they are triggered by a condition common to all channels. For instance, a neutron flux going over a threshold limit. As we know that software faults can only be design faults, the best way – and may be the only way- to prevent software SCCF is to make sure that SCCF prone software components are “as error free as possible”.

Performing a software FMEA allows to:
- identify the SCCF prone software components in the software program
- cross-check the validation testing performed on these components. The validation tests give the assurance that known critical paths in the software are free from software faults
- find out what are the “defense in depth” measures to use in order to prevent or mitigate the consequences of a failure mode
- find out the technical and/or quality dispositions best suited to prevent the occurrence of classes of software faults which could lead to critical failure modes

The tests provided by the FMEA are not intended to be a proof that the software is free of SCCFs. They are not sufficient when testing is not exhaustive, which is the most frequent situation. They can only be used as a demonstration added to the technical and quality dispositions taken for the development and the V&V of the software.
These dispositions should be at a minimum compliant with the “shall” requirements of IEC60880 and preferably with most of the “should” clauses.

Lessons learned from the SPINLINE3 OSS software FMEA

The *SPINLINE3 OSS* is a pre-existing software component developed and validated according to IEC 60880.

The test cases given in the FMEA are a subset of the tests already performed during the validation of the OSS. No new test cases have been necessary. This is because the validation strategy and the FMEA are based on a functional approach, one consisting in a systematic testing of the functions of the software, the other consisting in finding ways to guarantee that critical failure modes of theses functions are unlikely to happen or mitigated.

Some tests cases have been done with more input values when practicable, in order to increase test coverage and confidence in the demonstration.

The FMEA has not caused significant changes in the development process and technical rules used to produce 1E software in our department. Rules for software fault prevention and mitigation were already defined in our methodology and have provided acceptable prevention for SCCF situations identified by the FMEA.

Performing the FMEA for the Tihange 1 project has proved to be a good way to discuss in depth safety aspects of software-based systems with our customer and with the licensing authority.

Conclusion

The New TIHANGE 1 Nuclear Instrumentation System successfully started operation on the beginning of Marsh 2001 after the plant outage, as planned at the beginning of the project. The choice of a software-based technology has raised the issue of the risk of CCF due to the same software being used in redundant independent units. Implementing functional diversity or equipment diversity has been considered but found either not practicable or of little value within this context.

The safety characteristics of the *SPINLINE3* solution and the stringent and proven safety software development process applied by the Nuclear department of the Schneider Electric company have made acceptable the principle of a design based on redundant identical processing units for this project. In addition, because of the possible consequences in case of the NIS not performing its protection function on demand, the licensing authority has required an FMEA oriented toward the SCCF risk as part of the safety case.

This FMEA has been performed on :
- the NIS architecture
- the *SPINLINE3* Operational System Software
- the three Tihange 1 application software (i.e. source, intermediate and power range)

The process used and the results have been elaborated by Schneider Electric and reviewed by the customer and the licensing authority all along the project development until final acceptance. Issues have been raised and answers and/or complementary analyses provided, some of them making direct references to the code itself.

In this paper, we have presented this software FMEA experience including:
- adaptation of the principles of FMEA to analyze a software program
- choice of a “block of instruction” (BI) approach to identify the components to analyze
- definition of the software failure modes associated with the BIs
- examples of the analyses performed on the *SPINLINE3* Operational System Software
- feedback of experience

References

[1] – ARP4761 – Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment – 1996 –§ 4.2 and annex G

[2] – IEC 60812, Ed. 2: Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

[3] – A. Villemeur. - Sûreté de fonctionnement des systèmes industriels, Eyrolles, 1988

[4] – C.Esmenjaud, M.Prunier A.Parry - Use of the *SPINLINE3* generic safety digital I&C platform for the refurbishment of the French 900MW Nuclear Instrumentation System, NPIC&HMIT, Washington, DC, November 2000.

[5] - C.Esmenjaud, Reviewability guidelines for computer-based safety systems OECD/NEA – Munich 1996.

Qualification of Pre-Developed Software for Safety-Critical I&C Application in NPP's

M. Kersken[1]

[1] Institute for Safety Technology (ISTec), Garching
Tel.: +49 89 32004-546, Fax: +49 89 32004-300, e-mail: ker@grs.de

Summary

Implementations of I&C functions important to safety in nuclear power plants are increasingly realized with computer based systems, i.e. by its software. Often so called equipment families are used to develop these I&C functions. Besides a hardware platform, these equipment families provide pre-developed software in the form of basic components from which I&C functions can be composed by configuration and parameterization; but also larger components which have been developed by conventional software engineering, as e.g. operating systems, I/O drivers, self-supervision software, etc. are included. Outside the equipment families, it may be desirable to introduce also other types of pre-developed software, e.g. for simulation and for analysis purposes.

The assessment and qualification of software for computer based systems important to safety requires (as e.g. in IEC 60880) a set of detailed documents according to the development steps of the software life cycle. For pre-developed software the amount of documentation available and its detail will not be sufficient in most cases. On the other hand, the pre-developed software may have been operating in many applications, and it should be possible to evaluate this operating experience to demonstrate dependability.

The objective of this paper is to provide (as an example) a set of staggered criteria for the qualification of pre-developed software to be used in different categories for safety critical I&C. These qualification criteria appear in the form of requirements for the application of methods and measures in the different safety categories. The three safety categories are those from IEC 61226.

Besides the safety categories, there are also usage categories which denote whether the pre-developed software is executed directly online, or is used to directly generate online executed software, or is used to support the generation of online executed software.

Introduction

Pre-developed software which is used in I&C systems important to safety may range from small software elements up to large and complex software products. Small software consists e.g. of the elements of a function block library (of an equipment family) which are configured and provided with parameters to implement an I&C function, or part of it. Large and complex software may be e.g. operating systems, communication drivers, software for computer self-supervision or simulation packages. General purpose pre-developed software may be commercially available (commercial-off-the-shelf, COTS) or may have been developed for a similar application as the envisaged one. In the latter case this may be a non-nuclear application important to safety or a development in the nuclear context for a different plant and/or within a different safety category.

In any of these cases, before the inclusion of a piece of pre-developed software into a new system, there must be a demonstration that the pre-developed software is suited for the envisaged purpose, is reliable, and is of sufficient quality. This demonstration is denoted here as “qualification”.

Different research projects have been investigating into the problem of qualification of pre-developed software for applications with high risk potential and their results are already incorporated in summarizing reports or documents which seek for consensus concerning such a qualification. Also standards can be considered as a kind of summarizing document, because they are developed with an involvement of the different parties engaged in the development, procurement, qualification, operation and licensing of such systems. All these summarizing documents are, however, dependent on geographical differences, i.e. emphasis is put on different aspects of the qualification process. The objective of this paper is to give a more unified approach to the qualification of pre-developed software.

One of the basic summarizing documents which is used here is the report [7] which has been obviously discussed widely in the U.S. between NRC and LLNL and in a pre-review conducted by Mitre Corporation. The IEC standard [1] was heavily discussed for almost ten years on an international basis. In Europe a kernel of technical support organizations discussed for five years some of the most important and practical issue areas raised by the licensing of software important to safety [3], among them the issue of use and validation of pre-existing software. This chapter is also contained as an annex in the IAEA safety guide on software /12/. These three documents form the basis for the proposal of a qualification process for pre-developed software in this paper.

Grading of requirements

In order to spend the effort for qualification effectively, criteria are needed which can be used to focus on functions and systems which are most important to safety and deserve the highest qualification effort, and those of lower importance to safety with (in general) lower associated qualification effort.

In the nuclear field grading is tied to the consequences of the failure of a system in most of the national and international categorization/classification models[1]. An attempt to develop a standard where the probability of occurrence of a failure is also included, i.e. a risk based categorization, was made in IEC. This resulted, however, not in a standard but in a report [10] which contains four examples for a categorization using probabilistic safety analysis PSA.

[1] Functions important to safety are put into categories in IEC 61513 [6], whereas systems important to safety are put into classes.

The following refers to the categorization/classification of IEC 61226 [2] because this standard is

- internationally agreed in the nuclear field by vote,
- introduced in Germany by DIN (German Standards Institute),
- very similar to other German guidelines [4].

Assignment criteria for the three categories A, B and C according to [2] are:

Category A

An I&C function and the associated systems and equipment FSE shall be assigned to category A if it meets any of the following criteria:

a) It is required to mitigate the consequences of a postulated initiating event(PIE) to prevent it from leading to a significant sequence;

b) its failure when required to operate in response to a PIE could result in a significant sequence of events;

c) a fault or failure in the FSE would not be mitigated by another category A FSE, and would lead directly to a significant sequence of events;

d) it is required to provide information or control capabilities that allow specified manual actions to be taken to mitigate the consequences of a PIE to prevent it from leading to a significant sequence of events.

In reference to point d), factors such as the availability of redundant information sources, sufficient time for operator evaluation of alternative sources of information, and whether the manual actions are the only sources of mitigation of the sequence of events shall be considered in categorizing FSE. If manual action is required to preserve NPP safety, the I&C FSE that enables this action shall be assigned to category A.

Category B

An I&C FSE shall be assigned to category B if it meets any of the following criteria and is not otherwise assigned to category A:

a) it controls the plant so that process variables are maintained within the limits assumed in the safety analysis;

b) a requirement for operation of a category A FSE in order to avoid a significant sequence would result from faults or failures of the (category B) FSE;

c) it is used to prevent or mitigate a minor radioactive release, or minor degradation of fuel, within the NPP design basis, but of less importance than a significant sequence of events[2];

d) it is provided to alert control room staff to failures in category A FSE;

e) it is provided to monitor continuously the availability of category A FSE to accomplish their safety duties;

f) it is used to reduce considerably the frequency of a PIE as claimed in the safety analysis.

Category C

An I&C FSE shall be assigned to category C if it meets any of the following criteria and is not otherwise assigned to category A or category B:

a) it is used to reduce the expected frequency of a PIE;

b) it is used to reduce the demands on, or to enhance the performance of, a category A FSE;

c) it is used for the surveillance or recording of conditions of FSE, to determine their safety status (fit for operation, operating, failed or inoperative), especially those whose malfunction could cause a PIE;

d) it is used to monitor and take mitigating action following internal hazards within the NPP design basis (e.g. fire, flood);

e) it is used to ensure personnel safety during or following events that involve or result in release of radioactivity in the NPP, or risk of radiation exposure;

f) it is used to warn personnel of a significant release of radioactivity in the NPP or of a risk of radiation exposure;

g) it is used to monitor and take mitigating action following natural events (e.g. seismic disturbance, extreme wind);

h) it is the NPP internal access control.

After the assignment of I&C functions to safety categories it is necessary to find criteria for the implementation of these functions. Criteria for the implementation of functions of category A via computer-based systems and newly developed software for the specific purpose of such functions are given in [9], for pre-developed software of the same category A guidance is given in [1]. For categories B and C, there is an evolving standard [5] in IEC at the moment, which is meant to become valid for new as well as for pre-developed software.

[2] The definition of a minor radioactive release or minor degradation of the fuel shall be according to national practice. A minor radioactive release might be that due to a release of coolant without additional fuel damage. Minor degradation of the fuel might involve damage to a small amount of fuel cladding without release of coolant or loss of ability to cool the core satisfactorily.

Usage categories of pre-developed software

The categorization of software also depends on the characteristics of its usage. If the piece of software under consideration is directly executed in the application, then it is classified according to IEC 61226 as the function which it is implementing. Category A software implements a function of category A; the same holds for B and C.

However, if the piece of software under consideration is used to produce – more or less directly – the application software, and there are means to check the output of the software under consideration, then it might be possible to chose a lower category as a qualification goal. The proposal made in this paper is to keep software that produces directly application software (denoted as “indirect 1” here) in the same category as the latter, if no other means for the thorough verification of the application software exists. If such a possibility exists, then the software that produces directly application software can be put into the next lower category. An example for software that directly produces application software is an automatic code generator which receives as input a syntactical and semantical fully defined specification and delivers either source code or executable code at its output. This kind of specification and automatic code generation is a widespread technique in I&C equipment families for process automation. Of course there is always the possibility to perform tests with the output of software of usage category “indirect 1”. This is, however, not regarded as sufficient (see also chapter 2.2 of [11]). The reason for this is, that by automatic code generation one or more design steps are skipped, respectively are not visible for the purpose of qualification. If there is such a gap, the analyst performing the qualification should at least have access to a “good” representation of the software at the beginning and at the end of this gap. Good means in this context, that the representation is understandable for the analyst. At the front end of the gap this may be easily given by e.g. a graphical representation of the I&C specification by standardized symbols. The “low end” may be source code representation of a high-level language. In addition it would be desirable, that at the “low end” of the gap, which is the code, the representation of the software is accessible by a tool, e.g. a static analyzer, which can support the software analyst in understanding, finding of faults and inconsistencies, and also in the specification of test cases, if this is wanted.

Software, that produces indirectly application software is denoted as “indirect 2” here. These are tools which support the development of software by a structured approach (CASE tools). Examples for such a structured approach are methods like SA (Structured Analyses), SD (Structured Design), SADT (Structured Analysis and Design Technique), etc. The tools based on approaches like this establish a framework within which the application software can be interactively developed.

With software of usage category “indirect 2” code can be produced that is understandable by humans and accessible by tools as e.g. static analyzers and debuggers. Moreover such tools deliver documented information on development levels of the application software, thus providing input to a human-centered analysis of the application software. As the development part and the analysis part for application software produced by software of category “indirect 2” is strongly human-centered, the probability that a fault in the tool results in a fault in the application software is much lower than with category “indirect 1”. Therefore this type of software is treated as non-classified NC. Also the verification and validation tools which are used by the analyst, like static analyzers and debuggers are categorized as NC. Their application is primarily human driven, and a tool fault is not likely to introduce a fault in the application software. This is in line with IEC 60880, which requires in clause 8: “Hardware and software tools used for computer system validation need no special verification. They should, however, be shown to be suited to their purpose.”

In the following the usage categories and their relationship to the categories of IEC 61226 are summarized.

Usage category	Characteristics of the software	IEC 61226 category
DIRECT	**DIRECTLY EXECUTED IN AN APPLICATION OF CATEGORY A OR B OR C**	A or B or C
indirect 1	generates automatically code (source code or executable code) for	
	- category A	A or B[1]
	- category B	B or C[1]
	- category C	C or NC[1]
indirect 2	supports the development of code for category A or B or C (CASE-Tool)	NC

[1] The next lower category of IEC 61226 may be chosen, if the output of the code generator is understandable and can be verified by a human by means in addition to testing and/or an independent tool is available for verification.

Table 1: Usage categories of software and their relationship to categories of IEC 61226

Qualification criteria for pre-developed software

The ideal situation for pre-developed software would be that it has been developed for an exactly identical function as the envisaged one, according to the quality requirements of the safety category of this function. Usually, however, this is not the case, and one or more of the following issues must be tackled with:

- missing elements in the production process,
- product documentation missing or of insufficient quality,
- operational profile in the past very different from the envisaged one,
- only a (small) part of the pre-developed software is used (unused code),
- unintended resident functions (functions not documented).

A benefit of pre-developed software may be a wide and/or frequent use with positive results, i.e. a long operating time free of failure, or with acceptable few failures. Advantage can only be taken from positive operating experience, if

- enough data are collected,
- the data collection is assessed to be dependable, and
- the evaluation of data is statistically valid.

Besides the compensation for missing knowledge on the product and for its production process by the evaluation of operating experience, there is also the possibility to develop retrospectively by re-engineering techniques missing documentation on product features and levels of product development.

Testing of the pre-developed software has of course to be performed for all safety categories. Even for non-classified software NC, tests will be necessary, as this is the state of practice to demonstrate that the software is suited for its purpose (as required by IEC 60880).

Qualification criteria independent of safety categories

The first step in the acceptance process is the identification of the environment within which the pre-developed software will have to work. This environment is determined by the system-level safety function as described in the system requirements specification. Also the interface and performance requirements, as well as the safety category should be contained in the system requirements specification. This means, that during the establishment of the plant safety design base a risk and hazards analysis has been performed which rendered the categories of safety functions to be implemented by pre-developed software. This risk and hazard analysis – in spite of being out of the scope of I&C engineering – has been taken as the first of four acceptance criteria that should be applied to pre-developed software independently of its safety category.

Besides the requirements which are coming from the system-level safety function, there are also category-independent requirements for the (sub-)function where the function implemented by pre-developed software fills in. There are, the clear identification of the (sub-)function to be fulfilled by the pre-developed software and of the means (software tools) for its production, taking into account their usage category, determination of their safety category, and the configuration management and change control necessary for the pre-developed software. Table 2 summarizes these qualification criteria.

Table 2: Qualification Criteria Independent of Safety Categories

Criterion	Description	Document
I 1	The system-level safety function shall be clearly identified.	IEC 60880-2 [1], 4.3.3.1.1.1; IEC 61513 [6], 6.1.1, 6.1.2
I 2	Risk and hazard analysis shall have been performed to determine the safety category of the system-level safety function.	LLNL [7], Table 4; EUR 19265 [3], 1.1.3.1
I 3	The safety (sub-)function to be implemented with pre-developed software shall be clearly identified.	IEC 60880-2, 4.3.3.1.1.1; IEC 61513, 6.1.1.1.1; LLNL, Table 4; EUR 19265, 1.3.3.1
I 4	The safety category of the pre-developed software shall be determined. GOTO A, B, C.	IEC 61513, 6.1.1.1.1; LLNL, Table 4
I 5	The pre-developed software shall be under configuration and change control	IEC 60880-2, 4.3.3.1.1.2, 4.3.4.3; LLNL, Table 4; EUR 19265, 1.3.3.2

Qualification criterion I 5 is necessary because the whole qualification process cannot be applied to a piece of software which is permanently changing.

Criterion I 4 delivers the output of this preliminary qualification, i.e. the category A or B or C of the pre-developed software under consideration.

First Level Qualification criteria for category A

Pre-developed software for category A functions has to fulfil almost all the stringent requirements that are applied to newly developed software for this category. Therefore, the application of pre-developed software in category A presumes that only small parts of the life cycle documentation are missing, and can be compensated by the evaluation of operating experience and/or additional testing.

Table 3 shows the category A first level qualification criteria. First level in this context means, that these are principal criteria, which must be detailed in subsequent levels.

As an example for a subsequent level, the second level qualification criteria for criterion A 1 (suitability assurance) are given in table S1 . Table S 2 gives the second level criteria of a part (namely the quality assurance part) of first level criterion A 2 (product assurance). The second part would be a table for V&V, which has not been included, as only the principle of the qualification process is shown in this paper. For the same reason, also the further details of the first level criteria documentation, product safety, system safety, interface, compensation by operating experience, error reporting, and modification are not elaborated. Thus the "GOTO ..." and other references in the description part of the tables, which are the pointers to the more detailed criteria are in most cases empty.

Table 3: Category A, first level qualification criteria

Criterion No.	Description	Document
A 1 Suitability Assurance	An evaluation of suitability of the pre-developed software shall be performed, to confirm that the functional, performance and architectural specifications of the pre-developed software comply with the requirements of the system specification. GOTO S 1, No. 1-7	IEC 60880-2, 4.3.3.1
A 2 Product Assurance	A quality evaluation of the pre-developed software shall be performed, to provide evidence that the feature of its design are appropriate to implement a category A function, and that appropriate V&V and quality assurance has been exercised through the life cycle. This evaluation shall be performed against the requirements of IEC 60880. GOTO ...	IEC 60880-2, 4.3.3.2; LLNL, Table 5; EUR 19265, 1.3.3.4, 1.3.3.5
A 3 Docu-mentation	Documentation shall be available for review to demonstrate that criterion A 2 has been met during development of the pre-developed software. GOTO ...	IEC 60880-2, 4.3.3.2; LLNL, Table 5, A6; EUR 19265, 1.3.3.7
A 4 Product Safety	It shall be demonstrated that criterion I 3 is met by the pre-developed software. GOTO ...	IEC 60880-2, 4.3.3.4.2; LLNL, Table 5, A7

Criterion No.	Description	Document
A 5 System Safety	It shall be demonstrated that no features of the pre-developed software violate safety requirements or constraints on the system level. GOTO ...	IEC 60880-2, 4.3.3.1.2.4; LLNL, Table 5, A8; EUR 19265, 1.3.3.8
A 6 Interface	The interfaces through which the pre-developed software is involved shall be identified, clearly defined, thoroughly validated, and under configuration management. GOTO ...	LLNL, Table 5, A9; EUR 19265, 1.3.3.3
A 7 Compen-sation, Operating Exper-ience	If the application of criterion A 2 reveals minor deficiencies, then the evaluating of operating experience may be used for compensation. GOTO ...	IEC 60880-2, 4.3.3; LLNL, Table 5, A10; EUR 19265, 1.3.3.9
A 8 Error Reporting	All errors shall be reported, analyzed and classified according to their severity. Their impact on the function to be fulfilled by the pre-developed software shall be evaluated. GOTO ...	IEC 60880-2, 4.3.3.3.1.6; LLNL, Table 5, A11; EUR 19265, 1.3.3.11
A 9 Modifi-cation	Modification of a piece of pre-developed software shall be performed compliant with IEC 60880. The implementation of the modified component shall be handled in the frame of the system life cycle as in IEC 61513. GOTO ...	IEC 60880-2, 4.3.3.1.2.2; IEC 61513, 6; EUR 19265, 2.7.3.1, 2.7.3.2

First level qualification criteria for category B

Whereas pre-developed software will be exceptional in category A, because of the stringent requirements on product, process and their documentation, this type of software will be found more frequently in category B and C. The proposed relaxations of qualification criteria in category B against category A are mainly the reduced amount of documentation required and a weaker process of product assurance. Table 4 shows the first level qualification criteria for category B.

Table 4: Category B, first level qualification criteria

Criterion No.	Description	Document
B 1 Suitability Assurance	An evaluation of suitability of the pre-developed software shall be performed, to confirm that the functional, performance and architectural specifications of the pre-developed software comply with the requirements of the system specification. GOTO S 1, No. 8-9	IEC 62138, 5.4, 6.2.3

Criterion No.	Description	Document
B 2 Product Assurance	A quality evaluation of the pre-developed software shall be performed, to provide evidence that the features of its design are appropriate to implement a category B function, and that appropriate V&V and quality assurance has been exercised through the life cycle. GOTO ...	LLNL, Table 6, B 5
B 3 Docu-mentation	Documentation shall be available for review to demonstrate that criterion B 2 has been met during development of the pre-developed software. GOTO ...	IEC 62138, 6.2.1; LLNL, Table 6, B 6
B 4 Product Safety	It shall be demonstrated that the pre-developed software can implement its safety function as identified in criterion I 3. GOTO ...	LLNL, Table 6, B 7
B 5 System Safety	It shall be demonstrated that the pre-developed software does not violate safety requirements and/or constraints on the system level. GOTO ...	LLNL, Table 6, B 8
B 6 Interface	The interfaces through which the pre-developed software is communicating shall be identified, validated and under configuration management. GOTO ...	IEC 62138, 6.2.1, 3
B 7 Compen-sation, Operating Expe-rience	If the application of criterion A 2 reveals deficiencies, then the evaluation of operating experience may be used for compensation. GOTO ...	IEC 62138, 6.2.2.2; LLNL, Table 6, B 9
B 8 Error Reporting	All errors shall be repeated and analyzed. Their impact on the system-level function shall be evaluated. GOTO ...	LLNL, Table 6, B 10
B 9 Modifi-cation	Modifications of a piece of pre-developed software shall be performed compliant with the requirements of IEC 62138 (clause 6.9). GOTO ...	IEC 62138, 6.9

First level qualification criteria for category C

The suitability analysis for category C pre-developed software follows no specific requirement; it is just a fit-for-purpose analysis.

The product assurance activities aim to assess whether appropriate standards have been systematically applied during software development, that configuration management is effectively employed, as well as a minimum of V&V activities.

Table 5: Category C, first level qualification criteria

Criterion No.	Description	Document
C 1 Suitability Analysis	The suitability analysis is reduced to a simple fit-for-purpose analysis. GOTO S 1, No. 10	IEC 62138, 7.2.3
C 2 Product Assurance	A quality evaluation of the pre-developed software shall be performed, to provide evidence that the features of its design are appropriate to implement a category C function. Minimum V&V shall have been performed. GOTO ...	LLNL, Table 7, C 1
C 3 Docu-mentation	Minimum documentation as described in table S .., including documentation of V&V required in C 2 and detailed in S .. shall be available for inspection. GOTO ...	IEC 62138, 7.2.1; LLNL, Table 7, C 6
C 4 Product Safety	It shall be demonstrated that the pre-developed software can implement its safety function as identified in criterion I 3. GOTO ...	IEC 62138, 7.2.1, 3
C 5 System Safety	It shall be demonstrated that the pre-developed software does not violate safety requirements and/or constraints on the system level, and those of A and B systems. GOTO ...	LLNL, Table 7, C 8
C 6 Interfaces	The interfaces through which the pre-developed software is communicating shall be identified and under configuration management. GOTO ...	IEC 62138, 7.2.1, 3
C 7 Compen-sation Operating Expe-rience	The pre-developed software shall be shown to have an operating past without serious malfunctions. GOTO ...	IEC 62138, 7.1.5, 4; LLNL, Table 7, C 9
C 8 Error Reporting	An error reporting history to demonstrate fulfillment of criterion C 7 should be available. Within the actual application, there should be an error reporting schema, too. GOTO ...	LLNL, Table 7, C 9
C 9 Modifi-cation	Modifications shall be performed compliant with a reduced set of requirements of IEC 62138. GOTO ...	IEC 62138, 6.9

From the first level qualification criteria “pointers” (GOTO) are leading to a set of second level qualification criteria, which are more detailed requirements than the first level ones.

Second level qualification criteria

The second level qualification criteria are not grouped according to safety categories; they should be regarded as a pool of requirements which are accessed from the first level. In many cases first level C criteria point to a smaller set of second level criteria than first level B criteria, and the same holds for the relationship between B and A first level criteria.

The following tables with second level qualification criteria are not meant to be exhaustive; criteria with this grade of detail may in many cases be project specific.

The tables with second level qualification criteria are denoted with "S". Table S 1 contains criteria for a suitability analysis.

Table S 1: Criteria for suitability assurance

Criterion No.	Description	Document
1	System specification documentation shall be available, containing functional, performance, and interface requirements to be fulfilled by the pre-developed software (PDS).	IEC 60880-2 (Cat. A)
2	Specification and user documentation of the pre-developed software shall be available, defining explicitly all characteristics that are relevant in fulfilling the systems functional and performance specifications.	IEC 60880-2 (Cat. A)
3	The specifications of the PDS shall be evaluated with respect to the system requirements specification. If discrepancies exist, the PDS shall either be rejected or modified or the requirement specifications shall be adapted to resolve them, provided that the overall safety function is preserved.	IEC 60880-2 (Cat. A)
4	If it is necessary to modify the PDS an evaluation shall be completed, based on the PDS design documentation, to determine if the change can be performed in a manner compliant with IEC 60880. If the change cannot be performed in a compliant manner, the use of the PDS shall be rejected.	IEC 60880-2 (Cat. A)
5	For a PDS that is contained in a library except when the whole library has to be assessed, it should be possible to tailor the library to build a restricted library meeting the software needs and to link the program with this restricted library which shall be composed of assessed components.	IEC 60880-2 (Cat. A)

Criterion No.	Description	Document
6	The suitability evaluation shall identify the functions that are included in the PDS which are unintended an unneeded by the system and also the measures to ensure that these functions do not interfere with safety functions.	IEC 60880-2 (Cat. A)
7	When the evaluation is concluded, a document shall be produced to record whether the functional and performance specifications of the PDS comply with the software requirement specifications of the system; and where the PDS is not adequate, the reasons for rejection.	IEC 60880-2 (Cat. A)
8	The safety documentation (for description see IEC 62138, 6.2.1) of operational PDS shall be evaluated against system specification (and system design). Inconsistencies shall be resolved.	IEC 62138, 6.2.3 (Cat. B)
9	The functions of operational PDS which are not required to support the system requirements specifications should be identified. Evidence of harmlessness should be given. For application functions of PDS, see Crit. No. 3 of this table.	IEC 62138, 6.2.3 (Cat. B)
10	No specific requirements are given for a suitability analysis for operational PDS of Class 3. It should be shown to be fit for purpose on the basis of its user documentation.	IEC 62138, 7.2.3 (Cat. C)

This table is an example for more detailed second level criteria to support first level criterion on suitability assurance. Criteria 1 to 7 in table S 1 are supporting criteria A 1, 8 and 9 are supporting B 1, and C 1 is supported by criterion 10.

Table S 2: Product assurance, criteria for software quality assurance

Criterion No.	Description	Document
1	The requirements of the PDS software quality plan and the corresponding verification and documentation shall be evaluated for conformance with the requirements of IEC 60880.	IEC 60880-2, 4.3.3.2.2 (Cat. A)
2	The PDS design shall be consistent with the constraints on the architecture and deterministic internal behavior of the system.	IEC 60880-2, 4.3.3.2.2 (Cat. A

Criterion No.	Description	Document
3	If practices differing from those of appendices A to F of IEC 60880 have been used for the development of the PDS, their adequacy shall be analyzed and justified according to clause 1 of IEC 60880. Their importance in the assurance of the software quality characteristics shall be evaluated in conjunction with the system requirements. The results of the evaluation and analysis shall be recorded for independent review.	IEC 60880-2, 4.3.3.2.2 (Cat. A
4	Non-conformities to IEC 60880 requirements, properties that cannot be verified, weakness or missing steps in the verification or documentation process shall be identified. Each shall be ranked according to its importance in the assurance of the software quality characteristics, and the importance to safety of the functions implemented in the system..	IEC 60880-2, 4.3.3.2.2 (Cat. A
5	The qualification documentation shall provide evidence that PDS integrated in hardware components, has been validated to demonstrate that it meets its functional and performance specifications.	IEC 60880-2, 4.3.3.2.2 (Cat. A
6	Where PDS components contain features that cannot be validated other than in the final system configuration, then validation of these features shall be performed in the final system configuration.	IEC 60880-2, 4.3.3.2.2 (Cat. A
7	The quality and degree of coverage of the validation tests performed on the PDS shall be evaluated with reference to the requirements of clauses 7 and 8 of IEC 60880 and additional validation tests performed if necessary.	IEC 60880-2, 4.3.3.2.2 (Cat. A

Criterion No.	Description	Document
8	When the evaluation of the design and of the life cycle is concluded, a document shall be produced to record that a) the PDS quality has been proved and no additional test or analysis of operating experience is required; b) complementary qualification shall be performed when the system configuration is available; c) lack of information has been detected during the evaluation, but this can be compensated by the completion of additional verification and validation, testing or code analysis and documentation; d) lack of information has been detected during the evaluation, which can be compensated for by use of operating experience; e) the PDS (or part of the PDS) requires modification for the intended use in the system and that it has the appropriate level of quality so the modifications may be performed in accordance with IEC 60880; f) significant problems can be expected because of the transfer of the PDS to new hardware; g) the PDS quality is not adequate and the PDS shall be rejected on grounds that the weakness are to great or the information inadequate for effective compensation; and h) the independence of the qualified functions/properties of the PDS from those not qualified has/has not been established.	IEC 60880-2, 4.3.3.2.2 (Cat. A
9	The criteria 1 to 8 may be reduced, especially those requiring full application of IEC 60880. Quality assurance shall divide the development and the modification phases of the software safety life cycle into specified activities. These activities shall include all what is necessary to achieve the required software quality, to verify that this quality is achieved, and to provide objective evidence to that effect.	IEC 62128, 6.1, 7.1 (Cat. B) and (Cat. C)

Also in this example for second level criteria supporting the first level criterion on product assurance, there is a staggered stringency; criteria 1 to 9 support the first level criterion A 2, criterion 10 support B 2 and C 2.

The missing difference in criterion 10 must be put in further details concerning “activities necessary to achieve the required software quality”, i.e. in “third level” criteria.

The tables S 1 and S 2 in this example are dealing only with the first level criterion “suitability assurance” and one part of the aspects of the first level criterion “product assurance”, i.e. with software quality assurance. The other part of the criterion “product assurance” is verification and validation, V&V, which also has to be broken down in more detailed criteria. Also the other first level criteria of tables 3, 4 and 5, i.e. documentation, product safety, system safety, interface, compensation by operating experience, error reporting, and modification should be detailed into appropriate levels of refinement. Examples for this process can be found in [7].

Conclusion

Extensive research work has been performed, mainly in the last ten years, to tackle the problem of qualifying pre-developed software for inclusion into systems important to safety. This research work did not render a unique solution how to do this, because of the great variety of applications, the differences in the usage of the software (application software, system software, tools, ...), and the safety relevance.

The results of this work, however, influenced some practical approaches, which tried to analyze systematically the issues involved, and to provide recommendations for the use of pre-developed software.

Also standardization groups in the nuclear field issued or are about to issue requirements for the application of pre-developed software.

In this paper an attempt is made to demonstrate exemplary a procedure how the different approaches can be brought together, to form a usable set of staggered criteria for the acceptance of pre-developed software.

This first examples show, that there will be no principal difficulty for a unified approach, because there are no major contradictions in the requirements / recommendations of the analyzed documents. The acceptance of such a unified procedure, however, needs the involvement of a broad international group of experts.

Literature

[1] IEC 60880-2: Software for computers important to safety for nuclear power plants – Part 2: Software aspects of defense against common cause failures, use of software tools and of pre-developed software, Dec. 2000

[2] IEC 61226: Nuclear power plants – Instrumentation and control systems important for safety – Classification, May 1993

[3] EUR 19265 EN: Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors, May 2000

[4] RSK-Leitlinien für Druckwasserreaktoren, Fassung 11.96, Kapitel 7: Elektrische Einrichtungen des Sicherheitssystems und der anderen Systeme mit sicherheitstechnischer Bedeutung, Nov. 1996

[5] IEC 62138 Draft: Software for I&C systems of safety class 2 & 3, March 2001

[6] IEC 61513: Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems, March 2001

[7] Preckshot, G.G., Scott, J.A:
A proposed acceptance process for commercial-off-the-shelf (COTS) software in reactor applications, Lawrence Livermore National Laboratory, UCRL-ID-122526, 1995

[8] Scott, J.A:, Preckshot, G.G., Gallagher, J.M.
Using commercial-off-the shelf (COTS) software in high-consequence safety systems, Lawrence Livermore National Laboratory, UCRL-JG-122246, 1995

[9] IEC 60880: Software for computers in the safety systems of nuclear power stations, 1986

[10] IEC TR 61838: Nuclear power plants – Instrumentation and control functions important for safety – Use of probabilistic safety assessment for the classification, Feb. 2001

[11] IAEA Technical Reports Series No. 384: Verification and validation of software related to nuclear power plant instrumentation and control, May 1999

[12] IAEA Safety Guide No. NS-G-1.1: Software for computer based systems important to safety in nuclear power plants, Sept. 2000

A Bayesian Approach to Risk Informed Performance Based Regulation for Digital I&C QA Programs

Swu Yih[1] Chin-Feng Fan[2] Sun-Li Chyou[1] Li-Sing Wang[1]

[1] Institute of Nuclear Energy Research, PO Box 3-11, Lung Tang, Taiwan, ROC.
Tel: +3-4711400-6335, e-mail: syih@iner.gov.tw

[2] Dept. of Computer Science, Yuan-Ze University, Chung-Li, Taiwan, ROC
Tel:+3-4638800-360, e-mail: csfanc@saturn.yzu.edu.tw

Summary

The purpose of applying Risk Informed Performance Based Regulation (RIPBR) is to reduce unnecessary conservatism existed in current regulations. This paper proposes a systematic way to find such unnecessary conservatism based on Bayesian Belief Network (BBN) modeling technique. First, a Bayesian based QA process model is developed, and the correspondent event tree based on the BBN is then derived. Risk insight into different QA activities can thus be investigated by comparing their contribution to final quality to determine their necessity. Independent V&V, prescribed by RG 1.168, is selected as a case study to demonstrate the effectiveness of this approach. The proposed Bayesian approach appears to be very promising in supporting the RIPBR practice for digital I&C QA programs. Related issues and future work are also discussed.

Introduction.

In last few years NRC has announced its PRA Policy Statement (NRC, 1995) and a series of Regulatory Guides (RG1.174~RG1.178) to promote the application of Risk Informed Performance Based Regulation (RIPBR) in all its regulatory activities. The purpose of RIPBR is to reduce *unnecessary conservatism* existed in current regulations, and thus reduce unnecessary burden to both licensees and regulators. This policy has created much incentive to nuclear industry to actively look for potential areas for cost saving. This paper introduces one of such potential areas and explains how to prepare evidence to justify it is unnecessary.

Based on a reported study (Waite, 2000) and our licensing review experience (Yih, 1999), we consider the current regulatory requirements for QA programs of digital I&C systems to be a proper candidate for applying RIPBR. On one hand, the current digital I&C QA program regulations probably are the most complicated in terms of the number of documents involved (Waite, 2000). On the other hand, digital I&C system development, especially in software quality assurance aspect, always involves certain degree of uncertainty and unpredictability (Padberg, 1999). Moreover, industry experience clearly shows that various nuclear digital I&C projects exhibited a large fluctuation in resource utilization efficiency. For example, Sizewell B (Marshall, 1994) and Chooz B (MacLachlan, 1994) spent significant resources on their QA program, while they still suffered from critics and doubts about their safety quality. On the contrary, K6/K7 digital I&C project (Fukumoto,1998) consumed relatively less resource on its QA program, but still achieved satisfactory safety performance. Obviously, these realistic cases reveal that the current regulations of digital I&C system QA programs indeed do have ample space for resource efficiency improvement. Meanwhile, our on-going Lungmen Project is gradually showing difficulty in fully complying with the current digital I&C regulations (Yih, 1999). All these cases justify the need for application of risk-informed approach to digital I&C systesms. The problem is how to meet relevant RIPB regulatory requirements. This problem can be divided into two questions. The first one is whether RIPBR

is applicable to digital I&C systems? If the answer is *yes*, then the second question will be how to prepare needed information to meet regulatory requirements. Our previous paper (Yih, 2000) has investigated the applicability of RIPB and the answer is positive. The purpose of this paper is to further develop a practical approach to implementing the concept.

In the following, we will first describe the related regulatory issues. Then, we will present the basic approach to performing qualitative risk analysis based on Bayesian Belief Network (BBN) to identify unnecessary conservatism. A case study dealing with the issue of independent verification and validation (IV&V) will then be discussed, followed by a conclusion.

Regulatory issues for applying RIPBR to QA programs of digital I&C systems.

We will give an overview of the current digital I&C QA requirements to show their complexity and overwhelming document size. Then we will explain relevant regulatory requirements needed when applying RIPBR to digital I&C QA programs.

Current licensing requirements for digital I&C QA programs.

The major regulatory requirements for digital I&C QA programs are described in Chapter 7 of Standard Review Plan and associated references. There are more than 30 documents related to QA program requirements. The general structure of these documents can be presented in a hierarchical format as shown in Fig. 1.

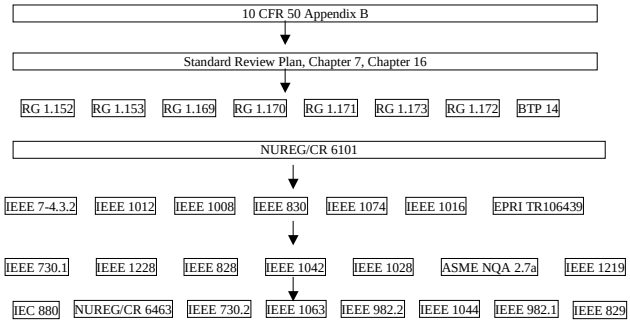


Fig. 1. Document structure of regulation and guides for digital I&C QA programs

The kernel part of these documents consists of IEEE Software Engineering Standards. IEEE standards are written for general application purpose; therefore, they tend to be very comprehensive and generic. The total number of pages of QA related standards exceeds 2,000. One can easily imagine what a huge load it will be on those people who have to prepare documents and those who have to review the documents. On the other hand, it should not be too difficult to find unnecessary conservatism for a specific case from these general-purpose documents.

Applicable regulatory guides for applying RIPBR to digital I&C QA program.

First we will review the RIPBR in general, then we will discuss Regulatory Guide 1.176 in more details because it is the most relevant guidance to digital I&C QA activities.

On August 16, 1995, NRC announced its Policy Statement (USNRC, 1995) of applying PRA techniques to "*all regulatory activities*" to the extent supported by the state-of-art methods of PRA. The phrase "*all regulatory activities"* naturally encompasses digital I&C QA programs but under the pre-

condition that the *state-of-art* PRA techniques can support the corresponding risk-informed decision-making process. The purpose of this policy statement is to improve the regulatory process by promoting "*more efficient use of agency resources*," and "*reduction in unnecessary burden to licensees."* Several Regulatory Guides have also been issued to help the industry to implement this policy. The most important guide is RG1.174: "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant Specific Changes to the Licensing Basis." (USNRC, 1998a) This guide sets up the basic principles and procedure of using PRA insights to modify existing licensing basis so as to reduce burden to public utility. The application of RIPBR has been expanded to several areas, and the results are promising. For example, South Texas Nuclear Power Plant has applied RIPBR to component classification. The number of safety components is significantly reduced; it is estimated that two million dollars can be saved due to this re-classification (Apostalakis, 2000). This also reduces the workload of regulators because fewer components need to be inspected.

RG 1.176: "Approaches for Applying RIPB to Graded QA Programs" (NRC, 1998b) is the most suitable guide for the digital I&C QA programs. RG 1.176 prescribes basic concept and necessary steps when evaluating a graded QA program application. Fig. 2 shows five principles to be considered during evaluation process. Our preliminary evaluation concludes that digital I&C RIPBR can meet four of the five principles quite straightforwardly. Only the fifth principle needs to be elaborated in more details. In the next section, we will present a technique for assessing risk impact due to a QA program change.

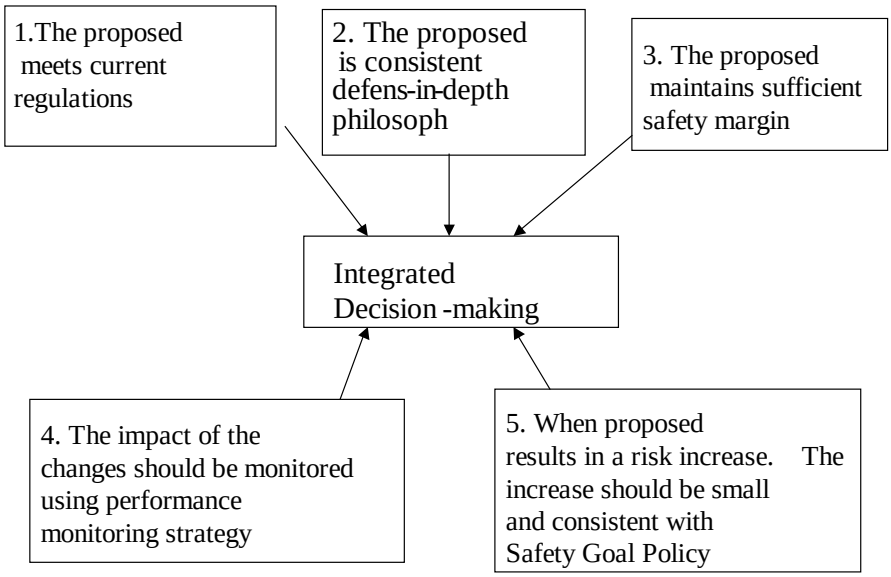


Fig. 2. Principles of RIPBR Decision-Making Process

Development of a risk analysis technique for digital I&C QA programs.

Our intention of applying RIPBR to digital I&C system is to reduce unnecessary conservatism existed in QA requirements. To justify such reduction, RG 1.174 requires an assessment of risk impact due to the proposed reduction. However, current state-of-art PRA techniques do not support an acceptable quantitative risk assessment for a typical QA program. Fortunately, RG 1.176 accepts a *qualitative* risk assessment for the graded QA activities that do not have quantitative PRA data. In this section, we will present our proposed approach to such assessment.

Basic concept of risk analysis for QA programs.

The purpose of QA program risk analysis is to explore the detailed information of undesired events associated with the QA program. Its task is to analyze potential scenarios and their occurring probabilities of a poor quality product produced under this QA program. Once such information is available, we can compare and rank the importance of relevant QA activities, and thus, identify the location of the vulnerable weak points. Our approach to obtain such scenario information is to develop a QA process model to generate QA failure scenarios.

A QA process model consists of elements representing software development staffs, software QA staffs, development activities, QA activities and documents generated. Our major concern, quality, is represented as defects density. Each element is represented as a node and is connected based on its casual relation with other elements. Each node is further designated with 2~5 states representing its status, for example, the undesired event is represented as defect density at *high* status. In reality, the relation between QA process elements is not static and fixed, i.e., the influence of one node on the other node often exhibits probabilistic and interactive behavior. In order to represent the probabilistic behavior of QA process, we apply Bayesian Belief Network (BBN)(Jensen, 1996) technique. A typical QA process represented in BBN is shown in Fig 3.

Concept of Bayesian Belief Network (BBN).

Bayesian Belief Network is a system modeling technique for representing systems that exhibit probabilistic behavior. A BBN consists of groups of connected nodes; it is basically a directed acyclic graph representing the causal influence between nodes. Each node represents a random variable with discrete values, and edges represent cause-effect relationship between nodes. The influence relations between nodes are described by Conditional Probability Tables (CPT). The value represents the degree of strength of the casual relation between two linked nodes. BBN provides formula to update CPT values once an entry of CPT changes. The initial values of CPT can be determined by experts; the table indicates that the node is in a specific state given the state

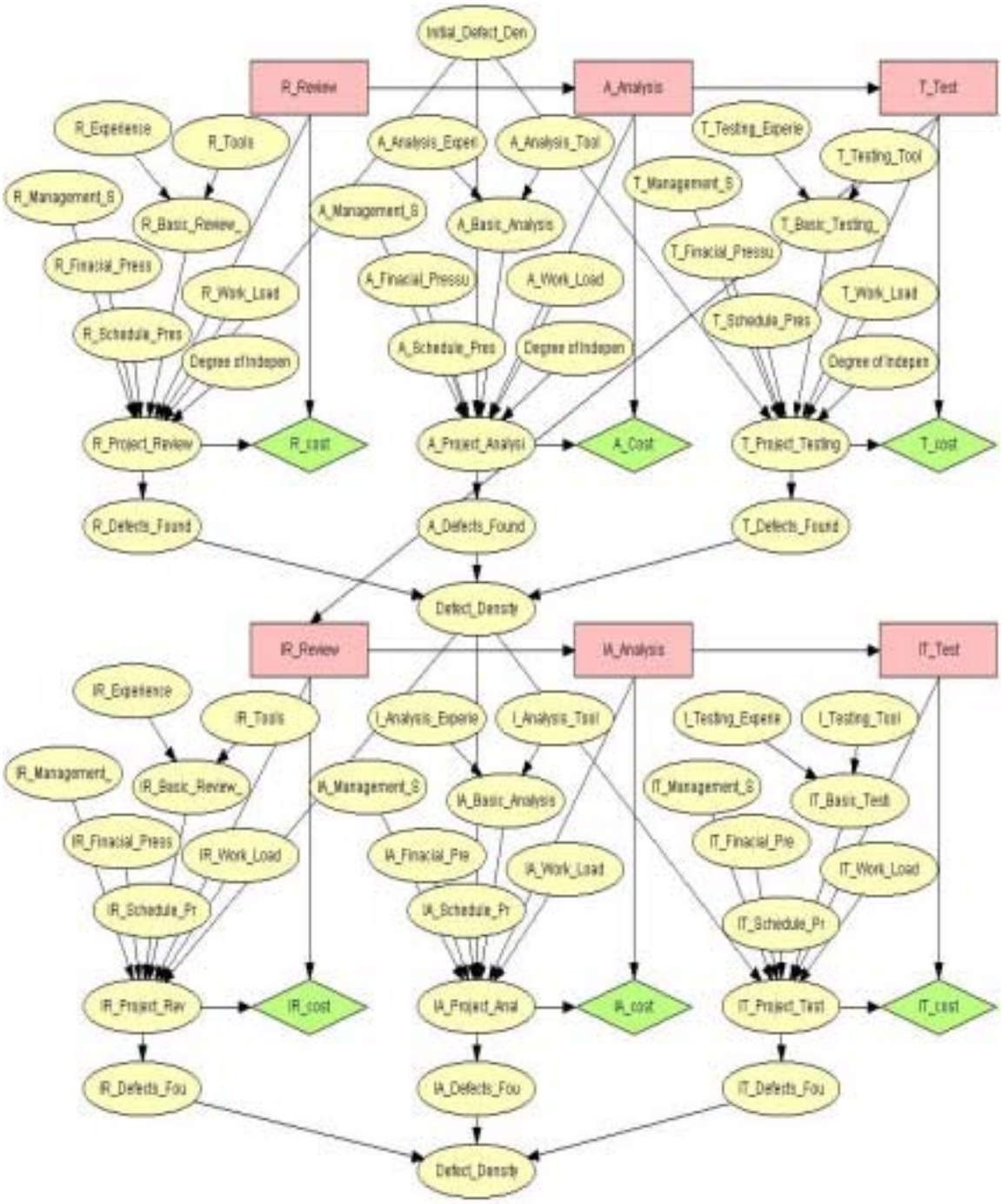


Fig. 3.
BBN Model of Software QA Process

of the influence nodes (parent nodes). Once there is a new evidence, the values of nodes can be recalculated either from parent nodes to child nodes or vice versa. Thus the dynamic behavior of modeled system is determined by CPT values. A BBN based QA process model is shown in Fig. 3.

Derivation of QA program failure scenarios.

The QA process model then is used to generate complete QA process scenarios. The process of failure scenario generation is shown in Fig. 4 and also explained as follows:

Step 1: From the BBN, get the next node, which either has no parents or whose parents have been all processed.
Step 2: add the node to the event tree and calculate its path probability
Step 3: examine whether truncation or stopping rules are met
Step 4: if yes go to Step 7
Step 5: mark this node as processed
Step 6: Increase the event sequence number by 1 and go to step 1
Step 7: Is there undeveloped node, if yes go to Step 1
Step 8: stop

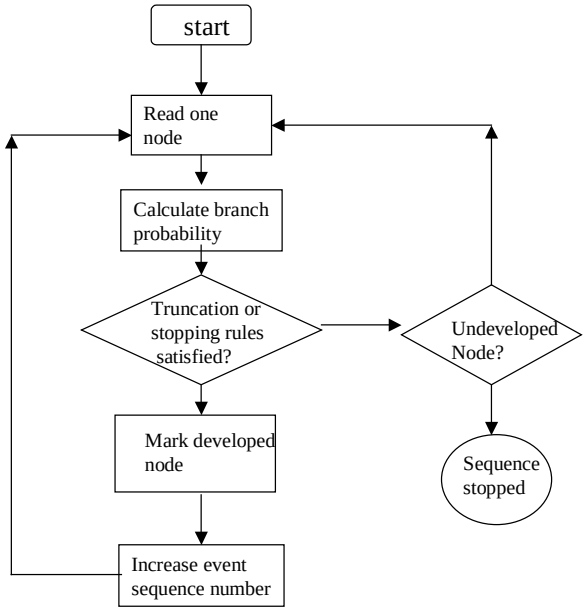


Fig. 4. Event Tree Derivation Process

Our proposed method first enumerates major influence factors, and constructs the BBN for system risk; an event tree based on same influence factors is then generated using the above procedure. Tree trimming will be performed to delete the impossible branches and thus control the exponentially explosive problem in the event tree construction. The numbers of occurrences of final outcomes of the tree will then be counted to draw the *risk profile* graph. The graph can help identifying potential areas of unnecessary conservatism. It can also help determining whether the resulting outcomes of proposed QA program change are acceptable or not.

Case Study: Is IV&V requirement prescribed by RG 1.168 an unnecessary conservatism?

In this section we apply the proposed technique for finding a potential unnecessary conservatism existed in current digital I&C QA requirements.

Background and motivation.

Software *verification* and *validation* (V&V) is a critical task of digital I&C QA programs. Verification determines whether the output of a given development phase satisfies the requirements of a previous phase and validation determines whether the final product satisfies intended use and user needs. Independent Verification and Validation (IV&V) is the V&V performed by independent group other than the development team. The V&V can be done internally or externally (i.e., IV&V). Obviously the cost of later (IV&V) will be significantly larger than the former (V&). Thus, the issue of IV&V naturally becomes a critical concern for every stakeholder involved in digital I&C projects. The issue whether to use IV&V or not has drawn lots of questions and hot debate. In the following, we will briefly describe IV&V related experience and reports that can demonstrate its importance and controversy.

Nuclear Industry

- Sizewell B ((Marshall, 1994) invested a great amount of resource in conducting an independent verification and validation task. This IV&V added 60% extra cost to the overall expense without finding any important defects. This is the most famous case of an over-killed digital I&C IV&V project in nuclear industry.
- Because RG 1.168 explicitly requires that V&V has to be done *independently*, Lungmen I&C project therefore still needs to hire another consultant company to perform IV&V in order to comply with this requirement.

Aviation / Space Industry

- After spending 3.2 millions per year on IV&V activities (Gruman, 1992) without significant defect finding, NASA space shuttle software QA program considered IV&V was not worthwhile and decided to stop its IV&V contract with Intermetrics. But US Congress stepped in, and NASA decided to resume its IV&V project due to Congress' intervention.
- The Airworthiness regulation mandatory requires some software QA activities be performed "with independence" (RTCA, 1992). In a large scope industry survey (Hayhurst, 1999), digital avionics manufactures considered *independence* as a questionable requirement and asked Federal Aviation Agency to re-consider its value.

Academic /Research

- A research was conducted by J.D. Arthur (Arthur, 1999) to evaluate the effectiveness of IV&V. It found that IV&V is more effective in requirement and design phrase.
- A project sponsored by NASA evaluates the financial effectiveness of IV&V (Raffo, 2001). Its purpose is to convince stakeholders that IV&V is important and worthwhile.

These reports and experiences clearly demonstrate the controversial nature of IV&V within a QA program. Thus it is worthwhile to conduct risk analysis of IV&V to explore more detailed information of its cost-effectiveness.

Assess risk impact of IV&V for a digital I&C QA program.

In the following, we will use IV&V as a case study to demonstrate the usage and effectiveness of the proposed approach. We proceeded the case study as follows:

Steps 1: Collect influence factors of QA program and IV&V.

In general, IV&V may be performed through review, testing, and analysis. The technique differences mainly lie in that analysis needs mathematical skill and maturity, review depends on experience, while

testing requires comprehensive test cases and tools. As to the differences of IV&V and V&V, we focus on the schedule and financial pressure of the internal V&V, while the IV&V can be free from it. Thus, the influence factors for verification and validation are listed in Fig. 3. These factors can be categorized into four groups:

(1) General factors
(2) Technique-related factors
(3) Activity-related factors
(4) Performance shaping factors

General factors deals with schedule/financial pressure and degree of independence. Technique-related factors consist of review experience, analysis capability, as well as testing and analysis tools. Activity-related factors may have review depth and scope, testing coverage, as well as analysis rigorousness. Performance shaping factors consist of documentation quality, software initial defects, workload, and management support.

Step 2: Bayesian-based QA causal influence model

We then construct the corresponding BBN, shown in Fig.3. Note that in the network, technique-related factors influence verifiers' potential; while verifiers' potential, and the rest types of factors influence V&V effectiveness. The rectangles in Fig. 3 are decision nodes; the diamond nodes represent costs of different activities.

Steps 3 : Event Tree and failure scenarios derivation

We now can construct the event tree with the same influence factors using the procedure described in Fig. 4. However, the original BBN is somewhat complicated for our explanation. Instead of considering analysis, review, and testing, we simplified the network to include general internal V&V and IV&V parts. We also further simplify the factors by starting with V&V potential, and by considering only the initial defects and time pressure. Fig. 5 is a portion of the generated event tree.

Step 4: Create Risk Profile

In the event tree, results both from V&V and IV&V will be categorized into five levels (very high, high, medium, low, and very low). There exist many unlikely branches, which can be trimmed. For example, when the initial defect density is low, the resulting V&V defect density cannot be *very high* or *high.* For the remaining branches, since there is no evidence of their occurring frequencies, we may assume evenly distributed probabilities among them. We calculated the numbers of occurrences in each level of the product's final defect density for the cases with IV&V and that without IV&V. Resulting figures are shown in Table 1. After getting the occurrence counts, we can draw the risk profile graph as shown in Fig. 6, where the region under the dashed line represents acceptable risk.

Step 5: Performance Monitoring (Update BBN based on performance data)

If IV&V requirements is relaxed then a performance monitoring scheme is needed. Once the project starts, more information can be gathered. The BBN built in Step 2 can then be used to assess the potential risk of the project. BBN can be employed to constantly monitor and assess the potential project risk using the evidence (data) observed during the progress of the project. Predictions can be made to answer the what-if questions; thus, appropriate process and resource adjustment can be made based on BBN assessment.

Two extreme cases were examined to judge the effectiveness of IV&V. Case 1 deals with a good quality product with capable internal V&V team. Case 2 considers a poor quality product with low capability internal verifiers. In the former, the costly IV&V is not justified; while in the

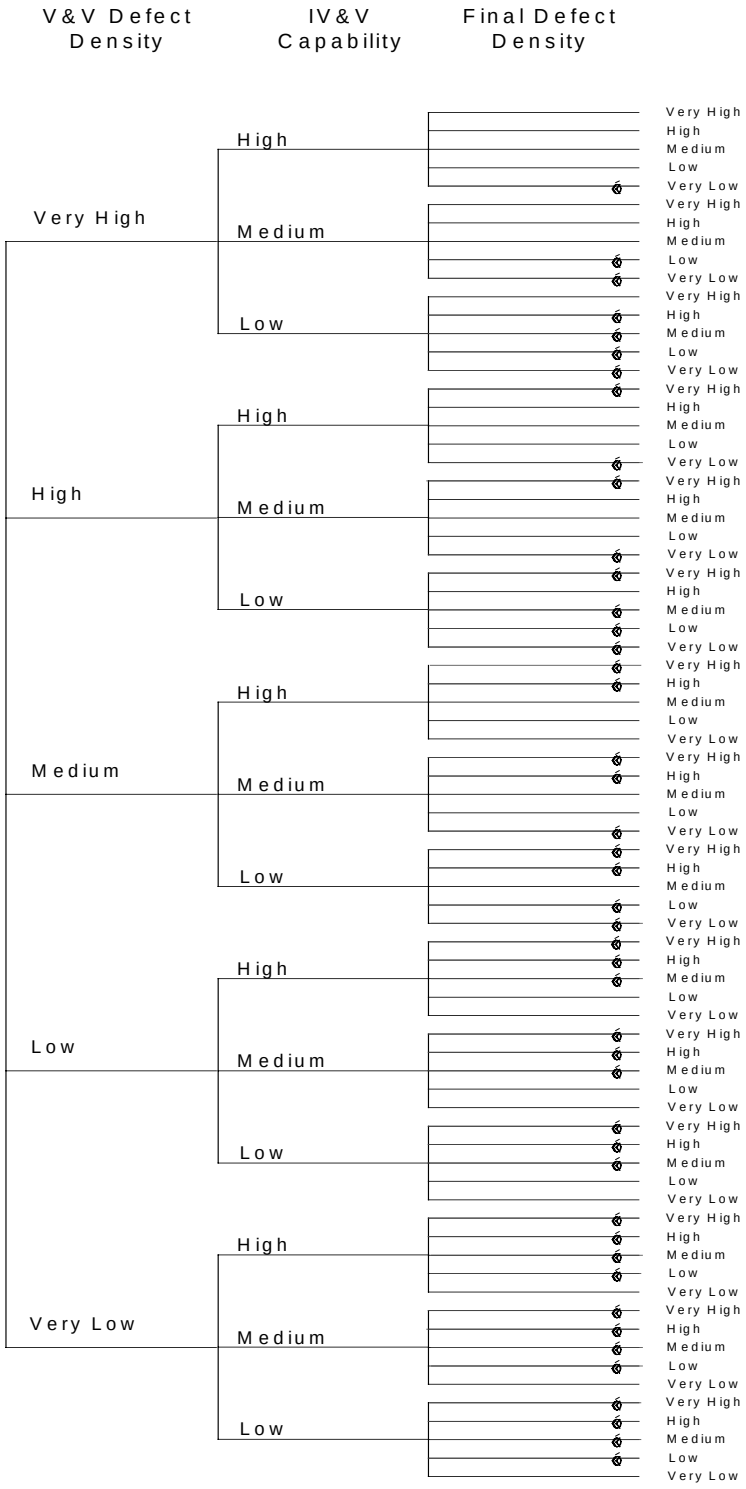


Fig. 5. Partial event tree for simplified IV&V

Table 1. Counts of resulting branches in the event tree

Item counts	With internal V&V & IV&V	Without IV&V
Total branches	1350	90
trimmed	1058	42
Valid	292	48
Final defect density(=*very high*)	12/292=0.041	4/48=0.083
high	41/292=0.140	11/48=0.229
medium	78/292=0.267	16/48=0.333
low	94/292=0.322	12/48=0.250
Very low	67/292=0.229	5/48=0.104

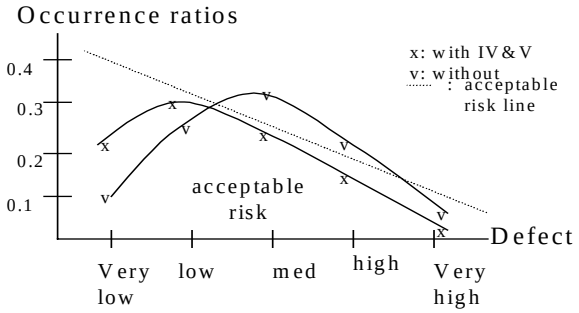


Fig. 6. Risk Profile generated by factors with equal probabilities

latter, IV&V does greatly improve the product quality. It can be seen from this risk profile that whether IV&V is conservatism really depends on various initial conditions. That is, the conservatism can be determined only after these initial conditions are identified. This figure can also be used to explain why Sizewell B was an over-killed case and K6/K7 was successful.

Conclusion

It is a consensus view between licensees and regulators that there may exists unnecessary conservatism in current digital I&C QA regulatory requirements. If such conservatism can be identified and reduced then the limited resources of both licensees and regulators can be utilized more effectively. The goal of RIPBR promoted by USNRC is to provide a generic regulatory framework to eliminate such conservatism in all NRC's regulatory activities (NRC, 1995). However, in order to take the advantage of RIPBR, one needs to develop techniques to *identify* unnecessary conservatism, and such techniques have not been fully established for digital I&C systems yet. This paper proposed a Bayesian-based approach to identifying unnecessary conservatism in current digital I&C QA program requirements. A QA program causal influence model is developed first, and then a correspondent event tree enumerating potential scenarios is derived based on this model. Thus risk insight into different QA activities can be investigated by comparing their contribution to scenario results. The QA activities that do not have significant impact on results apparently can be classified as unnecessary conservatism. *Independent V&V*, prescribed by RG 1.168, is selected as a case study using the proposed technique to assess its necessity.

In summary, the proposed Bayesian approach appears very promising in supporting the RIPBR practice for digital I&C QA programs. However, there is still more work yet to be done before this technique can be fully utilized; for example, issues of uncertainty, sensitivity and importance, criticality measures, etc.; all are necessary information items to be submitted in a formal RIPB application. In the future, we will conduct a more comprehensive investigation to consider more QA related factors and to develop methods to address the sensitivity and uncertainty issues.

References

(Apastolakis, 2000) Apastolakis, G, Speech presented at Atomic Energy Council, Taipei, Taiwan, July 17,2000.

(Arthur, 1999) Arthur, J.D., et al., Evaluating the Effectiveness of Independent Verification and Validation, *IEEE Computer* 32(10): 79-83.,1999.

(Fukumoto,1998) Fukumoto,A, et al**,** A verification and validation method and its application to digital safety systems in ABWR nuclear power plants, *Nuclear Engineering and Design*, V183N2, pp.117-132, July 1998.

(Gruman, 1992) Gruman, G., Under Pressure, NASA Renews IV&V Contract, IEEE Computer, p.106, November, 1992.

(Hayhurst, 1999) Hayhurst, K. et al., Streamlining Software Aspects of Certification: Report on the SSAC Survey, NASA/TM-1999-209519, August 1999.

(Jensen, 1996) Jensen, F. V., *An Introduction to Bayesian Networks*, UCL press, 1996.

(NRC, 1995) NRC, Use of Probabilistic Assessment Methods in Nuclear Activities, Final Policy Statement, Federal Register, V60P42622, August, 1995.

(NRC, 1998a) NRC, RG 1.174: An Approach for using Probabilistic Risk Assessment in Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis ,

(NRC, 1998b) NRC,RG 1.176 An Approach for Plant-Specific, Risk-Informed Decision-making: Graded Quality Assurance

(MacLachlan, 1994) MacLachlan, A, French Regulators 'lost hope' of Proving Chooz-B Digital I&C System., *Inside NRC*, 30 May, p6-7, 1994.

(Marshall, 1994) Marshall, P and Silver, R. Sizewell B Computer Controversy Looms Over Fuel Load Schedule, *Nucleonics Week*, 34, p1. 1994

(Padberg, 1999) Padberg, F., A Probabilistic Model for Software Projects, ESEC/FSE'99, LNCS 1687, pp.109-126, Springer-Verlag, 1999.

(Raffo, 2001)NASA, Financial Measures for Evaluating Software IV&V Activities, www.sba.pdx.edu/faculty/davidr/draccess/web/reasearch

(RTCA, 1992) RTCA/DO 178B, Software Considerations in Airborne Systems and Equipment Certification, Dec. 1992. (Waite, 2000)

Waite, C., Digital System Assessment: Great in Practice, But It Will Never Work in Practice, NPIC&HMIT 2000, Washington DC, Nov. 2000.

(Yih,1999) Yih, S, Chan-Fu Chung, 1997~1999 Lungmen I&C Licensing Progress Report, AEC Internal Report, Oct.,1999.

(Yih, 2000) Yih, S, et. al., The Applicability of Applying Risk Informed Performance Based Approach to Digital I&C Regulation, NPIC&HMIT 2000, Washington DC, Nov. 2000.

TECHNICAL SESSION 4;
SOFTWARE LIFE CYCLE ACTIVITIES
Chairmen: G. Dahll, F. Krizek

Implementation of Software Independent Verification and Validation for Lungmen Distributed Control and Information Systems

Jiin-Ming Lin[1] - Jeen-Yee Lee[2]

[1]*20F, 242, Roosevelt Road, Sec. 3. Taipei, Taiwan Power Company, Taiwan, ROC*
Tel.: +886 2 23667165, Fax: +886 2 23671675, U827725@taipower.com.tw

[2]*20F, 242, Roosevelt Road, Sec. 3. Taipei, Taiwan Power Company, Taiwan, ROC*
Tel.: +886 2 23667156, Fax: +886 2 23671675, D02705@taipower.com.tw

Summary

This report presents the implementation of the software independent verification and validation (IV&V) for the Distributed Control & Information Systems (DCIS) of the Lungmen Project. It covers the codes and standards as applicable, the scope of the software IV&V and the documents reviewed, the organizational structure and activities for performing the IV&V work. Furthermore, the problems which were encountered during the implementation are discussed, along with solutions for them.

1. Introduction

Digital instrumentation and control systems share data transmissions, functions, databases, and process equipment to a much greater degree than analog systems. While this sharing forms the bases for many of advantages of digital systems, it also raises concerns with respect to its vulnerability to a different type of failure. A concern is that using shared databases and process equipment has a potential for common cause failure in redundant equipment. Another concern is that the software, if not properly designed, may have errors which may defeat the redundancy achieved by the hardware architectural structure. Because of these concerns, the software of digital I&C systems must be verified and validated by a rigorous certification process to ensure with high confidence that the requirements of the software were met. This is particularly important for applications in nuclear power plants.

Based on the country of origin concept, in performing the software V&V for the Lungmen project, the USNRC Standard Review Plan (SRP) Chapter 7, BTP-14 and USNRC Regulatory Guide 1.168 are followed. Two teams-the GE independent verification and validation team (GE IVVT) and the owner (the TPC) IVVT (OIVVT), are organized by GE and TPC respectively to carry out the IV&V tasks.

In this paper, Section 2 first presents the codes and standards as applicable. In Section 3 we describe the scope of the software IV&V and documents reviewed. In Section 4 we describe the organizational structure and the IV&V activities performed at different levels of the organizations. In Section 5 we discuss the problems encountered during the implementation process, along with solutions for them. Finally, conclusions and recommendations are given.

2. Applicable Codes and Standards

Codes and Standards that are applicable for the software development and IV&V in the DCIS for Lungmen Project are primarily those of the country of origin, i.e., the United States of American. The major Codes and Standards are as follows:

- 10 CFR 50, Appendix B
- Regulatory Guide 1.168, Verification, Validation and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants, Sept. 1997
- NUREG/CR-6101, Software Reliability and Safety in Nuclear Reactor Protection Systems, Nov. 1993
- Lungmen Standard Review Plan (SRP), Chapter 7, Branch Technical Position (BTP)HICB-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation & Control Systems.
- IEEE 1012-1986, Standard for Verification and Validation Plans
- IEEE 1028-1994 Standard for Software Reviews and Audits
- IEEE 7-4.3.2 1993, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.
- EPRI TR-106439, Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Applications.

3. IV&V Work Scope and Documents Reviewed

All safety systems of the Lungmen plant are covered in the software IV&V work. In addition, five (5) R (reliable)- class systems are selected and included. The work scope is described in this section. Design documents related to all of these systems are reviewed by the OIVVT, the GE IVVT reviewed only design documents related to safety systems.

3.1 Safety Systems

There are five safety systems in Lungmen DCIS. They are Reactor Protection System (RPS), Neutron Monitor System (NMS), Process Radiation Monitoring System (PRMS), Containment Monitoring System (CMS), and Engineered Safety Features (ESF). The software development for all these safety systems follows the BTP-14 requirements. Along with the development, the IV&V activities are performed. Of the safety systems, RPS, NMS, PRMS and CMS are designed by GE NUMAC, and ESF is sub-contracted by GE to Eaton Corporation.

3.2 Control Systems (Class R system)

According to the USNRC SRP Section 7.7 requirements, control systems having a significant impact on plant safety, should be a focal point of regulatory review. Considering this five class R control systems, which are Feedwater Control System (FWCS), Recirculation Flow Control System (RFCS), Automatic Pressure Regulator (APR), Steam Bypass and Pressure Control System (SBPC), and Rod Control Information System (RCIS) are selected and included in the software OIV&V scope. For these five systems, GE sub-contracts to Foxboro with FWCS, RFCS, and APR, and Foxboro uses Intelligent Automation (I/A) Platform to perform the software development. Also, GE sub-contracts SBPC to GEIS

(GE Industrial Systems) and GEIS uses GEIS MARK VI SPEEDTRONIC turbine control system to implement software for SBPC. Still another sub-contractor from GE for the RCIS, Hitachi base on K7 experience to manufacture the I&C of Lungmen RCIS. In the development process, GE provides a system design description (SDD), hardware/software specification (HSS), hard/software I/O, and logic diagrams (LD) to sub-vendors for all functions of the above five systems. Then, the sub-vendors follow GE's requirements to develop hardware and software design.

3.3 Documents to be Reviewed

As part of the IV&V activities, the documents that are to be reviewed for Lungmen project are as follows:

3.3.1 Design Documents

For each phase, design documents of safety systems, based on SRP BTP-14, of the software development life cycle, include software plans, software requirement specification, software design output, source code listing, and test reports. These documents are subject to the IV&V review.

3.3.2 Software Safety Analysis Reports

Software safety analysis reports are prepared by the software safety engineers of software design team based on IEEE 1228-1994 standard requirements in each software development phase. These reports are reviewed by the IV&V teams.

3.3.3 Internal V&V Reports from Vendor

As a general engineering practice, most companies have design reviews or verification by peers or qualified engineers other than the engineers responsible for the work. The reports from this effort are called internal V&V reports in the Lungmen project.

- **GE NUMAC**

The internal V&V reports will be prepared by software design organization in accordance with EOP 42-6.00 (Independent Design Verification) and EOP 40-7.00 (Design Reviews) of GE engineering operation procedure (EOP) or equivalent to ensure the quality of the design process and the associated documents produced.

- **Eaton**

The internal V&V reports of Eaton will be prepared by Eaton nuclear quality assurance team based on Eaton's software V&V plan to perform the internal V&V activities. These reports and abnormal condition event reports will be summarized to V&V summary reports and delivered to GE IVVT for review.

3.3.4 The Evaluation Report for Acquired Software

Acquired software refers to:

1. Support software: such as commercially available software and development tools (i.e., compilers and databases).
2. Third party software: software produced from outside sources and incorporated into the final software-based product.
3. Previous developed software

All acquired software should be evaluated, reviewed, or tested by GE responsible engineers in design team based on relevant code or standard prior to use. Also, these evaluation reports will be submitted to GE IVVT for review.

4. Organizational Structure and Activities for Software IV&V

Software IV&V tasks of Lungmen project are performed by GE IVVT and the OIVVT. Furthermore, the regulatory authority, the ROCAEC will perform the audits, on as-needed basis, to TPC and vendor site during the software development. The organizational structure basically corresponds to the licensing frame as shown in Figure 1. Also, the software V&V activities performed at different organizational levels are briefly described as follows:

4.1 GE IVVT

4.1.1 Members

The GE IVVT members include: individuals transferred from the GENE service department that do not participate in the Lungmen design activities; qualified third-party organizations for specific independent V&V tasks; TPC engineers; experts from Institute of Nuclear Energy Research (INER).

4.1.2 Activities

The GE IVVT is responsible for

- Preparation of the software IV&V plan, according to the applicable Code and Standard in Section 2.
- Reviewing internal V&V reports, acquired software evaluation reports, software safety analysis reports, and Eaton's V&V summary reports.
- Review of all software development plans and software requirement specification based on NUREG/CR-6101 checklist for safety systems developed by GE NUMAC and Eaton.
- Preparing the sampling criteria to perform the independent review of the software design output during detail design, coding, and testing phase.
- Establishing the GE IVVT Tracking System. The GE IVVT Tracking System is for record tracking for evaluation records, meeting minutes, anomaly items, open items, and review status. This system allows GE IVVT and TPC to track the anomaly and open items.

In addition, as the consultant to the GE IVVT, Computer Dependability Associates (CDA), provides advice on GE IVVT strategy, IV&V plan and other software development Plans. Also, they evaluate the performance of GE IVVT in each software phase, and provide support in interpretation of the Codes and Standards as necessary.

4.2 OIVVT

4.2.1 Members

The OIVVT consists of members from MPR Corporation, TPC, INER, and Stone & Webster (S&W). MPR is responsible for conducting and coordinating all OIV&V activities.

4.2.2 Activities

The OIVVT performs the following activities to assist TPC in fulfilling the role of self-regulation, as expected by the regulatory authority.

- Document Reviews

Based on Section B.4 on Review Procedure, BTP-14 of SRP Chapter 7, document reviews are required to ensure that the software of GE and his sub-contractors meets the acceptance criteria as defined in Section B.3 Acceptance Criteria, BTP-14 of SRP Chapter 7.

- Site Visits:

Site visits are conducted during each phase. A minimum of 30 site visits is planned to GE and his sub-contractors. The objective of the site visit is to observe and obtain objective evidence that programs, policies, and procedures are being appropriately applied.

- Thread Audits:

Thread audits are conducted during each phase. The OIVV team will "pull" a minimum of 50 threads for audit. The objective of the thread audit is to evaluate the consistency in translation from requirements to designs through review of documents and procedures.

- Phase Reports

The OIVV team prepares phase reports and submits to regulatory authority for reference after accomplishing each phase. The report covers document review reports, site visit reports, thread audit reports, and anomaly reports completed by OIVV team during each phase. Also, all anomaly items are

delivered to GE and his sub-vendors for process, and tracked by the tracking system provided by MPR until accepted by the OIVVT

4.3 Republic of China Atomic Energy Council (ROCAEC)

As Lungmen project is the first application of software in protection, control, of a nuclear plant in Taiwan, ROCAEC has high concerns about the software development and V&V activities of Lungmen DCIS. For these activities, ROCAEC required that TPC periodically report to ROCAEC on the status of these activities. In addition, ROCAEC performed audits on TPC's management of Lungmen DCIS at TPC headquarters in April, 2000, and in June 2000, participated in an OIV&V site visit to GE, Eaton, and Foxboro to evaluate compliance by the vendor to the regulatory requirements in the software development. From these audits, ROCAEC issued audit reports requesting improvements by TPC. ROCAEC will keep performing such audits to TPC, GE, and sub-vendors to ensure the quality of Lungmen DCIS software meets regulatory requirements. .

5. Problems & Solutions

Problems that are encountered during the implementation are originated primarily from the first implementation of the related codes and standards, and include independence of the organizations performing IV&V and potential over-oversight of the software development.

5.1 Interpretation of R.G. 1.168 for Requirements on Independence

GE IVVT is organized under GE Nuclear Engineering (GENE) and is independent of the design team for the Lungmen project. However, measured from a restrictive perspective the independence of the GE IVVT is questioned, and an issue as to the interpretation of the real regulatory requirement came up. In addition, there seems to exist an inconsistency among 10CFR 50 App. B, BTP-14, and R.G. 1.168 requirements, in regards the V&V independence requirements[1]. For resolution of this issue, TPC, MPR, GE IVVT, and CDA held a meeting in San Jose in July, 1999. From this meeting, a resolution was reached based on CDA's proposed interpretation for the independence of R.G. 1.168 that "*The person accountable for V&V must also be independent of the person accountable for the design*." And that "*This independence must be sufficient to ensure that the V&V process is not compromised by schedule and resource demands placed on the design process.*" A key word here is "accountable," and it means exactly what it says. No more and no less. In GE's context, the IVVT Chairperson is accountable for the software V&V and he has sufficient independence from the designers. On this subject of independence, there is a good discussion in the 1998 edition of IEEE 1012, Annex C, which can be used for background reading and clarification.

During planning stage for the Lungmen project, TPC had surveyed the implementation of software IV&V activities in Chooz B of France and Sizewell B of U.K. Recognizing the importance of software V&V, TPC allocated a special budget for an OIV&V to enhance independence of the V&V.

In addition, due to the large amount of documentation produced during software development cycle, TPC also allocated another budget to contract with INER for reviewing all software design outputs. This also somewhat enhanced independence of the software IV&V.

5.2 Potential Work Duplicate between the OIVVT and GE IVVT

In order to augment the independence of software V&V, TPC organized the OIVVT to perform the V&V activities. This resulted in the OIVVT having scope of work which has some potential duplicate with the GE IVVT, and the software design team of GE having to make more efforts in addressing duplicated comments from GE IVVT and OIVVT, and schedule became a concern. Finally, through coordination, an agreement was reached that GE IVVT summarized the OIVVT and GE IVVT comments before delivering to GE design team for resolution. All open items were followed up through the GE IVVT tracking system. Of course, OIVVT used its own tracking system to follow up items of anomaly in design reviews, site visits, and thread audits from OIVVT activities.

When the OIVVT activities were planned to be included into the Lungmen project, GE had objection because they believed that OIVVT activities, such as site visit, would affect the design schedule. TPC clarified that the OIVVT activities would serve the function as self-regulation so as to facilitate licensing, and in the long run, would be beneficial to schedule control. This view point was finally accepted by GE and the work proceeded smoothly.

6. Conclusions

Since the establishment of the IV&V teams (the GE IVVT and the OIVVT) in 1999, the IV&V activities have been progressed smoothly. Two problems have been encountered though, but resolved. Also, from this implementation, a couple of recommendations for performing future software IV&V activities can be made. One is to fully understand the regulatory requirements on software IV&V before an IV&V project gets started. The other is to establish a tracking system for IV&V activities in IV&V project to facilitate control and monitoring of the issues identified.

7. Reference

1. Swu Yih, et al, ":Preliminary Evaluation of NRC Digital & Regulations based on Lungmen Licensing Experiences". In NPIC&HMIT 2000, Nov. 2000.

* Note•OIVVT(Owner Independent Verification & Validation Team)
ROCAEC(Republic of China Atomic Energy Council)

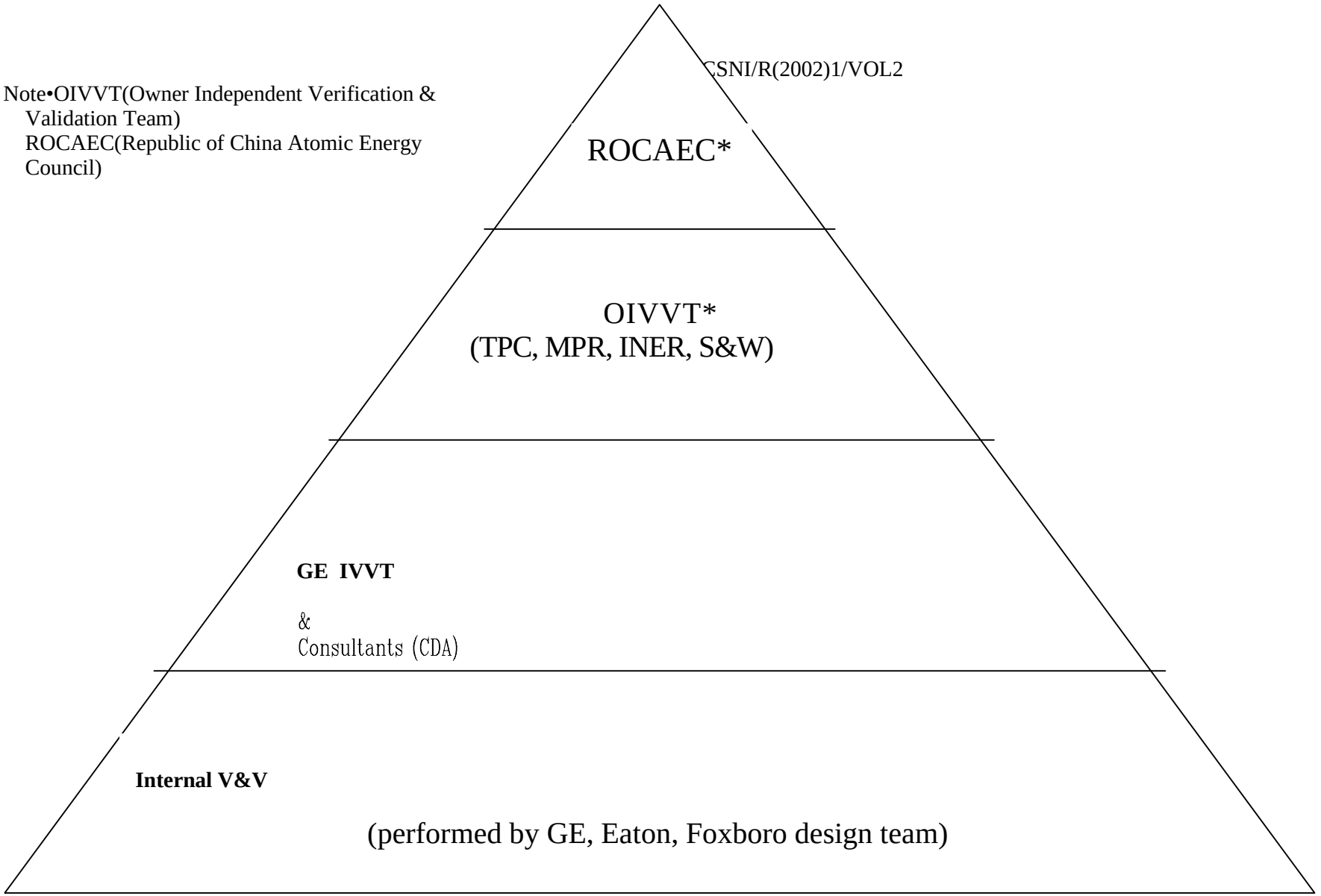


Fig. 1•Licensing frame of software IV&V on Lungmen Project

Static Analysis of the Software used in Safety Critical System of the NPP Temelin

Z. Piroutek, S. Roubal, J. Rubek

I & C Energo s.r.o., 190 11 Praha 9 – Bechovice, Czech republic
Tel.: +420 2 67062182, Fax: +420 2 67062182, e-mail: zpiroutek@ic-energo.cz, sroubal@ic-energo.cz, jrubek@ic-energo.cz

Summary

The presentation describes the Static Analysis used in project the Independent Assessment of the Temelin Safety System Software. There is described used methods, tools and process of performing of activities which were performed in collaboration of I&C Energo company with TA Group.

Introduction

The Independent Assessment of the Temelin Safety System Software was required by the Czech State Office for Nuclear Safety as a part of licensing process. The Independent Assessment was performed by the consortium under leading of American company SAIC (Science Applications Internal Corporation - founded in 1969) in 1999 - 2000. The other members of the consortium were TAG (TA Consultancy Service Ltd.), RRA (Rolls Royce and Associates Ltd.). As subcontractors were British Nuclear Electric and Czech company I&C Energo.

Independent Assessment was required on the four safety systems: Primary Protection System (PRPS), Diverse Protection System (DPS), Post Accident Monitoring System (PAMS), Diverse Monitoring System (DMS).

The assessment activities were performed on system documentation and source code included the following:

- assessment of adequacy of system software,
- verification of system requirements,
- verification of software requirements against system requirements,
- verification of source code against software requirements by using static analysis,
- dynamics testing of one PRPS division,
- verification of configuration and calibration data,
- safety case preparation.

General Description of NPP Temelin Primary Reactor Protection System (PRPS)

The PRPS is divided into three redundant reactor trip and ESF actuation safety Divisions (Divisions I, II and III). All reactor trip and ESF actuation Divisions are physically and electrically separated from each other. Each of the three redundant safety Divisions is composed of safety grade field sensors, Nuclear Instrumentation System (NIS) excore flux monitoring detectors and equipment, the Integrated Protection Cabinet (IPC) and associated Reactor Trip Switchgear (not supplied by I&C vendor). Each of the three redundant ESF actuation Divisions consist of the Engineered Safety Features Actuation Cabinet (ESFAC), the Integrated Logic Cabinets (ILCs) with associated Non-Programmable Logic Cabinets (NPL), the Main Control Board and Emergency Control Board Multiplexers (MMC) and the Data Highway Gateway cabinets (DHG). The Main Control Board and the Emergency Control Board manual system level signals interface directly to the IPCs and the ESFACs via hardwired I/0 lines. Manual control of each of the ESF components in each Division is provided through the Control Board Multiplexer cabinets to the Integrated Logic Cabinets over the optical Logic Bus data highways.

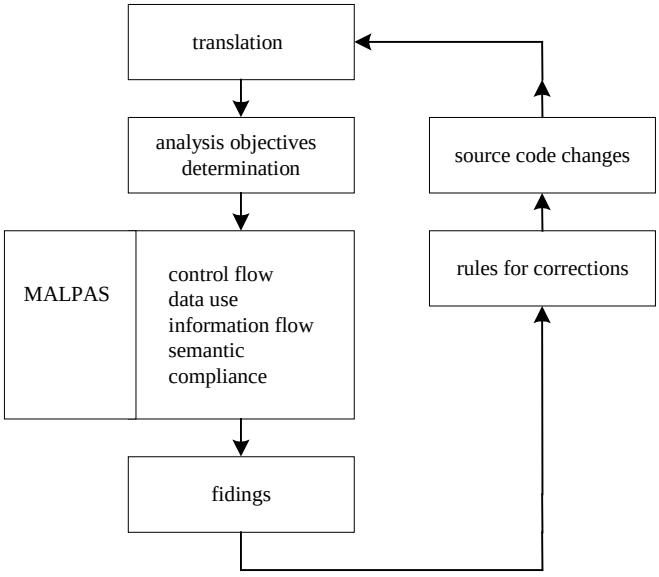
Static Analysis

The standard way of the SW testing is to use the dynamic testing method when the testing data are entered to the code input and the calculation is performed consequently. The results of this calculation are then compared with expected values and evaluated. However, this method is based on testing on the target hardware, but for large distributed system like protection system the problem of generating test data which exercises every path through the software adequately, in insoluble. Static analysis, which used mathematical techniques, is capable of achieving full path coverage. Using such technique it is therefore possible to demonstrate to high degree of confidence the absence of errors.

For complete static analysis the support tools are necessary. Such a tool can be the MALPAS code of English company TAG, which has been originally developed for military purposes and modified for civil purposes consequently. MALPAS uses directed graphs and regular algebra to represent the program under analysis. This tool was successfully used for independent testing of the protection system of the Sizewell B NPP in the UK. Because the similar protection system is used also in case of the Czech NPP Temelin, this tool was used for testing of the reactor protection system (PRPS and DPS). Our company I&C Energo participated under this project. of Independent Assessment of the Temelin Safety System Software.

Scope of Static Analysis

The static analysis process can be drawn in the following figure:



Documentation
Requirements are normally specified in the following documents:
Composite Block Diagrams
Software Design Description
Software Requirements Specification
Software Design Specification
Application Data Sheet

The main stages in the analysis process can be divided in the following:
- Translation + Review
- Goal Setting
- Syntax Analysis
- Semantic Analysis
- Optional Review
- Compliance Analysis
- Creation of PROCSPECS
- Review
- Finding + Sentencing

Translation

The first stage in the analysis process is to perform translation of the source code into MALPAS Intermediate Language (IL) program.
The translation process adopted for each of the safety critical modules consists of the following stages:
- Perform the actual translation. This may involve some degree of modification to the source code (pre-translation edits). Translation of a module is normally possible when PROCSPECs of the procedures are available.
- Perform any necessary post-translation edits.
- Run the IL Reader to identify all remaining IL errors.

The translation report shall be written including the resolution of errors and warning messages, any pre or post translation edits that were made.

Goal Setting

The goal setting is the process by which correctness properties are identified and the corresponding analysis objectives are captured. It is necessary to perform a subsystem - wide review of the software to identity correctness properties and corresponding analysis objectives prior to the start of the analysis proper.

These fall into two categories:
- Ensure integrity of language use (goal setting identify functional integrity properties, non-functional properties are checked by the other MALPAS analysers).
- Identify hidden assumptions.

The Goal Setting report should identify the analysis objectives for each procedure in the module or subsystem. The report should also include an overview of the module or subsystem's functionality.

Syntax Analysis

Syntax analysis is a collective term used to encompass Path Assessor, Control Flow, Data Use and Information Flow analysis, and it is used for the initial investigation of the software under analysis.
Control Flow analyser examines the structure of a procedure to identify all entry and exit points. It also identifies all loops with their entry and exit points. Control flow analysis also reveals more serious errors within the source code such as unreachable code and dynamic halts.
Data Use analyser checks how data (variables and formal parameters) is used within the procedure and from this one can check (for example that all outputs are written on each path through the procedure).
Information Flow analyser identifies all information upon which each output depends and provide an initial check that the procedure outputs are depend upon the correct inputs. If the dependencies are specified in a

DERIVES list than the analyser compares these against the calculated dependencies. DERIVES list reflects the intended or specified information flow properties. The aim of Data Use and Information Flow analysis is to choose access modes that reflect the true data use properties; not to get empty error sets.

When completing the Syntax Analysis report care must be taken that all the sections of the report are completed correctly. The Syntax Analysis report should provide a complete description of the Syntax Analysis activity in terms of changes made to the IL model, the classification of parameters given access mode and any anomalies discovered.

Semantic Analysis

The principal aim is to show conformance of the source code to its design documentation. The analysis identifies each path through the procedure by a condition on the input value. For each path, the analyst reveals the actions taken when the path condition is met. The analyst should then compare this against the design documentation to decide if the procedure will behave correctly.

The analysis has the following objectives:

- checking that each source module implements its module design specification,
- correctness of real arithmetic will be informally considered,
- consider the possibility of overflow during expression evaluation without making implementation dependent assumptions about order of evaluation,
- possible ambiguities are flagged and explained,
- only legitimate values are written to variables,
- confirm that base pointers are correctly set for all accesses to based variables,
- aliasing of parameters does not occur,
- addressability of objects is investigated where necessary,
- all preconditions for changed to the IL model should be formalised in IL wherever possible,
- demonstration that return values for typed procedures are well-defined for all inputs.

At completing the Semantic Analysis report care must be taken that all the sections of the report are complex correctly.

PROCSPEC

PROCSPEC is an IL representation of the interface and behaviour of an analysed procedure, and is used in the Malpas analysis of higher-level procedures. When an analysis subtask is completed, it is subjected to review. Once the analysis is judged satisfactory and approved, any PROCSPECs are released for use in subsequent analyses.

The PROCSPEC file is produced for each procedure and the analyst should test it.

Peer Reviewing

All the analysis work shall be reviewed to ensure that it meets the required standards. The aim of reviewing is as follows:

- to ensure that specified quality standard was met,
- to ensure that all found anomalies were adequately reported,
- to assist in achieving consistency of analysis among the assessment team,
- to identity inconsistencies in the specifications and coding of different parts of the SW,
- to agree a satisfactory interface description of each procedure.

The Review Comments form is used to record all deficiencies found in an analysis during the course of a review. All work performed to correct deficiencies identified during a review shall be documented to the same standard as required for the original work by updating the analysis report as necessary. If the rework requires any of the MALPAS analysers to be re-run, the analysis record should be updated to record the new files created. However, the previously reviewed files should still be recorded on the analysis record.

Finding

As the analysis proceeds, anomalies are found in the software or its documentation, and are documented in the various analysis reports. Anomalies shall be reported as findings.

The following activities are:

- Anomaly categorisation
- Finding reporting
- Finding sentencing

Process Activities to Quality Assurance

Training

In order I&C Energo to undertake work on the static analysis it was necessary for them to resource up team of software engineers who could be trained and work in English and be capable of undertaking the technical analysis to the required standard. In order to facilitate this initial training course in the UK for several I&C Energo engineers was organised. After this course these engineers led the I&C Energo analysis work in Czech Republic and provided the necessary technical interaction with TAG. Also, they held technical training courses for the other I&C Energo engineers.

Engineer Selection and Qualification Acceptance

I&C Energo engineers were selected by I&C Energo management based on their technical experience and training plus feed back from the team leaders on particular skills considered to be important. During the first month of the Czech training course TAG was provided with feedback from I&C Energo on the progress of each engineer. When I&C Energo team leaders had been satisfied that an engineer can perform the analysis to an acceptable standard one of the last analysis undertaken was provided to TAG for review. TAG examined the technical accuracy of the work to confirm that it is technically correct and contains the correct information. Based on this review this engineer became a full team member.

I&C Energo's Review of Completed work

As part of the analysis process it was required that all analyses were peer reviewed and then updated to take account of the comments raised in the review. The Czech team leaders undertook an additional review of each analysis and the analysis report in particular to confirm that it met the required technical standard. All work was countersigned to indicate that such a review has taken place and found to be acceptable.

TAG Review and Acceptance of Completed Analyses

A technical review of all work delivered to TAG by I&C Energo was undertaken. This review has ensured that all outputs were complete and that build standard references were correct. The review also confirmed that the anomaly report was supported by the analysis. The annotations were also examined to confirm that they were sensible and appropriate. If the raised problems could not be satisfactorily resolved by email/fax then the rework was required and a new delivery of outputs and results prepared by I&C Energo and subsequently delivered to TAG for acceptance.

TAG Sample Audits

The acceptance process outlined above has ensured that the work delivered by I&C Energo is consistent, complete and from a brief review is technically acceptable. The acceptance process did not provide a full and detailed confirmation of the correctness of the work as this would require much of the analysis to be repeated by a TAG engineer. However, to provide added assurance that I&C Energo are providing work at the required standard a sample audit was undertaken of delivered analyses.

The audits were be organised so that all engineers on the team were examined at least once during the period of the I&C Energo work programme.

Resource Planning

The need to plan the way, in which the work was performed, was under continuous management attention in order to prevent non-productive effect. To minimise non-productive effort the decomposition procedures were examined by TAG and I&C Energo and detailed plans were prepared for each software module and progress monitored during analysis.

Progress Reporting

After the end of each accounting month Progress report was prepared and sent to TAG providing a monthly overview of work performed on the static analysis an the time sheets of each engineer. The progress metrics developed by TAG was applied on the analysis activities assured overview of the development status of each analysed module.

Risk Management

The potential risk for the project was evaluated at the first phase of the project (during the training of two I&C Energo training in the UK). The minimisation of the risk was solved by the introduction of the Czech language for the work, by strict selection of the candidates for the work and by good preparation of the training process and organisation of the real analysis. At the current time it is considered that this solution has been effective.

Quality Control

I&C Energo‘s Quality Control was defined in the I&C Energo document „Quality Assurance Programme“ prepared as part of the subcontract work. This programme deals with the whole process from the general company quality system, subcontract review to quality assurance and control during the project realisation.

The scope of the main quality objectives was the following:

- to meet TAG technical and quality requirements of the contract specification,
- to assure that quality, audits, reviews and inspections will be performed according to the Quality Assurance Programme and procedures and applicable codes or standards,
- to achieve professional level comparable with TAG,
- to assure that all significant deviations from specification, procedures, etc., will be submitted to TAG for review before applying,
- to ensure that the Quality Assurance Programme will be correctly applied.

Configuration Control

Configuration management process was defined in the I&C Energo document „Configuration management for Static Analysis”. This document ensured that all elaborated input/output software files had been correctly and consistently configured on VAX computer and all elaborated report on PC so that TAG could provide an identical file structure for VAX computer or PC and the contrary I&C Energo to TAG.

Conclusion

The used approach for the Static Analysis of software used for the Independent Assessment of the Temelin Safety System Software was cost consuming. However it makes possible to discover software anomalies which could be not found in manual check. It results from experience, that this way of assessment software is suitable not only for safety control system analysis in nuclear power systems but for transport and aviation as well.

Assessment Methodology of the Temelín NPP Control System Performance and Quality

I. Petružela [1], K. Bednařík [2], J. Rubek [3]

[1] *I&C Energo, Areál VÚ, 190 16 Praha 9 - Běchovice, Czech Republic*
Phone: +420 2 6706 2181, Fax: +420 2 6706 2182, e-mail: ipetruzela@ic-energo.cz

[2] *I&C Energo, Areál VÚ, 190 16 Praha 9 - Běchovice, Czech Republic*
Phone.: +420 2 6706 2185, Fax: +420 2 6706 2182, e-mail: kbednarik@ic-energo.cz

[3] *I&C Energo, Areál VÚ, 190 16 Praha 9 - Běchovice, Czech Republic*
Phone: +420 2 6706 2183, Fax: +420 2 6706 2182, e-mail: jrubek@ic-energo.cz

Summary

The performance and quality of the NPP Temelín control system is demonstrated by means of tests during the power ascension testing stage. A methodology has been developed in I&C Energo for the test assessment in which there are defined criteria determining the grade of meeting the design requirements. The assessment of the control process quality is based on the evaluation of the behaviour of the main controlled quantities in the course of transients of the test.
The design responses of the transient processes have been acquired by means of the unit model DYTE. Eight criterial conditions are assessed which are posed on the controlled quantities. It is by meeting these criteria that it can be demonstrated that control system quality corresponds to the requirements defined in the design specifications. The criteria structure makes possible an automated processing of the measured data.

1. The Method Of The Control System Quality Assessment

A control system makes it possible to purposeful act on the controlled object so that the required conditions of the process system are always reached in compliance with the design, at meeting technical standards and regulations. The supplier of the control system is obliged to demonstrate to the customer both performance and quality of the provided work.

The control quality parameters are always defined by the customer and they become then an integral part of the design. Already in the course of the control system development, definitions of the control system quality features are mutually agreed upon, including the methods and conditions under which the required quality is to be achieved.

For complex process facilities, the criteria for the control system determination would not be unambiguously established. In practice, the assessment of the controlled technology process at dynamic events is used for the evaluation of the control system quality. The control quality is then assessed by means of the response patterns to a unit impulse or to a unit jump or by means of integral criteria.

At the Temelín NPP, the I&C supplier is not the supplier of the technology in the same time. That called for the need of an exact formulation of the control system quality criteria. The criteria serve for the check whether the unit control system (major unit controllers, logical control, limitation system) perform in compliance with the design requirements.

1.1. Mathematical Formulation of the Control Quality in Complex Processes

The NPP process system can be subdivided into the controlled object and to the control system. The controlled object are the process systems that are usually mutually interconnected, complex non-linear systems. From the mathematics point of view

- it is composed from finite number of elements each of which is unambiguously described by a finite number of measurable quantities
- it has mutual links among the elements unambiguously formulated

Therefore, we can describe the dynamic features of the controlled object by means of differential equations the solution of which is a status vector. The status vector enables us to determine the system conditions at any time by means of a minimum number of quantities.

The control system must maintain certain physical quantities at predefined values. During the dynamic processes the control system modifies the process system conditions through action quantities so that design conditions are to be achieved. The mathematical notation of it is the following equations system

$$\dot{\vec{x}}(t) = \vec{f}[\vec{x}(t), \vec{v}(t), t] + G[\vec{x}(t), \vec{v}(t), t]\vec{u}(t) \qquad (1)$$

where there is

$\dot{\vec{x}}(t)$ the derivation of the status quantities vector (change of the TP status)

$\vec{x}(t)$ the status quantities vector (TP status)

$\vec{f}[\vec{x}(t), \vec{v}(t), t]$ the vector function (TP description)

$\vec{v}(t)$ the perturbation variables vector (TP perturbations)

$G[\vec{x}(t), \vec{v}(t), t]$ the functional matrix (describing the control system

$\vec{u}(t)$ the control variables vector (status of the control system)

If the control system meets all requirements defined in the design specifications, the time courses of the status variables vector $\vec{x}(t)$ achieved at the power ascension testing must be equal to those acquired in analyses provided by the manufacturer. A deficiency of this procedure is the fact that the above shown formalized notation is impossible with complex process systems and that not all status variables are measurable.

Therefore, the control quantities vector $\vec{r}(t)$ is used instead of the status quantities. In the course of the control process, the real values of the controlled quantities are measured and compared with the required values $\vec{z}(t)$. In accordance with the found deviations, individual controllers intervene into the process in compliance with the design requirements. The control deviations vector is marked $\vec{e}(t)$. The shown equation system (1) is reformed to:

$$\vec{r}(t) = \vec{f}\left[G\left(\vec{z}(t) - \vec{r}(t)\right), \vec{v}(t)\right] \qquad (2)$$

The diagram on the Fig. 1 corresponds to this simplified equation

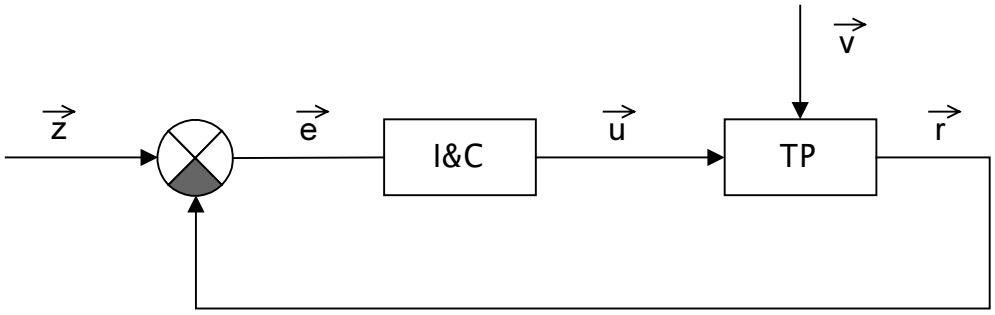


Figure 1: Principle diagram of the process control

1.2. Requirements Posed by the CSN on the Process Control Systems and on the Methods of Their Assessment

Generally, we can perform assessment of the control features of the control systems in the following states of the process system

1. steady state operation
2. transients (changes of the controlled quantities from the time $t=t_o$ into the state in time $t=\infty$)
3. long-term operation (stability of the results of the repeating control processes)

The behaviour of the shown states is not exactly defined in the standards and there is a requirement that the corresponding indicators must be a part of the supply of the manufacturer.

The first two states relate to the assessment of the dynamic features of the system at control as the result of the change of the process state (e.g. power change, failures of the equipment functions or due to fluctuations of the measured values. The third is used for the judgement of the fact whether the achieved quality has a long-term character. The basis is the comparison of the repeated processes. During the Temelín NPP commissioning, it would mean an exact circumscription of the controlled processes that will be more times repeated during the commissioning period under the same or similar conditions. Therefore, the indicators of this did not become a part of the control system quality assessment even if the I&C system supplier gives the necessary data in the documentation.

The methods of the assessment of the process control systems in accordance with ÈSN 180005 are based on the determination of the characteristics of the required functions accuracy meeting. Those functions are subdivided into

- static transfer function
- dynamic characteristics

1.3. Description of the Accuracy Characteristics of the Required Functions Performance

Static transfer function. It is the dependence of the output signal values on the values of the input signal or of the measured quantity or on the physical quantities coming to the input in the steady state.

Generally, it is determined as the line fitted to average values of the monitoring results in the measurement points. The evaluated transfer function, characteristics or quantity are marked with the fact that the influence of random failures has been removed. However, they include systematic errors due to the product features.

Dynamic characteristics. It is the dependence of the information parameter of the output signal on the prescribed time change of the information parameter of the input signal. It could be expressed by

- Transfer function
- Transient characteristics
- Impulse characteristics
- Frequency characteristics

The complete dynamic characteristics is a graphical transformation of the dynamic behaviour of the product at prescribed time changes of the input signal. There are given the following partial dynamic characteristics.

- Amplitude-frequency characteristics
- Phase frequency characteristics.
- Stabilization time
- Time of transportation delay
- Time constant
- Time of overshoot
- Value of maximum overshoot
- Time of the query

1.4. Assessment of the Control System Quality

The basic condition of the correct performance of the controlled process is its stability. The system is in an equilibrium state if the controlled quantity does not change with the time. The control is stable when the system returns into the original equilibrium state within a period after the system's deviation from the steady state and removal of the reason of the perturbation (that caused the deviation).

Simplified, we can say that after the transient event decay the controlled quantities stabilize within the band defined by the design and the control vector is no more changed. The band is called the control accuracy.

The stability condition is a necessary, however, not a sufficient condition of correct performance of the regulated systems. The behaviour of the systems is essential during the transient that could have various patterns. The system is controlled foremost for failure responses of the unit jump pattern since this is one of most adverse events that could be mastered by the control.

The most accurate picture of the system behaviour can be acquired by the explicit solution of the differential equations system. Due to the difficulty of an accurate formalization of all terms of the equations is the quality of the control process mostly defined as selected parameters of the dynamic characteristics. The deciding aspect is the way and velocity of the new required system state achieving.

The system assessment lies in the check of

- rated static transfer functions
- rated complete dynamic characteristics

The requirement of all Czech standards is that the system dynamic features must be described by the manufacturer and the description must be part of the delivery.

2. Draft Of Criteria For The Assessment Of The Temelín Npp Unit Major Controllers

2.1. Indicators Assessing the Process Control Quality at the Temelín NPP

In the preceding chapter, optional approaches have been presented to the assessment of the control systems quality. Not all of them are applicable for the NPP Temelín control system assessment. We have selected several basic indicators from the standards by which we will characterize the control process quality at the Temelín NPP. Those are:

1. the control accuracy- gives limits in which the control circuit keeps the controlled quantity
2. the control time (response time) - is the time period that lapses from the start of the perturbation till the moment when the controlled quantities of the process achieve the required values with the given accuracy
3. the maximum deviation of the controlled quantity (maximum overshoot) - it is the greatest value of overshoot in the response of the closed control circuit to a jump change of the specified quantity
4. the number of overshoots during the control process – it is equal to the number of extremes (maxima, minima) during the control process the value of which lies off the control accuracy band
5. the quadratic control area – the calculation of the quadratic control area is finished when the controlled quantity is kept in the limits or the operator intervenes into the process

In the same time, we have to supplement the above shown parameters by parameters that characterize safety. The system must not cause by its action any possible dangerous conditions in its surroundings. The safety properties of the instrumentation and control system of industry processes (mechanical, electrical, etc.) depend on its own (intrinsic) system safety and on external (extrinsic) aspects on the protection included into the system.

2.2. Design, Power Ascension Tests

We have to make the above shown concrete at the generation of criteria in accordance with the design documentation (diagrams of the control circuits, setup of the control circuits constants, accuracy of the control circuits). This is based on data given in the following documentation:

- The requirements on the unit control system in the scope of reactor protection, limitation systems and unit control, A1-3.2, EGP Praha, December 1993
- Reactor Control and Limitation System dPS-202A, Functional Design Report, TEM-I&C-RCLS-014, Revision 5, January 2000
- PCS Control Builder, TEM-I&C-PCS-2161, Revision 3, May 2000
- Nuclear Unit Operation Modes - 1st stage, dÚP (Supplement of the Input Design) No.463, EGP Praha, March 1998

The check of the design is performed during the power ascension stage of the commissioning by means of special tests a part of which will be evaluated from the point of view of the major control circuits quality.

We can acquire the necessary examples of the transient characteristics by means of a model that describes the simulated object in terms of mathematical equations. The equations are currently available and create a basis of the DYTE simulation code. The code makes it possible to acquire the missing transient characteristics of the non-linear systems of the Temelín NPP units. (As is shown on figure 2.)

The assessment of the Temelín NPP units major controllers performance can be then based on the evaluation of the control process quality of selected tests and their comparison with the design

specifications. The success of the tests, i.e. statement „complied - not complied„ corresponds to the degree of meting the criteria that characterize the control process quality.

After the test completion, following questions are assessed from the point of view of major control circuits quality:

1. Steady system state
   - stability of the steady state
   - variation band in the steady state (control accuracy)
2. Transient process of the controlled quantity
   - the time of achieving the target steady state (control time)
   - the maximum overshoot
   - the number of overshoots during the control time
   - the way of achieving the steady state (quadratic control area)
3. Functions of the logic circuits
   - the performance of the logic circuits of the major controllers including the Control Coordinator (CC) in the transient process
   - the following of the desired value in the controllers that are not in action
4. CC, Limitation System (LS) and local protections performance
   - in case of LS actuation (in accordance with the design) time and reason of the LS actuation are evaluated
   - the actuation of local protections during the transient process
   - the margin to CC, LS or local protections actuation due to other reasons

2.3. Major Control Circuits and Controlled Quantities

The Temelín NPP unit control system is a sophisticated complex of mutually interconnected controllers, limitation system and protections. Individual control circuits have different effect on the way of achieving the desired state. From this aspect, we can select the so-called major control circuits that are part of the unit power control. In the CC documentation there is given the control accuracy that is in sense of the first chapter one of the most important parameters of the static characteristics. U the reactor controller has as well given insensitivity, i.e. magnitude of the deviation within which the controller does not respond. The parameters are shown in the following overview table:

Control circuit	Controlled quantity	Accuracy	Insensitivity	Units
Reactor controller	Reactor power	±3	±2	%
	Steam pressure	±0.2	±0.13	MPa
	Average temperature	±1.5	±1	°C
Turbine controller	Turbine power	±10		MW
	Steam pressure	±0.07		MPa
Controller of the steam dump to condenser	Steam pressure	±0.1		MPa
PZR pressure controller	PZR pressure	-0.12		MPa
	PZR pressure	+0.2		MPa
PZR level controller	PZR level	±15		cm
SG feeding controller	SG level	±1 to 3		cm
Deaerator level controller	Deaerator level	±2.5		cm
Deaerator pressure controller	Deaerator pressure	±0.05		MPa

The quantities on which the controllers act are the main controlled quantities. They represent the basic part of the state vector. Therefore, we can assess the Temelín NPP control system quality based on their evaluation.

2.4. Indicators and Criteria Definitions for the Assessment of the Performance of the Temelín NPP Unit Major Controllers

Based on the preceding analysis, we can assess the control system quality by eight indicators of dynamic characteristics of the main controlled quantities. Those are

K1 Control quantity variation band width after the transient decay

K2 Control time, i.e. the time necessary to bring the controlled quantity into the K1 band from the start of the actuation event

K3 Magnitude of the quantity maximum overshoot during the transient

K4 Number of the quantity overshoots during the transient off the K1 band

K5 Magnitude of the quadratic control area of the controlled quantity

K6 Performance of major controllers logic circuits including the CC during the transient

K7 The method of following of individual setting devices of the CC and of the major unit controllers

K8 The magnitude of margin to LS, protection system and local protections actuation

These indicators are required in the form of numeric values for analogue quantities (K1 through K5 and K8), for the logic circuits in their state (K6 and K7).

A criterial conditions corresponds to each indicator that determines the boundary between “satisfied-not satisfied” at the control system assessment. The criteria 1 through 5 relate to main controlled quantities, the criteria 6 and 7 to the activity of major unit controllers including the CC and LS, the criterion 8 relates to LS, protection system and to local protections.

Criterion 1 – the achieving of the system target state the variation of which in less than the control accuracy defined by the design is considered satisfying

Criterion 2 – the achieving of the control time that does not exceed the control time defined by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 3 – not exceeding of the overshoot magnitude that is defined by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 4 - not exceeding of the overshoots number that is given by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 5 – achieving of the quadratic control area that is less than the quadratic control area defined by the design (or in accordance with the design conditions determined by the DYTE model) is considered satisfying

Criterion 6 – it is considered satisfying if the sequence of the activities of the logic circuits of the major controllers including the CC corresponds to the sequence required by the design (or in accordance with the sequence determined by the DYTE model)

Criterion 7 – it is considered satisfying if the following of the individual setting devices of the CC and of the major unit controllers corresponds to the design

Criterion 8 - it is considered satisfying if the minimum margin will be greater than a value agreed upon by experts

If, howbeit, a single condition is not met from the above shown, the performance of the control circuit cannot be considered a quality one.

3. Conclusion

The criteria serve to the check of the performance of the Temelín NPP unit control system (major unit controllers, logical control, limitation system) against the design. They determine the borders of the area in which the numeric values of the assessed parameters should vary if the work is made in compliance with the design.

The criterial values make it possible to determine the achieved quality of the NPP Temelín unit major controllers after the completed test.

The construction of the criteria makes use of the automated measured data processing and makes it possible to formulate the assessment result in the form – "met, not met". Additional outputs are the determination of :

a) the magnitude (range) of the non-compliance of the real unit behaviour against the requirements of the design (or against the specifications requirements for the control system supplier)

b) the reasons of non-compliance found at testing in the frame of the power ascension stage of the commissioning

c) the impact of the found non-compliance on the further continuation of the power ascension stage of the commissioning, i.e. providing data for the Commissioning Control Group decision making, whether it is necessary to remove the reasons of the non-compliance

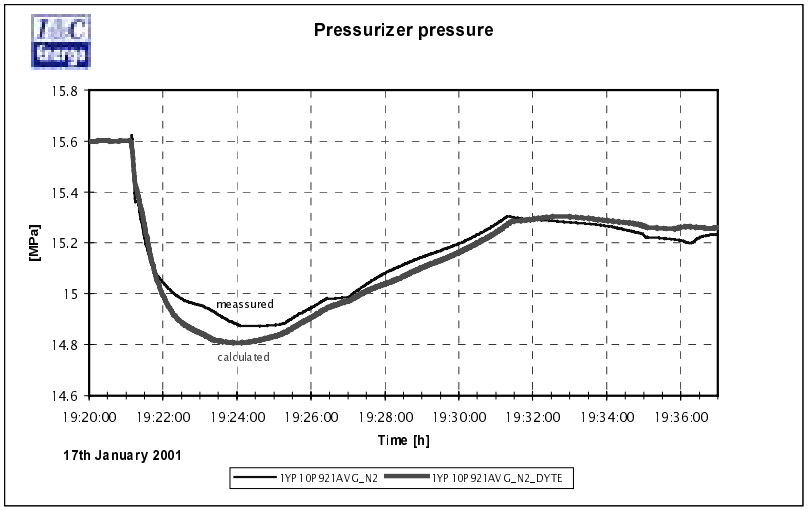
   – before any continuation of the power ascension testing

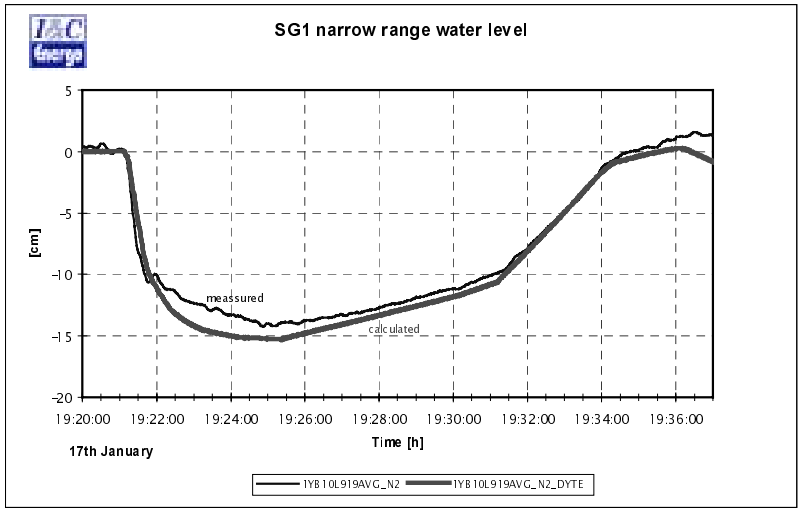
   – after the power ascension testing, in the frame of the tuning of the complete control system based on the commissioning results

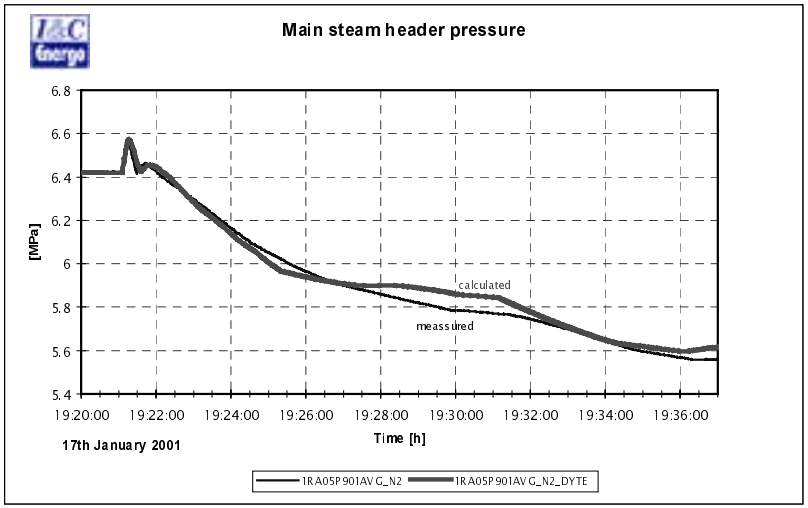
List of Abbreviations

PZR Pressurizer

LS	Limitation System
CC	Control Coordinator
SG	Steam Generator
NPP	Nuclear Power Plant
TP	Technology Process


Pressurizer pressure
[MPa]
Time [h]
meassured
calculated
17th January 2001
1YP10P921AVG_N2
1YP10P921AVG_N2_DYTE


SG1 narrow range water level
[cm]
Time [h]
meassured
calculated
17th January
1YB10L919AVG_N2
1YB10L919AVG_N2_DYTE


Main steam header pressure
[MPa]
Time [h]
calculated
meassured
17th January 2001
1RA05P901AVG_N2
1RA05P901AVG_N2_DYTE

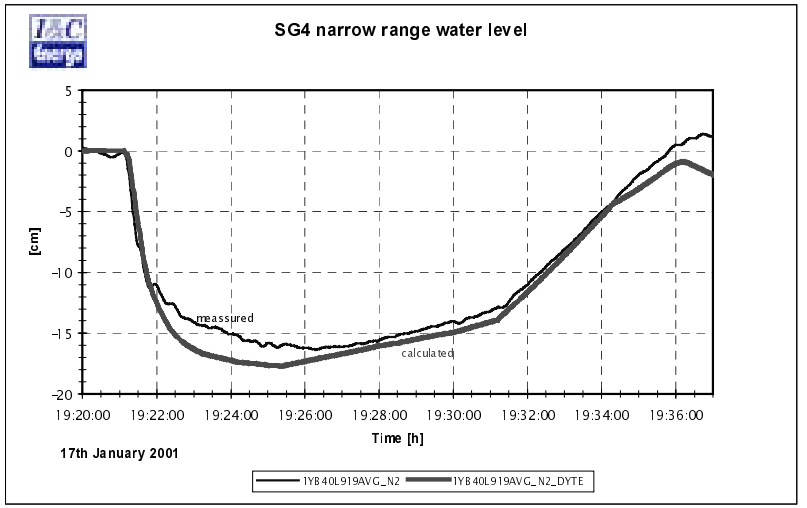

SG4 narrow range water level
[cm]
Time [h]
meassured
calculated
17th January 2001
1YB40L919AVG_N2
1YB40L919AVG_N2_DYTE

Figure 2

Methodology of NPP I&C System Algorithms and Software Verification Expert Analysis

V. Kharchenko, L. Lyubchik, M. Yastrebenetsky

State Scientific and Technical Center on Nuclear and Radiation Safety,
17 Artema str., Kharkov 61002, Ukraine
Tel.: +38 0572 471 700, Fax: +38 0572 471 700, e-mail: rel@online.kharkiv.com

Summary

The process of NPP I&C systems verification and validation (V&V) and expert analysis of V&V includes the stages of V&V and expert analysis of V&V both algorithms and software (A&SW). This paper is devoted to the elements of methodology development for complex expert analysis of NPP I&C systems A&SW verification and verification. One of the most important phases of A&SW verification and verification assessment is the stability analysis of digital closed-loop control circuits. The paper represents the technique of the main features of V&V and V&V expert analysis of technological controlled plants mathematical models, digital control algorithms, methods and software for stability analysis. The proposed methodology of A&SW verification and validation assessment was approbated during the expertise of a number state-of-the-art Ukrainian NPP I&C systems, particularly during the expertise of computer-based control system ASUT-1000M for Zaporozhey NPP.

Introduction

The process of NPP I&C systems V&V and expert analysis of V&V includes the stages of verification and validation and expert analysis of V&V both algorithms and software (A&SW). The quality of A&SW V&V execution is very important for the computer-based critical I&C systems reliability and safety ensuring. The requirements for verification have actually become more strict and methodology of V&V is the subject of regulatory bodies assessment. The problems of regulation of V&V are inseparable components of both national and international standards in critical engineering [1-3].

The process of A&SW verification and validation assessment is one of the essential parts of NPP I&C expert analysis and licensing. For the broad number of systems, particularly computer-based control systems, the problems of A&SW verification and validation assessment is desirable to consider simultaneously. This is a reason for theoretical and technological basis improvement for developing and realization of A&SW verification and validation assessment process.

The main problems of A&SW of NPP I&C verification and validation assessment are:

- analysis of requirements for control algorithms and software starting from the general requirements determined by the standard documents;
- checking of control algorithms developing and software design tasks statement conformity to the requirements mentioned above;
- review the quality of and V&V plans, testing methodology and completeness in accordance with the A&SW tasks;
- review the quality of and V&V reports and their conformity to the plans and methods of verification and validation.

It is necessary to underline that such problems are difficultly formalizing from the safety requirements ensuring point of view. In general case the assessment of V&V is performed by the traditional methods of inspection and analysis of documentation [4-6], and the single results may be performed using the specially design tools [7,8]. At the same time taking into account the great liability and importance of objectivity and completeness of A&SW verification and validation assessment, it necessary to develop its complex methodology.

This paper is devoted to the consideration and development of methodology elements for complex expert analysis of NPP I&C systems A&SW verification and validation. The proposed expert analysis methodology includes:

- strategy of complex A&SW expert analysis;
- system of A&SW verification and validation assessment criteria;
- requirements detailing the features of A&SW verification and validation assessment;
- methods of A&SW verification and validation assessment;
- elements and phases of A&SW verification and validation assessment technology.

The proposed methodology also covers the developing of conceptual scheme, criterions, requirements and elements of A&SW verification and validation assessment process technology for safety-related systems, as well as recommendations for its utilizations in practical applications. The presented results are obtained during the generalization of practical experience of expert analyzing of real NPP I&C A&SW, in particular ASUT-1000M system for Zaporozhey NPP.

1. Complex approach to A&SW verification and validation assessment

Proposed complex approach to A&SW verification and validation assessment is based on the next principles:

- algorithms and software verification and validation assessment of computer-based automatic control and regulation systems must execute simultaneously;
- main requirements and accepted criteria of algorithms and software assessment may be uniform;
- assessment of stability or robustness NPP safety related control systems must consist of plant modeling and simulation A&SW verification and validation assessment and closed- loop control system A&SW verification and validation assessment.

2. General scheme of A&SW verification and validation assessment

General scheme of the process of A&SW verification and validation assessment for safety-related I&S systems is based on the following principles:

- forming and structuring of the set of requirements for A&SW, which must be reviewed under the V&V process in the different steps of life cycle;
- development of the system of A&SW verification and validation assessment criteria;
- comparison of A&SW verification and validation assessment criteria system against set of requirement for the A&SW;
- formalization of the V&V process and assessment expert analysis using the basic criteria;
- development and utilizing of the utilities for automated safety analysis support under V&V, licensing and expertise.

Fig.1 illustrates the proposed general scheme of A&SW verification and validation assessment. The scheme includes three main stratums - A&SW requirements, verification and validation assessment requirements and assessment criteria.

2.1. Stratum of A&SW requirements, reviewed under verification

This group of requirements divides into the *A&SW characteristics requirements* and *A&SW development requirements*. In turn the characteristics requirements divides into *A&SW functional requirements* determined by the system specification in accordance with its assignment standards in the field of computer systems important for NPP safety [1,6,9,10] (Fig. 1).

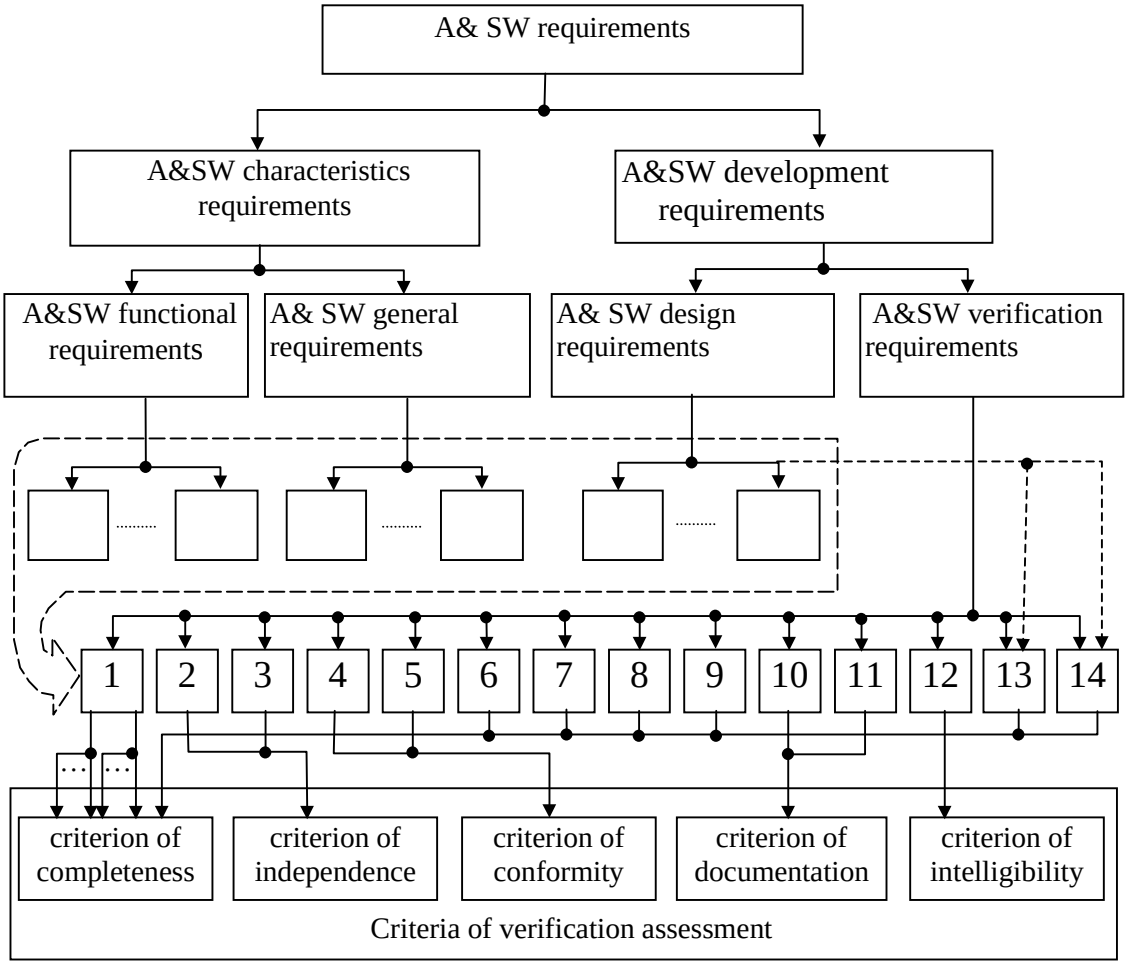


Fig.1. General scheme of A&SW verification and validation assessment

The *A&SW general requirements* include the groups of requirements to:

- A&SW structure and elements;
- diagnostics and self-testing;
- protection against failures because A&SW and human errors.

The *A&SW development requirements* including A&SW design and V&V requirements divide into the groups of requirement to:

- ensuring under development the A&SW accordance to the stated criteria of quality (reliability, correctness, modifiability etc.);

- utilization of the automated instrumental facilities (tools) for A&SW development and V&V;
- programming methods and techniques.

2.2. Stratum of A&SW verification requirements

On the assumption of expert analysis experience and normative documents, which are in service in Ukraine [10], it is possible to separate out the requirements into:

- execution of verification upon the stages of life cycle (requirement 1);
- independence of specialists caring out the verification process for the systems of different classes of safety (requirements 2,3);
- completeness of verification and discovered current shortcomings elimination (requirements 4,5);
- review of protection of general purpose failures (requirement 6);
- verification of previously developed A&SW (requirements 7-9);
- A&SW verification plans and reports (requirements 10,11);
- form of verification materials statement (requirement 12);
- instrument facilities (tools) utilizing under A&SW verification (requirement 13);
- formal methods utilizing under A&SW verification (requirement 14).

The detailed statement of the requirements to the SW V&V is described in [5,6,9,10]. The requirements to the control algorithms verification and validation have many particularities and specific features and will be considered below.

2.3. Stratum of A&SW verification assessment criteria

By analogy with expert analysis methodology for digital safety-related control systems SW verification [5,6], a number of criteria are used under A&SW verification assessment. They correspond the systematized set of showings and rules in accordance with that the assessment is carried out and final conclusion concern A&SW conformity to the presented safety requirements are come about. The proposed criteria system for A&SW verification includes the criteria of completeness, independence, conformity, documentation and intelligibility.

A&SW verification corresponds to *completeness criterion* if under verification the A&SW correspondence to all requirements of specifications, standards and over normative documents was reviewed.

A&SW verification corresponds to *independence criterion* if testing was carried out by group of specialists (organization) which is administrative and/or financially independent fro the specialists (organization) which has developed A&SW.

A&SW verification corresponds to *conformity criterion* if verification was completely finished before the system was put into operation, i.e. all detected failures was analyzed and eliminated by that time.

A&SW verification corresponds to *documentation criterion* if all plans and reports reflected verification process and results in details was issued.

A&SW verification corresponds to intelligibility criterion if all documentation of A&SW verification was stated in the form, which is clear to the specialists, doesn't involve in the developing and verification process.

Fig.2 illustrates correspondence between the requirements and verification assessment criteria. As a result under A&SW verification assessment the fulfillment of all requirements mentioned above must be checked. The model base for the verification assessment process formalization is [9]:

- model of A&SW functional requirements fulfillment review;
- model of A&SW and developing process general requirements fulfillment review;
- model of verification correspondence to assessment criteria review.

3. Technological control algorithms verification assessment features

The assessment features for verification of technological control algorithms (TCA) are closely connected with the character of TCA verification process and methodology [12]. The main tasks, which must be solved during TCA verification, may be divided in two groups:

- logical part of control algorithms verification;
- closed-loop systems stability analysis.

Verification of the logical part of TCA is connected with accuracy testing of technological blocking and protection operation, controller's mode changing, fulfilling of switch over condition from manual to automatic mode of operation. The review of operation requirements correspondence and accuracy carries out by TCA testing by means of special sets of input signals generation and output signals recording with sequential analysis of the testing results. In such a case the testing may be carried out with the help of control system program model as well as special testing hardware.

3.1. Logical part of TCA verification assessment

The assessment of logical part of TCA must include:

- test set completeness analysis, which must cover all typical situations both in normal operations and possible accidents;
- validity analysis concern conclusions about testing conformity and successfulness;
- detected failures and undertaken actions concern their elimination presence analysis.

One of the very important part of such a task is the verification assessment of special and instrumental SW used under the CA logical part verification, which must be performed using the criteria and requirements similar to the SW NPP I&C ones.

3.2. Expert analysis of stability of closed-loop control systems verification

One of the most important phases of A&SW verification and verification assessment is the stability analysis (SA) assessment of digital closed-loop control systems. The requirements of control systems stability is one of the most critical for the NPP safety and must be performed carefully elaborated. Under the SA many important features should be taken into account, particularly input and internal disturbances influence, technological plants nonlinearities and parameters variations, local control systems interconnections, measurement signals corruptions by random noise and so on.

The most widely distributed methodology of complex control systems SA is based on computer modeling and simulation (M&S) using special methods and software for stability analysis. The typical phases of closed-loop control systems SA by means of M&S are the following:

- technological controlled plants mathematical models design and evaluation;
- simulation SW design and verification;
- technological controlled plants mathematical models verification via the comparison of the simulation results and real transient characteristics obtained during the industrial experiments;
- pick of digital controllers algorithms tuning parameters;
- computer simulation of transient process in typical closed-loop control systems (TCLCS) in representative technological regimes;
- 'controllers part' of TCA evaluation upon the result of transient process simulation.

Under the assessment of closed-loop stability analysis results the following typical review steps must be fulfilled:

- technological controlled plants mathematical models verification assessment via the inspection of simulation and experiment results;
- completeness of simulated technological regimes, possible accidents and accountable disturbance factors evaluating;

- stability assurance testing for all typical regimes of NPP operation;
- digital TCA evaluation and controllers tuning parameters picking expediency assessment.

The SA report must be examined using the assessment criteria, which are similar to the criteria used for I&C SW verification assessment, which was described in section 1. A great attention should also be devoted to the verification assessment of special and instrumental SW, designed and used for the simulation purposes.

4. Experience of methodology of complex A&SW verification and validation assessment

4.1. Stages of A&SW verification and validation assessment

The proposed methodology of complex A&SW verification assessment was approbated during the expertise of a number state-of-the-art Ukrainian NPP I&C systems. Particularly the proposed methodology was used during the expertise of computer-based control system ASUT-1000M for Zaporozhey NPP. It is system for automatic control of turbine. The developed approach ensures the possibility of unification and standardization of A&SW assessment verification process. ASUT-1000M A&SW verification and validation expert analysis consists of three stages.

At the *first stage* preliminary analysis (inspection) of documentation (system and A&SW specification, algorithms and software verification and validation plans and reports, etc.) was carried out.

At the *second stage* V&V expert analysis working group performed assessment of A&SW verification and validation technology and V&V results on the manufacturing firms (LvivORGRESS and Kharkiv Plant named after Shevchenko) where system ASUT-1000M was developed. The selected testing of most important A&SW functions was carried out.

At the *third stage* summary assessment of A&SW verification and validation was formulated.

4.2. The general scheme and elements of A&SW verification and validation assessment

Taking into account features of ASUT-1000M A&SW verification and validation expert analysis performed in two "sections": "horizontal" section and "vertical" section. The general scheme of A&SW verification and validation assessment shown in the Fig.2.

In the "horizontal" section the next elements was analyzed:

- typical A&SW consisting of unified algorithm and program modules set. The technology control algorithms (TCA) and functional software developed by the use of these typical modules (TM);
- system A&SW. Expert analysis of this element introduced assessment of TCA, functional software and stability analysis (SA) of typical closed-loop (TCL) control systems (CS) and SA of multivariable (MV) CS;
- A&SW design and V&V tools. The base tools used for A&SW V&V was:
  - A&SW design tools (DT);
  - TCL control systems modeling and simulation (M&S) tools;
  - plant M&S (PM&S) tools;
- A&SW V&V carried out by developers.

In the "horizontal" section expert analysis performed on stages of system and A&SW development starting from EA of system and A&SW specification to functional software V&V on the computer-based control systems of ASUT-1000M. In this section V&V assessment carried out by use of:

- documentation (A&SW V&V plans and reports);
- results of A&SW testing by V&V working group.

Expert analysis of A&SW V&V (technology and process, plans and reports) performed taking into account the requirements and criteria described in the part 2. The most difficult stage of expert

analysis was assessments of stability analysis of TCLCS and MVCS. These assessments carried out on real plant models.

Conclusion

Expert analysis of NPP safety related computer-based automatic control systems algorithms and software expediently to perform simultaneously. Besides, tasks of V&V assessment are need to divide on the:

- tasks of V&V assessment of typical algorithm and software modules;
- tasks of V&V assessment of technology control algorithms;
- tasks of stability analysis taking into account results of plant models verification..

The requirements and criteria of algorithm and software verification may be uniform. For assessment algorithm V&V the some requirements and criteria must be modified.

The proposed methodology is base for development some techniques and tools for expert analysis processes decomposition, planning, management and A&SW assessment by use of formalized models [9].

References

1. IEC - 880, Software for Computers in the Safety Systems of Nuclear Power Stations, Geneva, 1986.

2. ECSS - E - 40A, Software Engineering for Space Systems, Paris, 1998.

3. IAEA Technical Reports, Series 384. Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control. International Atomic Energy Agency, Vienna, 1999.

4. Leveson N. Safeware: System Safety and Computers, New-York: Addison-Wesley, 1995.

5. Vilkomir S.A., Kharchenko V.S. Methodology of the Review of Software for Safety Important Systems// Safety and Reliability. Proceedings of ESREL'99 - The Tenth European Conference on Safety and Reliability, Munich-Garching, Germany, 13-17 September, 1999, vol. 1, pp. 593-596.

6. Vilkomir S.A., Kharchenko V.S. An "Asymmetric" Approach to the Assessment of Safety - Critical Software During Sertification and Licensing// Proceeding of the ESCOM - SCOPE 2000 Conference "PROJECT CONTROL: THE HUMAN FACTOR", Munich, Germany, 18 - 20 April, 2000, pp. 467 - 475.

7. TACS/1019/N7. User Guide for MALPAS Release 6.0// TA Consultancy Services Limited, The Barbican, East Street, Farnham, Surrey GU9 7TB, December, 1992.

8. Vilkomir S.A., Kharchenko V.S., Ponomarev A.S., Gorda A.L. The System Safety Assessment by the Use of Programming Tool During the Licensing Process// Proceeding of the 17th International System Safety Conference, Orlando, FL, August 16-21, 1999, pp. 222 - 227.

9. Kharchenko V.S. Vilkomir S.A. The Formalized Models of an Evaluation of a Verification Process of Critical Digital Systems Software// Proceedings of PSAM 5, International Conference on

Probabilistic Safety Assessment and Management, vol. 4, November 27 - December 1, 2000, Osaka, Japan, pp. 2383-2388.

10. NP 306.5.02/3.035-2000. Requirements of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety/ M.A.Yastrebenetsky (ed.), Yu.V. Rozen, V.S.Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

11. NP 306.7.02/2.041-2000. Technique of Nuclear and Radiation Safety to NPP I&C Systems Important to Safety Expert Analysis/ M.A.Yastrebenetsky (ed.), S.V. Vinogradskaya, V.S.Kharchenko et al., Nuclear Regulatory Administration of Ukraine, Kiev, 2000.

12. Lyubchik L.M. Engineering Aspects of Advanced Model-based Control Techniques for Industrial Applications// Proceeding of the 2-nd AMETMAS Workshop "Advanced Control Concepts for Manufacturing Systems", St. Petersburg, Russia, 2000.

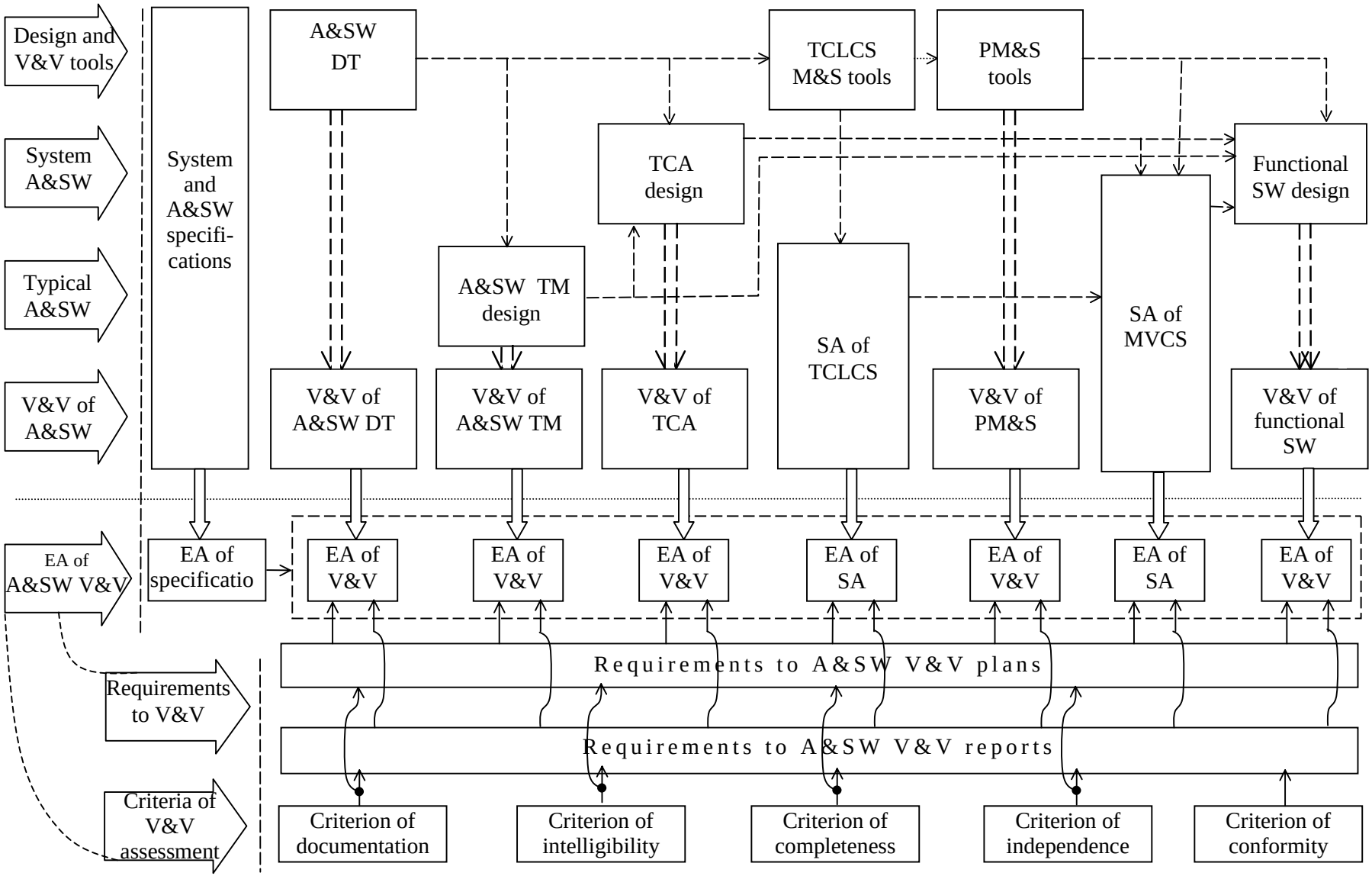


Fig. 2. Correspondence between the stages of A&SW development and V&V expert analysis

TECHNICAL SESSION 5:
EXPERIENCE WITH APPLICATIONS SYSTEM ASPECTS,
POTENTIAL LIMITS AND FUTURE TRENDS AND NEEDS
Chairmen: B. Liwång, M. Hrehor

Operating Experience of Digital Safety-Related System of Kashiwazaki-Kariwa Unit No.6 and 7

Shigenori Makino[1]

[1]*Tokyo Electric Power Company, 1-3 Uchisaiwai-cho 1-chome Chiyoda-ku Tokyo 100-0011 Japan*
Tel.: +81 3 3501 8111, Fax: +81 3 3596 8562, e-mail: Makino.S@tepco.co.jp

Summary

The digital safety systems were developed and installed to Kashiwazaki-Kariwa Unit 6 and 7 for the first time in Japan, based on these over 10 years experience of digitization of I&C systems. In the development and application process of the digital safety systems, the methodology to prove its reliability were discussed such as QA/QC including V&V procedures, the hazard analysis described in this paper etc.. The hazard analysis was performed in order to fully re-evaluate reliability of the digital safety systems. The results of the hazard analysis by FTA shows that the hazards latent in the software lifecycle, were extracted and verified completely. In this paper, the policies for application of the digital safety system are described to enhance its reliability.

Introduction

The digital control and network systems have been applied to the I&C systems in BWRs in Japan since 1980s. During the course of the application, careful stepwise introduction of digital controllers has been employed, so the scope of the application has been also widened gradually. The highly reliable redundant main controllers were first installed in 1980s, followed by the digital controllers and the network system for the radwaste plants, the non-safety systems introduced to Kashiwazaki-Kariwa Units 3 and 4 (K-3/4). Based on the results and experience gained through the stepwise introduction, almost whole I&C systems including the safety-related systems were finally digitized in Kashiwazaki-Kariwa units 6 and 7 (K-6/7) which first adopted the safety grade digital systems in Japan.

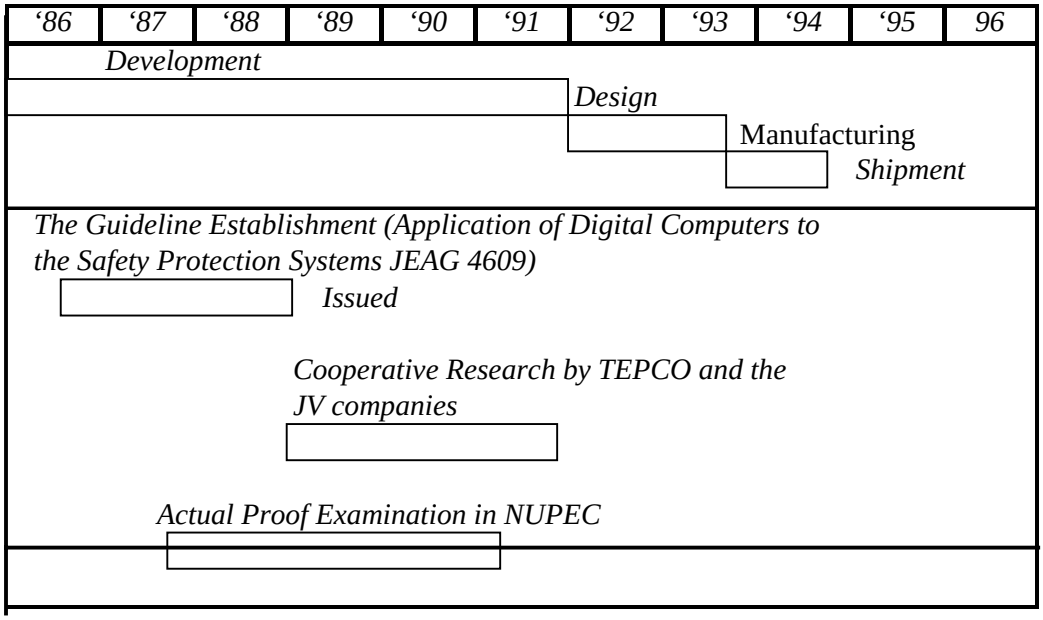
Experience on Digital Safety Protection System in K-6/7

Development Process

The introduction of the digital reactor protection system (RPS) was begun with the intensive study of the related guidelines and/or standards. Based on ANSI/IEEE Std.7-4.3.2 published in 1982, the development of Japanese domestic guidelines for the digital safety system of the nuclear power plants, was started in 1986. The development process had been continued for three years, which led to the publication of JEAG 4609:"Guidelines for Application of Digital Computers to Safety Protection Systems".

After the publication of JEAG 4609, the reliability analysis of the digital control systems were performed, in parallel with the verification test of digital control systems, which was performed by NUPEC (Nuclear Power Engineering Corporation) since 1989. The design of digital safety system for K-6/7 was started in 1991. Figure-1 shows the development process.

Figure 1: The development process of safety digital systems for K-6/7



Quality Assurance and Design

Quality Assurance

ANSI/IEEE Std. 7-4.3.2 requests to maintain the reliability of the software applied to safety system and to carry out V&V (Verification and Validation) in such a way that the independent personnel or organization can clearly understand.

Based on JEAG 4609 (1989) that also requires V&V, the concrete V&V procedures were discussed and first applied to the digital safety system for K-6/7. In addition, the digital control systems, that had been proved to have high reliability and good performance by their preceding application to non-safety systems in the previous plants, were applied to the safety system.

Design

In order to execute the above QA/QC activities effectively, following design was taken into consideration.

In application of the digital control systems to the safety system, a software language, POL (Problem Oriented Language), was adopted because of its visibility and good operating experiences gained through the application to the existing plants. The algorithm of safety system consists of and/or logic, which is defined by the document called IBD (Interlock Block Diagram). The syntax of POL is very similar to that of IBD, so the utilization of it brought lots of merit in performing V&V.

Regarding the software architecture of the safety system, the following features were introduced in order to make the processing simpler.

- No interruption in external signal processing
- Static memory allocation to avoid complex resource allocation
- Periodic processing

The safety system consists of 4 divisions and the 2 out of 4 logic is employed. As for consideration for common mode failures, some hard-wired back-up countermeasures were installed based on the defense-in-depth concepts. Figure 2 and 3 show the configuration of RPS (Reactor Protection System) and ESF (Engineering Safety Features), respectively.

Test Process

Factory Test

In manufacturers' factory tests, the combination test was performed after the component tests. In the combination test, the whole systems such as control systems in the main control room, local multiplex units, signal transmission networks etc., were connected and fully tested. The tests covered signal connection validity, system logic/interlock and so on. Through the factory tests, more than 2000 test cases were carried out to confirm the integrity for the single failure criterion, including single CPU failure in the redundant systems, single transmission line failure in the redundant network system and loss of power etc.

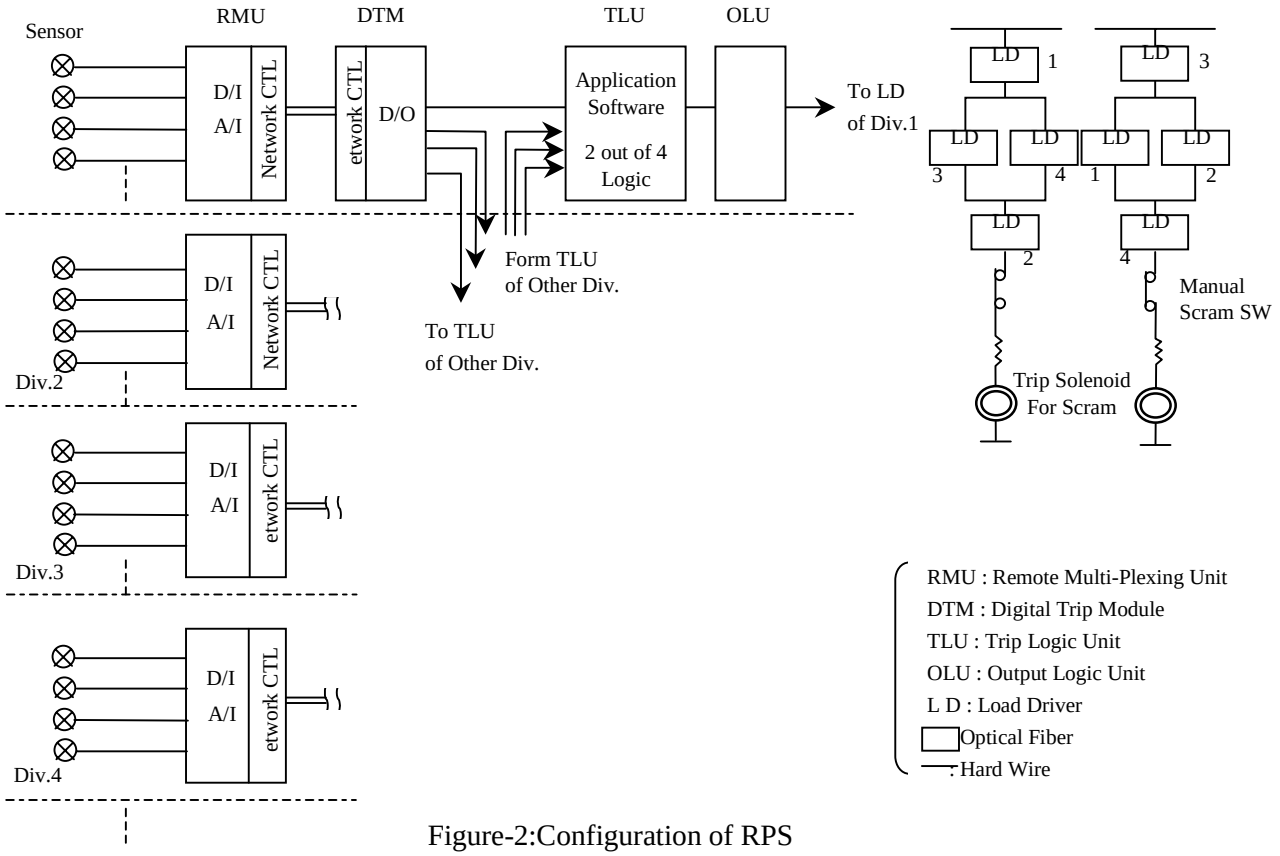


Figure-2:Configuration of RPS

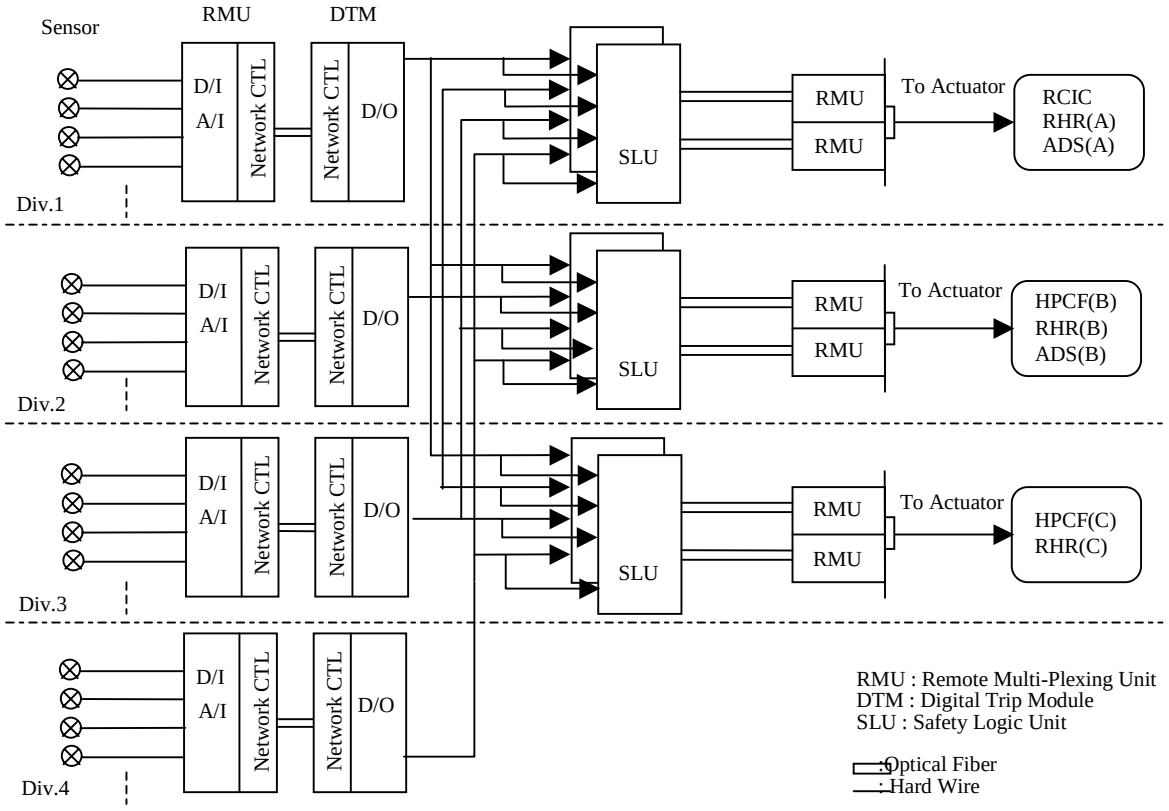


Figure-3:Configuration of ESF

Typical V&V tests were carried out strictly based on the guidelines and standards.

In addition to above, the integrity of POL software installed on the system was carefully checked by the comparison of graphically represented POL software diagram and graphically displayed actual software logic on system maintenance tool to investigate the POL compiler (Reverse Compilation Tests).

In validation process, the semi-dynamic simulation tests were also performed additionally to investigate the integrity for system requirement. By use of the plant simulators, their response to the transients were verified such as LOCA, LOPA, and Main Steam Isolation Valve Closure etc.

Figure 4 shows an example of the semi-dynamic simulation test result simulating a failure of reactor pressure control system.

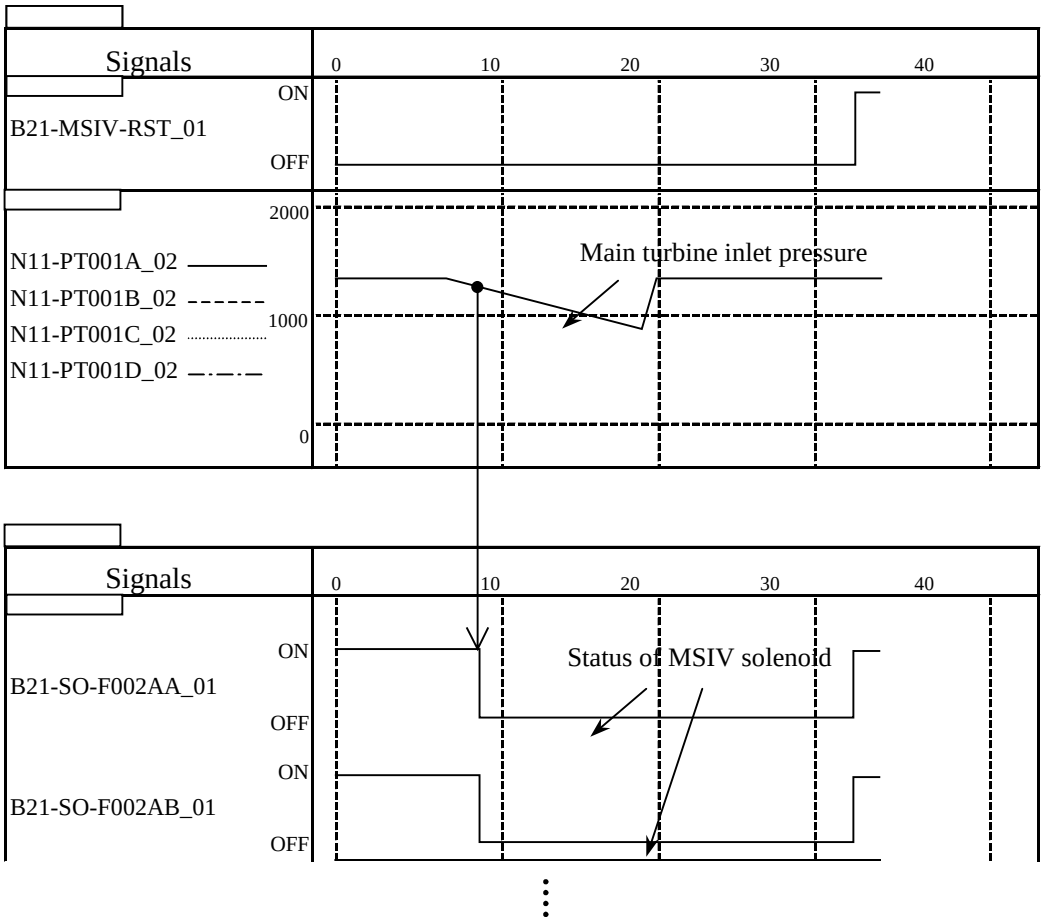


Figure-4: an example of the semi-dynamic simulation test results

Site Test (Pre-operation Test)

After the installation of the system, the whole system was tested to prove the installation integrity. This covered test items as same as the factory tests. In the pre-operation test, the system experienced more than 10 initiation against the transients such as load rejection at 20%, 50%, 75% and 100% power, LOPA at 20% power, plant trip at 50% power and Main Steam Isolation Valve Closure at 100% etc..

Evaluation of V&V activities

To investigate more efficient V&V methods, we evaluated the actual V&V activities of K-6/7 digital safety protection system.

Evaluation Results

Effectiveness of V&V

No major discrepancy was found in the factory and the site test, that demonstrates the effectiveness of V&V test.

Work-force Required

Most of man-hours were consumed for the documentation amounting to several thousand pages. The total man-hours required for them were about a few thousand man-days per plant. This amount of man-hours increased the plant cost.

Consideration on cost-effective V&V Method

In order to reduce the man-hours, the following improvements were discussed.

Software Modularization

The safety logic in BWR is quite simple and the similar software logic is used for initiation of some of ESF. So, by the help of the configuration management method, it is expected that design, manufacture and V&V could be achieved more efficiently. In order to apply the configuration management effectively, the modularization and capsulation of software are very important.

Software Reuse

Once the software is verified and validated through V&V procedures, it may be applicable to other BWR plants without V&V except for verification of the limited software which is unique to the target plant or modified from the baseline, and validation to confirm the system integrity.

Evaluation by means of Hazard Analysis

The hazard analysis is an method to identify the system element, design process, management process which might bring the plant to accidental state (called hazardous state). The hazard analysis aims at reducing the possibility to fall on the hazardous state by performing the intensive evaluation and verification of extracted elements through the hazard analysis. NUREG/CR-6430 introduced several techniques of the hazard analysis. In accordance with the technique, TEPCO performed the hazard analysis utilizing FTA method as follows.

Definition of Top hazard

The safety system initiates the trip function in the case that the values of monitoring parameters increase/decrease compared with their thresholds. Therefore, the system hazard could be actualized as an anomaly of trip initiation signals. So anomalies of the safety system are categorized into the following two cases.

- Failure of initiation against the trip request
- Unnecessary (erroneous) initiation with no trip request

In our analysis, these two are defined as the top hazards.

Development of the Top Hazard

The defined top hazard of the safety system is developed into the hazard of the lower layer step by step. And finally, the bottom hazard elements are extracted and identified in details.

Figure 5 shows an example of the development of the erroneous initiation of SCRAM with no request, that is the top hazard. In this example, the 4 bottom elements are extracted in 3rd or 4th layer, but most of the elements are developed into the still lower layers.

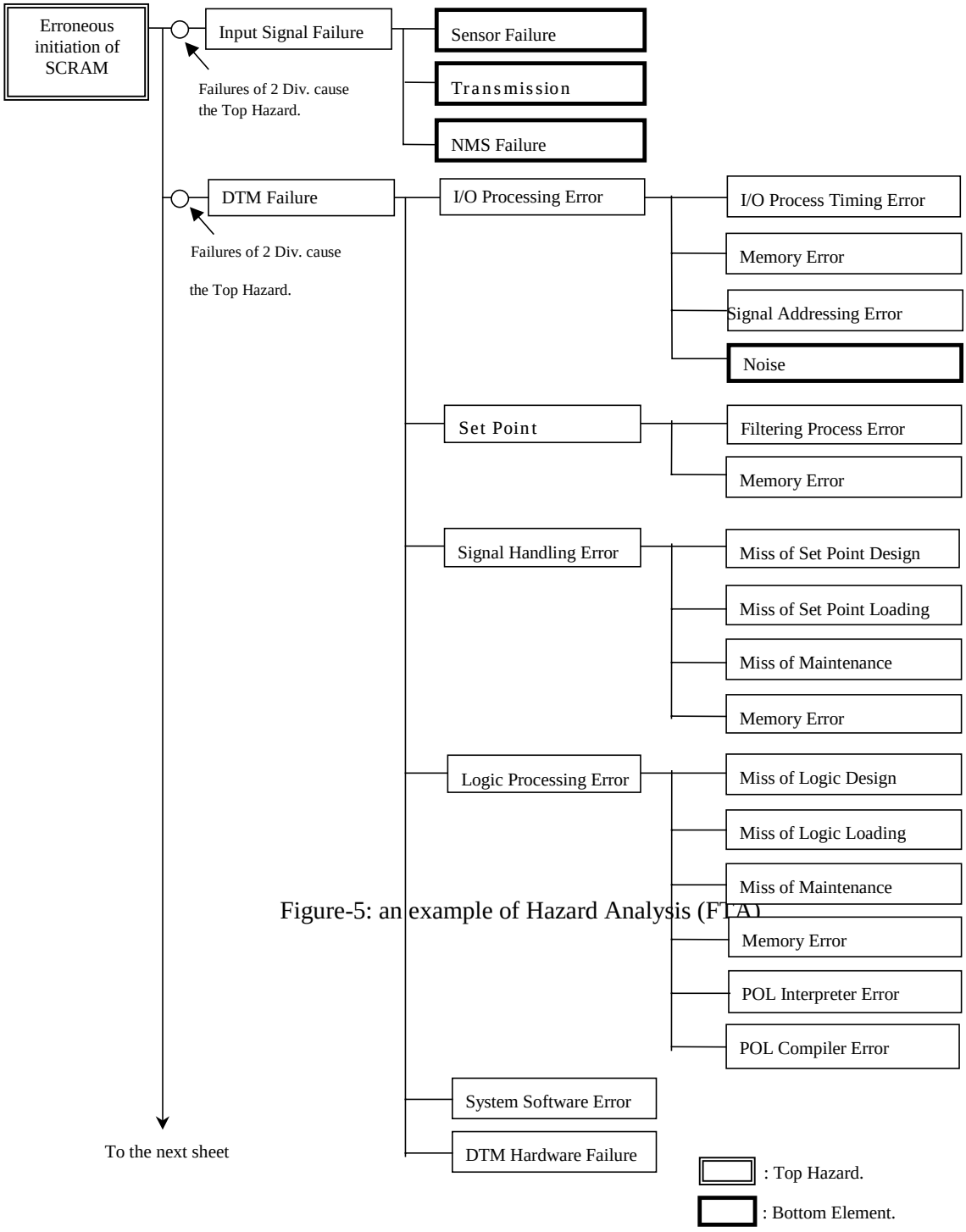


Figure-5: an example of Hazard Analysis (FTA)

Results of Hazard Analysis

FTA extracts a lot of bottom elements that seem to be latent in design process, manufacturing process, management process and so on. We examined every identified bottom elements and their verification process. An example of summary table is shown in Table-1.

It is found that the hazard elements latent in the application software can be found and solved by V&V, while the hazard elements latent in the system software can be solved by the design verification, V&V, the reverse-compilation and the semi-dynamic simulation test.

Table-1: an example of Hazard Analysis results

Category	the Bottom Element	Verification Process
System Software	POL Interpreter Error	- White Box tests and Black Box tests in Developing Phase - Validation - Semi dynamic Simulation tests - SSLC System tests and Startup tests on site
	System Software Designing Error	- Controller qualification Tests - Validation - Semi dynamic Simulation tests - SSLC System tests and Startup tests on site
	Diagnosis Error	- FMEA - Controller qualification Tests - Validation
Compiler	POL Compiler Error	- Controller qualification Tests - Validation Tests - Reverse Compilation between source code and object code
Application Software	I/O Process Timing Designing Error	- Verification (step3/4) - Validation
	Process Timing Designing Error	- Verification (step3/4) - Validation
	Memory Allocation Error	- Verification (step3/4) - Validation
	Filter Designing Error	- Verification (step2/3) - Validation

In specialty, as for the system software, it is very difficult to investigate details of it, because of its complexity. But the most important thing to achieve the high reliability of the safety system is not only to perform various tests in table-1 but also to choose the right software, which has the features as follows;

- Small size,
- Limited function,
- A lot of operation experience.

Conclusion

Policies to be applied to the digital safety systems

The good operating experience of K-6/7 demonstrates its high reliability and performance.

From the viewpoint of the experiences gained through the development, installation and operation of K-6/7, TEPCO believes that the following policies should be universally applied to the digital safety systems.

- Utilization of the digital control systems which have proved the performance and most operating experiences.
- Simple Software Architecture:

Static memory allocation, Avoidance of external interrupts, Periodic processing etc.

- Utilization of the graphical language in order to keep transparency and traceability for independent reviewers
- Execution of V&V
- Modularization of the safety software for its reuse and effective execution of V&V
- Considerations for common mode failures

The suitable backup measures against CMF should be applied.

Future Trends on the application of digital safety systems

In order to reuse the highly reliable software resource of K-6/7 effectively and to make this approach practical, JEAG 4609 (1989) was revised and published as JEAG 4609 (1999).

It covers the new subjects such as:

- Software Revision Control by Configuration Management
- Reuse of Software with Configuration Management
- Suitable Design Considerations for CMF

In Japan, several ABWR plants are under construction now. We believe that the digital safety systems developed and validated in K-6/7 would be basically applied to these plants.

Reference

1. K.Iwaki, "Control Room Design and Automation in Advanced BWR", In proceedings of the 1990 OECD/NEA international symposium, March, 9-13 July, 1990
2. Takao Tochigi, Yusuke Kajikawa, Chikara Takayama, "Development of integrated digital instrumentation and control system", In proceedings of 1992 OECD/NEA international symposium, Tokyo, 18-22 May, 1992
3. Hiromu Kikuchi, "Digital control technologies applied to TEPCO nuclear power plants", In proceedings of the 1995 INE international conference on C&I in nuclear installation, UK, 19-21 April, 1995
4. Takaki Mishima, Tomoaki Shirakawa, "The design requirement and development of software for the digital safety protection system in Kashiwazaki-Kariwa units6 and 7", In proceedings of the 1996 OECD/NEA international workshop on technical support for licensing issues of computer-based systems important for safety, Germany, 5-7 March, 1996

Technical Requirements on Maintenance of Digital I&C Systems Important to Safety

G. Schnürer[1], M. Kersken [2], F. Seidel[3]

[1] Institute for Safety Technology (ISTec), Garching
Tel.: +49 89 32004-523, Fax: +49 89 3200-300, e-mail: sgu@grs.de
[2] Institute for Safety Technology (ISTec), Garching
Tel.: +49 89 32004-546, Fax: +49 89 3200-300, e-mail: ker@grs.de
[3] Federal Office for Radiation Protection (BfS), Salzgitter
Tel.: +49 5341 885-863, Fax: +49 5341 885-865, e-mail: Fseidel@bfs.de

Abstract

The operation of digital safety I&C systems requires the availability of spare parts as well as the so-called configuration management procedures within the framework of maintenance and upgrading strategies. Requirements which are treated and discussed in this paper are (technical) solution oriented versus Guidelines do have an overall (general) character. This paper deals with the necessity of requirements on maintenance and upgrading of safety relevant digital I&C systems as a basis for the elaboration of proper maintenance and upgrade guidelines. Also the adoption of existing rules and guidelines is taken into account for precising these additional requirements for safety relevant I&C. Main goal of this paper is the introduction of possible safety relevant requirements with respect to

- maintenance of digital (hardware and software) safety relevant and safety I&C
- tracing and route cause analysis of incidents, caused by I&C maintenance
- support of the regulatory body as well as technical experts concerning the state of the art.

Introduction

Contrary to the complex of upgrade and refurbishment procedures In this paper the term maintenance is used in the following manner: Maintenance is the combination of all measures which ensure the specified system function. Maintenance procedures should have a small effort and a limited duration. For safety reasons maintenance procedures in NPP can just take place in one redundancy without reducing the availability of parallel systems as well as combined systems (e.g. CPU of software based systems) in an irregularly way. Consequently the update with new or modified SW-versions in this sense is no part of maintenance for safety systems.

With respect to the operational life time of more than 30 years for German NPPs the rapid innovation cycles of new I&C systems and the non availability of spare parts are leading to different maintenance and upgrading strategies for safety I&C systems. Generally, there are 3 different strategies The first one is based on a redesign of operation proved hardwired I&C electronics (sub-assemblies) on basis of compact electronic devices, like I&C circuits for o-ver-voltage protection, etc. Such redesigned sub-assemblies are to be qualified according to the German KTA-standards. the replacement with that redesigned sub-assemblies normally is part of a maintenance process. The second way is based on a redesign of hardwired I&C electronics with ASICs and/or FPGA. These ASICs/FPGA do not have any micro controller by means of they do not need any software support during operation. The advantage is an eased qualification in comparison to a software-based ASIC. The replacement with ASIC (FPGA) based

redesigned sub-assemblies may also be a part of a maintenance process. The third upgrade strategy is the introduction of PLCs by means of software-based I&C systems. This paper deals prior with safety relevant requirements on maintenance and SW-upgrading of digital safety I&C systems.

Whereas maintenance requirements for hardware in Germany are already existing or treated by ”business as usual”, respectively, requirements for software-based systems are only partly treated in the national and international regulations.

Consequently the missing requirements are to define and to elaborate. Requirements for maintenance and upgrading of digital systems should cover the following aspects:

- New designed software for a specific application. Therefore requirements for the specifi-cation (refurbishment procedure, formal methods, traceability and testability) as well as configuration and parameterization (requirements for tool application, software testing) are to fulfill.
- Software of existing systems (COTS) which needs to be adopted (configured) to a special application. Therefore requirements for development documentation, state of software modules as well as testing are to investigate.
- Hardware of the system or component (replacement of components). Requirements for the design tool, specification of the hardware architecture, documentation, testability are needed.
- Requirements for the factory acceptance tests (integration; in the case of maintenance, as far as it is a prerequisite for field testing) and field testing are to specify.
- Requirements for manual testing procedures are to elaborate.

This paper gives a brief overview of already existing requirements and discusses the necessity of additional national and international requirements on maintenance of digital I&C sys-tems important to safety.

State of the art

Software tools which are used for design, construction and implementation planning as well as qualification management do also have to specify the hardware structure and modules according to the computer system. This means, that instead of manual programming of I&C functions the configuration, parameterization and automatic coding of pre-developed soft-ware modules will take place. Such software programs are planned and task specific. Be-sides, tool systems are also managing software modules, which are developed by conventional methods of software engineering. This kind of software could be the operating system, in- and output drivers, communication software, self-testing procedures, diagnostic software as well as software for the treatment of exceptions. Therefore , there are also programs to add, which realize the processing of the automatic generic code, like functional diagrams and functional diagram groups. Such programs realize the runtime environment.

The runtime environment software contains the software which - also named as application software - is performed in the target system of nuclear power plants.

This paper deals with already existing requirements and with the elaboration of new requirements concerning testing and safety assessment of procedures to maintain and upgrade of digital I&C.

International requirements according digital upgrades important to safety during maintenance

Digital upgrades during maintenance for software of the highest category

The international standard IEC 60880 /1/ for software of the highest safety category contains the necessary elements for an acceptable software modification process. This software change process may be necessary during software production, i.e. design, coding, system integration, system validation and commissioning, but also during maintenance (see Fig. 1). The documentation related to the software modification comprises anomaly report, software modification "field document" and software modification field history, where the latter collects the information concerning software changes from the production and maintenance processes.

The necessity for the modification of software may be due to the occurrence of an anomaly, a change of functional requirements after delivery, new technological solutions (upgrading) and a change in operating conditions.

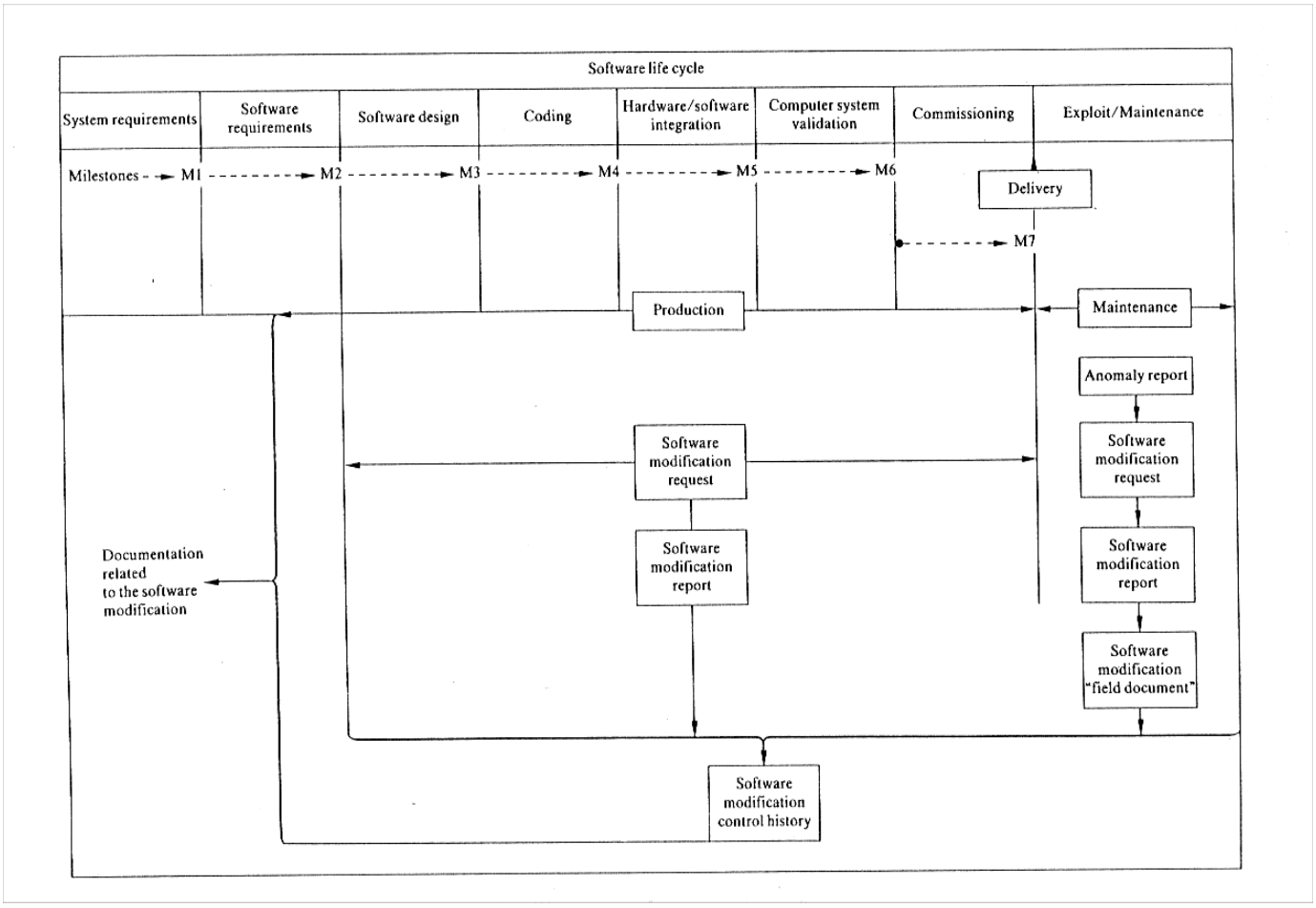


Fig. 1: Software change processes during production and maintenance /1/

In case of an anomaly, an anomaly report is written giving the symptoms, the system environment and system status at the time at which the anomaly was discovered and the suspected causes.

Anomaly correction requires the generation of a software modification request, the execution of which follows the modification request procedure described below.

In case of a change in software functional requirements or in operating conditions, the whole software development process is re-examined for that part of the system impacted by the change.

Any new hardware requirements and capabilities are examined with respect to their potential impact on the software systems. This evaluation should include all hardware considerations reviewed in the original software design. If it can be shown that the new system does not impact the software requirements, a simplified procedure may be used to implement the modification either at the design or coding phase.

In all cases, after implementation of the modification upon the in-the-field equipment, a field documentation is issued which gives the date of the implementation and the result of the specified observations. This document is filed in the software modification control history for the project.

The following aspects of maintenance and modification of software-based systems are covered in [1].

Modification request procedure for software of the highest category

This software modification request should identify its originator, the reason for the request, its aim and the functionality affected by the change.

Persons which are independent from those who issued the modification request should evaluate it, the result being either

- acceptance of the request, or
- rejection with the appropriate reasoning, or
- approve the request of minor importance and impact, or
- requiring a detailed documented analysis, written by software personnel knowledgeable in the system software.

The following items are examined in the evaluation of the modification request with respect to

- technical feasibility,
- impact upon hardware (e.g. memory extension) or upon other equipment (e.g. test sys-tems) in which case the request for modification addressing this impact area must be documented for the equipment,
- impact upon software including a list of affected modules,
- impact upon performance (including speed, accuracy, etc.)
- necessary effort for verification and validation; the analysis of the software reverification needed is documented in an audible form,
- the set of documents to be reviewed.

The software modification request is pending until the decision is made:

- to accept it (immediately, or after examination of the software modification analysis re-port) and to execute it, or
- to reject it and justify the rejection.

Execution of a modification

The procedure for executing a modification follows the development process; i.e. all phases of the software development lifecycle have to be repeated for any part of the system im-pacted by the change. This means that the modification is carried out according to the (many) rules for good (error-poor) development of software (as e.g. laid down in chapter 5 of /1/).

All the documents affected by the modification must be corrected and refer to the identification of the software modification request. a software modification report sums up all the actions made for modification purposes.

All these documents are dated, numbered and filed in the software modification control history for the project, i.e. they are held under configuration control.

A configuration management system provides a means to ensure this.

After implementation of the modification, the whole or part of the verification and validation process must be performed again according to the software modification analysis.

For modifications on site, the software supplier should have access to a test configuration which is identical to the real system in all relevant aspects (including installed machine, translator, testing tools, plant simulator, etc.) to ensure the validity of the modifications.

Licensing issues

The international standard IEC 60880 /1/ contains the necessary elements for an acceptable software change process. However, for regulatory purposes and for safety systems there is a need to add an additional dimension to the change process /2/. This additional dimension results from the need for : (i) an analysis of the effect of the change on safety; (ii) the provision of documentary evidence that the change has been conceived and implemented correctly; and (iii) a process of independent review and approval of the change. The requirements coming from this regulatory view are of course partly overlapping with the requirements imposed to the production (and V&V) process. They are summarized according to /2/ in the following.

General

The software change procedure and documentary process shall be applied to all elements of the software system including its documentation. This procedure shall apply equally to sys-tem functionality enhancements, environmental adaptations (resulting in a modification to the system requirements) and corrections of implementation errors.

An appropriate software architecture and a suitable software configuration management system shall be used during the lifecycle process in order to maintain safety. For safety sys-tems, no distinction shall be drawn between major and minor software changes since a wrongly implemented minor change could challenge safety.

Once a software or documentation item has been approved, i.e. has been placed under con-figuration control (usually following its initial verification and placing in the soft-ware/documentation library for release), any changes to this item shall be controlled by a procedure containing the elements given in the following paragraphs.

The software change procedure and the configuration management system shall include an adequate problem reporting and tracking system.

The software change procedure shall contain the following basic elements.

(i) the identification and documentation of the need for the change;

(ii) the analysis and evaluation of the change request, including: a description of the design solution and its technical feasibility; and its effect on the safety of the plant and on the software itself;

(iii) the impact analysis of each software change: for each software change, the implementers of the change shall produce a software impact analysis containing a short description of the change plus a list of software parts affected by the change plus the effect on non-functional system properties as, e.g. dependability, response time, system accuracy, hardware performance. Objective evidence that the full impact of each software change has been considered by the implementor for each software part affected shall be provided. As a minimum this shall consist of a summary description of the change to be implemented, plus documentary evidence of the effect of the change on other software parts. The software impact analysis shall also list data items (with their locations – scope of the data item) that are affected by the change plus any new items introduced.

(iv) the implementation (consistent with the standards employed in the original production process), verification, validation (as appropriate) and release of the changed software or document item. The V&V phases may make use of the software impact analysis to perform regression testing.

(v) The requirements of IEC 60880 sections 9.1, 9.2 and 9.3 shall apply.

Faults shall be analyzed for cause and lack of earlier detection. Any generic concern shall be rectified and a report produced.

Software Modification

A correction to a wrongly implemented software change, if found at the stage of site testing (i.e. following installation of the software on the plant), shall be processed as though it were a new software change proposal.

The commissioning team shall use the software impact analysis and the factory V&V report to develop their own series of tests in the form of a site commissioning test schedule.

Software Maintenance

All software changes in operation following the completion of commissioning at site (called software maintenance changes in the following), shall be controlled by procedures which meet the requirements of this section on software maintenance.

For safety systems, program and fixed data (including operational data) shall be held in read only memory (ROM) so that they cannot be changed on-line either intentionally or due to a software error.

For safety systems, software maintenance changes shall be tested on the computer system installed at site. Any divergence from this shall be justified in the test documentation.

Software maintenance changes shall be reviewed, from a safety perspective, by suitably qualified and experienced staff – e.g. manufacturers (suppliers), system designers, safety analysts, plant and operational staff – that are independent from those persons proposing, designing and implementing the change. The above review shall consider manufacturers (suppliers) V&V and independent assessment reports, as well as test specifications and test reports, or other such documentation as appropriate to the change being proposed. The results of the review shall be documented and shall include a recommendation for approval, or rejection of the change from the safety perspective.

Only software approved for release shall be installed at site.

Before the start of site testing of any changes to the software of a safety system, the test specifications shall be reviewed by independent reviewers.

Before permitting the operational use of software following a change, an updated and checked version of the system and safety demonstration documentation (including any routine test schedules) shall be available, fully reflecting the changes that have been made. This shall be confirmed by independent review

The independent reviews shall be documented.

Configuration management

All the items of software including documents, data (and its structures) and support software shall be covered by a suitable, readily understood and fully documented configuration management system (CMS) throughout the lifecycle. An item of software or documentation shall not be accessible (to persons other than those responsible for its design and verification) until it is approved and under configuration control.

A formal procedure shall be set up for version control and the issuing of correct versions. Provision shall be made for informing all relevant personnel of pending changes and approved modifications.

All software copies, including any pre-existing software that is being used, shall be clearly and uniquely labeled with at least title, version number and creation or acquisition date. Pro-vision should be made for the inclusion in the source code listing of information on changes made, approval status, and authors, reviewers and approvers names. The identification and version number shall be included in the code so that this can be checked by other software items.

After delivery of the software and its documentation, the same level of configuration management shall be maintained at the site where the delivered software is stored.

A configuration audit shall be performed on the safety system software prior to loading to establish that the correct items and versions have been included in the system. Following system loading, the loaded version shall be verified as being uncorrupted.

Conclusions

As already mentioned, IEC 60880 describes the modification process for software in computer-based systems of the highest safety category. Taking into account, that most of the software-based systems important to safety are also to be installed in lower safety classes, the importance and necessity of

staggered requirements for the lower safety categories is obvious. The German Guidelines of the Reactor Safety Commission contain already staggered requirements to prove the qualification of the software-based systems of lower safety classes in a general way. Furthermore, in Germany we have already requirements for hardware modifications within the lower safety categories. As a general requirement, in Germany the modified system must have at least the same qualification level than the previous system. Furthermore, also after modification the I&C shall not limit the availability of the safety system. For hardware the qualification level can be demonstrated via operational experience or via a type test procedure according to the German KTA rules, or, in case of introduction of new technologies a demonstration according to the state of the art.

For software-based systems important to safety following questions are to be answered:

- What qualification procedure is necessary in the case a hardwired equipment important to safety will be exchanged by a new software-based system? If the origin hardwired equipment is qualified via operational experience how to confirm the same qualification level of the new software based system?
- How to confirm the necessary qualification level considering the lack of operational experience with the new system?

How to consider the sufficient extent and deepness that in general any modification of the application software leads to a new software product? Within the frame of a research project of the German Ministry of Environment, Nature Conservation and Reactor Safety (BMU) ISTec is investigating different options for establishing new qualification and assessment requirements in the case of software modifications during maintenance. First results of that investigation are:

- Any modification within application software results in a new software product. Already existing operational experience of the former software product can hardly be used for qualification issues. Except, the operational experience is based on a unchanged soft-ware routine within the application software (e.g. functional software blocks inclusive in-terface environment).
- For the highest safety category operating experience can not replace a detailed documentation of the software product and its development process. Only missing parts of the necessary set of documentation can be replaced by operating experience.
- The collection of operating experience must also be governed by a whole set of requirements which ensures completeness, correctness and non-ambiguous of the data and their collection process. It should be possible to demonstrate that the data collection is appropriate although from the statistical point of view. Additional information concerning data acquisition are already introduced in an other contribution of this meeting.
- The need of requirements concerning software modifications during maintenance of the lower safety classes is obvious.
- Requirements according to IEC 60880 concerning maintenance and modification of soft-ware do have a general character. They should be specifically applied. Part 2 of IEC 60880 contains more details concerning the application of pre-developed software. But there remains also a certain area of free interpretation. Actual software modification proj-ects will show, whether at least the requirements of IEC 60880, part 2 are sufficient by means of covering all regulatory issues.
- Starting from the requirements of the German RSK-Guidelines or IEC 60880, respec-tively, staggered safety requirements should be elaborated. Possible requirements for the qualification of pre-developed software in staggered categories are introduced in another contribution of ISTec to this meeting.

Information about the project’s further progress will follow.

Summary and Outlook

This paper describes the already existing requirements concerning maintenance and upgrading of digital safety systems according to IEC 60880 and the common position of the European nuclear regulators for the licensing of safety critical software for nuclear reactors /2/. Whereas the requirements for hardware upgrades are already covered by the German nuclear standards additional guidelines for software maintenance are under discussion. Following aspects are considered:

- Completeness and applicability of the existing requirements concerning maintenance and upgrading of digital safety systems.
- Software maintenance requirements for systems of lower safety categories.
- Maintenance requirements concerning automatically generated software.

Literature

/1/ IEC 60880: Software for computers in the safety system of nuclear power stations, 1986

/2/ EUR 19625 EN: Common position of European nuclear regulators for the licensing of safety critical software for nuclear reactors, May 2000

Requirements Management of I & C System Refurbishment of NPP Dukovany

J. Pliska [1], J. Cendelín [2]

[1] *I&C Energo, Prazská 684, 67401 TREBÍC, Czech Republic*
Tel.: + 420 618 893 300, Fax: + 420 618 893 999, e-mail: jpliska@ic-energo.cz
[2] *West Bohemian University in Pilsen, Faculty of Applied Sciences, Department of Cybernetics, Univerzitní 22, 30614 PLZEN, Czech Republic*
Tel.: + 420 19 7491 155, Fax: + 420 19 279 050, e-mail: cendelin@kky.zcu.cz

Summary

The Requirements Management System is a necessary precondition for the organisation, management, coordination, inspection and evaluation of the extensive project, both from the viewpoint of the contractor and customer, as well as from the viewpoint of the national regulatory body. It is a tool for systematic identification, requirement structuring, communication, control, monitoring and verification of user requirements.

The system is based on a list of individual requirements. The user requirements are organised into a hierarchic structure which observes the structure of the application area. Individual requirements are mutually interrelated in various ways. Each requirement is expressed in form of a written description. Some significant features of the requirements are clearly and simply expressed with a set of assigned attributes.

Introduction

Using an example of the Requirements Management System as implemented in the project: I&C System Refurbishment for NPP Dukovany the paper describes capabilities and usefulness of system analysis methods and the corresponding tools – generally designed CASE systems.
The purpose of this paper is to provide a closer look at these system analysis methods and tools. These methods and tools have not been sufficiently widespread in technical practice, although they offer a number of advantages and may significantly influence the resulting quality of the Work.
Frequently, the field of application for these methods and tools is confined to large-scale data processing and software engineering.

Basic Data of the Project: I&C System Refurbishment for NPP Dukovany

The described Requirements Management System has been used in the project of I&C System Refurbishment for NPP Dukovany. The project is very extensive and complicated and from the viewpoint of functions it includes the following I&C systems at NPP Dukovany:

A) Safety systems, participating in the implementation of safety functions:

- Reactor Trip System,
- actuation of technical means for safety assurance,
- gradual actuation of devices supplied from assured power sources,
- Post Accident Monitoring System.

B) Safety related systems, participating in the implementation of safety-related functions:

- supporting actions to actions which assure safety,
- protection of steam generators,
- automatic limitation and reduction of reactor power output,
- regulation of the reactor power output.

C) Not safety systems, participating in the implementation of functions monitoring condition of the unit:

- In-Core Measurements System,
- Computer Information System.

In all cases, with the exception mentioned below, the listed existing systems will be entirely replaced with new ones. The only exception is the Post Accident Monitoring System (PAMS) which is not currently a part of the I&C structure at NPP Dukovany.

Specification and Requirements for the Requirements Management System

The Requirements Management System has been created through a controlled transformation of the Contract and its appendices containing requirements for supplies, works and services into a file of requirements which make up the system.

This transformation into the system has enabled well-organised administration and control of the requirements and has brought a number of other advantages.

Specification of the Requirements Management System.

The process of requirement management ranks among the essential processes in the project initiation and management. Its objective is to provide for the mechanisms to:

- analyse and review the input data, to check that they are formally and factually correct, complete, understandable and unambiguous,
- unambiguously identification and documentation of user requirements,
- identify and describe mutual relations between the requirements,
- change management of the requirements and to analyse impacts of such changes,
- monitoring, evaluation and documentation fulfilment of the user requirements and to implement corrective measures.

The Requirements Management System serves as an input for:

- Basic Design,
- Test Planing and Inspections,
- Detail Design,
- Realisation,
- Supplies and Installation,
- Commissioning.

A quality system of requirement management contributes to the development of effective partnership with the customer.

Characteristic Features of Correctly Defined Requirements.

A correctly defined requirement shall have a number of features. They include, in particular:

- Necessity (basic function)

  The requirement shall define a basic capability, physical characteristic or quality factor. Removal of the requirement without replacement shall result in a failure.

- Briefness

  The requirement description shall contain a single requirement. The requirement shall express WHAT is required but not HOW it should be achieved.

- Feasibility

  The requirement shall be feasible using one or more variants of system designs.

- Completeness

  The requirement shall be complete and shall not require any additional explanations or supplements. Each requirement shall be capable to exist independently of the other requirements.

- Consistency

  No requirement shall contradict to the other requirements.

- Unambiguous Description

  Each requirement shall have only one interpretation.

- Verifiability

  No requirement shall be general. It shall be possible to verify its fulfilment with a test or analysis.

Implementation of the Requirements Management System.

Application of System Methods and Tools.

System analytical methods may be efficiently and successfully used whenever a system is the subject matter – an object made up of mutually interrelated elements. These methods, which have been used and developed in system engineering for half twenty century, are truly universal.

The requirements file is a system made of elements - individual requirements. Each requirement is described with a structured text. Individual requirements are mutually interrelated in various ways. The requirements may be arranged into a hierarchic structure. Some important properties may be expressed in a clear and simple way with the assigned attributes.

Efficient implementation of the system is strongly dependent on the quality of applied supporting tools. The suitable tools for these purposes are generally designed CASE systems. There are not many suitable systems of this type suitable for the purpose because their significant proportion specializes in partial tasks, particularly in data processing and software engineering.

The general tool for system analysis - *case/4/0* , in its current 5.0 version, by microTOOL, Germany, has been used for the Requirement Management System in the project: I&C System Refurbishment for NPP Dukovany.

Description of the Implemented System based on case/4/0.

The Requirements Management System has been implemented using *case/4/0*. The tool contains a complete range of system analytical methods. A prevailing part of these methods is of graphic nature.

The key step for each solution is correct assignment of methods to structural properties of the requirements file.

There is a certain limitation caused by the fact that *case/4/0* has firmly established names of the objects it works with. Therefore the following pairs of terms have been introduced, see Table 1.

Requirement	=	Function
Hierarchic structure of requirements	=	Functional structure
Relations between requirements	=	Information flows between functions
Elements outside the requirements system (other projects)	=	External interface
References to standard and on	=	Data structure
Physically existing component of the requirement's content (text, attribute value)	=	Data element
Summary of information about the requirements and its factual content	=	Module
Structure of the requirement's factual content	=	Type structure (analogy of data structure)

Table 1

Apart from the these, additional terms have been introduced, see Table 2

Internal interface	-	Different graphic displaying of a requirement from the remote area of the requirements system; it is used to express relations between requirements
Memory	-	Summary identification of a data structure; it is used to identify a related documentation unit. e.g. standard, regulation etc.

Table 2

Requirements Hierarchy

Hierarchy of the requirements is displayed in a hierarchic functional diagram (functional structure). The diagram presents decomposition of requirements down to the basic units. The requirements are split into groups containing requirements with similar meaning.

The final product of decomposition is a requirement of reasonable scope, up to one page of text. At this level the text is structured into marked paragraphs.

Relations between:

- elements within one group,
- elements from one group and elements from other groups (internal interface),
- elements from one group and other projects,
- elements from one group and related documents (standards etc.)

are expressed with a information flows diagram. The above-mentioned elements represent junction points of the diagram.

The links between elements in the diagram represent relations between the elements and are identified (described) with terms referring to the data structure. The data structure may then express a simple or fairly complicated structure of the relationship.

Requirements Content and Attributes.

The set of requirements is displayed in a graphic form with a module structure. The requirements are always the so-called "leaf – requirements" from the hierarchic tree of requirements.

Each requirement in a module has an assigned element representing reference to the type structure, expressing the structure of the requirement's textual content (the requirement's content is structured).

The text expressing factual content of the requirement is linked to a data element. The data element may be linked to a leaf element of the data or type structures. One data element may be linked to more leaf elements of the data or type structures. This may be used in a case where the content of different requirements is factually identical.

A data element represents an actually existing data object, in this case a text. An element of the data structure only symbolically represents an information unit as a part of the requirement's text.

Each requirement (function element) may be complemented with attributes.

Change Management

The factual content of a requirement may change in time and the changes need to be recorded in the documentation for the purposes of change management. Therefore texts of the requirements are stored in individual versions of data elements, which may be positively identified with a number of the version and date of origin.

Generally, all elements of all diagram types may be complemented with a text commentary.

Monitoring and Evaluation of Requirements Fulfilment

A dedicated item in the type structure is used to monitor and evaluate the changes, i.e. to find out:

- how the requirements are being or have been fulfilled,
- how the fulfilment is checked,
- results of the checking.

Repository and Evaluation Functions

All data about the requirements system are entered into the CASE system via a database - repository and are available for further use.

The *case/4/0* system is provided with an extensive set of evaluating and generating functions. It is also possible to enter additional evaluation functions into the system. For this purpose a simple programming language of the BASIC type is available, which enables to use all types of information in the repository and generate arbitrary formatted prints using the MS Word processor.

The evaluating functions support creation and utilization of the requirements system by automatically checking it for errors and reporting them. They also provide to the user lists of requirements, sorted out based on entered criteria.
HTML Format.

The newly available HTML format has been used to generate outputs from the Requirements Management System. It enables to generate a document in which the user may easily browse a current version of the requirements file. Also an analogy of fulltext search has been implemented, using special evaluating functions.

Hierarchic Requirements Structure

One of the fundamental procedures in requirements analysis is a design of the n-level hierarchic structure of the requirements.

To design the first two levels the Work has been physically structured into the so-called parts of the Work, see Table 3.

Ident.	**Level 1**	**Ident.**	**Level 2**	**Note**
AXX	Common Part			Basic Design
BXX	Control Points/MMI	B1X	Control Rooms	Main Control Room and Emergency Control Room
		B2X	Control Counters and Panels	
		B3X	Local Switchboards	
		B4X	Controllers	
CXX	Field Instrumentation	C1X	Measuring and Sampling Points	Including Sensors
		C2X	Measuring Circuits	
		C3X	Actuators	
DXX	Cabling	D1X	Penetrations	
		D2X	Cables	
		D3X	Cable Supporting System	
EXX	Power Supply			Level 2 left out
FXX	HVAC			Level 2 left out
GXX	Mechanical Engineering Part			Level 2 left out

HXX	Construction Part			Level 2 left out
RXX	Control Systems	RTS	Reactor Trip System	RTS
		TRIP	TRIP Breakers	RTS
		ESF	Engineered Safety Feature Actuation System	ESFAS
		EXC	Ex-core Neutron Flux Measurement System	EX-CORE
		REKT	Reactivity Meter	EX-CORE
		RLS	Reactor Limitation System	RLS
		RCS	Reactor Control System	RCS
		RRC	Reactor Rod Control System	RRCS
		SGP	Steam Generator Protection System	SGPS
		SAS	Support Actions System	SAS
		ELS	Emergency Load Sequencer	ELS
		PCS	Computer Information System	PCS
		INC	In-core Measurement System	IN-CORE
		PAM	Post Accident Monitoring System	PAMS

Table 3

The functional viewpoint has been adopted to design additional (lower) hierarchic levels. Examples of the hierarchic levels 3 and 4 for control systems are shown in Table 4.

Ident.	**Level 3**	**Ident.**	**Level 4**	**Note**
01	Harmonization Concept			
02	Basic Requirements			
03	Initial Condition			No requirement
04	Operational Requirements			
05	Service Requirements			
06	Performance Requirements	06.0	Basic Requirements	
		06.1	Function	
		06.2	Capacity	
		06.3	Reserves of the Equipment	
		06.4	Availability and Reliability	
07	Architecture Requirements	07.0	Basic Requirements	
		07.1	Integrity	
		07.2	Diversity	
		07.3	Redundancy	
		07.4	Design and Implementation	
		07.5	Links to the Surrounding Environment	

		07.6	Placement in the Layout	
		07.7	Computer Systems	
08	Testing and Maintenance Requirements			
09	Documentation Requirements			
10	Legislation and Standards Requirements			
11	Limitations			
12	Quality Requirements			
13				Not used
14				Not used
15				Not used
16	Implementation Requirements			
17	Requirements for Works			
18	Requirements for Services			
19	User's rights			

Table 4

Requirements Identification.

Unambiguously identification of user requirements is a fundamental for the Requirements Management System. In the example below a structured alphanumeric symbol has been selected:
XXXCC.D.D.D.D

where:

- **XXX** three-letter symbol; see Table 3
- **CC** two decadic digits; see Table 4
- **D** one decadic digit; see Table 4

The selected alphanumeric code is closely related to the requirement's position in the hierarchic structure and enables more organized and easier work with the requirements.

Requirements Attributes and Relations between Requirement

Requirements Attributes are a very powerful tool which enables additional manipulations with the requirements and various analyses in a selected set of requirements to study them from different viewpoints and find new interrelations between them.

In the concerned case the following attributes have been used:

- requirement status,
- traceability,
- affiliation to a particular part of the Work,
- requirement type (e.g. influence on nuclear safety),
- and other attributes added on as-needed basis in the course of individual stages of the Work implementation.

Another significant characteristic of the requirements are their mutual relations. In the concerned case there are two types of relations:

- relation between local requirements – relation between requirements at the same hierarchic level and subordinated to one common requirement at a higher level,
- relation between remote requirements – agreement, connection, parent/child.

Each relation between requirements may be described with an arbitrarily complex data structure.

Other important relations include:

- relation between a designed requirement and a requirement resulting from legislation or standards (one-way dependence),
- relation between a designed requirement and the so-called other project (one-way or two-way dependence).

Each relation may be described with an arbitrarily complex data structure.

Conclusions

The concerned solution represents an example of system approach in the application area outside the so-called data processing or general software development. The solution shown here is an example of its use on a potentially huge market – industrial computer applications.

The practical experience has proved that a good CASE system provides many more options for solutions in Requirements Management Systems than common specialised tools. Moreover, the CASE system may be used in the projects to solve other tasks too.

The use of the CASE system has increased efficiency of the work due to the extensive potential of this system to identify errors.

The basic version of the requirements file is a repository of 50 MB. It takes less than an hour to generate an updated version of the documents on a computer (500MHz, 64MB operating memory). However, partial and the most significant portions of the documents may be generated in a few minutes.

The entire system of requirements is in the HTML format represented with 14 000 files with the total size of 50 MB. Any evaluation or sorting takes from several seconds to several minutes. The most time-consuming is fulltext search, taking less than 10 minutes in the whole system. In case limiting conditions are used the search is significantly faster.

Licensing process of the digital computer-based I&C systems to be implemented within the NPP Dukovany I&C system refurbishment project

OECD/CNRA/CSNI Workshop on Licensing and Operating Experience of Computer-Based I&C Systems, Hluboká nad Vltavou, 25 – 27 September 2001

Author: Ceslav Karpeta (Scientech, Inc.- organizational component in the Czech Republic)

Co-author: Josef Rosol (CEZ – NPP Dukovany)

Abstract

A brief outline of the NPP Dukovany I&C system refurbishment project is given including a survey of the equipment and services suppliers and the scope of their involvement in the project activities. The adopted licensing process for the overall project is described and the Czech Republic regulatory authority project specific requirements relating to the digital computer-based I&C safety systems are summarized. The methods and ways the plant operator has adopted to ensure meeting some of those requirements are presented.

1. Introduction

The NPP Dukovany operates four units of the VVER-440/213 type. The design of the plant dates back to the 1970-ties. The designer of the Nuclear Steam Supply System (NSSS) was LOTEP Leningrad, the designer of the Balance of Plant (BOP) was Energoprojekt Praha which was bearing also the responsibilities of the so-called general designer and design supervisor during the plant construction. The first unit went operational in 1985. The other three units followed within next two years and the plant reached the rated capacity at the end of the year 1987.

I&C equipment for the NSSS was designed, manufactured and delivered by companies from the former Soviet Union. I&C systems of the BOP were designed, manufactured and installed by companies of the former Czechoslovak Republic.

During the 16 years of operation the NPP Dukovany has been achieving very good performance which provides evidence that it is a safe, efficient and reliable source of electric power.

The results of a number of assessments and audits conducted at the plant by national and international organizations in the 1990-ties indicated that the plant operation could continue till the year 2025, as a minimum. To ensure the achievement of such a goal an extensive and comprehensive program has been launched to support the plant long time competitiveness and public acceptability. This program is also intended, to the extent reasonably achievable, for the plant harmonization with the current safety requirements and practices.

One of the components of this program is the plant I&C system refurbishment. The existing plant I&C was grouped into the following 5 modules which could be refurbished relatively independently one from the other:

- module M1: reactor protection and limitation, engineered safety features actuation, post-accident monitoring, reactor power control
- module M2: unit information system

- module M3: logic/modulating control of the NSSS
- module M4: turbine-generator protection and control
- module M5: logic/modulating control of the BOP.

This paper addresses some licensing aspects of that portion of the refurbishment activities, which cover the modules M1 and M2. They are implemented under a separate project, which is referred to in the sequel as the I&C refurbishment project.

2. Scope of the I&C system refurbishment project and the vendors involved in its implementation

The scope of the module M1 and M2 refurbishment project is as follows:

- Design, manufacture, installation, and documentation of the replacement of the module M1 consisting of:
  - Digital Neutron Instrumentation System (DNIS) which is a replacement of the existing AKNT system
  - Digital Process Parameters Instrumentation System (DTPIS)
  - Digital Reactor Protection System (DRPS) which is a replacement of the existing HO-1 and SOB
  - Diesel Load Sequencer (ELS) which is a replacement of the existing APS system
  - Digital Reactor Limitation System (DRLS) which is a replacement of the existing HO 3, HO 4, and ROM systems
  - Control Rods Control System (RRCS), which is a replacement of the existing PNČI system
  - a replacement of the existing reactor trip breakers
  - Reactor Control System (RCS) which is a replacement of the existing ARM system
  - Support Actions System (SAS) which is a replacement of the existing TOPG system plus the non-trained part of the existing SOB, i.e. SOB-N.
- Design, manufacture, installation, and documentation of the replacement of the module M2 which consists of:
  - Steam Generator Protection System (SGPS) which is a replacement of the existing LOPG system
  - In-core instrumentation system (IN-CORE) which is a replacement of the data acquisition and processing portion of the existing KVRK system
  - Unit computerized information system (PCS) which is a replacement of the existing IVS-URAN system.
- Design, manufacture, installation, and documentation of a Post Accident Monitoring System (PAMS), which is an entirely new system. The scope includes all data acquisition and data processing equipment, any necessary new measurement circuits, and MMI equipment. This system is included in module M1.
- For module M1, replacement of:
  - Sensors associated with the upgraded systems including installation of new cables when required

  - Installation of all the other equipment that is needed for the new systems to function such as transducers, power supplies, etc.

- The module M2 systems will use the existing field instrumentation (measurement circuits).
- Interconnecting of all the new systems, connections to new cabling and to existing plant equipment. This includes temporary connections required because of step-by-step implementation of the Project during three or four refueling outages.
- Construction modifications in the main and emergency control rooms due to removal of the old I&C equipment and installation of new equipment.
- Local construction modifications to accommodate the replacement of old I&C equipment with new equipment and the installation of new cables.
- Modification of the existing full-scope unit simulator so that it reflects the main control room of unit 2 after completion of the I&C refurbishment project for this unit.

A prime contractor and several sub-contractors are involved in the refurbishment project. The prime contractor is ŠKODA JS a.s., located in Plzen, Czech Republic. ŠKODA JS is responsible for overall management of the project and it oversees the activities of the subcontractors.
FRAMATOME and SCHNEIDER have formed a consortium and share the responsibility for various portions of the supply of the module M1 systems.
The various sub-contractors that provide essential services or equipment for the replacement are:

- FRAMATOME ANP, France. FRAMATOME has overall responsibility for all activities needed to implement the module M1 systems including documentation, design, manufacturing, and participation in installation and commissioning, and personnel training.
- SCHNEIDER ELECTRIC, France. SCHNEIDER is responsible for the documentation, design, manufacture, and test of the DRPS, DTPIS, DNIS, DRLS, RCS, SAS, and ELS systems, plus the reactor trip breakers.
- CERME, France. CERME, as a sub-contractor to FRAMATOME, is responsible for the development of the PAMS system software, and for the manufacture and test of the PAMS.
- ŠKODA ENERGO s.r.o., Controls Division, Plzen, Czech Republic. ŠKODA ENERGO is responsible for the design, documentation, manufacturing, and installation of the RRCS system of Module M1.
- ZAT a.s., Příbram, Czech Republic. ZAT is responsible for the design, documentation, manufacturing, and installation of the module M2 systems, which are the IN-CORE, SGPS, and PCS systems. The in-core upgrade is the data processing portion only. The in-core instruments (thermocouples and neutron detectors) will not be replaced.
- IFE Halden, Norway. IFE was a direct contractor to ČEZ for the supply of the core monitoring software (SCORPIO – VVER), which was developed under an OECD sponsored project.
- I&C ENERGO a.s., Třebíč, Czech Republic. I&C ENERGO is responsible for the design, documentation and supply of the field instrumentation of the replacement systems. Regarding the implementation of the core monitoring system SCORPIO I&C was the prime contractor for the design and installation of the interfaces to the existing HINDUKŠ data acquisition subsystem and for the design and installation of the SCORPIO hardware.

- ORGREZ SC a. s., Brno, Czech Republic. ORGREZ, a direct contractor to ČEZ, is responsible for the development and verification of algorithms used in the existing I&C systems and for verifying the algorithms used in the innovative I&C systems.
- MEACONT PRAHA s.r.o., Praha, Czech Republic. MEACONT is a sub-contractor to ŠKODA JS and is responsible for developing and coordinating the basic design documentation for the whole Project. The basic design covers the interfaces and interconnections between the various systems and between the systems and the plant equipment.

All of the suppliers must provide support for training and for commissioning of the equipment they are responsible for.

The relationship between the various contractors and subcontractors is shown in Figure 1. The architecture of the refurbished module M1 systems, based on the use of the SPINLINE 3 platform, as designed during the basic design phase of the project is shown in Figure 2.

3. Licensing process applied to the refurbishment of the NPP Dukovany I&C systems important to safety

As per the provisions of the Atomic Act, reconstruction or implementation of other changes in nuclear facilities that affect nuclear safety, radiation protection, emergency preparedness and security falls into the category of activities for which a permission (license) must be granted by the Czech Republic regulatory authority, i.e., the State Office for Nuclear Safety (SUJB). The Act also outlines the contents of the documentation that must be submitted to the SUJB in support of the application for such a license. The documentation shall include the following information:

- description and justification of the planned reconstruction or other changes
- updating of the documentation that was approved by the regulatory authority during the nuclear facility commissioning and operation
- time schedules for implementation of the planned reconstruction or other changes
- evidence that the reconstruction or other changes will not negatively affect nuclear safety, radiation protection, emergency preparedness and security of the nuclear facility.

Documentation quoted in the second bullet has to be approved by the SUJB. It includes, among others, the limits and conditions of safe operation (plant technical specifications – Tech Specs) and the list of the so-called Selected Equipment as stipulated by the SUJB Regulation No.214/1997 Coll.

The “one-step” licensing process stipulated by the provisions of §9, (1), f) of the Atomic Act and commonly applied to the implementation of smaller scope reconstructions or other changes that affect nuclear safety, radiation protection, emergency preparedness and security of nuclear facilities, was felt to be not quite adequate for the NPP Dukovany large-scope several-stage I&C system refurbishment project. Therefore, a project specific licensing process has been conceived in several rounds of discussions between the plant operator and the regulatory authority. This process is copying to certain extent the licensing process applied to new nuclear power plant projects.

More specifically, the licensing process applied to the refurbishment of the NPP Dukovany I&C systems important to safety is structured to the following stages.

Stage 1

The objective of this stage is to obtain the regulatory authority position on the concept of the refurbishment project based on the evaluation by SUJB of the general technical and implementation aspects of the project. This stage is broken down into two phases:

Phase 1A:
The safety case of this phase is based on the information generated by the conceptual design of the refurbishment. The following topics are addressed in the documentation submitted to SUJB for assessment:

- description and justification of the plant I&C system refurbishment project
- general specification of the plant I&C system after completion of the refurbishment project
- preliminary discussion of the plant Tech Specs changes
- draft attachment to the list of the Selected Equipment
- preliminary time schedules of the refurbishment project implementation
- evidence on meeting the applicable requirements for ensuring nuclear safety at the level of detail corresponding to the outputs from the conceptual design.

Phase 1B:
The safety case of this phase is based on the information generated by the next stage of the conceptual design that is referred to as the preliminary design. The topics addressed in the documentation submitted to SUJB for assessment are the same as those of the phase 1A but the level of detail reflects the evolvement of knowledge resulting from the next stage of the design. Main focus of the phase 1B safety case is on the conservative safety analyses results to support the intended implementation of some new and modified functions of the reactor trip system and the engineered safety features actuation system.

Both the conceptual design and the preliminary design as well as the safety case documentation were worked out by the Czech design company Energoprojekt and reviewed by the project team members and their consultants. Some outputs of these efforts were also used in preparation of the documentation that was passed on to the bidders for the refurbishment project implementation.

Stage 2

The objective of this stage is to obtain, as per the provisions of §9(1)f) of the Atomic Act, the permission (license) to implement the refurbishment of the plant I&C systems important to safety. The safety case of this stage is based on the results of the basic design of the refurbished I&C systems important to safety performed by the supplier contracted for the implementation of the project and by its subcontractors. The documentation submitted to the SUJB for licensing assessment consists of:

- a series of Topical Reports covering the following subject areas:
  - software life cycle planning (software development plan, software quality assurance plan, software verification and validation plan, software configuration management plan, software safety analysis plan)
  - equipment qualification (description of methodologies to be used in the environmental, seismic and electromagnetic compatibility qualification)
  - system reliability (description of methodologies to be used in qualitative and quantitative reliability analysis of the individual I&C systems and, at least, some preliminary results of these analyses)
  - design of the individual I&C systems

- amendment to the existing Final Safety Analysis Report (evidence that the applicable requirements of the design for safety have been met is provided here at the level of knowledge reflecting the results of the basic design to document that the refurbishment will not impair the nuclear safety of the plant)
- draft update of the limits and conditions of the plant safe operation
- draft attachment to the list of the Selected Equipment
- time schedules of the project implementation.

Stage 3

This stage is also broken down into two phases.

Phase 3A:
The objective of this phase is to obtain the regulatory authority position on the implementation aspects of the refurbishment project in each individual unit of the plant. The safety case will be a kind of an update of the stage 2 safety case based on the results of the detail design of the refurbished I&C systems for each unit. It will also include plans for installation, testing, and commissioning of the refurbished I&C systems during individual implementation phases of the project at the subject plant unit. Positive position will provide the plant operator with a sound basis for giving its consent to the commencement of manufacturing of the I&C equipment by the suppliers.

Phase 3B:
This phase is aimed at obtaining the regulatory authority consent to the implementation of a specific part of the refurbishment, which is to be accomplished during a particular planned outage of the subject unit for refueling. Hence, it will be repeated as many times as is the number of outages necessary for the completion of the refurbishment at this unit. The safety case will again be a kind of an update of the previous phase safety case, i.e. either of the 3A phase or 3B phase safety case, and will in addition include:

- description of the initial and final state of the unit I&C system with respect to the actual phase of the refurbishment implementation
- installation, testing and commissioning plans specific to the actual implementation phase
- updates of the Tech Specs and of the list of the Selected Equipment specific to the actual implementation phase
- reports on the results of the equipment qualification and system verification and validation activities performed at the manufacturer on the systems to be implemented during the actual implementation phase
- evaluation of the quality assurance plan fulfillment during manufacturing of the equipment to be implemented during the actual implementation phase.

Stage 4

The objective of this stage is to obtain the SUJB permission for the reactor start-up after refueling as per the provisions of §9(1)e) of the Atomic Act, which at the same time will include the SUJB consent to the operation of the refurbished I&C systems important to safety implemented during the current implementation phase. Hence, this phase will also be repeated as many times as is the number of outages necessary for the completion of the refurbishment at the subject plant unit. The safety case will again be a kind of an update of the preceding phase 3B safety case, and will in addition include:

- description of the actual state of the plant I&C system after completion of the current implementation phase
- evidence of the equipment and personnel readiness for operation (this will include the evaluation of the refurbished I&C system installation and pre-operational tests)

- update of the Tech Specs (if necessary).

After the completion of the last refurbishment implementation phase at a particular unit, the outcome of the stage 4 of the licensing process will be the SUJB permission for permanent operation of the unit refurbished I&C systems important to safety.

The safety case documentation providing evidence that the applicable requirements of the design for safety have been met in the design and implementation of the refurbished I&C systems important to safety will have the format and contents as per the US NRC Regulatory Guide 1.70 and Chapter 7 of the US NRC Standard Review Plan (year 1997 issue).

Present status of the licensing process is as follows: Stage 1A of the I&C system refurbishment project licensing process was completed at the end of 1999. Safety case of the stage 1B was submitted to the SUJB in May 2000. Its assessment has been completed without any significant negative findings. The safety case of the stage 2 of the licensing process was submitted to SUJB in May 2001. Its regulatory evaluation is now nearing completion.

4. Project specific regulatory requirements relating to the digital computer-based I&C safety systems

Czech Republic legislation which governs the safety aspects of siting, design, construction, commissioning, operation and decommissioning of nuclear facilities can be viewed as structured into the following two-level hierarchy:

- the Atomic Act passed by the Parliament (Act No.18/1997 Coll.)
- a series of regulations issued by the State Office for Nuclear Safety (SUJB).

The provisions of the Atomic Act which specifically apply to the implementation of changes affecting nuclear safety, radiation protection, security and emergency preparedness of nuclear facilities, hence also to the refurbishment of the I&C systems important to safety, are those that:

- define the powers and responsibilities of the SUJB
- set forth general and specific conditions for performing activities associated with the uses of nuclear power
- cover handling of radioactive wastes
- define the contents of the documentation that has to be submitted to the SUJB as the documentation accompanying the nuclear facility operator's application for the permission (license) to implement changes affecting nuclear safety.

The lower-level legislation, which is most relevant to the I&C systems of nuclear facilities, is the following group of the SUJB regulations:

- regulation No. 195/1999 Coll. on the requirements for the assurance of nuclear safety, radiation protection and emergency preparedness in nuclear facilities
- regulation No. 214/1997 Coll. on quality assurance in activities relating to the uses of nuclear power and activities having a potential for causing irradiation and on specification of criteria for assignment of the Selected Equipment to safety classes
- regulation No. 106/1998 Coll. on the assurance of nuclear safety and radiation protection in commissioning and operation of nuclear facilities.

Regulation No. 195 sets requirements pertinent to the design of systems important to safety. These requirements are of rather general nature comparable e.g. to the US NRC General Design Criteria. The

provisions of this regulation which address the design for safety of the plant I&C systems provide functional and design requirements covering the following areas:

- defense-in-depth
- quality assurance
- protection against equipment failures
- fire protection
- protection against the effects of natural events
- protection against events caused by human being activities outside the nuclear facility
- plant instrumentation and control systems
- plant protection systems
- relations between the plant protection and instrumentation and control systems
- plant control points
- systems for tripping the reactor
- power supply systems.

Compliance with this regulation was focused upon in establishing the design basis and system requirements both for the innovated plant I&C system as a whole as well as for the I&C portions of the individual plant safety and safety-related systems. Design and implementation of the refurbished I&C systems important to safety will have to meet, in the first place, all the applicable requirements of this regulation.

Regulation No. 214 deals in detail with quality assurance aspects of the activities associated with siting, design, construction, commissioning, operation and decommissioning of nuclear facilities. It covers the following topics:

- implementation of the quality system
- quality system requirements
- requirements for quality assurance of the Selected Equipment as assigned to safety classes
- requirements pertinent to the scope of the quality assurance programs
- criteria for the assignment of the Selected Equipment to safety classes
- the format and contents of the list of the Selected Equipment.

The I&C refurbishment project overall quality assurance program was established in line with the requirements of this regulation pertinent to such entities as processes, activities, products, organizations, personnel, and their combinations. More specifically, the provisions of the article 23 of this regulation which apply to the so-called “special processes”, i.e. processes the results of which cannot be fully verified through checking and testing, have been used as a regulatory basis for setting requirements to be met by the software development process of the safety critical software to be implemented in the refurbished I&C systems built on programmable digital platforms. Quality systems of all the contractors participating in the refurbishment of the I&C systems important to safety will have to be compliant with the applicable provisions of this regulation.

Regulation No. 106 addresses those aspects of safety assurance, which are relevant to the commissioning and operation of nuclear facilities including start-up of nuclear power plants after refueling. It specifies:

- general requirements for the commissioning and operation of nuclear facilities
- technical and organizational conditions of safe commissioning of nuclear facilities which cover, in particular:
  - the specification of the individual phases of the nuclear facility commissioning
  - the specification of documentation to be submitted to the regulatory authority for evaluation in the process of issuing permissions to begin and proceed through the individual phases of the commissioning

- limits and conditions of the nuclear facility safe operation (technical specifications)

♦ technical and organizational conditions of safe operation of nuclear facilities

♦ requirements to be met when reaching reactor criticality after refueling.

Conformance to the applicable provisions of this regulation will be the subject of those I&C refurbishment project activities that relate to updating of the existing plant technical specifications and operational procedures during and after completion of the innovated I&C systems implementation, and to testing of the installed new I&C systems prior to the plant start-up after completion of the individual stages of the I&C system refurbishment.

It is obvious that the design, implementation and operation of the refurbished I&C systems important to safety must meet all the applicable requirements of the above discussed legislation. Being aware of the importance of the licensing process to the success of the project the NPP Dukovany I&C refurbishment project team has been in close touch with the relevant SUJB staff members from the early stages of the project preparation to brief and discuss with them all the applicable safety issues. These efforts resulted in laying down by the regulatory authority, in some areas of concern, project specific requirements with respect to the scope of the refurbishment and the design of the I&C systems important to safety.

A summary of the SUJB project specific requirements is presented in the sequel.

Scope of the refurbishment project

Refurbishment of the following I&C systems shall be implemented:

♦ reactor protection system

♦ engineered safety features actuation system

♦ emergency load sequencer

♦ reactor limitation system.

Common requirements

Common requirements for the reactor protection system, engineered safety features actuation system and emergency load sequencer on one side, and for the reactor limitation system on the other side have been set forth in the following areas:

♦ ensurance of functionality

♦ ensurance of reliability

♦ ensurance of performance

♦ ensurance of equipment qualification

♦ ensurance of quality.

Classification of the I&C systems important to safety

Safety classification of the I&C systems important to safety shall be performed on the basis of deterministic criteria in compliance with the guidance given in the IEC Std. 61226, i.e. assignment of the I&C functions and the associated systems and equipment to the following categories: category A, category B, and category C.

Acceptability of the digital computer-based I&C systems important to safety

Implementation of the refurbished I&C systems important to safety using software-based digital computer technology is acceptable provided that:

- the design, manufacturing, installation, testing, commissioning and operation of those systems will meet all the applicable provisions of the Czech legislation
- those systems will meet all the requirements stated in the SUJB resolution No. 79/1999
- those systems will meet, to the extent reasonably achievable, the requirements and recommendations of the applicable IAEA documents, IEC standards, national industrial standards such as the CSN and IEEE standards, and the US NRC General Design Criteria and Regulatory Guides.

In addition to this, a number of project specific requirements have been set fourth. Those of them, which apply to digital computer-based I&C systems are summarized below.

Software development process for the I&C systems important to safety

Software development process for category A I&C functions shall be a well-structured process consisting of the following activity groups:

- planning activities
- development activities, i.e. requirements activities, design activities, implementation activities, validation activities, and installation activities
- integral activities, i.e. verification activities, configuration management activities, and safety analysis activities.
-

Software development processes for category B I&C functions shall be basically the same as the one for category A functions.

Software development process for category C I&C functions shall be the same as that for high quality industrial I&C applications.

Verification and validation of the software for the I&C safety systems

For the software implementing category A I&C functions the following shall apply:

- V&V activities compliant with the requirements of the IEC Std. 880 and NRC RG 1.152 shall be performed during the software development process as well as during the consecutive life-cycle phases
- no third party independent V&V activities are required provided that the software V&V team at the manufacturer is management and financial independent of the development team
- audits of the software development process shall be performed right from the start-up of this process.

Defense against common cause failures (CCF) in the software of safety systems

With respect to the postulation of CCF the following shall apply:

- CCFs will not need to be postulated in safety system hardware including the sensors
- CCFs will have to be postulated in complex software implementing safety functions
- CCFs will not need to be postulated in simple software modules participating in implementation of safety functions provided that:
  - these software modules can be fully tested, or
  - extensive positive operational experience from previous applications in similar safety applications is available and well documented
- CCFs will not need to be postulated in software modules implementing support functions such as e.g. software for on-line diagnostics provided that it can be proved that errors in this software cannot degrade performance of the safety functions.

Implementation of diverse means of protection against the postulated CCFs:

- is required with respect to the ANSI Condition II and III plant design basis events (postulated initiating events) with the estimated frequency of occurrence greater than 10E-3 per year
- is not required for less frequent plant design basis events, i.e. for some ANSI Condition III events and all ANSI Condition IV events.

The following relaxed acceptance criteria can be applied in the accident analysis of the safety actions initiated by the diverse means of protection:

- maintenance of coolable core geometry
- maintenance of the primary coolant system integrity
- maintenance of the hermetic zone integrity
- availability of sufficient time (not less than 30 minutes) for taking manual safety actions as the diverse means of protection.

The following two approaches in diversity implementation will be viewed as adequate:

- functional diversity implemented in two functionally isolated subsystems of a safety system which process two different groups of input signals, or
- implementation of a separate diverse protection system which features functional isolation of the primary protection system, different hardware and different software.

Adequacy of the diversity implementation shall be supported by analysis.

Communications between subsystems of the digital computer-based I&C safety systems

Requirements set forth on the communications between subsystems of the I&C safety systems are as follows:

- no failure in a subsystem of a safety system division shall affect the performance of safety functions in the redundant divisions of this system
- sharing of data among the redundant divisions of a safety system, including sharing of input signals, shall not degrade the functional isolation of those divisions
- loss of communication between redundant divisions shall not cause interruption of the division activities
- all communication links shall be checked by on-line diagnostics
- the fail-safe design principle shall be applied where practically achievable to provide for pre-defined response of the safety system to the loss or degradation of the communications.

Testability of the digital computer-based I&C safety systems during reactor operation

The SUJB position on testability during operation has been stated as follows:

- the on-line diagnostics shall perform three functions:
  - upon system start-up and re-starts it shall check the status and the correctness of hardware functioning and the configuration of the installed software
  - during system operation it shall check sequentially in each code execution cycle the status and correctness of hardware functioning in such a way that the full-scope checking be completed in about 10 minutes

  - during system operation checking of the communications based on the diagnostic information contained in the messages transmitted over the communication links and supported to the maximum possible extent by implementation of deadman timers which indicate interrupts in the communications
- periodic surveillance testing shall provide for:
  - testing of the hardware of the system equipment involved in information processing portions of the safety functions and in on-line diagnostic functions that is not tested to the full extent by the system on-line diagnostics
  - if there are no hardware components tested completely by the system on-line diagnostics then the periodic surveillance testing need not to be implemented
- the provisions of §18 section (1) of the SUJB regulation No.195/1999 Coll. must be met during system testing, i.e. the single failure criterion and the minimum redundancy requirement.

Compliance to the single failure criterion

The requirement for compliance of the I&C safety systems with the single failure criterion is stated from two perspectives:

- what concerns the type of single failures, the effects of the plant design basis events on the safety systems, and the impacts of a single failure occurrence the provisions of the IEEE Std. 379 are required to be met
- what concerns the impacts of a single failure occurrence the provisions of the §18 section (1b) of the SUJB regulation No. 195/1999 Coll. are also invoked to comply with the minimum redundancy requirement.

Exemptions from the conformance to the single failure criterion under extraordinary situations could be considered by the regulatory authority on a case-by-case basis; this, however, does not apply to regularly occurring situations such as periodic surveillance testing. Separate diverse protection systems if implemented within the I&C system refurbishment project are not required to meet the single failure criterion.

Equipment qualification

The regulatory authority requires that an equipment qualification program be established for the refurbished I&C systems important to safety encompassing the following activities:

- program preparation
- equipment qualification implementation
- maintenance of the equipment qualification.

Program preparation activities should include specification of:

- the equipment to be qualified
- the functions to be performed by this equipment and the time interval during which the functions are required
- the equipment location in the plant
- the environmental and operational conditions of the equipment
- methods and procedures for performing the qualification.

Equipment qualification implementation activities should include one or a combination of the following:

- qualification by type testing as the preferred qualification method
- qualification by analysis
- qualification based on operational experience.

Qualification maintenance activities should include:

- preventive maintenance
- procurement and stock of spares
- monitoring of the environmental and operational conditions
- tracing of failures
- personnel training.

Acceptance of qualification certificates will be governed by the applicable provisions of the Act No.22/1997 Coll.

Reliability

The regulatory authority requires that:

- numerical values of the quantitative reliability indicators be established for the individual I&C systems important to safety
- in setting those values for the safety systems the plant safety goal represented by the calculated core melt frequency of 10E-4/year shall be considered; for the other systems those values should be derived from operational considerations
- as a minimum set of the reliability indicators the instantaneous or average system availability and the frequency of spurious initiations shall be used
- qualitative reliability analyses shall be performed for all safety category A and B I&C systems employing the FMEA methodology or its FBA version for the digital computer-based systems
- quantitative reliability analyses shall be performed for all I&C systems important to safety using the FTA method; in these analyses the potential for CCF and human errors shall be considered, as appropriate.

Documentation

The project specific regulatory requirements include also specification of documentation that is to be submitted for licensing evaluation in addition to the amendment to the existing plant Final Safety Analysis Report, such as a series of Topical Reports addressing specific safety issues.

The above quoted project specific requirements have been derived from the applicable provisions of:

- the Czech Republic legislation
- the IAEA Safety Series documents and Technical Reports
- the IEC standards
- the US NRC Regulatory Guides and NUREGs
- national standards such as IEEE and CSN standards.

The results of the EU project OJC 316 “Licensing-Related Assessment of Digital Computer Based Technology for I&C Important to Safety”, which is aimed at transferring of the licensing methodologies employed in the EU member states to the countries wishing to join the EU, have also been considered in setting those requirements.

5. Planning and conducting audits of the design and manufacturing processes

Many of the to be implemented digital computer-based I&C systems are essential to continued safe operation of the plant, so it is imperative that the suppliers design, manufacture, and install the equipment in conformance to their Quality Assurance (QA) programs, applicable national and international QA requirements, and any additional requirements intended to assure continued safe, efficient, and reliable plant operation.

CEZ intends to perform various audits to assure compliance with the applicable requirements, assure that the installed equipment will operate as intended, and to provide information needed to support the SUJB licensing activities. An Audits Plan has been developed to provide a basis for those activities.

The following were considered in the preparation of this Plan:

- the range and scope of the audits should provide CEZ with objective proof that the supplier processes meet the project quality requirements and SUJB requirements
- the requirements against which compliance is to be verified by the audits should be specified including identification of their sources in the form of references
- the Plan should specify the purpose and timing of the audits.

The objectives of the audits to be conducted during the NPP Dukovany I&C refurbishment project have been defined as follows:

- to support confidence that the hardware and software development processes of the refurbished I&C systems important to safety have been adequately planned for

- to support confidence that the design and manufacturing of the hardware and software of those systems, including the verification and validation activities as well as the configuration management activities, are being performed to the plans.

The following audit types will be conducted to this end:

Audit Type A, Design Requirements.

This audit will be performed only once (prior to the first outage for unit 3) at Framatome/Schneider, SKODA/MEACONT, SKODA ENERGO, and ZAT since they are preparing design requirements.

Audit Type B, Hardware and Software Design.

This audit will be performed prior to each outage for each vendor that is supplying detailed design documentation and equipment for the upcoming outage.

Audit Type C, Manufacturing and Test.

This audit will be performed prior to each outage for each vendor that is supplying equipment for the upcoming outage.

Audit Type B/C, Hardware Design plus Manufacturing and Test.

This audit will be performed at I&C Energo prior to selected outages.

Audit Type D, Algorithm Development.

This audit will be performed only once (prior to the first outage for unit 3) at ORGREZ SC.

The new I&C systems have been assigned classifications in accordance with IEC standard No. 61226. The selection of standards to be used as the basis for the audits follows this classification and addresses all of the important issues at a level of detail that is suitable for conducting the audits and for addressing the applicable SUJB requirements. Hence:

- the software development process for IEC 61226 category A systems (SUJB safety class 2) will be audited for compliance to IEC 60880 and 60880-2; the software development process for IEC 61226 category B and C systems (SUJB safety class 3) will be audited for compliance to ISO 9000-3 and ISO/IEC 12207
- the hardware development process for IEC 61226 category A systems (SUJB safety class 2) will be audited for compliance to IEC 60987. The hardware development process for IEC 61226 category B and C systems (SUJB safety class 3) will be audited for compliance to ISO 9001
- the audits will also address configuration management issues because of the importance of assuring compatibility between the efforts of the several vendors involved in the project. ISO 10007 will be used as the basis for the configuration management auditing.

While performing the audits, US NRC BTP HICB-14 may also be used to provide additional guidance for evaluating the application of the above mentioned IEC standards.

A set of checklists has been has been developed for the following audit groups:

- *Design Requirements Audit.* The standards references in this group include sections that:
  - directly relate to developing the design requirements
  - relate to activities that need to be performed to develop the requirements such as verification, documentation, modifications, etc.
  - relate to items that need to be addressed in the requirements such as CCF, MMI, test requirements, etc.
  - relate to activities that need to be in place prior to start of the hardware and software design such as engineering tools, plans, etc.
- *Hardware/Software Design Audit.* The standards references in this group include sections that:
  - directly relate to performing the design
  - relate to activities that need to be performed to support the design such as verification, documentation, modifications, etc.
  - relate to items that need to be addressed in the design such as integration, validation, operation, etc.
- *Manufacture and Test Audit.* The standards references in this group include sections that:
  - directly relate to performing the manufacturing and factory test
  - relate to activities that need to be performed to support manufacturing and test such as error reporting, control of instruments, documentation, etc.
- *Special Requirements Audit.* The standards references in this group includes sections that:
  - relate to the configuration management issues
  - apply to the preparation and validation of the algorithms for the individual systems.

The Dukovany I&C refurbishment project involves several suppliers with various responsibilities and scopes. Therefore the audits will also consider issues that need to be addressed to ensure adequate co-ordination between the suppliers such as to whether:

- the interfaces between the equipment from the various suppliers are well defined, consistent, and provided to all involved suppliers
- the overall response of the systems adequately consider the cumulative response of equipment from the various suppliers
- the terminology used by the various vendors is consistent and conforms to CEZ's terminology
- installation requirements and restrictions that are placed by equipment supplied by one vendor are defined and provided to other impacted suppliers and to the installer.

6. Conclusions

The first audit in the series of audits to be conducted during the NPP Dukovany I&C module M1 and module M2 systems refurbishment project implementation was performed at Framatome ANP and Schneider Electric companies at the end of June and beginning of July 2001; it took 8 working days. The audit program was to evaluate the preparation of the system requirements, configuration management plans, software requirements and hardware requirements. The audit was performed in accordance with the following three checklists:

- checklist for system requirements preparation per ISO 9000-3 and configuration management per ISO 10007
- checklist for software requirements preparation per IEC 60880 and 60880-2
- checklist for hardware requirements preparation per IEC 60987.

The audit team was composed of four members: two of them, including the audit team leader, were the NPP Dukovany I&C refurbishment project staff members, the other two were I&C consultants of the Scientech, Inc. company. A nuclear safety inspector of the SUJB and two staff members of the prime contractor, i.e. SKODA JS, participated in the audit as observers.

References

1. SUJB position with respect to selected aspects of the NPP Dukovany I&C refurbishment project; Prague, September 2000.

2. Quality assurance program for the I&C refurbishment project; CEZ-NPP Dukovany, October 2000.

3. Safety case of the NPP Dukovany I&C refurbishment project for the stage 2 of the licensing process; CEZ-NPP Dukovany, May 2001.

4. Plan for auditing the design and manufacturing process implemented for the NPP Dukovany I&C Innovation Project; Scientech, Inc.-organizational component in the Czech Republic, June 2001.

5. Implementation of new digital safety systems on NPP Dukovany; WANO-Paris Center workshop on computer based I&C systems: Necessity for continuous improvement; Beznau NPP, Switzerland, August 2001.

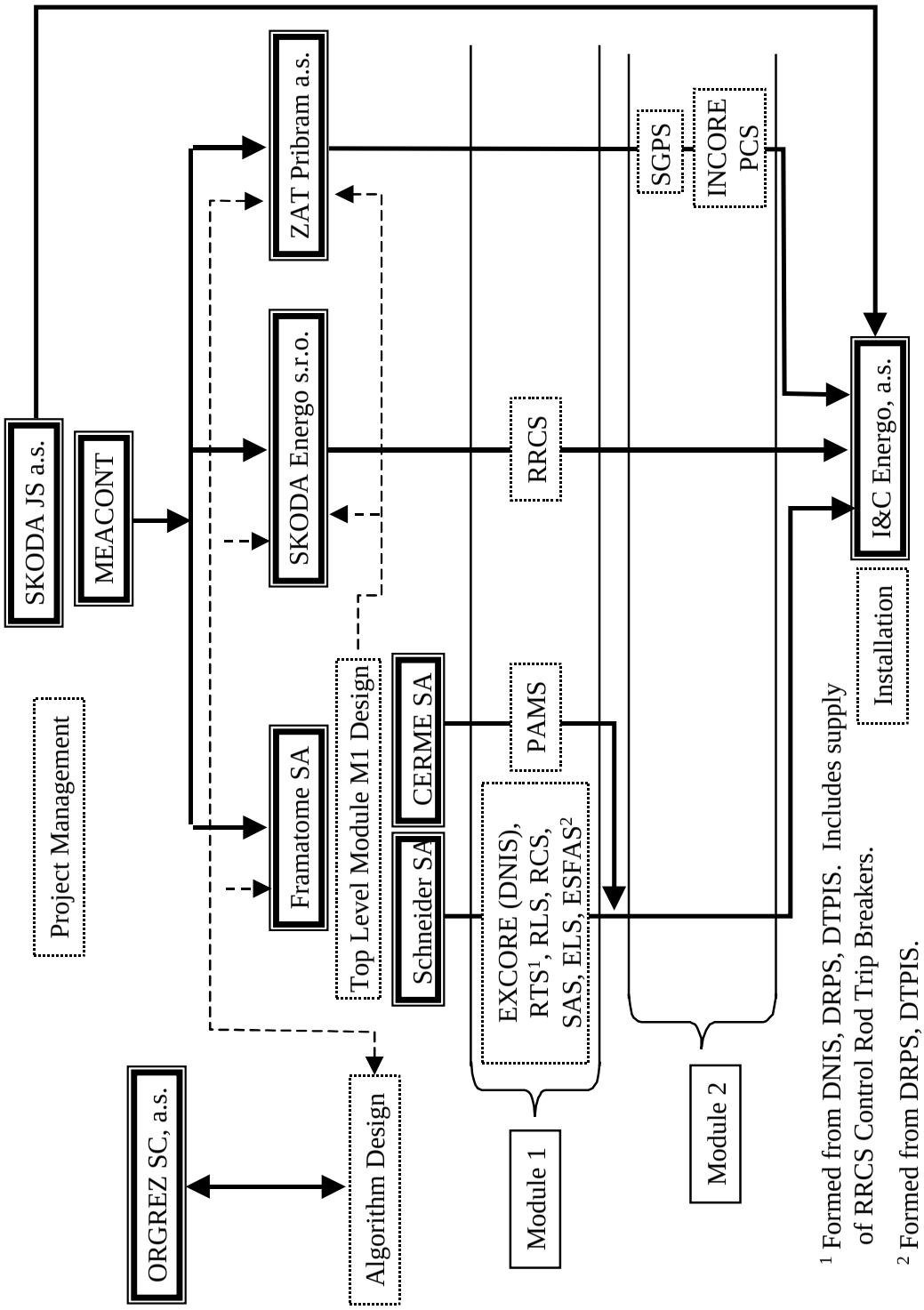


Figure 1. Relationship between suppliers

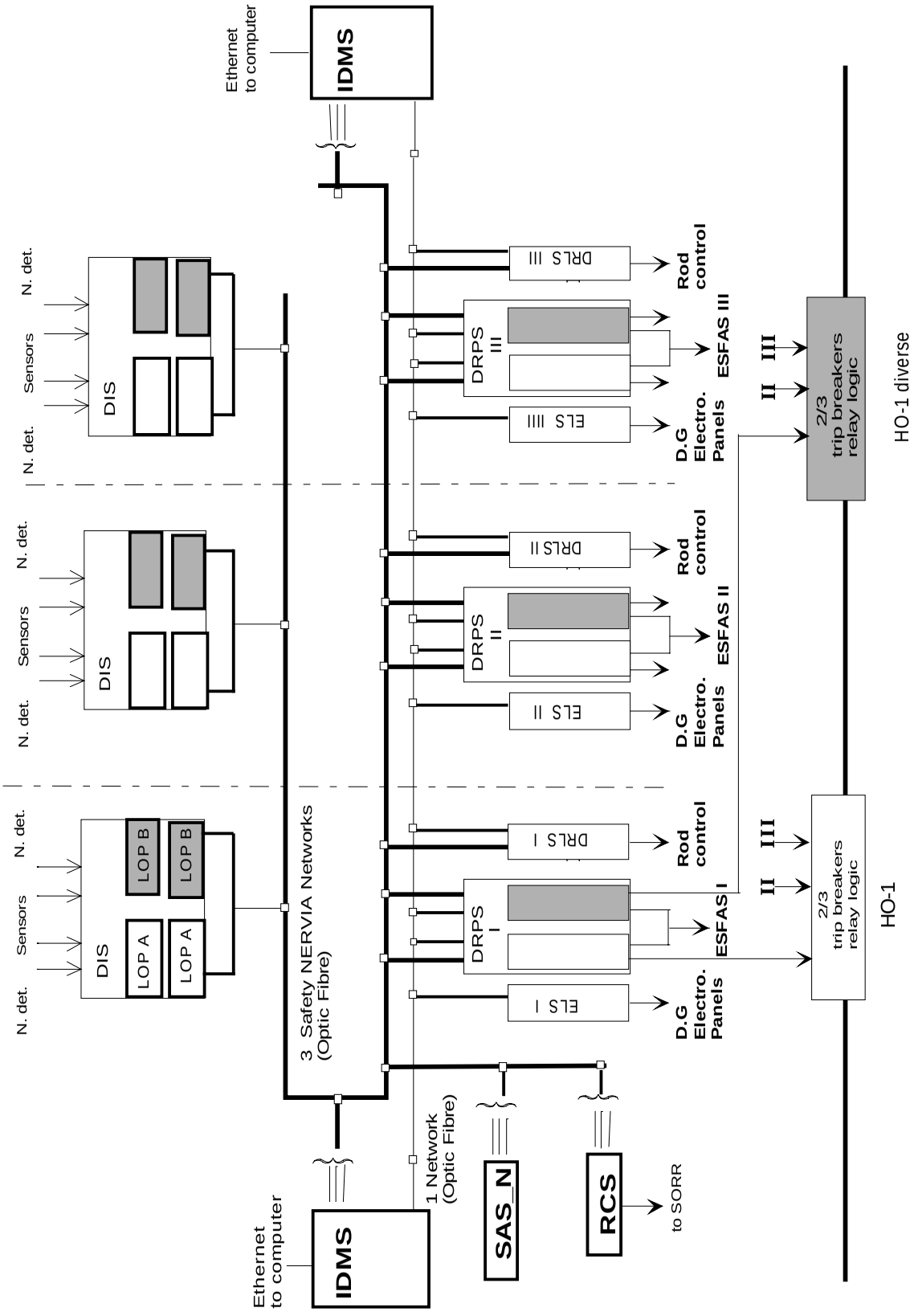


Figure 2. Architecture of the module M1 I&C refurbished systems

E. LIST OF PARTICIPANTS

♠ - visit of NPP Temelin

BELGIUM

COURTOIS, Pierre J.
Advanced Technologies Dept.
AIB-Vinçotte Nucleaire
Avenue du Roi, 157
B-1060 Brussels

Tel: +32 2 536 83 22
Fax: +32 2 536 85 85
Eml: courtois@info.ucl.ac.be

CHINESE TAIPEI

♠JEEN-YEE LEE,
Taiwan Power Company
20F, 242, Roosevelt Road
Sec. 3. Taipei, Taiwan

Tel.: +886 2 23667156
Fax: +886 2 23671675
Eml.: *D02705*@taipower.com.tw

♠SWU YIH,
Institute of Nuclear Energy Research
PO Box 3-11
Lung Tang, Taiwan

Tel: +3-4711400-6335
Fax: +3-4711400-6335
Eml: syih@iner.gov.tw

♠DER-JEH SHIEH
Institute of Nuclear Energy Research
PO Box 3-11
Lung Tang, Taiwan

Tel: 886-3-4711400-6300
Fax: 886-3-4711415
Eml: djshieh@iner.gov.tw

♠CHANG-FU CHUANG
Nuclear Regulation Division
Atomic Energy Council Taiwan
67, Lane 144, Keelung Rd., Sec. 4
Taipei, Taiwan 106

Tel.: +886 2 23634180, ext. 307
Fax.: +886 2 23635377
Eml.: chuang@aec.gov.tw

CZECH REPUBLIC

KRIZEK, Karel
Head of I&C Operation
NPP Temelin
CEZ, A.S.
373 05 Temelin

Tel: +420 334 422 223
Fax: +420 334 422 3815
Eml: Krizek_Karel/4430/ETE/CEZ@.mail.cez.cz

KRS, Petr
State Office for Nuclear Safety
Senovazné Square, 9
110 00 Prague 1
Tel: +420 2 216 24 206
Fax: +420 2 216 24 396
Eml: petr.krs@sujb.cz

PETRUZELA Ivan
I&C Energo s.r.o.
Areál VÚ
190 16 Praha 9 - Bechovice
Tel.: +420 2 6706 2181
Fax: +420 2 6706 2182
Eml.: ipetruzela@ic-energo.cz

BEDNARIK Karel
I&C Energo s.r.o.
Areál VÚ
190 16 Praha 9 - Bechovice
Tel.: +420 2 6706 2185
Fax: +420 2 6706 2182
Eml.: *kbednarik@ic-energo.cz*

PIROUTEK Zdenek
I & C Energo s.r.o.
190 11 Praha 9 – Bechovice
Tel.: +420 2 67062182
Fax: +420 2 67062182
Eml.: zpiroutek@ic-energo.cz

ROUBAL S
I & C Energo s.r.o.
190 11 Praha 9 – Bechovice
Tel.: +420 2 67062182
Fax: +420 2 67062182
Eml.: sroubal@ic-energo.cz

RUBEK J.
I & C Energo s.r.o.
190 11 Praha 9 – Bechovice
Tel.: +420 2 67062183
Fax: +420 2 67062182
Eml.: jrubek@ic-energo.cz

ZAVODSKY Petr
CEZ, a. s.
Division of Construction
NPP Temelín
Tel: +420 334 78 2151
Fax: +420 334 78 3815
Eml: Zavodsky_Petr@mail.cez.cz

PLISKA Petr
I & C Energo s.r.o.
Prazska 684
67401 Trebíc
Tel.: + 420 618 893 300
Fax: + 420 618 893 999
Eml.: jpliska@ic-energo.cz

WAAGE Herbert
CEZ, a. s.
Division of Construction
NPP Temelín
Tel: +420 334 78 3560
Fax: +420 334 78 3815
Eml: waage_herbert@mail.cez.cz

CENDELÍN J.
West Bohemian University in Pilsen
Faculty of Applied Sciences
Department of Cybernetics
Univerzitní 22,
30614 PLZEN
Tel.: + 420 19 7491 155
Fax: + 420 19 279 050
Eml: cendelin@kky.zcu.cz

♠KRYL Petr
Orlík 266
Nuclear Engineering SKODA
316 06 Plzen
Tel.: +420 19 704 2825
Fax: +420 19 75 20 600
Eml.: pkryl@jad.in.skoda.cz

ZATLOUKAL Jan
Nuclear Researh Institute Rez a.s.
250 68 Rez
Tel.: +420 19 7441099
Fax: +420 19 7441097
Eml.: zat@ujv.cz

KRÁKORA Petr
Nuclear Researh Institute Rez a.s.
250 68 Rez
Tel.: +420 19 7441098
Fax: +420 19 7441097
Eml.: krakora@ujv.cz

KUBÍNOVÁ Jana
Schneider Electric CZ, s.r.o.
Thámová 13
186 00 Praha 8
Tel.: +420 2 810 88 634
Fax : +420 2 248 10 849
Eml.: jana_kubinova@cz.schneider- electric.com

♠ KARPETA Ceslav
Scientech, inc. - CR
A. Staška 30
146 00 Praha 4
Tel.: +420 2 22 13 53 38
Fax : +420 2 22 13 53 37
Eml.: scikar@mbox.vol.cz

KUBANOVÁ Iva
I&C Energo a.s.
Husova 17
370 05 Ceské Budejovice
Tel.: +420 38 510 23 11
Fax : +420 38 534 49 17
Eml.: ikubanova@ic-energo.cz

FINLAND

♠REIMAN Lasse
STUK
P.O.Box 14
FIN-00081 Helsinki
Tel.: +358 9 7598 8379
Fax : +358 9 7598 8382
Eml: lasse.reiman@stuk.fi

♠JÄRVINEN, Marja-Leena
Finnish Centre for Radiation
and Nuclear Safety (STUK)
P.O. Box 14
FIN-00881 Helsinki
Tel: +358 (9) 759 88 304
Fax: +358 (9) 759 88 382
Eml: marja-leena.jarvinen@stuk.fi

♠LINDEN Ulf
Fortum power and Heat Oy
Loviisaa Power Plant
P.O. Box 23
07901 Loviisa
Tel.: +358 10 45 53800
Fax:
Eml.:ulf.linden@fortum.com

FRANCE

♠BOUARD, Jean-Paul
Division Contrôle Commande
E.D.F. - SEPTEN
12-14, avenue Dutriévoz
F-69628 Villeurbanne Cedex
Tel: +330472 82 71 66
Fax: +330472 82 77 04
Eml: jean-paul.bouard@edfgdf.fr

SOUBIES, Brigitte
IPSN/DES/SAMS
Centre d'Etudes Nucleaires
60-68 ave General Leclerc
Batiment 08, BP 6
92265 Fontenay-aux-Roses CEDE
Tel: +33 1 46 54 84 06
Fax: +33 1 47 46 10 14
Eml: brigitte.soubies@ipsn.fr

♠POIZAT Francois,
EDF Industry/Basic Design Department,
12-14 avenue Dutrievoz,
69628 Villeurbanne Cedex
Tel.: +33 4 72 827 479
Fax: +33 4 72 82 77 04
Eml.: francois.poizat@edf.fr

♠ESMENJAUD Claude
Schneider Electric Industries M3
38050F Grenoble
schneider.fr
Tel.: +33 476 605 860
Fax: +33 476 606 462
Eml.:claude_esmenjaud@mail.

BUREL Jean-Pierre
Schneider Electric Industries M3
Safety Electronics and Systems, Usine M3
23 Chemin du Vieux Chene
F-38240 Meylan
Tel.: +33 476 606 884
Fax: +33 476 606 992
Eml.:jean-pierre_burel@mail.schneider.fr

MOSIO Bernard
Nuclear International Project Manager
Schneider Electric Industries M3 plant
23 Chemin du Vieux Chene
F-38240 Meylan
F-38050 Grenoble cedex 9
Tel.: +33 476 60 55 90
Fax: +33 476 60 63 52
Eml.:bernard_mosio@mail.schneider.fr

LAPASSAT Anne-Marie
DSIN/SD2
F92266 Fontenay-aux -Roses
Tel.: 33 1 43 19 71 03
Fax : 33 1 43 19 70 66
Eml: anne-marie.lapassat@industrie. gouv.fr

GERMANY

♠LINDNER, Arndt
Institute of Safety Technology (ISTec)
P.O. Box 1213
85 740 Garching
Tel: +49 89 32004 529
Fax: +49 89 32004 300
Eml: lia@grs.de

♠SCHNÜRER Günter
Institute of Safety Technology (ISTec)
P.O. Box 1213
85 740 Garching

Tel.: +49 89 32004 523
Fax: + 49 89 32004 300
Em.: sgu@ grs.de

♠KERSKEN Manfred
Institute of Safety Technology (ISTec)
P.O. Box 1213
85 740 Garching

Tel.: +49 89 32004 546
Fax: + 49 89 32004 300
Eml.: ker@ grs.de

♠SEIDEL Freddy
Federal Office for Radiation Protection (BfS)
P.O. Box 100149
D-38201 Salzgitter

Tel.: +49 5341 885 863
Fax: +49 5341 885 865
Eml.:fseidel@bfs.de

HUNGARY

HAMAR, Karoly
Nuclear Safety Inspectorate, I & C Sec.
Hungarian Atomic Energy Comm.
Nuclear Safety Inspectorate
P.O. Box 676
H-1539 BUDAPEST 114

Tel: +36 1356 5566-2221
Fax: +36 1355 1591
Eml: hamar@haea.gov.h

JAPAN

♠OGISO, Zen-ichi
Manager, Nuclear Power
Engineering Corp. (NUPEC)
Fujitakanko Toranomon Bldg.
17-1, 3-chome, Toranomon
Minato-ku, Tokyo 105

Tel: +81 3 3435 3427
Fax: +81 3 3435 3428
Eml: ogiso@nupec.or.jp

♠MAKINO Shigenori
Tokyo Electric Power Company
1-3 Uchisaiwai-cho
1-chome Chiyoda-ku
Tokyo 100-0011

Tel.: +81 3 3501 8111
Fax: +81 3 3596 8562
Eml.: Makino.S@tepco.co.jp

♠MITO Yoichi
The Kansai Electric Power Co. Inc.
Nuclear Power Division
3-3-22, Nakanoshima Kita-ku
OSAKA 530-8270

Tel.: +81-70-5938-2709
Fax: +81-6-6444-6279
Eml: K576277@kepco.co.jp

♠UTSUMI Utsumi,
Mitsubishi Heavy Industries Ltd
Nuclear Energy Systems Engineering Center
1-1-1, Wadasaki Hyogo-ku
KOBE 652-8585
Tel.: +81-78-672-3305
Fax: +81-78-672-3268
Eml: utsumi@atom.hq.mhi.co.jp

♠MIYAUCHI Katsumi
Design Section Nuclear Power Department
Hokkaido Electric Power Co.,Inc.
Higashi 1-Chome , Ohdori
Chuo-ku , Sapporo , 060-8677
Tel.: 81-11-251-1111
Fax: 81-11-218-5786
Eml: H1998088@epmail.hepco.co.jp

♠YAMAGISHI Hitoshi
Design Section Nuclear Power Department
Hokkaido Electric Power Co.,Inc.
Higashi 1-Chome , Ohdori
Chuo-ku , Sapporo , 060-8677
Tel.: 81-11-251-1111
Fax: 81-11-218-5786
Eml: hitoshi-y@epmail.hepco.co.jp

♠FUJII Sumio
Design Section Nuclear Power Department
Hokkaido Electric Power Co.,Inc.
Higashi 1-Chome , Ohdori
Chuo-ku , Sapporo , 060-8677
Tel.: 81-11-251-1111
Fax: 81-11-218-5786
Eml: s-fujii@epmail.hepco.co.jp

KOREA (REPUBLIC OF)

YUN H. CHUNG
Korea Institute Of Nuclear Safety
19 Guseong-Dong Yusung-Gu
Taejon, 305-338
Tel: +82 42 868 0245
Fax: +82 42 861 9945
Eml.:yhchung@kins.re.kr

D. I. KIM
Korea Institute Of Nuclear Safety
19 Guseong-Dong Yusung-Gu
Taejon, 305-338
Tel: +82 42 868 0246
Fax: +82 42 861 1700
Eml.: dikim@kins.re.kr

♠TAEYONG SUNG
Integrated Safety Assessment Team
Korea Atomic Energy Research Institute
P.O. Box 105 Yusung, Taejon, 305-600
Tel.: 82-42-868-8923
Fax : 82-42-868-8256
Eml.: tysung@kaeri.re.kr

SLOVAK REPUBLIC

♠SÚKENÍK Peter
Nuclear Power Plant Bohunice
919 31 Jaslovské Bohunice
Tel.:+421 33 597 2808
Fax:+421 33 597 4720
Eml.:sukenik_peter@ebo.seas.sk

♠BÁNOVCOVÁ Mária
Nuclear Power Plant Bohunice
919 31 Jaslovské Bohunice
Tel.:+421 33 597 2356
Fax:+421 33 597 4720
Eml.:banovcova_maria@ebo.seas.sk

♠LIBOSVAR Kamil
Nuclear Power Plant Bohunice
919 31 Jaslovské Bohunice
Tel.:+421 33 597 2356
Fax:+421 33 597 4720
Eml.:libosvar_kamil@ebo.seas.sk

♠ARBET Ladislav
Nuclear Power Plant Research Institute
Okru ná 5 Eml.:arbet@vuje.sk
918 46 Trnava
Tel.:+421 33 599 1726
Fax:+421 33 599 1153

♠GESE Augustín
Nuclear Power Plant Research Institute
Okru ná 5
918 46 Trnava
Tel.:+421 33 599 1105
Fax:+421 33 599 1153
Eml.:gese@vuje.sk

SLOVENIA

♠ Pecek Vladimir
Nuclear Regulatory Authority
Vojkova 59
1000 Ljubljana
Tel.: (+386) 1 472 11 42
Fax : (+386) 1 472 11 99
Eml: vladimir.pecek@gov.si

SWEDEN

LIWÅNG, Bo
Deputy Head
Dept. of Plant Safety Assessment
Swedish Nuclear Power Inspectorate
S-106 58 STOCKHOLM
Tel: +46 (0)8 698 84 92
Fax: +46 (0)8 661 90 86
Eml: bo.liwang@ski.se

♠ANDERSSON Jan-Ove
IoC, research and Development
Barsebäack Kraft AB
Box 524
SE-246 25 Löddeköpinge
Tel.: +44 46 72 41 48
Fax: +46 46 72 46 93
Eml.:jan-ove.andersson@ barsebackkraft.se

♠JONSSON Nils
Engineering department
Barsebäack Kraft AB
Box 524
SE-246 25 Löddeköpinge
Tel.: +44 46 72 40 00
Fax: +46 46 77 48 58
Eml.:nils.jonsson@barsebackkraft.se

♠ERIKSSON Karl-Erik
OKG Aktiebolag
Oskarsham NPP
SE-572 83 Oskarsham

Tel.: +46 491 78 76 82
Fax: +46 491 78 68 65
Eml.:karl-erik.eriksson@okg.synkraft.se

SWITZERLAND

REDDERSEN Hans-Georg
Colenco Power Engineering
Mellingerstrasse 207
CH-5405, Baden

Tel.: +41 56 483 1563
Fax: +41 56 493 7356
Eml.:hans-georg.reddersen@colenco.ch

UKRAINE

♠ YASTREBENETSKY Michael
State Scientific and Technical Center
on Nuclear and Radiation Safety
17 Artema str.
Kharkov 6100

Tel.: +38 0572 471 700
Fax: +38 0572 471 700
Eml.: rel@online.kharkiv.com

♠ KHARCHENKO V.
State Scientific and Technical Center
on Nuclear and Radiation Safety
17 Artema str.
Kharkov 6100

Tel.: +38 0572 471 700
Fax: +38 0572 471 700
Eml.: rel@online.kharkiv.com

UNITED STATES OF AMERICA

♠CHIRAMAL, Matthew
Senior Advisor for Digital Technology
Office of Nuclear Reactor Regulation
US Nuclear Regulatory Commission
M.S. 0-11D 19
20555 Washington DC

Tel.: +1 301 415 2845
Fax: +1 301 415 2444
Eml: mxc@nrc.gov

DURYEA John Luis
Westinghouse Electric Co.
Nuclear Automation,
P.O. Box 355, Pittsburg PA 15230

Tel.: +420 334 77 34 46
Fax:+420 334 77 34 49
Eml.: Duryeljl@notes.westinghouse.com

International Organisations

OECD/Halden Reactor Project, Institutt for Energiteknikk, Halden

♠DAHLL Gustav
Institut for Energiteknik
OECD - Halden Reactor Project
Os alle 13, P.O. Box 173
N - 1751 Halden

Tel: +47 69 21 22 00
Fax: +47 69 21 24 40
E-mail: dahll@hrp.no

OECD/Nuclear Energy Agency

♠HREHOR Miroslav
Nuclear Safety Division
12, boulvard des Iles
92 130 Issy-les-Moulineaux
France

Tel: +33 1 45 24 10 58
Fax:+33 1 45 24 11 10
Eml:miroslav.hrehor@oecd.org