# Development of a Diversity and Defense-In-Depth Strategy for the TerraPower TWR-P Advanced Nuclear Power Plant

**Baofu Lu**
*I&C Systems Development Lead*
*TerraPower*
*330 120th Avenue, NE, Suite 100*
*Bellevue, WA 98005*
*blu@terrapower.com*

**Eric Williams**
Manager, Reactor Safety and Plant Control
TerraPower
330 120th Avenue, NE, Suite 100
Bellevue, WA 98005
ewilliams@terrapower.com

**Jerry Mauck**
*TechnologyResources*
*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*

**Richard Wood**
*Professor*
*University of*
*Tennessee*
*Pasqua Nuclear*
*Engineering Building*
*1004 Estabrook Road*
*Knoxville, TN 37996*
*rwood11@utk.edu*

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

## ABSTRACT

A Diversity and Defense in Depth (D3) analysis was performed for the Traveling Wave Reactor, which is a Generation IV fast reactor design. The analysis demonstrated that the current I&C design for TWR-P provides sufficient diversity in the reactor shutdown system, the engineered safety features, and the post-accident monitoring system. In addition, an analysis was performed for the Embedded Digital Devices (EDD) to ensure a postulated Software Common Cause Failure (SWCCF) will not affect the safety functions of the TWR-P I&C system.

## 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 TerraPower Traveling Wave Reactor-Prototype (TWR-P) Advanced Nuclear Power Plant. The TWR-P Digital Control System (DCS) is currently being designed by TerraPower. The Instrumentation and Control (I&C) design and configuration were based on standard digital control products. The control systems making up the DCS were selected because of their applicability to the functions required by TerraPower and the United States Nuclear Regulatory Commission (USNRC)**.** The installation of a digital-based Plant Protection System (PPS) and other systems throughout the TWR-P enhances safety in many areas when compared to the previous generation of analog-based instrumentation systems.

The TWR-P PPS design incorporates the Reactor Shutdown System (RSS), the Engineered Safety Feature Actuation System (ESFAS) and Post-Accident Monitoring System (PAMS) functions. The installation of a digital platform PPS that includes all the safety-related functionality 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 TWR-P D3 evaluation described in this paper has demonstrated that there is sufficient defense-in-depth and diversity to cope with a postulated SWCCF to the two safety platforms in the RSS, ESFAS and the applicable Augmented Quality control systems.

A recently issued Regulatory Issue Summary (RIS) RIS-2016-05 identified concerns associated with Embedded Digital Devices (EDD) and states they should be part of the overall D3 analysis. As a result, the prospective use of these devices was treated in the TWR-P D3 analysis and the potential impact of a SWCCF is discussed for each of the identified EDD categories.

## DESCRIPTION OF THE DEFENSE-IN-DEPTH AND DIVERSITY ASSESSMENT

The defense-in-depth assessment considered four echelons of defense, as discussed and defined in NUREG/CR-6303 (**Ref. 1**).

1. Non-Safety plant control systems
2. Reactor Trip System (RTS)
3. ESFAS
4. Monitoring and indicator system

The possibility of a common cause resulting in failures to more than one echelon of defense was 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 I&C equipment and personnel. Physical and electrical independence represents only one of the dependencies considered in the analysis. Another interdependence evaluated is shared software that can lead to failures between the echelons, hence a SWCCF.

The installation of a digital-based PPS that includes the Reactor Trip functions and the ESFAS functions presents a licensing concern that a postulated SWCCF of the digital platform might propagate in such a fashion that defeats the required safety functions. Furthermore, there is a concern that using the same digital platform in non-safety systems can result in accidents or transients that are outside the boundaries of those events discussed in the current Safety Analysis. The D3 evaluation described in this paper is intended to demonstrate that there is sufficient defense-in-depth and diversity to cope with a postulated SWCCF for the TWR-P digital platform in the RSS and the ESFAS and the other applicable safety and non-safety control systems.

D3 evaluations are usually accomplished with the addition of a Diverse Actuation System (DAS) that automatically actuates Reactor Trip and some selected ESFAS functions using a select group of input parameters and a diverse I&C platform. The DAS performs the required actuations upon failure of associated digital PPS (RSS and ESFAS) functions. NRC Branch Technical Position (BTP) 7-19, (**Ref 2**) allows credit for certain manual actuations using diverse indicators to guide the operator, for proper operation of an anticipated Trip without Scram/Trip (ATWS/ATWT) system, and for proper operation of all digital platforms outside the one being evaluated.

## TWR-P D3 ASSESSMENT

The main objective of the TWR-P D3 Assessment was to determine the vulnerability of the RSS/RTS and ESFAS to a postulated SWCCF on the digital platform by performing a systematic assessment of the proposed architecture. If design features were identified as being susceptible to SWCCFs and impact the Safety Analysis, then the following actions were considered:

- The architecture was modified to remove the design aspects vulnerable to a common cause failure, or
- The design was modified to compensate for the identified vulnerabilities by implementing DAS functionality which includes ATWT functionality, or
- Best-estimate analyses were 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' Safety Analysis meet the acceptance criteria outlined in BTP 7-19 (**Ref. 2).**

Guidance presenting both the methodology and acceptance criteria for D3 assessments in support of the implementation of digital based systems in the RSS and ESFAS at either operating or new nuclear power plants has been established. NUREG/CR-6303 (**Ref. 1**), BTP 7-19 (**Ref. 2)**, and NUREG/CR-7007 (**Ref. 3)** document the methodology and acceptance criteria supporting DCS implementation. Based on the USNRC position documented in BTP 7-19 (**Ref. 2)**, the goal of the D3 assessment was to determine and correct potential vulnerabilities to undetected software common mode failures occurring with potential initiating events. In addition, the goal of the D3 assessment was to ensure that automatic protective system response and/or operator 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, were evaluated based on realistic assumptions.

The D3 assessment process was reduced to three major process steps. The first step was to determine the susceptibility of the safety systems (PPS) to postulated SWCCF. This step was accomplished by reviewing the overall I&C architecture including both safety and non-safety systems due to the potential correlation between these systems. The architecture was divided into the four echelons as discussed above. The objective of dividing the plant I&C systems into echelons was to segregate the equipment by function and then place them into the pertinent diverse blocks. The purpose of the blocks was to determine which systems may fail given a digital platform SWCCF, or any other plant software failure, and which systems continue to be available. The systems that were determined to be available could be either safety

or non-safety and include all passive systems. In addition, diverse manual actuations were credited as long as the necessary time was available and the proper indications and alarms were available given the SWCCF. To accomplish the block segregation, the diversity between the digital platforms was analyzed in accordance with the guidance of NUREG/CR-6303 (**Ref. 1**) and NUREG/CR-7007 (**Ref. 3)**. The goal of the analysis was to establish an acceptable level of diversity between each block based on six forms of diversity listed in NUREG/CR-6303 (**Ref. 1**). This was where the diversity between the components was examined, i.e., the microprocessor and Field Programmable Gate Array (FPGA) platform and non-safety digital platforms. For the case of the TWR-P analysis, acceptable diversity levels have been found between the PLC, FPGA and plant control platforms.

The second major step was 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 TWR-P licensing basis. Secondly, a review and evaluation of these Chapter 15 events for relevance to the D3 analysis was 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 for each event was based on conservative licensing basis assumptions such as including a loss of offsite power, single failure, stuck rod, etc. As part of a best estimate evaluation approach, the plant initial conditions would be less severe than those analyzed and non-safety related systems would be credited to mitigate the consequences. Accordingly, the resulting event conditions for the best estimate evaluation were less severe than the Safety Analysis.

The impact of the SWCCF to either of the diverse platforms, the microprocessor or the FPGA based PPS (i.e., essentially all PPS functions are unavailable under one of the platforms) was evaluated based on the sequence of events developed as described above. The main objective was to determine the timing 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 steam line break event and the onset of a Doppler feedback power reduction during a rod ejection event. After the evaluation of the sequence of events, if automatic safety or non-safety 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 (**Ref. 2)**. This task relied on experience and engineering judgment to determine a more realistic sequence of events and identify which available control systems, functions and manual operator actions could be credited to mitigate the event.

The best-estimate approach required that a decision be made as to whether the current acceptance criteria as listed in the TWR-P licensing basis should be maintained, or whether alternate acceptance criteria should be proposed based on BTP 7-19 (**Ref. 2)**. 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 this D3 analysis, the current acceptance criteria for each of the TWR-P licensing bases events was maintained.

For the third step, the results of this assessment were placed into categories that distinguish how the event can be mitigated, or in certain cases identified 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 were specified for further evaluation. At the same time, the protective features that would be required to meet the acceptance criteria were outlined to specify a preliminary DAS, if required. This included both the automatic and manual functions along with the related input parameters required for each function. This provided the specification of a potential conservative DAS system that may be reduced in functionality after the best- estimate modeling of the selected group of events has been completed, if required. 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 was necessary to determine if the operator can successfully mitigate an event based on manual actions. The following questions were addressed in making this determination.

- Does the operator have sufficient indication to take the appropriate actions?
- Is the appropriate instrumentation available and functioning?
- Do operating procedures provide adequate guidance?
- Does the operator have adequate training?
- 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, the preliminary results concluded that the TWR-P design has sufficient diversity in the two safety platforms to meet the acceptance criteria without the addition of a DAS.

All known safety EDDs were analyzed for their impact to the safety analysis upon a postulated SWCCF to each EDD system software block. Based upon this EDD analysis, it was concluded that these SWCCFs were within the envelope of the existing TWR Safety Analysis. As the TWR design is finalized, additional EDDs could be added as the TWR-P design is finalized and will be analyzed for their safety impact at that time.

After the categorization of all of the evaluated events, the preliminary TWR-P D3 report has been completed. The next phase of the D3 assessment is to perform an additional assessment on all events identified to require further evaluation found in the current analysis, either by performing a quantitative analysis, event simulation, plant modification, risk-based analysis or other resolution. Completion of this assessment will demonstrate that these events are either bounded by a more limiting event, thus protected by a diverse automatic function embedded in the design, or successfully mitigated by manual operator actions. The next phase analysis is intended to identify 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 should enable the crediting of certain systems and manual actions discussed in the D3 report as being available to mitigate the event. After these steps, a final D3 report will be issued that includes the quantitative review performed by TerraPower and will be ready for submittal to the appropriate owner and regulatory agency.

## CONCLUSION

The TWR-P D3 assessment has demonstrated that there is sufficient diversity and defense-in-depth to cope with a postulated SWCCF to the digital platforms in the RSS, ESFAS and the augmented quality

plant control systems. It has been determined that even with a postulated SWCCF there are adequate defenses and diversity in the current digital I&C architecture to meet the applicable acceptance criteria. The final D3 analysis results will be ready for submittal to an owner and associated regulatory agency in the future.

## REFERENCES


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

**2)** NRC Branch Technical Position BTP 7-19, Rev 6

**3)** NUREG/CR-7007, " Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems", February, 2010

**4)** Regulatory Issue Summary (RIS) RIS-2016-05