An Approach To Assess The Impact Of Instrumentation With An Embedded Digital Device

Richard T. WOOD[1], Tanner G. JACOBI[2], and Dan C. FLOYD[3]

1. Nuclear Engineering Dept., University of Tennessee, Knoxville, Tennessee, 37996 USA (E-mail: rwood11@utk.edu)
2. NE Dept., University of Tennessee, Knoxville, Tennessee, 37996 USA (E-mail: tjacobi@vols.utk.edu)
3. NE Dept., University of Tennessee, Knoxville, Tennessee, 37996 USA (E-mail: dfloyd7@vols.utk.edu)

Abstract: The instrumentation and control (I&C) equipment used in currently operating U.S. nuclear power plants (NPPs) is primarily based on mature analog technologies that are progressing towards obsolescence. The continued reliance on this legacy analog technology imposes performance penalties and maintenance burdens in comparison with modern digital I&C equipment. However, the nuclear power industry has been slow to adopt digital technology in large part as a result of regulatory concerns about common-cause failure (CCF) vulnerabilities. In many instances, currently available I&C equipment contain embedded digital devices (EDDs) such as microprocessors and programmable logic devices. Consequently, there is a clear need to develop cost effective qualification methods to contribute to the assessment of CCF vulnerability posed by EDDs in modern instrumentation that could be used in NPPs.

This paper describes findings from research regarding qualification methods for equipment with EDDs that is sponsored by the Nuclear Energy Enabling Technologies (NEET) Advanced Sensors and Instrumentation (ASI) program of the U.S. Department of Energy (DOE). Specifically, a classification framework was defined and an extended diversity and defense-in-depth (D3) analysis approach was developed to treat equipment with an EDD based on the functional impact of the device. These outcomes can contribute to a more systematic, predictable assessment of equipment with an EDD that can potentially reduce the burden of having to perform a full D3 analysis for every device.

Keyword: embedded digital device, instrumentation and control, diversity, defense-in-depth

1 Introduction

The instrumentation and control (I&C) equipment used in currently operating U.S. nuclear power plants (NPPs) is primarily based on mature analog technologies that are progressing towards obsolescence. The continued reliance on this legacy analog technology, which is also being propagated into new NPP designs, imposes performance penalties and maintenance burdens in comparison with modern digital I&C instrumentation[1]. In many instances, currently available I&C equipment contain embedded digital devices (EDDs) such as microprocessors and programmable logic devices. Experience in other industries, such as avionics, has shown that digital I&C equipment containing EDDs can provide significant benefits over analog-based equipment in terms of performance, reliability, and maintainability.

In recent years, due to the high demand for digital technologies in the industrial I&C marketplace, it is becoming increasingly difficult for NPPs to acquire instrumentation that is not equipped with an EDD. However, the nuclear power industry has been slow to adopt digital technology, especially in safety-related systems, in large part as a result of regulatory concerns about common-cause failure (CCF) vulnerabilities of equipment with an EDD.

The specific concern about potential safety issues arising from EDDs is explicitly stated by the U.S. Nuclear Regulatory Commission (NRC) in the recently issued Regulatory Issue Summary (RIS) 2016-05[2]. Consequently, there is a clear need to develop cost effective qualification methods to contribute to the assessment of CCF vulnerability posed by EDDs in modern instrumentation that could be used in NPPs.

This paper describes findings from research regarding qualification methods for equipment with EDDs that is sponsored by the Nuclear Energy Enabling Technologies (NEET) Advanced Sensors and Instrumentation (ASI) program of the U.S. Department of Energy (DOE). As an initial step in the research, an investigation was conducted of commercially available instrumentation marketed for nuclear or industrial application to identify the usage of EDDs and to determine the types of functional roles allocated to the devices[3]. Based on the available information on the nature and role of the digital technology implemented in the instrumentation, a classification approach for EDDs was developed focusing on the functional impact of the device.

Classifying digital devices according to their role in the operation of the instrumentation in which they are embedded can enable determination of the potential functional impact of failure of that device and contribute to determination of the potential safety significance of a CCF event disabling all instances of that device. Adopting the classification scheme based on functional impact, an approach was developed for extending the customary diversity and defense-in-depth (D3) analysis[4][5] to address equipment with an EDD. The classification scheme and extended approach to evaluating CCF vulnerability for equipment with an EDD can contribute to a more systematic, predictable assessment that can potentially reduce the burden of having to perform a full D3 analysis for every device.

2 Framework for classification

Because of the limited detail available from public sources, the evaluation of the functional roles and failure impact for EDDs is highly generalized[3]. Consequently, the classification structure by which equipment with an EDD can be categorized is necessarily abstract. Nevertheless, the binning of equipment by the significance of the EDD functionality to the equipment's performance of its core function is appropriate. Too fine a classification structure would result in difficulty assigning specific instrument of widely varying types and core functions into closely related classes. A coarse classification structure provides a suitable framework through which significance in the potential effect of a digital failure can be more readily distinguished and it should allow the assignment of equipment among classes to be a more tractable effort. In addition, a simple, intuitive structure can facilitate determination of what level of analysis and testing are appropriate for generating the necessary evidence to support decisions about whether smart equipment is suitable for nuclear application and qualified for the type of function it performs (e.g., safety, safety-related, non-safety).

The roles identified for an EDD in the survey of instruments include three almost universally available functionalities: communications, equipment condition monitoring, and self-diagnostics. Other EDD functionality can include control (or execution of the main functions of the instrument), protection, and configuration. Each of these digital functionalities have high value for enhancing the reliability and performance of instruments and improving maintainability and availability. Depending on the equipment architecture and its interfaces, the impact of failure for the communications and equipment condition monitoring functionality can range from no impact to degradation of an instrument's performance to loss or unavailability of the instrument's function (e.g., failed communications of measurement results). The self-diagnostic functionality can provide several tangible benefits in terms of increased reliability, enhanced performance, and improved maintainability. However, as with all digital systems, the presence of code or logic to execute the self-diagnostics adds complexity and can be a source of failure unless fault management provisions are in place. Therefore, this digital functionality can have an impact on the performance of the instrument's function but design measures can mitigate that threat. The other identified functionalities (control, protection, and configuration) tend to have a clear impact on the execution of the main function of an instrument. Again, design measures can help mitigate the vulnerability associated with the

digital device but more detailed evaluation of the impact of failure of these functions is warranted in assessing the suitability of equipment with an EDD fulfilling any of those roles. The bottom line is that the functional role of EDDs range from minor (no role in the safety function) to significant (integral to execution of the safety function) and the potential impact of failure of an EDD corresponding ranges from none to critical.

Based on the findings of the equipment survey and evaluation of the functional impact of EDDs, a four-category classification structure is proposed. The classification is based on the high-level characterization of potential impact of failure of an EDD on an instrument's performance of its fundamental function. The four classes provide a broad grouping of effects and are defined as the following:

- No Impact
- Low Impact
- High Impact
- Critical Impact

For equipment with an EDD to classified as No Impact (EDD-NI), the digital functionality should have no connection to the analog electrical or mechanical elements of the instrument other than through non-intrusive or passive measurement. Examples would include on-board measurement of local environmental conditions, passive monitoring of performance indicators related to the instrument's function, or parallel communication paths that retains traditional analog transmission in addition to distinct digital interconnections. In these cases, loss of the digital functionalities would not affect the performance of the main function of the instrument. To be included in this class, an instrument must be able to perform it function fully and within specifications with the digital functionality disabled.

For equipment with an EDD to classified as Low Impact (EDD-LI), the digital functionality may be connected to the analog electrical or mechanical elements of the instrument and may be able to influence the output or performance of the instrument's fundamental function. An example would be communications functionality for smart transmitters. If the digital datastream is superimposed on the hardwired analog signal, it would be necessary to confirm that no failure mode of the digital communications function to bias or corrupt (i.e., excessive noise) that analog communications. To be included in this class, an instrument should be able to execute its function in the face of digital failure or malperformance with only limited degradation such as detectable deviations of the output, reduced responsiveness, or loss of non-vital information (e.g., condition data). The significance of the impact of the EDD failure may be elevated for safety applications and result in a more appropriate higher classification. Thus, there may be cases where an instrument might be EDD-LI for non-safety applications for needed to be at an elevated class for more safety-critical applications.

For equipment with an EDD to classified as High Impact (EDD-HI), the digital functionality is likely to be integral to the analog electrical or mechanical elements of the instrument and is able to affect and potentially compromise the output or performance of the instrument's fundamental function. An example is the digital circuitry of a smart transmitter where signal processing functions are performed in software. If the signal processing functions fail outright or erroneously adjust the measurement output, then the instrument's function would be compromised or degraded. The latter case, where the signal is transmitted and the measurement value is incorrect but plausible, could potentially lead to instances where the effect of the failure is propagated because the erroneous result may be difficult to detect without sophisticated signal validation. Of course, it the instrument's architecture provides a parallel analog circuit that can bypass the digital processing, then the instrument would be more appropriately classified in one of the lower categories. Another example would be protective functionalities that could inhibit response to actuation commands based on the detected status of the actuator. To be included in this class, the performance of the instrument's fundamental function should depend on the proper

execution of the digital functionalities or could be compromised by failure or malperformance of the digital element.

For equipment with an EDD to classified as Critical Impact (EDD-CI), the digital functionality is highly integrated with or replaces the analog electrical or mechanical elements of the instrument and is essential to the execution, output and/or performance of the instrument's fundamental function. A prime example is a digital priority logic (or component interface) module in which the priority function is implemented in complex logic on a programmable logic device. Other examples would include unique sensors that require significant digital signal processing to extract process information (e.g., guided wave radar for level measurement or Johnson Noise thermometry for temperature measurement). To be included in this class, the instrument must not be able to perform its fundamental function without proper execution of the digital element.

The classification framework can provide a means of preprocessing information about equipment with an EDD to support a determination of when and how a D3 analysis is to be performed. If equipment with an EDD is classified as and confirmed to be EDD-NI, then it is reasonable to conclude that there is no credible CCF vulnerability (i.e., CCF Not Credible) and a D3 analysis should not be necessary. It should be possible to confirm the EDD-NI classification by disabling the digital functionality provided by the EDD and performing functional testing of the instrument across its range of input to demonstrate that the instrument can still acceptably perform its fundamental function. For the other classes, testing with the digital functionality disable would likely only partially resolve concerns about CCF vulnerability since it only addresses the potential impact of loss of function. Where the digital functionality of the EDD can affect the fundamental function of an instrument, further assessment is needed to address any prospective failure modes that could degrade the instrument's performance in order to ensure that no disruptive or deceptive (erroneous but plausible) responses are overlooked. If 100% testing is not feasible, additional design analysis and/or testing may be needed for equipment assigned to the other classes to enable determination of how to conduct a D3 analysis (i.e., whether to proceed through the entire process include best estimate analysis) or what supporting evidence can be generated to reach a conclusion that potential CCF vulnerability is resolved. Depending on the expected impact of a digital failure, it may be possible to identify defensive measures (e.g., analog signal pass-through, switching out digital functionality on selected instances of an instrument, fault management provisions) or testing (e.g., fault injection or model-based testing) to reasonably confirm that malperformance of the digital functionality provided by the EDD cannot inhibit or compromise the instrument's fundamental function nor induce spurious action.

3 Assessment approach for extended D3 analysis

Much of current regulatory guidance on treating CCF vulnerabilities focuses on mitigating the impact of CCF in safety systems (reactor trip (RTS) and engineered safety feature actuation systems (ESFAS)). The prevailing NRC policy and guidance specifically invokes a consequence-based assessment approach that is primarily applied at the safety system (or redundancy/subsystem) level for sense and command functions. These safety functions are generally characterized as on-demand, where safety action is commanded and executed when indication of an infrequent (transients) or rare (accidents) postulated initiating event (PIE) is sensed. This conventional assessment approach has not been extensively applied at the component level or to equipment whose safety-related function is generally characterized as continuous, frequent, or predictable (such as for many sensing, actuation, and support service equipment).

Because the consideration of CCF vulnerability for equipment with an EDD is a recent regulatory concern and guidance on assessing and addressing

potential vulnerabilities is evolving, a systematic approach should be employed to determine when and how a D3 analysis is to be performed for equipment with EDDs. To this end, an assessment approach for systematically evaluating the potential impact of prospective CCF vulnerabilities for equipment with an EDD has been defined and is described below.

First, the presence of an EDD should be reviewed for each electrical and electronic component evaluated/selected for the implementation of the I&C architecture of an existing or new reactor. To help ensure awareness of EDDs, all specifications to vendors for the supply of safety-related equipment or commercial products should include requirements that any EDD be identified and that sufficient documentation of the quality of any commercial equipment be provided (as noted in RIS 2016-05[2]).

If, at any point in the following stages of an assessment of CCF vulnerability of equipment with an EDD, alternate equipment that is determined diverse is found to be available, the I&C architecture can incorporate the diverse equipment as a means of mitigating the impact of potential CCF of the equipment with an EDD. This solution presupposes the result of a conventional D3 analysis to be that diverse means to ensure the safety function supported by the equipment is necessary. If diverse equipment is employed, then the basis for determining that the equipment is diverse should be documented to support justification that the potential impact of CCF is mitigated.

Where equipment with an EDD is identified, the role of the digital device in the performance of any safety-related function either performed or supported by the equipment should be investigated. This is equivalent to assessing the classification of the equipment with an EDD based on functional impact, as described above. Where it is determined that the EDD is either not involved in or cannot adversely affect the performance of any safety-related function of the equipment (e.g., EDD-NI), no further analysis would be necessary but the basis for the determination that the EDD does not impact safety functions should be documented. Where it is determined that the EDD has an impact on the equipment performance or sufficient information on the role of the EDD is not available, then further assessment of the potential for CCF vulnerabilities should proceed. If the EDD is integral to the safety function of the equipment (e.g., EDD-CI), then it is likely to necessitate a full-scope D3 analysis.

In accordance with the approach identified in Branch Technical Position (BTP) 7-19[4], a further aspect of the investigation of the equipment with an EDD involves determination of whether the implementation of relevant functions in the EDD meets either of the two criteria for which it is considered that the potential for CCF is resolved. The first criterion is that there is sufficient internal diversity incorporated in the equipment or the design of the EDD. The second criterion is that the software or software-designed logic is sufficiently simple that it has been or can be fully tested. Assessing the compliance with either criterion requires detailed knowledge of the equipment and the application of the EDD. If either condition can be demonstrated, then no further analysis would be necessary and the basis for this determination should be documented. If the vendor does not provide or have available such information, then further assessment of the potential for CCF vulnerabilities should proceed.

The next stage of the assessment involves evaluating the performance characteristics of the equipment to determine the nature of its failure response. Given that this assessment applies to equipment rather than systems, a key question for the evaluation is whether the equipment performs a function for which failure is self-revealing. For example, if the equipment is continuously or regularly operating (transmitting, maneuvering, controlling), is its failure readily observable? Generally, failure to function of active equipment is apparent. Degraded performance may also give clear, immediate indication (as would generally be the case for equipment classified as EDD-LI). Alternatively, if there is not direct, short-term indication of failure (e.g., failure responses such as “fail as is” or “incorrect but plausible”), then the evaluation should consider whether failure of

the equipment can be detected through available or additional monitoring. For example, a sensor output may be plausible but incorrect and, given an assumption of a CCF, comparison against the output of identical sensors could not be expected to reveal the failure. However, comparison against a group of different sensors whose collective behavior is predictable based on physics (i.e., expected process behavior) could detect the failure. Examples are seen in monitoring and surveillance capabilities that have been developed for the nuclear power and other industries based on pattern recognition[6]. Thus, potential CCF of equipment with EDDs with continuous, frequent, or predictable behavior may be self-revealing or available detectable through surveillance and monitoring techniques.

If the results of the evaluation of the equipment performance characteristics demonstrate that failures are self-revealing or detectable, near-term notification of failure and opportunity to respond rapidly (e.g., restart, transition to a safe state, manual action for reset, bypass, or repair) may provide the means of mitigating the impact of CCF. These conditions should be documented and may be employed as part of a strategy to mitigate the impact of CCF. The additional information necessary to provide justification for such a strategy are the time available for detection and response as well as the response approach itself. The time for detection and response depends on the progression of the event postulated to result from the failure and can be determined through analysis (e.g., conduct of an engineering analysis of appropriate fidelity or proceeding to the best-estimate accident and transient analysis of the conventional D3 analysis). If it is determined that adequate time is available for detection, then a strategy for corrective action (either automatic or manual) should be developed and assessed to ensure that both detection and response can be accomplished in the available time (with margin) before the consequences of a postulated CCF violate applicable acceptance criteria. If it is determined that a "detect and respond" strategy provides adequate mitigation of the impact of CCF, then the strategy itself and the basis for this determination should be documented.

At this stage, the assessment of equipment with an EDD transitions to the conventional D3 analysis. In assessing the impact of a failure of multiple instances of the equipment with an EDD, the context of the architecture, system, redundancy, or subsystem to which it is assigned should be considered. In developing a block representation (as specified in NUREG/CR-6303) of the I&C architecture, including the software or software designed logic of the EDD, the availability of diverse means to provide the same or similar safety function should be considered. In the specific case of smart sensors, an evaluation should be performed to determine whether a diverse measurement from another dissimilar (diverse) sensor is available. Regarding safety functions, this assessment involves considering the sensor and functional diversity provided in the safety system design to identify whether alternate indicators are incorporated in the plant design for each PIE indicated by the measurement from the smart sensor. If such diversity is present within the safety system block structure, then it may not be necessary to postulate CCF of the equipment. If the measurement from the smart sensor is also shared with the control system echelon, then it would also be necessary to confirm that the anticipated failed behavior of the associated control function is bounded by safety analysis. As is normal in a D3 analysis, documentation should capture the justification that the impact of potential CCF is either mitigated or remains within safety bounds.

If the considerations described in the assessment approach above do not fully resolve the potential impact of CCF in equipment with an EDD, then the equipment should be further treated as part of the conventional D3 analysis (see BTP 7-19[4] and NUREG/CR-6303[5]). The assessment of equipment with an EDD, including the results of a D3 analysis, are expected to demonstrate that there is sufficient defense-in-depth and diversity to cope with a postulated digital CCF of the EDDs in equipment of the RTS and ESFAS, including the credited control systems.

All of the assumptions and decisions involved in conducting this kind of assessment and its full execution during the design phases of an I&C architecture should be confirmed as part of a final assessment when equipment selection and acquisition is completed and the final I&C architecture is established.

4 Conclusions

Nuclear facilities are slowly increasing their use and reliance on digital technology in systems and equipment (e.g., I&C, electrical systems, and fluid systems). In addition to digital I&C systems for protection and control, examples of safety-related equipment that may use digital technology include emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, time-delay relays, and uninterruptible power sources. Because of the high demand for digital functionality in high-volume industries, the industrial I&C marketplace is dominated by digital technology such that it is increasingly difficult to acquire instrumentation that is not equipped with an EDD intended to enhance its performance, reliability, and flexibility. Concerns about CCF vulnerability are the primary issue that serves to inhibit deployment of advanced instrumentation (e.g., sensors, actuators, microcontrollers) with EDDs in nuclear power applications.

The primary objectives of the reported research are to define a classification framework for equipment with an EDD based on the functional impact of the device and then establish the basis for an extended D3 analysis approach. The outcomes are intended to support further development of cost-effective qualification methods to facilitate the acceptance of digital technology for widespread application in NPPs.

An initial investigation of commercially available equipment with an EDD gave some insights into the functionality performed by EDDs and the associated role in the performance of the host equipment's primary function[3]. However, the available information is very limited. Nevertheless, some insights were drawn to establish a generalized determination of characteristics indicating the potential functional impact of incorrect performance or outright failure of an EDD.

A coarse classification structure has been developed to provide a suitable framework through which significance in the potential effect of a digital failure can be more readily distinguished. The classification framework provides a simple, intuitive structure can facilitate determination of what level of analysis and testing are appropriate for generating the necessary evidence to support decisions about whether smart equipment is suitable for nuclear application and qualified for the type of function it performs (e.g., safety, safety-related, non-safety). The four-class structure provides a broad grouping of effects and is defined as the following:

- No Impact
- Low Impact
- High Impact
- Critical Impact

For equipment with an EDD to classified as No Impact (EDD-NI), the digital functionality should have no connection to the analog electrical or mechanical elements of the instrument other than through non-intrusive or passive measurement. To be included in this class, an instrument must be able to perform it function fully and within specifications with the digital functionality disabled.

For equipment with an EDD to classified as Low Impact (EDD-LI), the digital functionality may be connected to the analog electrical or mechanical elements of the instrument and may be able to influence the output or performance of the instrument's fundamental function. To be included in this class, an instrument should be able to execute its function in the face of digital failure or malperformance with only limited degradation such as detectable deviations of the output, reduced responsiveness, or loss of non-vital information (e.g., condition data). The significance of the impact of the EDD failure may be elevated for safety applications and result in a more appropriate higher classification.

For equipment with an EDD to classified as High Impact (EDD-HI), the digital functionality is likely

to be integral to the analog electrical or mechanical elements of the instrument and is able to affect and potentially compromise the output or performance of the instrument's fundamental function. To be included in this class, the performance of the instrument's fundamental function should depend on the proper execution of the digital functionalities or could be compromised by failure or malperformance of the digital element.

For equipment with an EDD to classified as Critical Impact (EDD-CI), the digital functionality is highly integrated with or replaces the analog electrical or mechanical elements of the instrument and is essential to the execution, output and/or performance of the instrument's fundamental function. To be included in this class, the instrument must not be able to perform its fundamental function without proper execution of the digital element.

Classifying digital devices according to their role in the operation of the instrumentation in which they are embedded can enable determination of the potential functional impact of failure of that device and contribute to determination of the potential safety significance of a CCF event disabling all instances of that device. Consequently, a graded approach to D3 analyses of CCF vulnerabilities and to qualification testing may be possible based on classification.

Much of current regulatory guidance on treating CCF vulnerabilities focuses on mitigating the impact of CCF in safety systems. The prevailing NRC policy and guidance specifically invokes a consequence-based assessment approach that is primarily applied at the safety system (or redundancy/subsystem) level for sense and command functions. These safety functions are generally characterized as on-demand where the safety action is commanded and executed when indication of an infrequent or rare PIE is sensed. This conventional assessment approach has not been extensively applied at the component level or to equipment whose safety-related function is generally characterized as continuous, frequent, or predictable (such as for many sensing, actuation, and support service equipment). Therefore, it was recognized that an assessment approach for systematically evaluating the potential impact of prospective CCF vulnerabilities for equipment with an EDD was needed.

Considering the prospective classification of equipment with an EDD, an approach to assessing such equipment as part of an extended D3 analysis was developed. The analysis approach extends the customary D3 analysis by identifying steps and considerations through which the significance and functional impact of potential failures of the EDD can be taken into account. This approach involves evaluating equipment to ensure awareness of the presence of an EDD, determining the role and safety-relevance of the digital device in the performance of any safety-related function either performed or supported by the equipment, investigating whether the implementation of relevant functions in the EDD meets either of the two criteria (internal diversity or testability) for which it is considered that the potential for CCF is resolved, evaluating the performance characteristics of the equipment to determine the nature of its failure response (e.g., is failure detectable and is adequate time available to respond), assessing whether the component-level CCF has an unacceptable system-level or safety function impact (e.g., performance of a best-estimate analysis), and, if necessary, determination of the availability of diverse alternatives to mitigate the impact of CCF. The treatment of equipment with an EDD within this extended D3 framework can be informed by prior classification of the role of the EDD in the function of the equipment.

Acknowledgement

The material herein is based upon work supported by the U.S. Department of Energy, Office of Nuclear Energy, under the Nuclear Energy Enabling Technology (NEET) Advanced Sensors and Instrumentation (ASI) Program. The authors would like to acknowledge Suibel Schuppner, the DOE NEET ASI program manager, for her oversight and assistance on this project. This paper presents an account of work sponsored by an agency of the United States Government. Neither the United States

References

[1] E. Quinn, J. Mauck, and K. Thomas, Digital Technology Qualification Task 2 – Suitability of Digital Alternatives to Analog Sensors and Actuators, INL/EXT-12-27215, Idaho National Laboratory, Idaho Falls, ID, 2012.

[2] U.S. Nuclear Regulatory Commission, Embedded Digital Devices in Safety-Related Systems, Regulatory Issue Summary 2016-05, April 2016 (ADAMS Accession No. ML15118A015).

[3] T. Jacobi et al., "Investigation of Instrumentation Containing an Embedded Digital Device," Proceedings of NPIC&HMIT 2017, San Francisco, CA, June 11-15, 2017.

[4] U.S. Nuclear Regulatory Commission, Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems, Branch Technical Position (BTP) 7-19, Rev. 6, March 2010 (ADAMS Accession No. ML093490771).

[5] U.S. Nuclear Regulatory Commission, Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, December 1994 (ADAMS Accession No. ML071790509).

[6] Electric Power Research Institute, On-Line Monitoring Implementation Guidelines: Use of Multivariate State Estimation Technique (MSET), EPRI 1003360, November 2002.