Design Implementation of the Post-Accident Monitoring (PAM) System for Wolsong NPP Units 2,3&4 in Korea

SPECIALISTS' MEETING

on

INSTRUMENTATION AND EQUIPMENT FOR MONITORING
AND
CONTROLLING NPP POST-ACCIDENT SITUATIONS

12-15 September 1995
Dimitrovgrad, Russian Federation

Sang-Joon Han
Korea Atomic Energy Research Institute
P.O.Box 105, Yusong
Taejon, Korea

Title : Design Implementation of the Post-Accident Monitoring (PAM) System for Wolsong NPP Units 2,3&4 in Korea

Summary

Wolsong NPP Units 2,3&4 (hereinafter "Wolsong 2,3&4") are unique CANDU-type reactors originally designed by Atomic Energy Canada Limited (AECL), and now being jointly designed in collaboration between Korean engineers and their Canadian counterparts, and constructed in Korea. The units are referenced to the design implemented for the existing Wolsong NPP Unit 1 which has been in service since 1983, except that many design improvements are incorporated to enhance plant safety as well as operational performance.

The post-accident monitoring (PAM) system is part of these improvements, and plays a vital role providing the operator with the necessary information to manage the outcome of the event by monitoring & displaying critical safety parameters after plant accidents. The fundamental design concept of the PAM system for Wolsong 2,3&4 conforms to the requirements of the Canadian Standard which was established after TMI Accident in 1979. The functional requirements for the PAM system are to provide sufficient information for 1) verification of reactor shutdown, 2) verification of reactor heat removal, 3) verification of a barrier to reactivity release, 4) evaluation of radiological conditions, and 5) assistance in carrying out recovery actions and for the operator to monitor the post-accident state of the plant.

This paper is intended to introduce the actual design implementation of the post-accident monitoring system and to provide a good opportunity to understand what issue items are at the design implementation stage for Wolsong 2,3&4.

1 . Introduction

In the event that a nuclear power plant accident occurs, initial protecting and mitigating actions are taken automatically by the plant safety systems. As the duration of the accident progresses, the operator will tend to have an increasing role in managing the outcome of the event. The post accident monitoring system provides the monitoring and display of necessary information for the plant operator to manage the event. The system has been designed to meet the requirements of applicable Codes and Standards which are issued by Canadian Standards Association (CSA) N 290.6 which has a similar design approach to other types of nuclear reactors. The functional requirements for this system are to provide sufficient information for 1) verification of

reactor shutdown, 2) verification of reactor heat removal, 3) verification of a barrier to radioactivity release, 4) Evaluation of radiological conditions, and 5) assistance in carrying out recovery actions and for the operators to monitor the post accident state of the plant. Table 1 shows some examples of PAM Variables and the safety function as recommended by CSA 290.6. The design approach for this system is to ensure the information is available to the operator in either the main control room (MCR) or the secondary control area (SCA), which is used as a backup in case MCR is uninhabitable.

This PAM system is not an independent system but a process to ensure that the instrumentation required for post accident monitoring is systematically identified and meets specific requirements. It makes maximum utilization of existing instrument loops of process, safety and safety-related systems for obtaining the necessary information. The components of instrument loops for PAM are essentially seismically and environmentally qualified in order to perform their own safety functions during the mission time as required by the applicable codes and standards (Reference 2). Where the existing loops with the necessary information are not covered for the sensing ranges to meet the PAM monitoring, these loops were upgraded to include post accident conditions. The upgraded loops are identified for each system designer to confirm and implement these new PAM requirements during detail design stages. Where the coverage of the sensing ranges and qualification requirements is not within existing equipment, some additional loops and instruments are installed to meet these requirements. These are in addition to as the referenced existing Wolsong Unit 1. Furthermore, always-available voice and site communication links are required by the operator to carry out the specific management of post accident activities. These necessary links utilize the plant telephone system inside and/or outside the plant, and then follow the plant emergency procedures.

As compared with American type PWR plants of which applicable codes and standards are based upon US NRC Reg. Guide 1.97, ANSI/ANS-4.5 and IEEE 497, the requirements for CANDU reactors are essentially the same approach but the detailed design implementation is slightly different due to the different Canadian reactor systems and reactor safety design principles.

2. Applicable codes and standards

CSA N290.6 (Reference 2) provides the basic requirements to provide rules and recommendations for the design, manufacture, installation and qualification of components for the PAM system. The general design principles and rules recommended by this standard are summarized below :

- The system design should be kept simple.
- Equipment accuracy and availability should be verified.
- Ensure that the system is not rendered inoperative by the specific design basis events.

- Design should facilitate maintenance.
- Same equipment as normally used.
- Design to avoid giving anomalous indication.
- Design to be clearly distinguishable to the operator.
- Design man-machine interface using ergonomic principles.
- Design to provide sufficient information chains to ensure independence, reliability and redundancy.
- Measuring ranges of instruments should be adequate to cover all the possible range of during and following the accident situation.
- Instruments should be qualified to remain in operation during and following design basis events.
- Design target of availability should be better than 99.0% on a parameter basis for information chains and power supply sources .
- No single information chain component failure should incapacitate any of the PAM parameters.
- An alternate information chain should always be available.
- The alternate chain components should be physically and functionally independent of each other.
- Verification of proper operation by means of on-line, off-line testing and/or comparing with alternate measurements at all time including post-accident should be provided.
- The ability foreplacement, repair, adjustment and calibration of components at full power should be considered.
- Easily distinguishable identification from other process system for components and modules in the form of nameplate tagging, color coding, physical positioning, etc. should be provided.
- Indications of displays and panel meters should be located close to the area where the operator performs his role, and always be visible to the operator.

3. PAM Design Basis Events

The design basis initiating the events for which PAM is required are based on the safety analysis reports carried out by plant safety design group for defined postulated events during plant operation. These design basis events are categorized as

follows depending on the total or partial failure and consequent threat to the integrity of 1) reactor fuel sheath, 2) primary heat transport system, and 3) the containment system, which provides the physical barrier preventing the release of radioactivity to the environment:

- Loss of coolant accident (LOCA) which directly affects on reactor safety.

- Loss of secondary side accident inside and outside containment which directly affects the loss of coolant heat sink :

    . Loss of feedwater accidents
    . Main steam pipeline breaks accidents

- LOCA plus Loss of emergency core cooling system which is the most serious postulated accident affecting reactor safety.

- LOCA plus Loss of normal electric power (called "class VI power") which could seriously affect reactor safety.

- Single fuel channel event which might be one of the following :

    . Stagnation feeder break accident
    . Pressure tube rupture accident
    . Channel flow blockage event
    . End fitting failure

- LOCA plus site design earthquake

- Design basis earthquake

It is noted that normal process upsets and minor events such as loss of pressure and inventory control of primary coolant, loss of reactor regulation, loss of forced flow and normal electric power are not considered as design basis events because these kinds of events are basically anticipated during normal operational plant transient and do not require post accident monitoring beyond what is already provided by normal existing monitoring means for these transients. In addition, common mode events such as fire, tornado, flooding, etc. are not treated as PAM events since the plants are normally designed for these common mode events by complementary safety design principles and guidelines, such as grouping and separation requirements and fire protection requirements.

The event sequences which are used to develop each of the PAM initiating events are also characterized chronologically for the predicted post accident conditions and thus establishes the determination of the nature and course of the accident. As an example of event sequences, a typical sequence of events of a large LOCA is shown on the Table 2. To meet this type of event scenario, the PAM mission time and parameters are selected and essentially determined.

From the PAM event sequences, the credited safety and safety related systems define its function following any specific accident. The system function to mitigate the accident are credited in safety analysis design by using analytical methodology.

In addition to the identification of the required safety and safety-related systems, the predicted PAM event sequences also reveal the required action to be undertaken by the operator. There are approximately 12 main courses of generalized operator actions to lead the plant to the final safety state even if most of plant safety systems are actuated automatically by the sensing of initiating conditions (Table 3). These generalized operator actions are also considered as the basis for the identification of information grouping associated with PAM parameters since for any operator action, only specific parameters may be required to monitor the accident trends. It is noted that not all instruments are required to be environmentally and seismically qualified for all events but are qualified for each credited event to ensure its functional capability following each of the design basis events.

4. PAM Design Implementation

As discussed above for the selection of PAM parameters, the main design factors are how to identify parameters properly by the indication of the conditions that pose a threat to the integrity of fuel sheath, primary heat transport system and containment following postulated accidents so that the operator would be able to adequately verify reactor shutdown, fuel cooling and heat removal, and containment radioactivity.

The reactor shutdown states are indicated by the reactor power measurements by means of in-core and out-core flux detectors. Fuel sheath failures are prevented by maintaining adequate fuel cooling which depends on the reactor power, the circulation of the coolant and the heat sink. The effectiveness of coolant circulation and heat removal is contingent on the operating condition of the primary heat transport system and verified via coolant pressure and temperature. The effectiveness of the heat sink would be mainly verified by the steam generator level and pressure or alternately by the shutdown cooling system when used for primary heat removal.

The integrity of the primary heat transport system boundary can fail as a result of overpressure, overheating or metallurgical degradation from postulated initiating events. The critical PAM parameters used to verify fuel cooling and heat removal, the integrity of primary heat transport system are the coolant pressure and temperature. Metallurgical degradation is usually a much longer term effect and should be treated as an operational issue.

The reactor building pressure and radioactivity parameters are used to button up the containment envelope. Radioactivity in the effluent streams reveals containment leakage or bypass. Monitoring of containment isolation status provides additional assurance of containment integrity.

In summary, the main PAM parameter sets are selected to verify the safety functions following postulated events via systematic coverage as derived from the PAM event sequences (see Table 1.) :

- Verification of reactor power,

- Verification of primary heat transport system pressure and temperature,

- Verification of steam generator pressure and level.

- Verification of reactor building pressure and radioactivity.

PAM design implementation consists of identification and verification of the selected parameters as required by applicable codes and standards. As already discussed, the design basis events and event sequences are categorized by the safety analysis design group and the identification of selected parameters are verified in order to make maximum utilization of existing instrument loops. These loops consist of signal sensing devices, signal transmitters (or signal conditioning devices), and indicators (panel meters) or display devices (computer CRT display) available in main control room and/or secondary control area. Each instrument loop is identified with the specified safety function of the instruments, the specified ranges for the instruments, and the specified postulated design basis scenarios and mission times for instruments and to which they must be qualified. The channelization of the information chains are finally examined with care to provide redundancy so that single component failure of each instrument will not deprive the operator of the PAM information. As a minimum, physical and functional separation are maintained between two redundant channels and if possible, diverse parameters for redundancy are preferred.

Operator-Machine interfaces are also part of design implementation of the PAM design. Colour-coded bezel of indicators (or display devices) around the meter in the main control room provide a contrast in appearance. Where the separate PAM indicators are adjacent to each other, a colour-coded group bezel with cutouts are provided around the indicators. Several plant communication systems such as the telephone and paging telephone system are designated to provide the main control room personnel with access in a diverse and redundant fashion to the various relevant plant and external personnel to enable actions requested b6y the operator to be carried out. The plant control computer, called as "Digital Control Computer", which mainly performs the plant control function as well as the display functions, provide the means to improve the Operator-Machine interfaces. Information is displayed on the operator console utilizing colour CRT screens. The computers can be interacted with by depressing either a dedicated function pushbutton or by using the "call any function" pushbutton so that an interrupt in the computer can execute the operator's request for the following functions:

- call up a display,

- revise some attribute of display, such as modify bar chart or trend display,

- enter numeric information,

- cancel entry or request,

- making hard copy of any information.

In the event that the main control room becomes uninhabitable due to such events as earthquake, smoke, fire, toxic gases, flooding, etc., adequate special safety back-up parameters are also displayed in the secondary control area to allow plant monitoring.

5. Operation of PAM

Under normal operation when all information chains are functioning properly, the operator can compare the redundant indications of each parameters. In the post accident situation, the appropriate emergency procedures would be followed for operators to take action for maintaining the plant in a safe state. The PAM indications must assist the operators in minimizing possible plant damage, and to allow the operator to return the plant to the normal state. In case of degraded operation, when one or more information chains are impaired, the readout from the failed chain will usually be irrational. If a discrepancy between two readings occurs, the operator could test the information chains or compare the readings with related variables to determine which one is correct. The maintenance action would be undertaken to repair the defective chains. In case of both plant computers failure (one is normal and the other is back-up operation), the fail-safe action would result in the loss of one of the redundant chains for PAM parameters. For this eventually a redundant analog meter indication is provided as backup.

6. Conclusion

From the above discussions, the PAM design implementation on Wolsong 2,3&4 is well established from the point of view of the design basis, approa operational requirements, and the applicable codes and standards. This PAM system st provide information which enables the operator to have an increasing role in managing the outcome of the event by continuously monitoring the plant critical safety parameters as the event progresses. At the start of an accident, it may be difficult for the operator to determine immediately what accident has occurred or is occurring, and therefore to determine the appropriate response. For this reason, plant safety systems are designed to perform automatically during the initial stages of any accident. Judging from various aspects of design implementation, the post-accident monitoring(PAM) system for Wolsong 2,3&4 is considered to effectively incorporate basic concepts of the applicable codes and standards, and to have an important role which enables the operation of manually initiated safety systems and other appropriate operator actions involved with systems important to safety.

7. References

1) 86-68930-DM-001, Design Manual for Post Accident Monitoring System of Wolsong NPP 2,3&4

2) CSA CAN3-N290.6-M82, "Requirements for Monitoring and Display of CANDU Nuclear Power Plant Stations in the Event of an Accident", National Standard of Canada

3) Wolsong Nuclear Power Plant Units No. 2/3/4, Final Safety Analysis Report (VOL. 5), 1995 May, Korea Electric Power Corporation

Table 1. Examples of PAM Variables and Safety Functions

VARIABLES	A	B	C	D	E
Primary Heat Transport Coolant System Pressure		X			
Primary Heat Transport Coolant System Flow		X			
Primary Heat Transport Coolant System Channel Outlet Temperature		X			
Primary Heat Transport Coolant System Pressurizer Level		X			
Primary Heat Transport Coolant System Storage Tank Level		X			
Neutron Flux	X				
Neutron Flux Rate of Change	X				
Shutdown System 1 Status	X				
Shutdown System 2 Status	X				
Containment Pressure			X		
Containment Temperature			X		X
Containment Activity				X	
Containment Isolation Status			X		
Containment Hydrogen Concentration			X		X
Containment Dousing Tank Level					X
Emergency Coolant Injection Heat Exchanger Outlet Temperature		X			
Emergency Coolant Injection Sump Level		X			
Emergency Coolant Injection Pressure and Flow		X			
Moderator Flow		X			
Moderator Temperature		X			
Steam Generator Pressure		X			
Steam Generator Water Level		X			
Deaerator Storage Tank Water Level		X			

Steam Generator Steam Relief Valve Status		X			
Emergency Water Supply Tank Level and Emergency Power Supply Status					X
Standby Electric Generator Status		X			X
Shutdown Cooling System Status		X			X

Where

A : Verification of reactor shutdown

B : Verification of reactor heat removal

C : Verification of a barrier to radioactivity release

D : Evaluation of radiological conditions

E : Assistance in carrying out recovery action.

Table 2. Event Sequence for Large LOCA

Time after Initiating Event	EVENTS
0-2 s	Power pulse
	Sharp increase in R/B Pressure [65 kPa(g)]
	SDS(s) activated
	Dousing spray system starts [14 kPa(g)]
	Containment isolation
2-10 s	Fission power decays below 10 %FP
	Fuel damage occurs
	PT/CT contact
10-900 s	Loop isol. activated - feed/bleed, pressurizer isolated
	LOCA signal activated - HTS pressure < 5.5 MPa(g)
	HPECC - Pressurize accumulators Open injection valves Open isolation valves
	MPECC - Open dousing tank isolation valves Open MPECC injection valves Start ECCS pumps Close HPECC valves when accumulator is empty
	Class III standby generator started by ECCCS
	SG crashcool activated
	HTS pumps tripped
	R/B pressure decrease
15 min - 1 day	LPECC
	R/B cooled by local air coolers
	Post-LOCA Instrument Air started by Operator
> 1 day	Post accident R/B depressurization (controlled release to environment)

Table 3. List of Generalized Operator Actions

No.	Operator Actions
1	Start EWS and EPS after LOCA/SDE or DBE
2	Establish Heat Sink (ECCS, SG, Moderator)
3	Open MSSVs after MSLB (or DBE)
4	Close Instrument Air to R/B
5	Start Shutdown Cooling System
6	Start D_2O Recovery System Dryers
7	Control Depressurization of Containment
8	Use HPECC to Break Rupture ECCS Discs for EWS after DBE
9	Initiate Controlled SG Cooldown
10	Terminate EWS Make-up Mode and Initiate Recirculation Mode
11	Maintain SG Level Manually
12	Provide EWS Flow to ECCS Heat Exchangers for LOCA/SDE When in EWS Mode