



GERMAN (GRS) APPROACH TO ACCIDENT ANALYSIS (PART I)

GERMAN LICENCING BASIS FOR ACCIDENT ANALYSES

K. Velkov

(R.Kirmse)

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Forschungsgelände, 85748 Garching, Germany
vek@grs.de

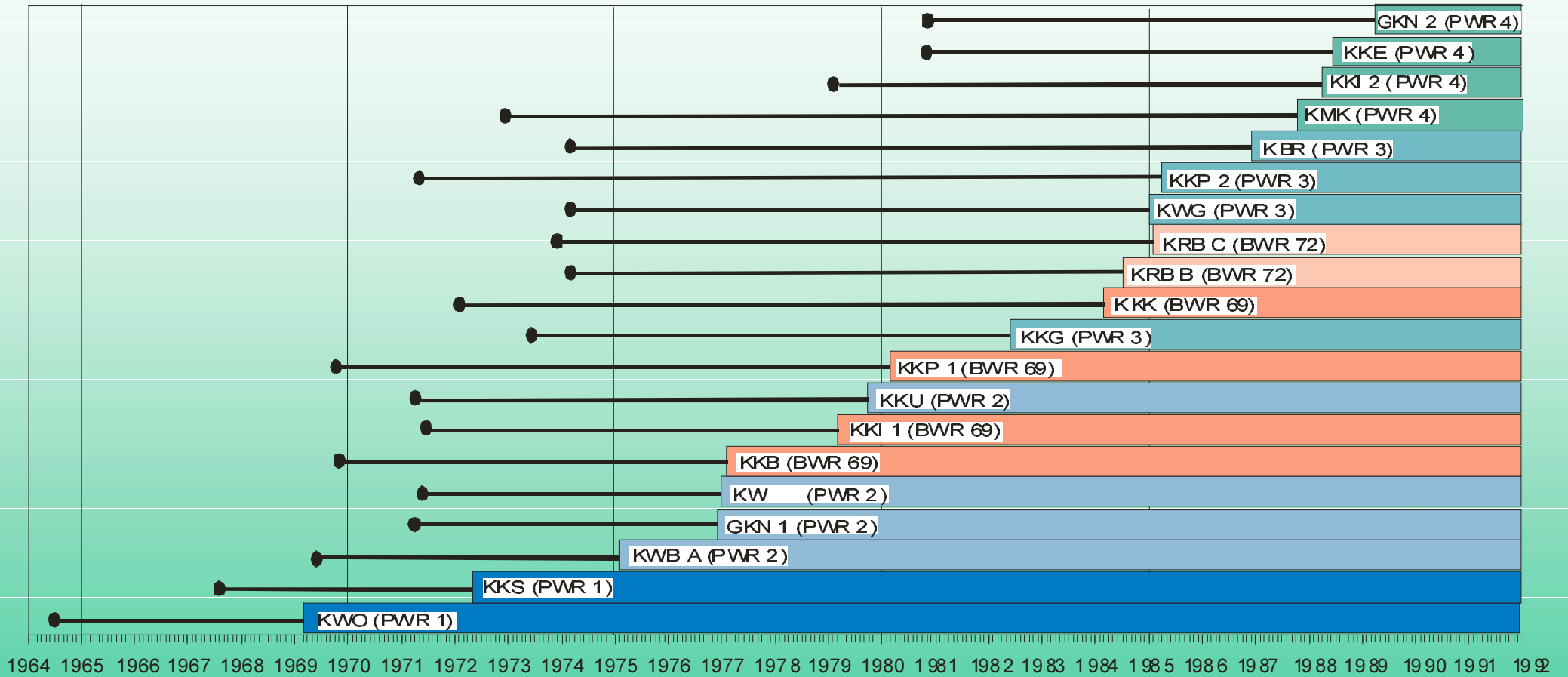
CONTENT OF THE PRESENTATION

- **WHO IS GRS**
- **OVERVIEW OF THE NPP OPERATION IN GERMANY**
- **LICENSING PROCEDURES IN GERMANY RELEVANT FOR ACCIDENT ANALYSIS**
- **GERMAN RULES AND GUIDELINES RELEVANT FOR ACCIDENT ANALYSIS**
 - **Content of ECC-Handbook**
 - **Content of Plant Dynamics Handbook**
 - **Content of Core Design Handbook**
- **SCOPE AND NATURE OF AA IN THE LICENSING PROCESSES**
- **PRESENT ACTIVITIES AND TRENDS**
 - **Periodic Safety Reviews (PSR)**
 - **KTA -2000**
 - **GRS Methodology Considering Operational Experience**

2. OVERVIEW OF THE NPP OPERATION IN GERMANY AND ACTIVITIES IN THIS FIELD

- 19 commercial units (installed power: 23.4 GW) in operation
- 6 BWR and 13 PWR.
- PWRs - four generations, the fourth generation – KONVOI
- Two types of BWRs - the 69 series and the 72 series.
- Most of the nuclear licensing processes for German NPPs are conducted in the decade between 1976 and 1986
- The latest NPP, GKN 2 (Neckarwestheim, unit 2), went into commercial operation in April 1989.
- In 1999 the average plant availability of the 19 operating units was 8004 hours (over 91%).
- Production in 2000 about 170 TWh (gross).
- June 2000 agreement between the German government and the utilities about the further utilization of nuclear power
 - A residual energy production, related to the beginning of the year 2000 was fixed for each unit
 - A residual energy production of 2623 TWh was calculated for all units
 - Hypothetical residual time of 15.4 years left

- There is no licensing of a commercial unit underway in Germany
- Procedure for the new research reactor Munich 2 (FRM 2) is in progress
- Licensing related activities exist continuously with regard to:
 - refueling
 - back-fitting measures and plant modifications for operating NPPs:
 - **increase of power**
 - **increase of the initial enrichment of fuel**
 - **use of different cladding material.**
- A new safety approach for future PWRs and corresponding technical guidelines were developed together with French partners in the years 1993 to 1998



Operating NPPs in Germany: ● — Date of Application, □ — Date of Commercial Operation

Date of Application and Commercial Operation of German NPPs

3. LICENSING PROCEDURES IN GERMANY RELEVANT FOR ACCIDENT ANALYSIS

Participants in the German licensing procedure:

- **Applicant** - this is usually the utility intending to operate the nuclear power plant (NPP) It presents the **Safety Analysis Report (SAR)** to
- **Licensing authority**, which is the **State Minister** in charge of nuclear safety in that state on which's territory the NPP is foreseen. **The Federal Minister is in duty of surveillance of the licensing procedure and he can give directives to the state licensing authority if he thinks that the Federal rules and guidelines are not fulfilled completely.**

The licensing authority requests their

- **Safety assessors**, which are commonly the **technical inspection agencies TÜV** and **other independent safety organizations like GRS**, to check the submitted analyses with regard to agreement with the **safety rules and guidelines** in force. The Federal Minister has his own advisory body.
- **Reactor Safety Commission (RSK)**

The **accident analyses** are documented as a part of the SAR or compiled in separate handbooks. Examples:

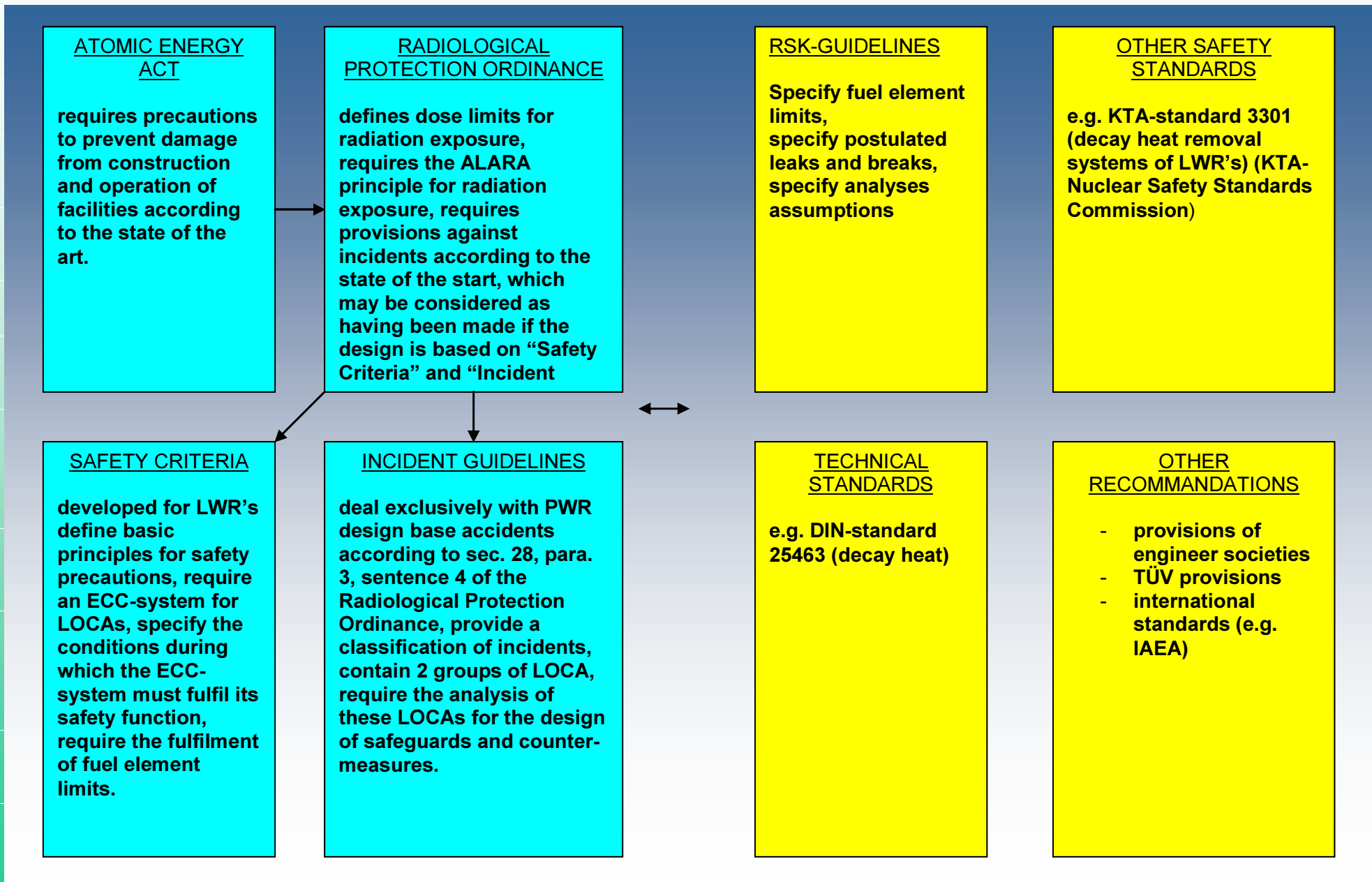
- **ECC-handbook** for the analyses of the loss of coolant accidents (LOCA)
- **transient's handbook** for the accidents without loss of coolant.

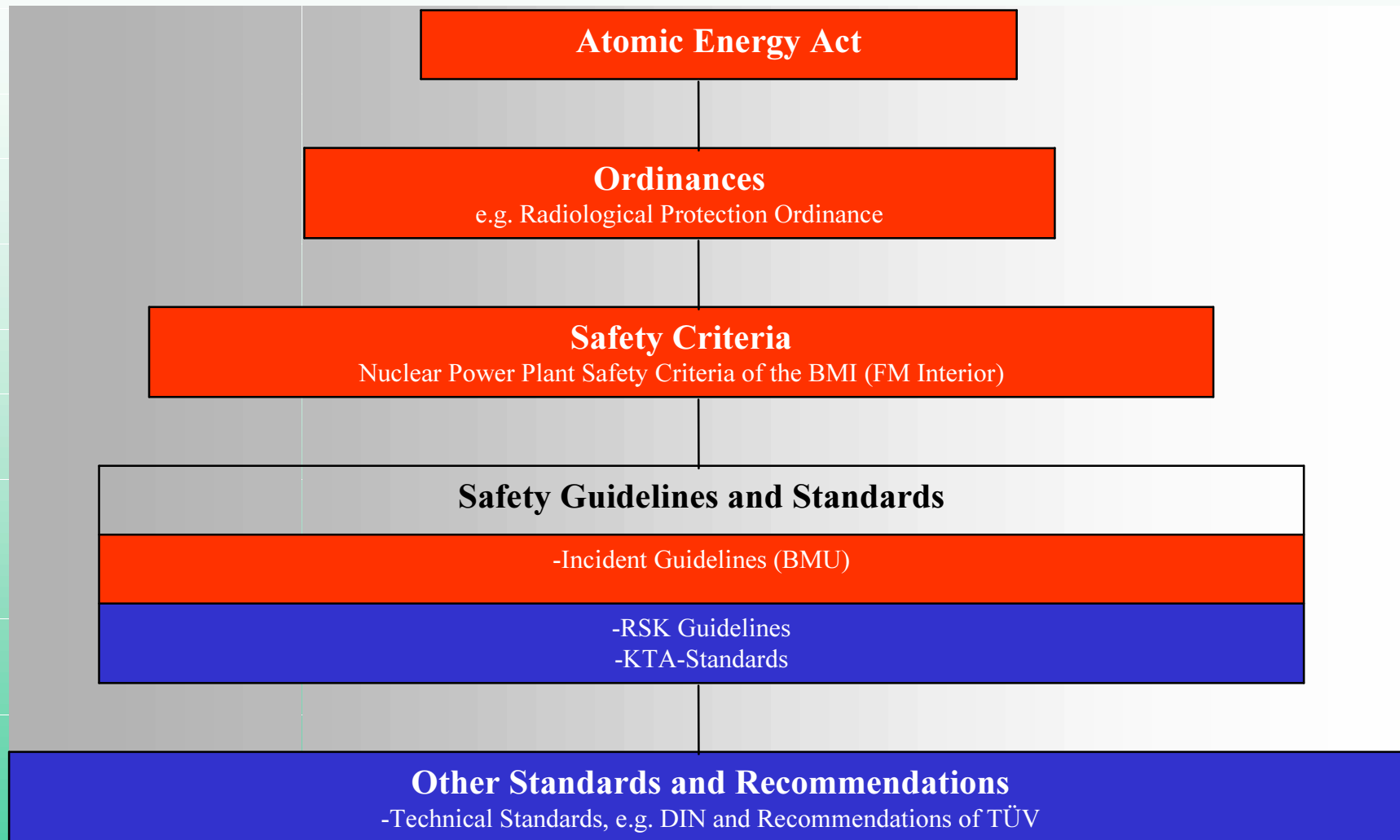
(for more information see the Appendix 1-3)

Most of the assessor's own calculations were performed with other accident codes than those used by the applicant. This has several advantages, however, there is no specific rule in the German rules and guidelines which prescribe this.


4. GERMAN RULES AND GUIDELINES RELEVANT FOR ACCIDENT ANALYSIS

- The major rules and regulations with relevance to the accident analysis are divided into **two groups**. **For the first group the rules are legally binding for each licensing case by law.** The second group of the rules depends on a case by case decision made by the licensing authority in a particular licensing process. Usually the fulfilment of the RSK-guidelines and the relevant KTA standards was requested by the authority.
- The legally binding rules which contain technical details are the **Safety Criteria** and the **Incident Guidelines**.
- **Important assumptions** for the accident analyses can directly be derived from these rules.
- The **RSK-guidelines** were formulated in order to ease the process of assessment within the RSK. They are a submission of references to safety-related requirements which the RSK considered necessary as a basis for a positive statement on the licensing request. Consequently its fulfilment accelerates the process of licensing. With regard to detailed requirements the **RSK-guidelines allow a certain degree of flexibility in order to provide the necessary latitude in the steady development of safety technology.** If particular requirements of the RSK Guidelines are not fulfilled, the applicant may demonstrate that other measures than those explicitly requested in a certain guideline will assure safety in at least an equivalent way.





 Legally Binding

 Deviations in Details Possible

According to safety rules and guides in Germany **many assumptions** in the safety analysis are **prescribed** and they have been applied in the various licensing processes. **The most important ones are derived from the following regulatory documents:**

- Criterion 4.3 of the Safety Criteria for NPP /Banz. Nr. 206 of 3.11.1977, p.1/ **requires a reliable and redundant system for emergency cooling of the reactor core after loss of coolant. It must be in such a condition, that it can fulfil its safety related function for all break sizes, operating conditions and transients to be considered in the reactor coolant system even during maintenance procedures and a simultaneous occurrence of a single failure in the system. The single failure is defined as a failure caused by a single event and includes consequential failures caused by this failure.** The single failure assumption is to be considered independently from the cause of the initiating event.

- The interpretations of the Safety Criteria /Bek.d.BMI v. 4.12.1981-RSI6-513301-4/ provide guidance to the application of the **single failure concept in more detail**. The single failure is a part of the deterministic design concept. **It is to be considered with respect to the decay heat removal of normal and abnormal operation and design basis cases for the reactor protection system, the emergency power supply systems and the containment heat removal system**. If several of these systems and components are needed simultaneously or sequentially, to cope with a postulated event, the single failure is applied to the sum of these systems, not to each system. Generally the single failure has to be assumed for **active** as well as for **passive components**. Exceptions from the assumption of a passive single failure are possible if it is demonstrated that the corresponding passive component is of extremely high quality, ensuring that its failure is highly improbable. **In this case the passive failure needs to be assumed only after 100 hours.**

- KTA rule 3501 (Reactor Protection System and Surveillance Equipment, revision June 1985) chapter 4.5.2 and Safety Criterion 6.1 of the Safety Criteria require that the formation of actuation signals for **the detection and control of an accident by the reactor protection system (RPS) must be accomplished by means of different process variables**. In order to prove that the RPS can cope with the initiating event successfully by means of its second actuation, **the failure of the first actuation signal of the RPS** has to be assumed in the accident analysis. KTA rule 3501 4.4.1 (3) determines that a single failure in any other active system shall also be assumed.

- Guideline 3.1.2 (9) of RSK Guideline for PWR, 3rd edition of 14.10.1981 with modifications and corrections /Banz #69a,1982, #104,1984, #106,1983, #158a,1996, #214,1996/ requires that the reactor scram system based on the insertion of control rods shall fulfil its safety function also if the most effective control element fails to move. Consequently the assumption of one rod not being inserted into the core has to be assumed for reactor scram (**stuck rod assumption**). This is relevant for sub-cooling transients with reactivity addition in the core due to temperature decrease, e. g. after a steam line rupture.
Furthermore, **the effect of the control rod scram system shall not be considered in the long term balance after a LOCA** (RSK guideline 22.1.1 (2)).
- KTA rule 3301 (Decay Heat Removal Systems of LWR, edition November 1984) requires that all electrical consumers, which are needed to perform the function of decay heat removal, must be connected to the **emergency power** supply system. Consequently the RSK-Guidelines require in chapter 22.1.1 (14) 2 that **the emergency power case has to be superposed in the analysis of loss of coolant accidents with small leaks. In the German practice this superposition is considered for large break LOCA analysis too.**

- According to RSK Guideline 21.1 (1) 2 the **reactor pressure vessel internals** must withstand the reaction and jet forces resulting from the load of LOCA **up to a cross section of 0.1A at any break position. Consequently the LBLOCA analyses with cross sections $\geq 0.1A$ of the main coolant pipe are performed without considering reactor scram by means of insertion of control rods because the system may fail mechanically.** The analyses serve to prove that the reactor is transferred to sub-critical condition and kept there without the control rod shutdown system only by means of **reactivity feedback and injection of borated water.**
- KTA rule 3501 requires in chapter 3.3 for the accident analyses to postulate the **normal operating plant condition as the basic initial condition.** Each event sequence should be at first analysed assuming the most probable initial condition. Additional analyses have to be performed for the most unfavourable initial conditions. **These are derived from quasi-stationary operational conditions plus possible deviations of measuring values of process variables** from their set point, superposed by quasi-stationary deviation of process variables due to a single random failure within the measuring and control system as a whole, which influence the operational parameter. Example: **LOCA analyses are performed typically with an initial power of 106% of nominal power. 103% are the level of the reactor limitation system intervention and additional 3% are the postulated measuring error.**

- KTA rule 3301, chapter 4.2.2. requires that the calculation of the **decay heat power** after reactor shutdown shall be determined according to the calculation scheme of DIN 25463. **For initiating events which occur during power operation an error band of double standard deviation (2xSigma) shall be assumed.** For all other cases, the single standard deviation is considered as sufficient. No error band is to be postulated for very improbable initiating events.
- Criterion 1.1 (2) of the Safety Criteria requires sufficiently reliable technical safety systems for the control of accidents. In licensing analyses it is therefore generally assumed that actions of **operational systems are not considered, unless the action of the control system is unfavourable for the event.**

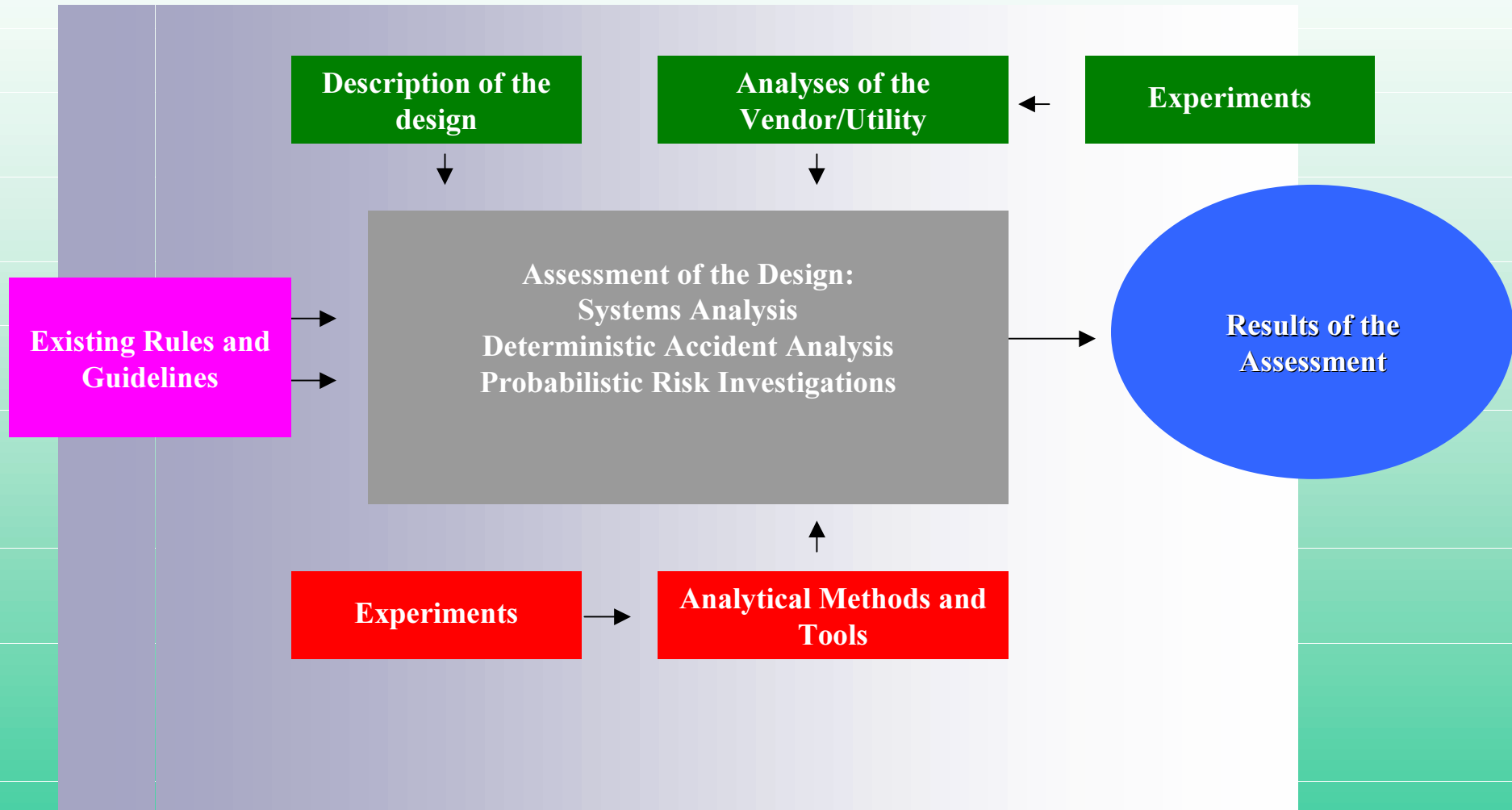
Most Important Failure Assumptions

- Single Failure Criterion
- Repair and Maintenance
- Stuck rod
- Operational system action
- Often: neglecting the first actuation signal for scram
- For LOCA: superposition of loss of power

5. SCOPE AND NATURE OF AA IN THE LICENSING PROCESSES

Purpose of Accident Analysis

- Safety Assessment in Licensing and Supervision
- Procedures Optimisation of System Design
- Validation of Design Base Procedures
- Validation of Accident Management Procedures
- Validation of Training and Analysis Simulators
- Probabilistic Safety Assessment In-depth
- In-depth Investigations of Occurred Events in NPPs
- Contribution to Problems of Pressing Importance at any Time



Requirements for the Format and Content of SAR

- The German Standard Safety Analysis Report has to be structured according to the **list of content specified in the TÜV guideline /TÜVIS-Examination basis**.
- 30.08.1976. **This guideline has been published by BMI in 1976**. It refers to §3 (1) 1 of Nuclear Licensing Procedure Ordinance (AtVfV).
- The list is a guidance, not intended to be complete in all details. In particular, the list does not contain any drawings, graphical representations, schemes of safety related functions, tables. It is expected that the applicant will transfer the requirements of the AtVfV in a meaningful way.
- There are six main chapters: (1) Site, (2) Nuclear Power Plant Description, (3) Radioactive Material and Radiation Protection, (4) Operation of the NPP, (5) Accident analysis, (6) Decommissioning
- Explanations are given about the content of each sub-chapter.

- **Conservative model assumptions**, required in the RSK-guidelines to **compensate for insufficient knowledge on certain physical phenomena or for insufficiently developed models, can be replaced by more realistic assumptions if reliable proof is given on the basis of relevant experimental verification.** At the time of licensing of the recent NPPs in Germany there were still basic conservative model assumptions involved. **Later on it has been demonstrated by repetition of the previous licensing accident analysis using today's advanced accident codes that these assumptions really were conservative.** Today's codes, developed, verified and applied in Germany, do not have anymore the same degree of model conservatism as before. To compensate for this, the uncertainty of calculated results has to be ascertained, in particular in those cases where results are not far from the limits.
- **A list of the content and structure for the Standard Safety Report** was prepared by order of the Federal Minister in charge for reactor safety in 1976 (document: BMI, 26.7.1976-RS I4-51380712). **The most comprehensive list of accidents which have to be considered in the safety analysis follows.** This does not necessarily mean that all of them have to be analysed in detail. If it can be shown that a particular case is covered conservatively by another one, a detailed analysis is not required. This official guide also defines in detail what has to be documented within the safety analysis

CLASSIFICATION OF EVENTS

Not by rule but **by practice** the accidents are classified into event classes which were compiled by a working group of the “Kerntechnischer Ausschuß” (KTA) in reference KTA-GS-47 (KTA document UA-SF/85/1). The five classes and there approximate frequency of occurrence of the events are:

Class 1: Normal operation and maintenance ($> 3 \times 10^{-2}$ /year)

Class 2: Events possible during lifetime of NPP, e.g. anomalous operation ($> 3 \times 10^{-2}$ /year)

Class 3: Events not expected during lifetime of one NPP, but possible within lifetime of several NPPs for one NPP, e.g. **design base accidents** (between 3×10^{-2} /year and 1×10^{-4} /year)

Class 4: Events not expected during lifetime of any NPP, but used as a limiting case for the safety relevant design, e.g. **design base accidents** (between 1×10^{-4} /year and 1×10^{-5} /year)

Class 5: Events not expected during lifetime of any NPP, in contrary to the classes 1,2,3,4 the NPP need not be designed to cope with these accidents, but measures of risk reduction are required. **These are the beyond design base accidents** ($< 1 \times 10^{-5}$ /year)

The application of the single failure concept, the permission to consider operational systems in the analysis, and the acceptance criteria are specific for each of the different classes. In a general way, they can be derived from the Safety Criteria and from the Incident Guidelines. For convenient practical use they are specified in detail in the report KTA-GS-47 with reference to the classes mentioned above. Some examples are given in the following.

- No critical heat flux in the core and no opening of pressurise safety valves is allowed for events of class 2. For class 3 and 4 events the acceptance criteria are the same as those of the USA appendix K of **CFR 50**, extended by the requirement to limit the fuel rod damage to a value of 10%. The application of the single failure concept is required for the analysis of design base accidents (classes 3 and 4). **Specific German requirements are its application on active as well as on passive components of safety systems and the simultaneous assumption of an additional component being under repair or maintenance.** For events of class 5 the single failure need not to be applied and the consideration of operational systems is allowed.
- For **anticipated transients without scram (ATWS)** the RSK-guideline 20 requires the analysis **of eight cases** with the aim to demonstrate that the maximum pressure in the primary coolant system stays below the ASME Code Section III, Division 1, NB-3224 Level C Service Limits and that the long term subcriticality and core cooling is assured.

- The events of classes 2,3,4 are usually organised in **10 physical groups** (the term group is used to characterise the physics but not - as in the U.S. - to characterise the severity of the event). For the **seven most important groups** tables are given (see **Appendix B**). The tables contain information on the events which belong to the group for the Convoi NPPs and for the Pre-Convoi NPPs, the corresponding event class (see above), the reference number in the Incident guidelines if there is any, the initial conditions which are to be considered in the analysis, and the systems for which the analysis is performed as a safety demonstration. The tables also inform about the **leading cases within each group**, for which a complete analyses was performed and about those cases which are covered by the leading cases. For certain cases accident analysis is not required because of special technical precautions foreseen in the plant, e.g.; double pipe of the main steam line between containment penetration and main steam valve.

(An example for WWER event grouping see in Appendix C)

A) The main chapters of the German Standard SAR are:

Introduction

Summary

§ 1 Site

§ 2 Nuclear Power Plant Description

§ 3 Radioactive Material and Radiation Protection

§ 4 Operation of the NPP

§ 5 Accident analysis

§ 6 Decommissioning

B) Content of § 5 (Accident Analysis):

5.1 Introduction

Explanation of the selection of the presented accidents and accident combinations on the basis of the required protection against damages according to the state of the art.

5.2 Accidents

Each analysis should consist of:

- assumption for the occurrence of the accident and information on the initiating event, also probabilistic evaluation of the initiating event (optional)
- analysis assumptions (initial conditions of the plant, failure assumptions)
- assumed criteria for the initiation of the reactor protection system
- description of the efficient countermeasures, from the reactor protection system initiated systems and components, manual actions
- summarising description of the analysis methods, physical models, mathematical solutions, reasons for the selection and application of codes, assumptions of the analysis (boundary conditions)
- assumptions and basic principles of the calculation of radiological consequences (e.g. activity release from fuel rod, specific activity of reactor coolant, deposit factors, filter efficiency, leak rates, dispersion factors, dose factors)

- assumptions and boundary conditions for the calculation of dispersion factors (e.g. source elevation, source shape, receiving point, meteorological conditions)
- description of the accident sequence (also schematic) and of the results of the analysis (with graphical representation)
- Consequences of the accident on the plant and the environment; in case of accidents with significant radiological consequences on the environment, the calculated whole body and thyroid inhalation doses should be given not only as maximum values but also in relation to distance and time, results of the deposition of radioactive material in the environment should also be presented

5.2.1

Withdrawal of most effective control element or control element group or control element bank from the following conditions: cold sub-critical, hot sub-critical, cold critical, hot critical, part load, full power

5.2.2

Ejection or dropping of one control element taking into account most unfavourable initial conditions of power, power distribution and reactivity

5.2.3

Inadvertent insertion of one control assembly

5.2.4

Start of one main coolant pump

5.2.5

Injection of cold water into the main coolant system from connected systems (e. g. bypass of the high pressure pre-heater of the CVCS, erroneous injection of ECCS, failure of high pressure feedwater pre-heater in BWR)

5.2.6

Pressure changes in the main coolant system

5.2.6.1

Pressure reduction (e. g. erroneous opening of valves)

5.2.6.2

Pressure increase (e. g. inadvertent pressuriser heating)

5.2.7 (PWR)

Inadvertent reduction of boron in the main coolant system

5.2.7.1

Inadvertent change of boron concentration of the coolant

5.2.7.2

Detachment of deposits containing boron

5.2.7 (BWR)

Disturbances of power control, starting from most unfavourable conditions

5.2.8

Turbine trip

5.2.8.1

Turbine trip with bypass available

5.2.8.2

Turbine trip with blocked bypass (e.g. due to loss of condenser vacuum)

5.2.9

Loss of main heat sink due to inadvertent closure of steam line isolation valves

5.2.10

Main coolant pump failures

5.2.10.1

Failure of one pump

5.2.10.2

Failure of several pumps

5.2.10.3

Influence of free running pumps against pumps electrically coupled to the grid

5.2.10.4

Pump shaft seizure

5.2.11

Loss of normal onsite and offsite AC power

5.2.12

Feedwater supply disturbances

5.2.12.1

Failure of one main feedwater pump

5.2.12.2

Failure of auxiliary (emergency) feedwater pump

5.2.12.3

Inadvertent closure of feedwater valves

5.2.12.4

Rupture of a feed water line

5.2.12.5

Rupture of an auxiliary (emergency) feed water line

5.2.13

Disturbances in the steam removal system

5.2.13.1

Failing function of feedwater system resulting in a deterioration of heat removal

5.2.13.2

failure of main steam pressure control

5.2.13.3

Inadvertent opening of valves (e.g. turbine bypass valve, main steam relief valve, main steam safety valve)

5.2.14

Damage of steam generator tubes

5.2.14.1

Leakage of steam generator tubes

5.2.14.2

Rupture of steam generator tubes

5.2.15

Rupture of main steam line (PWR) rupture locations with and w/o postulated consequential damages of steam generator tubes as well as with and w/o postulated loss of power

5.2.15.1

Steam line rupture downstream the external main steam isolation valve with intact steam generator tubes and with operational leakage

5.2.15.2

Steam line rupture upstream the external main steam isolation valve outside the containment

5.2.15.3

Steam line rupture in the annulus (in Germany: double containment)

5.2.15.4

Steam line rupture inside the containment

5.2.16

Loss of coolant accidents (LOCA)

5.2.16.1

Description of investigated leak sizes and locations and reasons for the selection

5.2.16.2

Rupture of a main coolant line inside the containment

In the frame of the description of the accident the following aspects have to be considered:

- accident sequence: depressurisation, reflood, heat removal phase, long term cooling

- thermal hydraulic events in the reactor cooling system
- acting forces on the core, internals of the reactor pressure vessel and components of the reactor coolant
- summarising description of the fuel rod behaviour and conclusions with respect to the releases of fission products, summarising description of zircon-water reactions and evaluation of the coolability
- containment loads and loads on internals of the containment (pressure, temperature pressure differences, jet forces, consequences of fragments on containment wall)
- description of measures to mitigate the consequences of high speed rotating main coolant pumps
- loads on the annulus (pressure, temperature)
- summarising description of hydrogen generation and control
- summarising description of initiation of building spray system (if applicable)

5.2.16.3

Leakage of the reactor coolant system boundary and rupture of connecting pipes, failure of valves (small break loss of coolant accidents including inadvertent opening of pressuriser relief and safety valves)

5.2.16.4

Rupture of a pipe connected to the reactor coolant system, outside the containment (interfacing

5.2.17

Transients with failure of the scram system (ATWS)

5.2.18

Accidents during handling and storage of fuel assemblies

5.2.19

Disturbances of the gaseous waste system

5.2.20

Disturbances of the liquid waste system

5.2.21

Disturbances of the turbine (e.g. leakage, behaviour during over-speed, oscillations)

5.2.22

Internal fire and explosions

5.2.23

External hazards

5.3 Summarising description of the calculated radiation doses

6. PRESENT ACTIVITIES AND TRENDS

- The further development of the rules and regulations in Germany is necessary in order **to take into account the state of the art**. Several attempts are presently underway. **They are influencing the licensing related activities including the accident analysis today and in the future.**
- The current nuclear regulations have been supplemented by the guidelines on the performance of **Periodic Safety Reviews (PSR)**. This was an important step on the way to adapt the rules and regulations to the defence-in-depth
- Generally there is **no direct legal obligation** to perform a PSR. However, for several plants there are respective requirements stipulated in the licences (7 out of the 19 operating plants, mainly PWR, have this requirement). The reactor safety commission **RSK recommended** the performance of PSRs for all operating NPPs in 1988 (Federal Gazette 47a, 1989) and specified details in 1995 (Federal Gazette 158, 1995). In order to allow a homogeneous procedure in all federal states, **guidelines for the PSR were generated and published in 1997 (Federal Gazette 232a, 1997).**
- In practice, PSRs have been performed for nearly all of the NPPs in Germany. According to the agreement between the German government and the utilities of June 2000 the utilities of the NPPs will continue this practice. The time frame for the next **PSRs is one of the appendices of the agreement.**

PSR-Guidelines

- Important step to adapt guidelines more formal to D-in-D Concept
- No direct legal obligation for PSR
- For several plants respective requirements in the license
- In practice, all NPPs have performed PSR
- Agreement of government and utilities includes binding time frame
- Every 10 years
- The owner of the license is responsible for the conduction
- Planning and conduction to be synchronised by owner and authority

PSR-Guidelines Consists of 4 Parts

- Fundamentals for the PSR of NPPs
- Guidelines for the safety status analysis (including the deterministic protection goal oriented review of engineered safety features)
- Guidelines for the probabilistic safety analysis
- Guidelines for the deterministic analysis of physical protection

The **fundamentals** contain the objective, principles, legal status, scope, parts of the PSR, final assessment of the results of the PSR, documentation by the owner of the license, and the assessment of the results by the regulatory body.

The objectives are related to the principle of defence-in-depth.

Defence-in-Depth Concept in German Standards

- On the next page is shown the cross reference of the four safety levels (they are equivalent to the **Plant Condition Categories PCC**, the term which is used in several countries and also by **IAEA-1, IAEA Safety Standard Series, 1999**) to the radiological requirements, to the type of events, to the qualitative frequency of the events, to the technical equipment and procedures to cope with, and the design principles involved.
- The technical systems and measures at the different levels have to be effective, independently of failures or loss of the precedent function, and cover the events not kept under control on the respective lower level. This is to maintain the integrity of the sequential barriers against release of radioactive material within the plant and into the environment and thus ensuring the protection against ionising.
- **In the frame of the PSR the operational experience is evaluated in the levels 1 and 2. Level 3 forms the main part of the PSR. It is demonstrated how far the postulated accidents are coped with satisfactory effectiveness and reliability by means of the foreseen technical equipment and measures.**

Safety Concept in the Defence-in-depth Strategy for NPP

Safety Level	Radiological Requirements		Plant conditions		Frequency	Technical equipment and objectives		Design principles
1	precaution against damage according to atomic law	§45 Radiation Protection Ordinance (StrSchV)	operating conditions	normal operation	regular	operational systems	operational components/systems to prevent abnormal occurrences	-conservative design -basic safety -quality assurance -surveillance -personal qualification
				abnormal operation	frequent		control/limitation systems component protection to prevent DBA	in addition: -inherent safety -stability (TH, nuclear physics)
2	precaution against damage according to atomic law	§28 (3) StrISchV	operating conditions	design basis accidents	rare	operational systems	safety systems to control DBA	in addition: -redundancy -diversity -fail safe -physical separation -automation -autarky
3				very rare	specific precautionary measures to control SVRE		specific design requirements	
4	precaution against damage according to atomic law	Limitation of radiation exposure (ALARA), no quantified radiation protection requirement	BDB severe accidents	a) special very rare events (SVRE)	very rare	operational systems	on-site AM measures to prevent core damage or limit impacts on environment	-flexible use of existing systems -engineering practice for AM equipment
				b) severe BDB conditions/emergencies			off-site emergency management and disaster control	off-site emergency management and disaster control
	residual risk		BDB severe accidents	damage states with significant impact on the	extremely rare, practically excluded		off-site emergency management and disaster control	

Typical staggered radiological^[1] and technical limiting values (acceptance criteria)

Radiological limits:

Radiological protection of the environment for **safety level 1 and 2**: § 45 StrSchV, (typical limits 0,3/0,9/1,8 mSV for uterus, gonads, red bone marrow / all remaining organs / surface, skin)

Radiological protection of the personnel: § 49, 54 StrSchV, limits staggered depending on the duration of occupation etc.)

Radiological protection of the environment for **safety level 3**: § 28 StrSchV (the typical limits 50/150 mSV are reduced in the new radiological protection ordinance)

Radiological protection of the environment for **safety level 4**: limitation of exposition without quantified criterion (“efficient activity enclosure”)

[1] In this compilation still the radiological protection ordinance valid until August 2001 is used as a reference.

Sub-criticality:

For safety levels 1 and 2

Shutdown with control rods: reactivity typically $< -1\%$

Permanent shutdown with surveillance of sub-criticality: $< -1\%$, without: $< -5\%$

Fuel element pool: $< -5\%$

For safety level 3

Fast shutdown (single failure or stuck rod): $< -1\%$

Long term shutdown (with surveillance of sub-criticality, including single failure, maintenance): $< -1\%$

Re-criticality of reactor core: short term, but cladding temperatures remaining below limits for steam line rupture (PWR).

Fuel element pool: $< -5\%$ (in specific cases $< -2\%$)

For safety levels 4a and 4b

Reactivity $< -1\%$ including surveillance of sub-criticality (4a), $< -0\%$ (4b)

Fuel element pool: $< -1\%$ (4a), $< -0\%$ (4b)

Fuel rod limits:

In normal operation and during anticipated transients (**safety levels 1 and 2**) no local fuel melting should occur (protection of the barrier fuel matrix).

For normal operation and during anticipated transients (**safety levels 1 and 2**) departure from nucleate boiling is not allowed ($DNB > 1.0$, including uncertainties) as a protection of the fuel rod boundary. [1]

[1] KTA rule 3101.1 (Design of reactor core of PWR and BWR, part 1: Fundamentals of thermal hydraulic design), chapter 3, allows for safety level 2 events an alternative to the avoidance of critical boiling conditions: It requires the limitation of cladding temperatures in such a way that the design values of the fuel rods are not exceeded thus allowing that the operation of the plant can be continued after the level 2 event.

After less frequent events (**safety level 3**), such as loss of coolant accidents, the function of the fuel rod barrier should not be lost. This is specified by a maximum cladding temperature (e. g. 1200 °C according to Appendix K of the U.S. CFR 50), a limitation of local percentage of fuel cladding oxidation (e. g. $< 17\%$ of initial cladding thickness), and a limitation of the amount of zirconium oxidation (e. g. $< 1\%$ of core mass inventory of zirconium).

There is a tendency to distinguish between more frequent and less frequent events within level 3 accidents (safety levels 3a and 3b): limitation of cladding temperature to 800°C ($>800^\circ\text{C}$ for less than 5 s) / 1200°C.

[1] KTA rule 3101.1 (Design of reactor core of PWR and BWR, part 1: Fundamentals of thermal hydraulic design), chapter 3, allows for safety level 2 events an alternative to the avoidance of critical boiling conditions: It requires the limitation of cladding temperatures in such a way that the design values of the fuel rods are not exceeded thus allowing that the operation of the plant can be continued after the level 2 event.

For **safety level 4a** events it is required that the coolability of the core should be maintained as far as possible and the ability to shut-down the reactor by means of insertion of control rods (exceptions are e.g. ATWS events).

Decay heat

In general the decay heat may be calculated according to DIN 25463. Surcharges are to be added in order to consider uncertainties (KTA rule 3301, § 4.4.2)

The KTA rule 3301 does not regulate the surcharge for operating conditions (**safety levels 1 and 2**). Following the general tendency that for more frequent events more strict requirements are to be applied, at least the surcharge of level 3 of two times the standard deviation is to be added.

For accidents (**safety level 3**) a supplementary uncertainty charge of two times the standard deviation is to be added.

For very rare events (**safety level 4**) no surcharge is requested.

Coolant system boundary limits:

- **For anticipated transients (safety level 2) no opening of pressuriser relief valve (special German requirement)**
- For less frequent transients (**safety level 3**) no opening of pressuriser safety valves (pressure below design pressure)
- For rare events such as ATWS primary system (**safety level 4a**) stresses should be below ASME code section III, division 1, level C service limits (typically 130% of design pressure).

Temperatures in fuel element pool:

- For **safety level 1**: $\leq 45^{\circ}\text{C}$
- For **safety level 2 and 3a**: $\leq 60^{\circ}\text{C}$
- For **safety level 3b and 4a**: $\leq 80^{\circ}\text{C}$
- For **safety level 4b**: Fuel elements must be covered with water



Obligations of Licensee and Authority (Regulatory Body) in PSR

PARTS	Safety Status Analysis		Probabilistic Safety Analysis (PSA)	Physical Protection
STANDARDS	Guide Safety State Analysis		Guide Probabilistic Safety Analysis	Guide Deterministic Analysis of the Physical Protection
Agreement on PSR Procedure between Licensee and Authority				
PROCEEDING OF THE LICENSEE	Current Plant Description			
	Assessment of the Plant's Safety Systems according to the Requirements and Standards of the Protection Goal Concept	Description of Operational Management and Evaluation of Operating Experience	Examination of the Balance of the Safety Concept and Determination of Cumulative Frequency of not Controlled Plant States by Probabilistic Methods	Report: State of Physical Protection
	Report: Deterministic Protection Goal Oriented Review	Report: Operational Management and Operating Experience	Report: PSA	
	Report: Final Review of the Safety Status involving the Respective Results of the Parts of the PSR			
PROCEEDING OF THE AUTHORITY	Protection Goal Oriented Evaluation, if necessary, with Consultation of external Experts		Evaluation, if necessary, with Consultation of external Experts	Evaluation, if necessary, with Consultation of external Experts
	Overall Assessment by the Supervisory Authority, Administrative Measures and Directives			

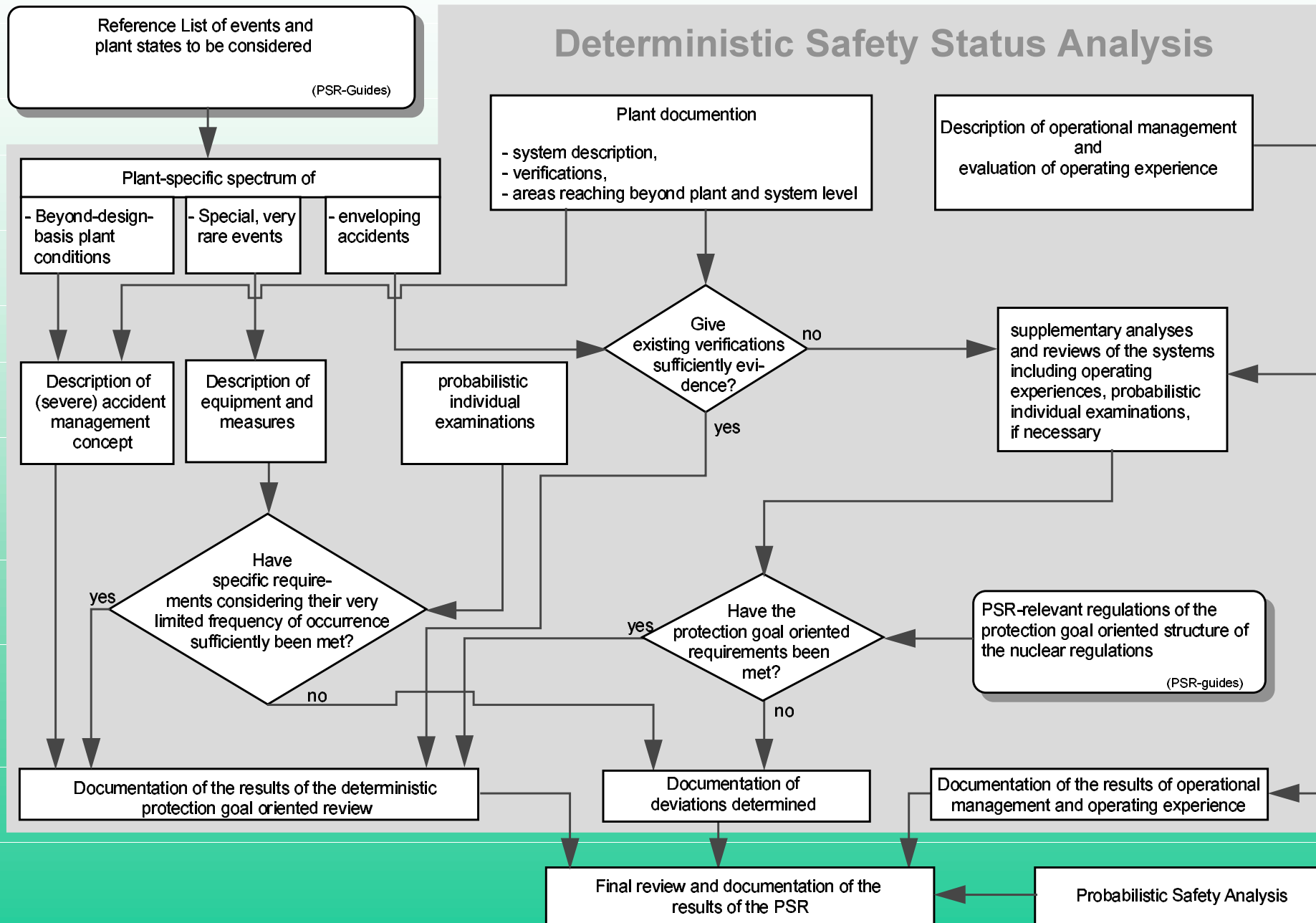


Fig. 2: Procedure of deterministic safety status analysis

KTA-2000

- Another attempt is underway to modernise the existing rules and guidelines, the [KTA-2000 project](#): comprehensive and hierarchical structure of reactor safety requirements
“KTA 2000” consists of the following parts:
 - the KTA Safety Fundamentals 2000,
 - **Seven** KTA basis rules, and the
 - KTA standards

Whereas the about 100 KTA standards are existing and under regular revision, the KTA fundamentals and the basis rules are presently in preparation.

- According to the **KTA fundamentals** the integral holistic safety concept is basically preventive and follows closely the defence-in-depths concept which **has to be applied for the three main areas: technology, man and organisation**. The concept of the **four safety protection goals** is mainly based on deterministic principles, it can be supplemented by probabilistic elements in order to allow to state the safety

The requirements necessary to achieve the **protection goals** are described in the **KTA Basis rules**. The first four rules contain design-independent requirements which can be directly assigned to the **four protection goals**:

- Reactivity control
- Cooling of fuel elements
- Confinement of radioactive substances
- Limitation of radiation exposure

The structure within these rules follows essentially the following order: protection goal, partial protection goals, operational or safety functions assigned to the partial protection goals, safety level. For example the structure of the second basis rule “cooling of fuel elements” contains the two partial protection goals “ensuring heat removal from fuel elements to ultimate heat sink” and “maintaining sufficient coolant inventory by minimising losses and by replenishment coolant from reservoirs”.

The corresponding functions for the **first** partial safety goal are:

- heat removal from core, heat removal from secondary system (PWR only), heat removal from wet well (BWR only), heat removal from spent fuel elements in pool, heat removal from containment, heat transport in cooling chains (including ultimate heat sink)

From the **second partial safety goal**:

- reactor coolant replenishment, minimisation of reactor coolant losses, steam generator feeding (PWR only), ensuring inventory of wet well (BWR only), minimisation of losses from wet well (BWR only), spent fuel pool water replenishment, minimisation of water losses from spent fuel pool.

The requirements for each of these functions are subdivided according to the four safety levels.

The remaining three basis rules contain additional design-independent requirements needed to achieve the protection goals. These rules are

- General technical requirements
- Methodology of safety demonstration
- Personal-administrative measures

GRS Methodology Considering Operational Experience

The existing rules and regulations are related mainly to design, construction and commissioning of NPPs and were not primarily developed to consider requirements that can be derived from a long-term operational experience. These rules and regulations were created at a time when there was a broad willingness of consent to solve problems and find results among all participants and when the necessary expertise was still present to the required extent. **It is therefore not surprising that the present rules and regulations have to be supplemented.** Furthermore, they almost exclusively concentrate on a deterministic safety assessment, but in the meantime probabilistic safety assessments have become the state of the art.

- **Break preclusion concept is applied.** The upper limit of the size of LOCA of level 3 can be restricted 0.1A. The LBLOCA can then be treated in level 4a in the safety assessment notwithstanding of the fact that the LBLOCA was the design basis for the emergency core cooling system and the containment.
- The accident analysis needed mainly for the assessment in safety level 3 shall be preferably “**best-estimate**” analysis of the selected events
- GRS applies assessment criteria to the NPPs in Germany that are internationally applied for future plants

- The basic deterministic safety requirements are supplemented by probabilistic parameters
- **GRS methodology** based on operational experience distinguishes:
 - system damage state (reference summation goal $< 10^{-4}/\text{ry}$)
 - core damage state (reference summation goal $< 10^{-5}/\text{ry}$)
 - plant damage state (reference summation goal $< 10^{-6}/\text{ry}$)

The three damage states are defined by considering the interconnections between the defence-in-depth concept and the PSA results.