Verification of PRA Results by Applications in Full Scale Simulators

Cilla Andersson[a*] and Antanas Romas[b]
[a] Ringhals AB, Väröbacka, Sweden
[b] GSE Power Systems AB, Nyköping, Sweden

Abstract: In this paper a new method to verify the results of PRA models and find possible improvements to make the models more realistic is described. The main idea of the method, which has been denoted MCS2SIM, is to apply the PRA results of a nuclear power plant as an input to the full scale simulator which is used for the training of the operators at that plant. The PRA results, in the form of Minimal Cut Sets (MCS), are in most cases easy to translate into the equivalent malfunctions which are used in the simulator since the level of detail and realism in PRA models and full scale simulators often are similar. In the simulator the actual differential equations that are modeling the physical systems and phenomenon are solved which provides detailed information about the effect of different failure combinations (MCS) on the plant. By comparing the assumed consequences in the PRA models with the consequences that are calculated in the simulator and finding explanations for the observed differences a comprehensive verification of both the PRA models and the simulators can be achieved. The method can also provide insights about possible improvements of the models and be used to design advanced training scenarios for the operators.

At Ringhals unit 1 (BWR) and 3 (PWR) a couple of pilot studies have been conducted by Ringhals AB in cooperation with KSU AB and GSE Power Systems AB. Ringhals provided results generated by the plant specific PRA models, KSU supplied the full scale simulators and experienced simulator engineers that performed the tests while GSE developed an approach to make the application of the MCS2SIM idea possible and organized the pilot studies. Both system failures based on fault tree analysis in the PRA models and more complex scenarios based on event tree models have been translated to malfunctions and studied in the simulators. The results, observations, conclusions and recommendations based on the outcomes of these pilot studies are introduced in this paper. The main conclusion is that the pilot studies prove that the MCS2SIM method can give valuable insights about the PRA models that otherwise are difficult to find.

The limitations of the method are the lack of automated tools for the translation of the MCS results into malfunctions in the simulator and for effective analysis of the simulation results as well as the simulation time needed to run the long-term scenarios since the simulators are normally run in real time. However, these limitations can be resolved using modern technologies as is further discussed in the paper.

Keywords: PRA, Simulator.

1. INTRODUCTION

There are many similarities between a PRA model and a full scale simulator for a Nuclear Power Plant and the same level of detail is often used for the modeling of plant systems. Hence, it is possible to translate the PRA results, in the form of Minimum Cut Sets (MCS), to malfunctions in the simulator and compare the results. This can be used to verify that the models are correct and to find possible improvements. At Ringhals unit 1 (a BWR built by Asea-Atom) and unit 3 (a three loop PWR of Westinghouse design) a couple of pilot studies have been conducted by Ringhals AB in cooperation with KSU AB and GSE Power Systems AB. Ringhals provided results generated by the plant specific PRA models, KSU supplied the full scale simulators and experienced simulator engineers that performed the tests while GSE developed an approach to make the application of PRA results in the simulator possible and organized the pilot studies. Both system failures based on fault tree analysis in

* cilla.andersson@vattenfall.com

the PRA models and more complex scenarios based on event tree models have been translated to malfunctions and studied in the simulators. The results, observations, conclusions and recommendations based on the outcomes of these pilot studies are introduced in this paper.

2. DESCRIPTION OF THE METHOD

In a PRA model both fault trees and event trees can be evaluated separately and the final result of the calculations are often presented as Minimum Cut Sets (MCS) of failure events. In many cases these events can be directly translated into malfunctions that are used in the full scale simulators. Here, this process and the application of the malfunctions in the simulator have been denoted as the MCS2SIM method.

By applying the MCS2SIM method the following can be achieved:

- Comprehensive verification of the results produced by the PRA models
- Comprehensive verification of the full scale simulators
- Identification of unknown combinations of failures and testing of consequences of such combinations, which could be used as a decision making ground for modernisations or improvements in a plant
- Advanced training of operators based on the PRA results and confidence that the operators are trained correctly

3. TEST CASES AND RESULTS

The method has been tested on four scenarios for the two units Ringhals 1 (BWR) and Ringhals 3 (PWR).

3.1. System failure of the safety injection system in Ringhals 1

The first attempt to use the MCS2SIM method was to apply the results from a system analysis of the safety injection system at Ringhals 1 (R1) in the R1 simulator. For the test a failure combination of the two flow transmitters 323K301 and 323K302 was chosen which is of significant importance for the PRA results.

In the simulator there is a considerably higher number of available malfunctions than only “signal is not available” as the failure mode in the PRA was denoted. Hence as a first step an investigation was conducted of what kind of malfunctions of the transmitters that were critical. After the initial experiments it was concluded that if the signals, coming from the transmitters, would fail by indicating no current the consequences would not be significant but if the current of the signals would be too high, it can lead to total loss of the safety system.

The failure of the safety system is caused by the logics, controlling the valves 323V9 and 323V10, which will force these valves to close and the flow paths would be partially or fully blocked depending on the strength of the faulty signal. An important observation from the simulation of this event is that the operators would not be able to conclude that the system has lost its function since the instrumentation in the control panel will be indicating high or full flow by 323K301 and 323K302.

The next step was to investigate and simulate the consequences in case of a large LOCA during power operation in combination with malfunction of the flow transmitters. During the simulation it was concluded that the safety injection system would not be fulfilling its function to provide spray to remove the decay heat from the core. The water level in the core would be dropping and result in core damage if no other system would be capable to supply water into the core region.

From the test case the following could be concluded:

- Verification of the PRA is possible to conduct. The test confirmed that the safety injection system will fail if the two transmitters 323K301 and 323K302 are indicating high flow incorrectly.
- In a simulator it is possible to understand and analyse the actual failure mechanisms created by the combinations of malfunctions.
- In a simulator an assessment if the operators would be capable to diagnose the scenario correctly and be able to take corrective actions can be made. In the current case there is a significant risk that the operators would not be capable to identify the failure. Hence no corrective manual actions would be taken to prevent system failure. If on the other hand the operators would be able to identify the problem they could bypass the automatics and open the valves blocking the spray flow manually. This indicates that it might be a good idea to train the operators to verify critical safety systems using alternative information like level behaviour in the RPV and indications of stem positions of the valves.

3.2. System failure combined with loss of offsite power at Ringhals 1

The second test with the MCS2SIM method was also conducted in the simulator of Ringhals 1 but this time the failure combination from the previous test was studied together with the initiating event loss of offsite power during power operation, failure of pump P1 in the auxiliary feed water system and stop of diesel generator 651DG160 within the first two hours.

During the first simulator run the results indicated that pressure relief system 314 was responding incorrectly during the transient which resulted in a less severe situation inside the RPV. The model of the logics, controlling system 314, was corrected and the simulations were repeated. This time the simulation indicated that the scenario would result in a very low level in the downcomer of the RPV, which is monitored in the panels in control room. However, the fuel should not be severely damaged. The maximum fuel temperature was not plotted during the simulation but no considerable increase of the fuel temperature was observed at any time point. The fuel temperature was maintained reasonably low due to intensive boiling at the lower part of the core and by cooling of the upper part due to a flow of a mixture of steam and water droplets. The reason that this scenario does not result in core damage is that the turbine driven pump in the auxiliary feed water system starts to operate and is feeding water into the RPV. For some reason this was not credited for this scenario in the PRA.

This test case clearly shows that a comprehensive verification of both PRA results and of the response of simulator can be achieved by MCS2SIM. Here the faulty response of the simulator was detected and the logic was improved. Further it was discovered that the auxiliary feed water system was not credited as it should for this sequence in the PRA.

3.3. System failure in the residual heat removal system at Ringhals 3

The MCS2SIM method was also tested in the simulator of Ringhals 3 by studying a system failure in the residual heat removal system. An MCS consisting of failure of the two pumps 715ASWAPCW-02 and 715ASWAPCW-04 was chosen for the test.

For the test in the simulator initial conditions for shutdown operation conditions were used. At these conditions the residual heat removal system is in operation and is the main heat sink removing the decay heat.

The simulation was started by operating all the pumps in the saltwater system 715 and by reaching steady-state operation of the plant. Later malfunctions to fail the two pumps 715ASWAPCW-02 and 715ASWAPCW-04 were activated. After the time point 17:33 the simulation was extended by defining extra malfunctions standing for unavailability of all four pumps. In that case it was possible to conclude that the system function would be lost and that the temperature in the RPV would start to rise. The simulation was also indicating the rate of temperature increase which is information that can be used to assess the time frame during which the system function must be restored.

From this test it was possible to conclude that the success criteria in the PRA model, where two pumps in the same train are required, are too conservative in this case. Another important conclusion is that the simulation results can provide reliable information about the available time interval in which preventive actions must be taken before severe consequences or damages would start occurring.

3.4. System failure combined with loss of offsite power at Ringhals 3

In the last test case the initiating event loss of offsite power during power operation was studied in combination with failure to initiate island mode operation and common caused failure (CCF) of the batteries in system 663.

It was expected that this combination of malfunctions would result in core damage if no actions would be taken to restore the residual heat removal and water supply to the RCS. In the simulator a trip of the reactor is activated as a first response to the initiating event and the reactor coolant pumps (RCPs) are stopped. The diesel generators are failing to start due to the failure of the batteries and hence all systems, supplying water to the RCS and steam generators, are unavailable. The only possible water supply is water pumped by the steam driven pump to one of the steam generators. After approximately two hours the other two steam generators are almost empty while the third steam generator is fully filled with water pumped by the steam turbine driven pump. Overfilling of the full steam generator could possibly cause mechanical failure of the steam turbine but the simulation model of the steam turbine is not accounting for such failure and is responding only to the thermodynamical properties of the mixture supplied from the SG2 and SG3. This is recognised as a limitation in the simulation model and it will be studied if this should be extended to account for possible mechanical failures if water is damaging the turbine blades. During this scenario the water from the RCS is leaking continuously via the RCP seals. That leakage is caused by loss of the RCP cooling and sealing system due to the loss of all AC power. The consequences of this leakage are that the pressure and level in the RCS are decreasing continuously. After some time boiling is established in the RCS, which is maintaining a more constant pressure. However, the water level continues to decrease and results in loss of natural circulation when the water level in the RPV is reaching the level of the upper point of the loop-piping elevation. Steam will be getting into the U-Tubes and create gas pockets in the top part that will break the circulation. The consequence of losing the natural circulation is that from that point heat removal by the full steam generator will no longer be possible even if the steam driven pump would still be available. After the last heat sink is lost the temperature in the core starts to rise considerably faster by evaporating the last water left in the RCS and core damage will occur.

The simulation is also indicating that most of the instrumentation in the control room will be unavailable if this failure combination would happen. Hence the operators would not have any information about the state of the plant and it would be difficult to diagnose and start the vital systems needed for the protection of the core against overheating.

4. IMPROVEMENTS REQUIRED FOR EFFECTIVE FUTURE USAGE OF THE METHOD

Although the pilot tests showed that it is possible to apply PRA results in the simulators it was time and labour consuming. Hence, a number of possible improvements were noted which can make usage of the MCS2SIM method more efficient.

There are thousands of variables in the full scale simulators and only experienced simulator engineers can identify, understand and interpret the state of the plant during the simulation. Such analysis has to be made more manageable for non-simulator specialists. To do this an artificial intelligence tool for diagnostics and analysis that is capable to perform the operations defined below is required.

- Automatically convert an MCS list to the equivalent malfunctions in the full scale simulators.

- Prepare simulation scenarios according to the scenarios described in the MCS list and execute the simulations of the scenarios including applications of different malfunctions as a function of time. As an example it can be required to stop a diesel generator after 2 hours of operation or simulate failure of steam driven auxiliary feedwater pump after 3 hours.

- Sample values of predefined important parameters that can indicate the state of the plant during the simulation. The system must be capable to make an analysis of such parameters and report important information automatically in the form of tables and comments generated by the predefined artificial intelligence. For example if the core thermal-hydraulics model is indicating that the temperature of the cladding is close to the 900 C in any of the calculation nodes it should generate a warning – "High cladding temperature is reached and there is a risk for Zirconium and Water reaction!".

- The application must be capable to generate reports in Word, Excel or PDF summarizing the computer based analysis and plot the pre-selected main parameters that would visualize the state of the plant during the simulation of the scenarios.

Another important finding is that it becomes time consuming if simulators are operated in the real time operation mode (RTEXEC-mode) during the analysis of initiating events like loss of offsite power. Therefore it might be preferable to be able to run simulators in IEXEC-mode and perform the calculations faster than in real time.

Simulators and TUSS systems are usually used for other purpose than use of MCS2SIM and the accessibility of the simulation systems might be limited due to training sessions and modernizations of the simulators. However, this limitation could be overcome by making a copy of the TUSS-system. Such copy of TUSS could be dedicated for the MCS2SIM analysis and operated unmanned by the artificial intelligence application, which would run pre-selected scenarios and perform automated analysis. The analysis results could then be reviewed by the safety analysts. If any important findings would be detected by the automated system the safety analysts would be able to find it from the available information and perform detailed studies manually.

Another limitation, discovered during the pilot tests, is that most of the simulators can not be operated in severe accident conditions after the deformations and melting points are reached. The reason for that is that models of reactors are designed without including the severe accident simulation codes like MAAP or MELCOR. In Sweden it is only the simulator for Ringhals 2 which is capable to handle severe accident scenarios since it has been upgraded to operate using the MAAP5 code. During the severe accident simulation, after the maximal fuel temperature is reaching 1400 K, the ordinary RCS simulation models are turned off and MAAP5-calculations are introduced. Such installation could be used for complete MCS2SIM studies without making too many assumptions.

5. CONCLUSIONS

Based on the pilot cases a number of conclusions can be drawn concerning the usage of the MCS2SIM method. The most important one is that it is possible to translate most of the MCS from a PRA into malfunctions that are used in the simulators which makes it possible to simulate equivalent scenarios. The simulations of the failure scenarios, defined by the MCS lists, are providing valuable information about the physics of the failure mechanisms and the severity of the consequences. By studying the results it is possible to identify weaknesses and errors both in the PRA models and in the simulators as was illustrated by the pilot cases.

The method can be a valuable tool in the identification of complex failure scenarios and in the training of operators to deal with such scenarios. A simulator is an excellent environment to use to identify if certain combinations of failures would result in warnings, informing operators about the presence of the problems, or if these would stay hidden and can be considered as hazardous latent problem. Experienced operators could be asked to participate in such exercises in the simulators and based on their performance it can be deduced if there is a need for more comprehensive warnings or alarms.

Form the pilot applications of MCS2SIM it was also concluded that some technical improvements, as the ones discussed in this paper, are required to make this method effective and easy to apply by safety analysts who are not experienced simulator engineers.