Development of a Diversity and Defense-In-Depth Strategy for the CNNC Fuqing and Fangjiashan Nuclear Plants

Gershon Shamay
RPS/ESFAS System Development Lead
Schneider Electric
26561 Rancho Parkway South
Lake Forest, CA 92630
Gershon.shamay@schneider-electric.com

Jerry Mauck
JLM Engineering and Technology Resources
5234 Green Bridge Road
Dayton, Maryland 21036
jerrymauck@verizon.net

Michael Howard
Principal Engineer, Safety & Transient Analysis
CSA Inc.
855 N. Capital Ave., Suite 1
P. O. Box 51596
Idaho Falls, ID 83405
mhoward@csai.com

Edward L. Quinn
ANS Past President
Technology Resources
23292 Pompeii Drive
Dana Point, CA 92629
tedquinn@cox.net

INTRODUCTION

The purpose of this paper is to provide an overview of the development of the Diversity and Defense-in-Depth (D3) strategy for the China National Nuclear Corporation Fuqing, Fangjiashan and Hainan Nuclear Plants. The Nuclear Power Plant (NPP) Digital Control System (DCS) and advanced control room design is currently being completed by Invensys and China Nuclear Power Engineering (CNPE)/Nuclear Power Institute of China (NPIC) for these eight new Chinese built Pressurized Water Reactor plants. The DCS design and configuration is based on standard digital control products designed and manufactured by Invensys and its industry partners. The control systems (Triconex "Tricon" and Foxboro "I/A") making up the DCS system have been selected because of their applicability to the functionality required by People's Republic of China nuclear regulations, CNPE performance requirements and desired system functionality. The installation of digital based systems in the Reactor Protection System (RPS) and other systems throughout the NPP enhances safety in many areas when compared to the older analog instrumentation based systems.

The Fuqing, Fangjiashan and Hainan RPS design incorporates the Reactor Trip System (RTS) functions, the Engineered Safety Feature Actuation System (ESFAS) functions and Post Accident Monitoring System (PAMS) functions. The installation of a digital based RPS that includes all this functionality within a single design presents a licensing challenge in that a postulated Software Common Cause Failure

(SWCCF) on the digital platform might propagate in a manner that defeats the required safety functions. The Invensys D3 evaluation describedherein has demonstrated that there is sufficient defense-in-depth and diversity to cope with a postulated SWCCF to the Tricon digital platform in the RTS, ESFAS, PAMS and the applicable Augmented Quality control systems. The Chinese regulator, The National Nuclear Safety Authority (NNSA) has approved the Diverse system installation for Fuqing 1 and the reactor went critical on 07/24/2014.

DESCRIPTION OF THE DEFENSE-IN-DEPTH AND DIVERSITY ASSESSMENT

The defense in depth assessment considers four echelons of defense,

1. Non-safety plant control systems,
2. RTS,
3. ESFAS, and
4. Monitoring and indicator system

These echelons are further discussed and defined in NUREG/CR-6303 (Reference 1).

The possibility of a common cause resulting in failures to more than one echelon of defense is the primary concern in considering postulated failures. These postulated failures affecting multiple echelons of defense can be caused by interdependencies between these echelons. Accordingly, the problem becomes one of specifying the degree of dependencies since it is impossible to have four completely independent echelons when certain features must be shared due to the commonality of the Instrumentation and Control (I&C) equipment and personnel. Physical and electrical independence is only one of the dependencies considered in the analysis. A second interdependence is associated with failures caused by common hardware features such as power supplies, sensors or other equipment. A third interdependence is shared software that can lead to failures between the echelons, hence a SWCCF.

The Tricon platform incorporates several design measures for error avoidance and fault tolerance that both prevent and minimize the consequences of a postulated Tricon SWCCF. Primarily, the inherent quality built into the Tricon software development methodology prevents, with a very high probability, software failures from occurring. One of these design measures is that the Tricon controllers operate asynchronously so that there are no time dependencies between systems or redundant channels. It should also be noted that safety related qualification and in-service testing afforded by the Tricon system minimizes the probability of failures of all types. Further, the Tricon and I/A digital I&C systems are designed so that challenges to the safety and non-safety I&C systems occur at a significantly low rate. Therefore, each RTS or ESFAS protection or mitigation function credited in the safety analyses remains available from Tricon with the same or better degree of reliability than from other digital or analog-based control and protection systems.

The main objective of the Fuqing and Fangjiashan D3 Assessment Report is to determine the vulnerability of the RTS and ESFAS to a postulated SWCCF on the Tricon platform by performing a systematic assessment of the proposed architecture. If design features are identified which are susceptible to SWCCFs and impact the safety analysis, then:

- the architecture must be modified to remove the design aspects vulnerable to a common cause failure, or
- the design must be modified to compensate for the identified vulnerabilities by implementing Diverse Actuation System (DAS) functionality which includes ATWT functionality, or

- best-estimate analyses must be performed to demonstrate the resultant plant response to the licensing basis anticipated operational occurrences (AOOs) as well as the postulated accidents presented in the plants' Preliminary Safety Analysis Report (PSAR) meet the acceptance criteria outlined in BTP 7-19 (Reference 2).

Guidance presenting both the methodology and acceptance criteria for D3 assessments in support of the implementation of digital based systems in the RTS and ESFAS at either operating or new nuclear power plants has been established. NUREG/CR-6303, BTP 7-19, and NRC ISG-02 (Reference 3) document the methodology and acceptance criteria supporting DCS implementation. Based on the Nuclear Regulatory Commission's position documented in BTP 7-19, the goal of the D3 assessment is to determine and correct potential vulnerabilities to undetected software common mode failures occurring with potential initiating events (PIEs). In addition, the goal of the D3 assessment is to ensure that automatic protective system response and/or operators manual actions have sufficient diverse instrumentation to support successful mitigation of the event. Effects of the combined initiating event resulting in a transient and SWCCF, including the sequence of events, are evaluated based on realistic assumptions.

The D3 assessment process is reduced to three major process steps. The first step is to determine the susceptibility of the safety systems to postulated software common cause failures. This step is accomplished by reviewing the overall I&C architecture including both safety and non-safety systems. The architecture is divided into the four echelons as discussed above. The object of dividing the plant I&C systems into echelons is to segregate the equipment by function and then to place them into the pertinent diverse blocks. The purpose of the blocks is to determine which of the systems may fail given a Tricon platform SWCCF and which systems will continue to be available. The systems that are determined to continue to be available could be either safety or non-safety and include all passive systems. In addition, diverse manual actuations can be credited as long as the necessary time is available and the proper indications and alarms are available given the SWCCF. To accomplish the block segregation, the diversity between the digital platforms is analyzed in accordance with the guidance of NUEG-6303. The goal of the analysis is to establish an acceptable level of diversity between each block based on six forms of diversity listed in NUREG/CR-6303. This is where the diversity between the components are examined, i.e., the Tricon and I/A digital platforms. For the case of the Fuqing, Fangjiashan and Hainan analysis, acceptable diversity levels were found between Tricon and I/A.

The second major step is to perform a best-estimate evaluation of the licensing basis event analyses to determine the sequence of events when including only the safety systems not impacted by the postulated SWCCF and the estimated timing of manual operator actions. This task was accomplished by first identifying the events presented in Chapter 15 of the Fuqing and Fangjiashan PSAR. Secondly, a review and evaluation of these Chapter 15 events for relevance to the D3 analysis is undertaken. Events reliant upon concurrent initiating events were eliminated from the assessment list based on the best-estimate evaluation approach.

After choosing the events to be evaluated, a realistic sequence of events was determined. Note that the sequence of events for each event as shown in the PSAR was based on conservative licensing basis assumptions such as including a loss of offsite power, single failure assumption, stuck rod, etc. As part of a best-estimate evaluation approach, the plant initial conditions would be less severe than those analyzed in the PSAR and non-safety related systems would be credited to mitigate the consequences. Accordingly, the resulting event conditions for the best-estimate evaluation are less severe than the results presented in the PSAR.

The impact of the SWCCF to the Tricon based RPS, i.e., essentially all RPS functions are unavailable, was evaluated based on the sequence of events developed as described, above. The main objective was to determine the timing of occurrence of key phenomena that could impact the progression of the accident scenario. Examples include items such as the availability of reactivity management during a main steamline break event and the onset of a Doppler feedback power reduction during a rod ejection event. After the evaluation of the sequence of events was performed, if automatic safety or non-safety related functions were unavailable, a determination of available operator actions was made which could mitigate the postulated event with a concurrent SWCCF. Successful mitigation was based on not exceeding the acceptance criteria outlined in BTP 7-19. This task relies on experience and engineering judgment to determine a more realistic sequence of events and to be able to identify which available control systems, functions and manual operator actions can be credited to mitigate the event.

The best-estimate approach requires that a decision be made as to whether the current acceptance criteria as listed in the PSAR should be maintained, or whether alternate acceptance criteria should be proposed based on BTP 7-19. This decision potentially has an effect on the time available for the operator to recover the plant and is also dependent on whether or not dose analysis will be performed in support of the best-estimate analyses. In the scope of work supporting the Fuqing and Fangjiashan plants, the current acceptance criteria for each of the PSAR events are maintained, with appropriate exceptions noted. The exceptions include a) no significant fuel damage (DNB> safety analysis limit), and b) Reactor Coolant System pressure less than ASME Boiler and Pressure Vessel Level C service limits. These criteria are consistent with those used in the best-estimate analysis of the beyond design basis ATWT event applicable to the Fuqing and Fangjiashan plants and are applied to specific PSAR event analyses where appropriate.

For the third step, the results of this assessment are placed into categories that distinguish how the event can be mitigated, or in certain cases identify that it cannot be mitigated with the current design. The events that cannot be successfully evaluated to meet the acceptance criteria given the DCS design are specified for further evaluation. At the same time, the protective features that would be required to meet the acceptance criteria are outlined to specify a preliminary DAS. This includes both the automatic and manual functions along with the related input parameters required for each function. This provides the specification of a conservative DAS system that may be reduced in functionality after the best-estimate modeling of the selected group of events has been completed. The D3 assessment report is segmented into four classifications of diverse actions:

1) diverse automatic actuations and initiating parameters,
2) system level manual actuations and the necessary indications and alarms for the operator to take action,
3) component manual actuations where the known time is such that the actions can be taken, and
4) a select group of diverse indications and alarms which are needed so that the operator can successfully manipulate the plant to a safe shutdown condition given the initiating events in conjunction with the SWCCF.

For each event, knowing the required operator actions for items 2) and 3) above is necessary to determine if the operator can successfully mitigate an event based on manual actions. The following questions must be addressed in making this determination.

a) Does the operator have sufficient indication to take the appropriate actions? Is the appropriate instrumentation available and functioning?

b) Do operating procedures provide adequate guidance?

c) Does the operator have adequate training?

d) Does the operator have sufficient time?

The D3 report provides the summary results of the qualitative analyses for each postulated initiating event. The resulting mitigation category for each event and the necessity for operator actions and alternate mitigation functions, are provided. The D3 report breaks down each of the PIEs that require additional analysis and details the mitigating diverse actuation functions for each. As noted above, this results in the preliminary DAS design that may be reduced in functionality following completion of the evaluation process, which may include best-estimate analyses.

After the categorization of all of the evaluated events, Phase 1 of the Fuqing and Fangjiashan D3 report was essentially completed. The next phase of the D3 assessment, Phase 2, performed an additional assessment on all events identified to require further evaluation, either by performing a quantitative analysis, event simulation, plant modification, risk-based analysis or other resolutions. Completion of this assessment resulted in demonstrating that these events are either bounded by a more limiting event, are protected by a diverse automatic DAS function or mitigated by manual operator action. Phase 2 identified and resolve all remaining concerns by addressing any event in which the results of the qualitative defense-in-depth and diversity study showed that the plant design was questionable with respect to withstanding a SWCCF. The results of the best-estimate modeling and manual operator action analysis enabled the crediting of certain systems and manual actions discussed in the D3 report as being available to mitigate the event. The final results provided a DAS design that is smaller in size than the preliminary design presently depicted in the D3 report and results in a D3 verification report including the final DAS design. The Chinese regulator, The National Nuclear Safety Authority (NNSA) has approved the Diverse system installation for Fuqing 1 and the reactor went critical on 07/24/2014.

CONCLUSION

The Fuqing and Fangjiashan D3 assessment has demonstrated that there is sufficient diversity and defense-in-depth to cope with a postulated SWCCF to the Tricon digital platform in the RTS, ESFAS and the augmented quality systems. It has been determined that even with a postulated SWCCF there are adequate defenses and diversity in the digital I&C architecture to meet the applicable acceptance criteria when supplemented with a DAS that includes the functions of the existing ATWT systems as well as those described in the D3 report. The DAS provides non safety-related RTS functions, ESFAS functions, and operator displays and alarms. In the DAS, both automatic and manual means are provided to trip the reactor and actuate selected ESFAS functions. The DAS is specifically implemented in hardware and software that is diverse from the primary RTS and ESFAS.

The final configuration for the DAS diverse automatic mitigating functions has been determined based upon the completion of the best-estimate modeling. The result of this effort has identified acceptable automatic actuation functions including setpoint selection. It also has been used to support manual operator actions discussed in the individual event discussions, thereby eliminating automatic actions for selected cases. The Chinese regulator, The National Nuclear Safety Authority (NNSA) has approved the Diverse system installation for Fuqing 1 and the reactor went critical on 07/24/2014.

REFERENCES

1) NUREG/CR-6303, "Method of Performing Diversity and Defense-In-Depth Analyses of Reactor Protection Systems, October, 1994.

2) NRC Standard Review Plan, NUREG-0800 Chapter 7 and BTP-7-19, Rev 5

3) DI&C ISG-02, DI&C Task Working Group TWG #2, Diversity and Defense-In-Depth Issues, Interim Staff Guidance (ISG), Rev 2, June 5, 2009