RECENT RESULTS FROM A TESTBED FOR THE RELIABILITY OF THE DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS AND CYBER-SECURITY IN NUCLEAR POWER PLANTS

Yongkyu An, Calogero Sollima, and Rizwan-uddin
Department of Nuclear, Plasma, and Radiological Engineering
University of Illinois at Urbana-Champaign
104 S. Wright Street, Urbana, IL
an24@illinois.edu; csollima@illinois.edu; rizwan@illinois.edu

Daniel Chen and Zbigniew Kalbarczyk
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
1308 W. Main Street, Urbana, IL
dchen8@illinois.edu; kalbarcz@illinois.edu

ABSTRACT

Transition from analog to digital instrumentation and control systems requires a systematic study of the modifications, and assessment of their reliability. Such studies are often carried out on a test bed. The test bed developed earlier includes a commercially available triple modular redundant (TMR) programmable logic controller (PLC) for testing not only the reliability of the digital I&C but also the cyber-security of the system during plant operation. This paper reports results of our preliminary analyses carried out using the test bed following the injection of faults mimicking faulty sensors. The fault injection tool generates faulty signals in single or multiple sensors located in the primary loop. These scenarios studied under steady-state operation conditions simulate a bad sensor, a cut wire, noise, etc. The faults injected can lead to information being displayed in the main control room (MCR) to not match the conditions in the plant. In addition to a fault injection module, a result analyzer module is also a part of this testbed. Operator actions can be based on information displayed in the MCR, or they can be informed by the result analyzer. Potential operator actions following these single- or multiple faulty signals are assessed. It is concluded that the result analyzer in some cases can be helpful in guiding operators to make the right decisions.

Key Words: Nuclear Power Plant (NPP), Digital I&C in NPPs, Fault Injection Methodology, Main Control Room, Digital Sensors in NPPs,

1 INTRODUCTION

Mainly analog and instrumentation and control (I&C) systems have been used in GEN-II reactors. Most currently operating nuclear power plants (NPPs) in the US have been running for several decades with such analog I&C systems. These plants may continue to operate for another couple of decades following the approval of their life extension applications. However, maintaining these I&C systems for two more additional decades is becoming a challenge. These complex analog systems require frequent maintenance and the cost of keeping the systems is becoming expensive; expert manpower to maintain the systems is becoming scarce; and spare parts to replace them are no longer being manufactured and thus difficult to procure [1, 2]. These challenges have led the nuclear industry to explore conversion from analog to digital I&C systems. Furthermore, this transition may also lead to improved performance and safer operations.

Main control rooms (MCR) in currently operating GEN-II reactors have a dizzying level of detailed controls and displays such as buttons, meters, lamps, indicators, etc. On the other hand, digital MCR will have graphical interfaces. It is expected to reduce maintenance period, cost, and manpower needed to operate and maintain it than the old analog system. However, because the human machine interface (HMI) will be entirely different in the digital MCR, the operators will need to be thoroughly retrained to make sure that operator errors do not increase.

Cyber security is another area of concern in digital MCRs. Even though the digital I&C systems communicate with NPPs via closed networks, and security tools such as a firewall block unwanted access from outside of the network, there is still the possibility of external attacks into the system [3]. Cho and Woo developed a model to analyze the possibility of cyber-terrorism in NPPs over their lifetime, and simulated the consequences that might follow a cyber attack [4]. Shin et al. developed a cyber-security risk model using Bayesian networks to analyze possible scenarios and the vulnerabilities of the system against cyber-attack [5].

In this paper, we report some recent developments on the test bed as well as results obtained using the test bed. Experiments are performed to identify conditions which may lead to undesirable transients due to operator actions following faulty signal(s). A fault injection methodology is applied to simulate faulty sensor signals and the result analyzer (RA) module is introduced to help analyze information that may not be reliable due to the possibility of one or more faulty sensors.

2 A TESTBED TO SIMULATE NPP AND MCR

A test bed is developed to simulate possible accidental scenarios that may occur in NPPs as well as to assess the reliability of the digital I&C system. This is designed not only to test faults from sensors but may also be useful to explore the consequences of cyber-attacks. Earlier version of the test bed has been described in Ref. [6].

2.1 Configuration of the Test Bed

The test bed consists of a NPP simulator, a multi-display digital MCR, a triple modular redundant (TMR) controller, and a fault injection module. Schneider Electric's Tricon® is used as the TMR controller. It is programmed by its own application called Tristation 1131. The model of the NPP simulator, developed in LabVIEW, is based on the primary loop of 1000MWe Westinghouse pressurized water reactor (PWR). The digital MCR panels are also designed using LabVIEW's in-house tools. A PXI-Chassis with several PXI-Cards is installed to allow communications between the NPP simulator and the TMR controller. Figure 1 shows a schematic diagram of the test bed.

2.2 Fault Injection Methodology

Fault injection (FI) is loosely defined as a dependability validation technique that relies on controlled experiments in which faults are deliberately injected into a closely monitored or observed system [7]. Fault injection in this paper is used to simulate conditions due to sensor errors. The basic concept of fault injection modules is borrowed from Benso et al. [8]. They divided the fault injection module into three parts: A fault list manager (FLM), a fault injection manager (FIM), and a result analyzer (RA). These modules have been developed in LabVIEW and are linked to the NPP simulator to generate faulty sensor signals. Figure 2 shows a diagram of the fault injection modules and their connections to the rest of the test bed.

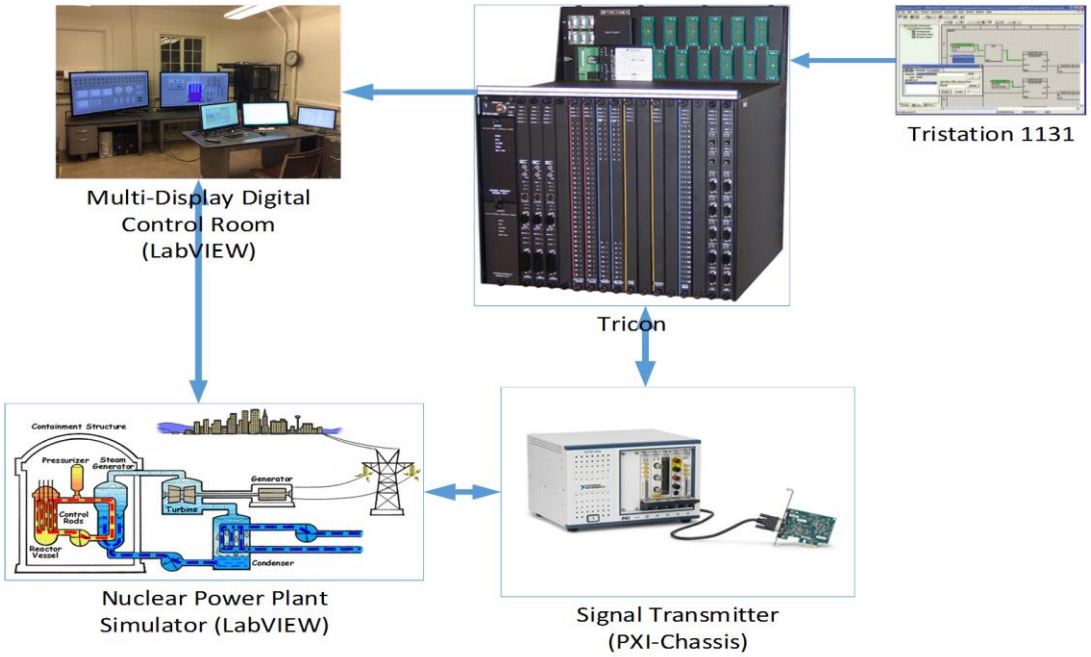

Figure 1. Configuration of the test bed

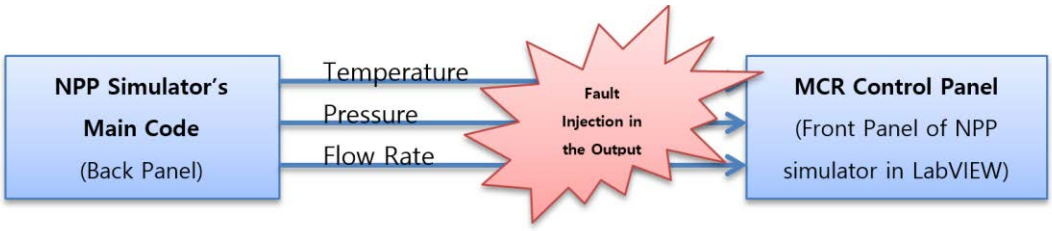

Figure 2. Connection between fault injection module and NPP simulator

The RA module analyzes the impact of injected faults on the system. The idea of the RA module is given by Rana, et al., and their basic structure is adapted for this test bed [9]. The structure of the RA module is described in Figure 3.

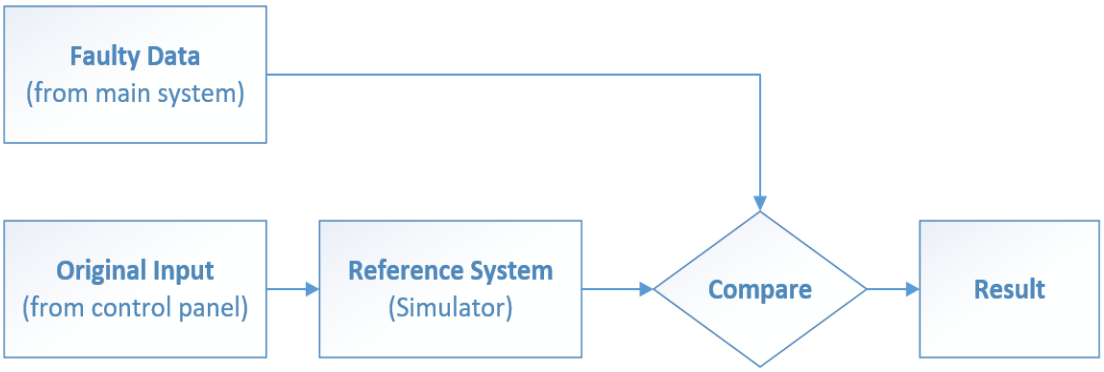

Figure 3. The structure of the result analyzer (RA)

The RA module receives original input values from the control panel and using a simulator determines the expected response of the system (NPP in this case). The outputs from the simulating module become the reference values. The values are then compared with the signals coming from the NPP which may contain faulty sensors. If the sensor values from the NPP differ by more than a certain degree from the simulation prediction signal, warning signals are flashed by the RA module. (Since this test bed is not connected to a NPP, another NPP simulator fills that role.)

3 NUMERICAL EXPERIMENTS

The test bed and the fault injection modules described in Ref. 4 are used to conduct numerical experiments to assess the system vulnerability. These numerical experiments need failure rates of sensors as input. Based on the statistical data, the commercial nuclear grade sensors are highly reliable. According to the field data, the actual failure rates of sensors are very low—only one or two faults may be expected for each sensor during 60 years of operation [10]. However, though the sensors are very reliable, the data from them may get compromised on the way to the MCR. The sensor data pass through the reactor protection system (RPS), where the TMR controller is located and the logic inside is programmable, and then to the MCR to display the status of the power plant. Even though the sensor itself is very reliable, the sensor data may be compromised by external factors and the compromised data displayed in the control room may make the reactor operators take decisions that will not be consistent with the actual state of the reactor. Thus, the numerical experiments performed in this chapter are aimed at identifying scenarios that may lead to such operator actions. The study involves single or multiple faults injection to the system.

3.1 Experimental Methodology

Because the NPP simulator in this test bed currently only has the primary loop of a PWR, only four major sensor values (hotleg temperature, coldleg temperature, system pressure, and flowrate) are identified for fault injection. Figure 4 shows the schematic diagram of the setup. The MCR and the NPP simulator are connected via LabVIEW. The sensor data from the NPP simulator passes to Tricon®. The data is processed using the logic programmed in Tricon for annunciators. The process can be monitored on Tristation 1131. When the fault injection module is on, it intercepts the sensor data from the NPP simulator, injects a fault, and passes the compromised data into Tricon®. The RA module continuously monitors the input signals of the Tricon® and shows the condition of the sensors.

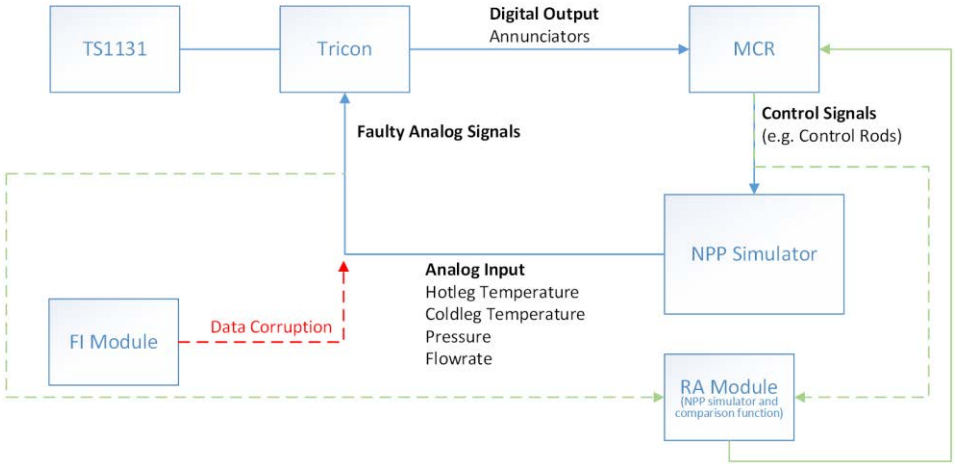

Figure 4. Experimental setup

Table I displays the permitted upper and lower limits of the four variables. These limits are programmed in the logic coded in Tristation 1131. Crossing these values activate the annunciators in the MCR. The RA module is used here to identify and mitigate conditions due to faulty sensor data that may lead to undesirable operator actions.

Table I. Upper and lower limits for temperature, pressure and flow rate

	Upper Limit	Lower Limit
Hotleg Temperature (°C)	345	295
Coldleg Temperature (°C)	315	275
Pressure (MPa)	16.0	15.0
Flowrate (kg/s)	4550	4450

3.2 Experimental Procedure

Three types of fault injection experiments are performed in this study: single fault injection, double fault injection, and triple fault injection. Each fault injection experiment is assessed with five different types of faults in four sensor locations. Table II describes the sensor locations and fault types.

Before starting the experiment, the number of faults, fault locations, fault types, and the magnitude of fault ranges are selected. These factors can be selected in the fault injection panel before starting the NPP simulator. After starting the simulator, the operator waits for a few seconds until the reactor reaches steady state, then injects the selected faults into the system by clicking on the "inject fault" button on the FI panel. The faulty sensor data as well as any annunciators activated due to the faulty data are displayed in the MCR. The operators are expected to react based on the information displayed on the panels in the MCR. The operator's actions are to be based on the "Emergency Response Guideline Development" report [11]. (The actual guideline includes all of the emergency heat removal systems (EHRS) and passive coolant systems (PCS), but these features are neglected because current simulator used in this study does not include the features yet.)

Table II. Types and ranges of faults in four sensor values

	Fault Range			
Fault Types	**1. Hotleg T**	**2. Coldleg T**	**3. Pressure**	**4. Flowrate**
1. Shift Up	~30 ˚C	~30 ˚C	~1.5 MPa	~500 kg/s
2. Shift Down	~30 ˚C	~30 ˚C	~1.5 MPa	~500 kg/s
3. Signal Cut-out	N/A			
4. Signal Stuck	Values at Steady State			
5. Noise	N/A			

4 EXPERIMENTAL RESULTS

This chapter describes the results of the numerical experiments. Only a few significant results are discussed in detail. The matrix for the experiments is described in Table III.

Table III. Experimental Conditions

Fault Location	1. Hotleg temperature 2. Coldleg temperature 3. Pressure 4. Flowrate
Fault Type	1. Shift up 2. Shift down 3. Signal cut-out 4. Signal stuck 5. Noise
MCR/Reactor Status	OP: Safe operation OPC: Operation with conditions SS: Shutdown immediately DoA: Deceptive or Ambiguous
RA Status	D: Detected ND: Not detected
Alarm	ON: Annunciators from Tricon are on OFF: Annunciators from Tricon are off

The results are analyzed for two cases: *with* or *without* the effect of the RA module. The goal of the experiment is to assess if the operators identify the state of the reactor correctly after fault injections and keep the reactor safe. The reactor would be considered to have one of four states identified in Table III. The reactor is considered to be in OP state if it is in normal steady-state operation; in OPC (operation with conditions) state when the reactor can continue to operate after checking the backup components; in SS (shutdown immediately) state if the reactor should be shut down; and in DoA (deceptive or ambiguous) state if the conditions are such that the operators may take actions that are not consistent with the reactor state. The last state, DoA, is the one that is of most concern.

4.1 Single-Fault Injection

A single-fault in one of four locations is injected to assess the system. In this case, redundancies in the system can be effectively used by the operators to continue safe operation by checking alternate components. Once an annunciator is activated and indicates one of the sensors is out of range, an operator checks other components' signals. For example, if there is a faulty signal on the hotleg temperature, the operator may counter-check the status of the hotleg temperature by monitoring the coldleg temperature, pressure, etc. Table IV describes all the related alternative sensors.

In most cases, the operator can identify the status of the reactor when an annunciator is activated. However, when the fault type # 4 (signal stuck at steady-state level) occurs during steady-state, identifying the fault in the MCR is impossible. Since the annunciator is not activated in this case, all informative panels appear normal unless the status of the plant changes to transient.

4.2 Double-Fault Injection

Any combination of two faults in four sensor locations are injected together in this case. (Since there is no emergency heat removal systems (EHRS) or passive cooling systems (PCS) in the current NPP simulator, injecting multiple faults at different times is not considered.) In most cases, double-fault injection does not lead to a critical scenario. By monitoring each sensor's backup components and the RA module's result, most scenarios lead to either OPC or SS. Since pressure has a good alternative component for counter check in the form of tank level, the faulty signal in pressure does not pose a serious condition. However, if the type-4 fault (stuck signal) is not detected by the RA module, it can

lead to a situation in which the operators may be making decisions that are not consistent with the state of the power plant. This will be the case when the locations of the double-fault injection are the two components that complement each other (alternatives in Table IV). One way to identify this fault is by forcing the reactor to go through a transient. Hence, when suspected, the operator can induce a (small) transient to detect its existence. Another ambiguous situation can result when the faulty sensor values indicate potential power loss (for example, low coldleg temperature - high flowrate, etc.). The RA module helps the operators to identify this situation if there are only two faulty signals. However, if more than two sensor signals suggest a subcritical condition of the reactor, the remedy must be very carefully chosen. Thus, this scenario will be assessed in the next section.

Table IV. Related alternative components for each sensor

Sensor Location	Alternatives
Hotleg Temperature	Coldleg Temperature Pressure Core Power Level
Coldleg Temperature	Hotleg Temperature Flowrate Pressure
Pressure	Pressurizer Water Level Temperature in Pressurizer
Flowrate	Hotleg Temperature Coldleg Temperature

4.3 Triple-Fault Injection

In this section, results are presented for the case of three faults injected into the system at the same time. Based on the results of the double-fault injection studies, hotleg temperature, coldleg temperature, and flowrate are selected for fault injection. Because these components are used as backups (alternative) for each other, two potentially serious consequences are identified. Tables V and VI summarize the conditions for these two scenarios. Table V shows the types of faults injected, range of faulty values of each fault, as well as the status in the MCR following the fault injection *with* or *without* the availability of results from the RA module. Table VI describes the warnings and suggested operator actions for the two faulty sensor scenarios in the MCR.

Table V. Results of triple-fault injected in the hotleg temperature, coldleg temperature, and flowrate

Scenario #	Fault HT	Fault CT	Fault FL	Range (HT)	Range (CT)	Range (FL)	MCR w/o RA	MCR w/ RA	Alarm (HT,CT,FL)	RA Status (HT,CT,FL)
1	2	2	1	5~30	5~30	50~500	DoA	SS	D/ND, D/ND, D	ON/OFF, ON/OFF, ON
2	4	4	4	N/A	N/A	N/A	DoA	DoA	ND, ND, ND	OFF, OFF, OFF

Table VI. Warnings and suggested operator actions following faults injected in the hotleg temperature, coldleg temperature, and flowrate

Scenario #	Warnings	Suggested Operator Actions
1	Operator may erroneously consider withdrawing the CRs to increase temperature while decreasing the flowrate. This may lead to an unanticipated transient moving toward a scram.	Check RA module. Insert CRs to avoid power increase.
2	The sensor values from major components are not reliable. In addition, it is hard to detect the existence of the faults in the system.	RA module cannot detect the faults. Insert CRs to gain time to make more informed decision.

First, the hotleg and coldleg temperatures are lower than the corresponding steady-state values while the flowrate is above its steady-state value. An MCR without a RA module suggests the status to be "deceptive or ambiguous" (DoA). Since the displayed information suggests a subcritical condition, an operator may erroneously consider withdrawing the control rods (CRs) to increase power (and thus temperature) while decreasing the flowrate. This may lead to an unanticipated transient, which may lead to an automatic scram. However, if the MCR was equipped with a RA module and if operators were to check the RA module, it would suggest the status of the reactor to be "steady-state" (SS). Thus, the RA module's assistance helps the operators in this case. Another ambiguous situation is identified when all three sensor signals are stuck at steady-state levels (fault # 4). In this scenario, even the RA module is not able to detect the problem, and therefore cannot identify the state of the reactor. Therefore, if operators suspect this scenario, they should check all components and data carefully, and lower the power level to avoid any undesirable situation.

5 CONCLUSIONS

The ultimate goal of this project is to develop a test bed and a methodology to determine the reliability of the digital I&C systems with TMR digital controllers in NPPs. The first step to achieve this goal is to develop a real-time in-house NPP simulator in LabVIEW and establish a connection to the TMR device via PXI-chassis. The TMR device (Tricon®) works well to initiate the annunciators in the MCR during normal operation. Fault injection modules are also developed to simulate faulty sensor signals in the system. In this study, the impact of faulty sensors is assessed to identify ambiguous or serious scenarios in the MCR. The results obtained show that signals stuck at steady state values on multiple sensors may lead to an ambiguous situation. The stuck sensor values suggest normal operation and hide any transients from the operators. Another noteworthy scenario is one that displays subcritical conditions to the operators in the MCR. This could lead to undesirable operator actions that are not consistent with the actual state of the power plant. Thus, identifying this situation is very important. The U.S. NRC defines such a situation as an accident in section 15.1 in the NUREG-75/087 [12]. Fortunately, the RA module is able to correctly identify this scenario, thus helping the operator in making the right decision.

6 ACKNOWLEDGMENT

This work is supported in part by a strategic research initiative (SRI) grant from the College of Engineering, University of Illinois at Urbana-Champaign.

7 REFERENCES

1. "Digital Instrumentation and Control Operating Experience Lessons Learned," Electric Power Research Institute (EPRI), Palo Alto (2008).
2. Y. An, Rizwan-uddin, W. Sanders, and C. Sollima, "Digital I&C and Cyber Security in Nuclear Power Plants," *American Nuclear Society (ANS) National Meeting*, Washington DC (2013).
3. D. Kushner, "The Real Story of Stuxnet," posted on Feb 26, 2013. Accessed on March 14, 2017. http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
4. H.S. Cho and T.H. Woo, "Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs)," *Annals of Nuclear Energy*, **Vol. 99**, pp. 47-53 (2017).
5. J. Shin, H. Son, R. Khalil ur, and G. Heo, "Development of a cyber security risk model using Bayesian networks," *Reliability Engineering and System Safety*, **Vol. 134**, pp. 208-217 (2015).
6. Y.An, C. Sollima, Rizwan-uddin, D. Chen, Z. Kalbarczyk, T. Yardley, and W. Sanders, "A Test Bed for Digital I&C and Cyber Security for NPPs," *Nuclear Plant Instrumentation, Control, & Human-Machine Interface Technologies (NPIC/HMIT) 2015*, Charlotte, North Carolina (2015). Also see: Y. An, A TESTBED TO ASSESS DIGITAL INSTRUMENTATION AND CONTROL AND CYBER SECURITY OF NUCLEAR POWER PLANTS, MS thesis, University of Illinois, 2016.
7. A. Benso and P. Prinetto, *An Overview of Fault Injection*, Kluwer Academic Publishers, Boston (2003).
8. A. Benso, M. Rebaudengo, and M.S. Reorda, "Fault Injection for Embedded Microprocessor-based Systems," *Journal of Universal Computer Science*, **Vol. 5**, pp.693-711 (1999).
9. R. Rana, M. Staron, C. Berger, and J. Hansson, "Improving Fault Injection in Automative Model Based Development using Fault Bypass Modelling," *Software-Based Methods for Robust Embedded Systems (SOBRES)*, Koblenz, Germany, September 16th, (2013).
10. "Component Reliability Data for Use in Probabilistic Safety Assessment," *International Atomic Energy Agency (IAEA)*, Report No. IAEA-TECDOC-478 (1988).
11. G.D. Storrick, A. Maioli, M.D. Carelli, "Emergency Response Guideline Development," *Westinghouse Electric Company LLC*, Report No. STD-AR-07-2 (2007).
12. "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, LWR Edition," *United States Nuclear Regulatory Commission (U.S. NRC)*, NUREG-75/087 (1980).