Limited Liability Company
«RESEARCH AND PRODUCTION COMPANY RADICS»

29 Geroyiv Stalingrada Street, 25009 Kirovograd, Ukraine
Tel:+380 522 395707 **Fax:** +380 522 555179
E-Mail: radics@radics-ua.com

Ref. № 082018/014

Dated: August 2, 2018

U.S. Nuclear Regulatory Commission
ATTN: Document Control Desk
Mr. Joseph Holonich
Senior Project Manager
One White Flint North
11555 Rockville Pike
Rockville, MD 20852-2738

Subject: Submittal of RadICS Digital I&C Platform Topical Report Supplemental Information Update (Docket Number 99902032)

References:
(1) Research and Production Corporation Radics letter to NRC dated September 20, 2016, "Submittal of RadICS Digital I&C Platform Topical Report" (ADAMS Accession No. ML16274A346)
(2) NRC letter to Research and Production Corporation Radics dated April 15, 2017, "Acceptance Review of "RadICS Digital I&C Platform Topical Report" Submitted September 20, 2016 (CAC NO. MF8411)" (ADAMS Accession No. ML16281A459)
(3) Research and Production Corporation Radics letter to NRC dated September 15, 2017, "Submittal of RadICS Digital I&C Platform Topical Report Supplemental Information" (ADAMS Accession No. ML17275A191)
(4) NRC letter to Research and Production Corporation Radics dated June 11, 2018, "Regulatory Audit Report for April 2-5, 2018, RadICS Digital I&C Platform Topical Report" (CAC NO. MF8411; EPID L-2016-TOP-0010)" (ADAMS Accession No. ML18106A025)

In Reference 1 Research and Production Corporation Radics (RPC Radics LLC) submitted a topical report for the RadICS digital instrumentation and control (I&C) platform. The RadICS platform is a generic digital safety I&C platform designed to implement Class 1E safety-related applications in United States nuclear power plants. The NRC accepted the RadICS Digital I&C Platform Topical Report for review in Reference 2.

During a review kickoff meeting on August 30, 2017, RPC Radics LLC discussed the availability of new information related to the RadICS Topical Report. The NRC Project Manager recommended that this information be submitted to NRC as supplemental information related to the review of the RadICS Topical Report. The supplemental

T007
4G01
NRR

information was submitted in Reference 3. The information included an expanded discussion on diversity and defense-in-depth.

In Reference 4, NRC requested RPC Radics LLC to develop a list of diversity attributes for internal self-diagnostic functions to support performance of diversity and defense-in-depth (D3) assessments. NRC also presented a draft list of plant-specific action items related to internal diversity features. RPC Radics LLC is providing additional information regarding diversity attributes for internal self-diagnostic functions to support performance of D3 assessments in Enclosure 1. RPC Radics LLC is also providing comments on the draft list of plant-specific action items related to internal diversity features in Enclosure 3.

RPC Radics LLC requests that the proprietary presentation documents be withheld from public disclosure. In accordance with 10 CFR 2.390, "Public inspections, exemptions, requests for withholding," an affidavit is enclosed identifying the specific portions of the above documents that are proprietary and the basis for making that determination. Non-proprietary versions of the documents are also provided with the proprietary information redacted.

Enclosure 1 provides the proprietary version of updated supplemental information.

Enclosure 2 provides the non-proprietary version of the updated supplemental information.

Enclosure 3 provides comments on the draft list of plant-specific action items related to internal diversity features.

Enclosure 4 provides an affidavit related to the proprietary material in Enclosure 1.

If you have any questions related to this submittal, please contact me at 423-834-4455 or by e-mail at mjburzynski@newcleardayinc.com.

Sincerely,

Mark J. Burzynski
US Licensing Manager
RPC Radics LLC

radICS
29 Geroyev Stalingrada Street
25009 Kirovograd, Ukraine

Affidavit

STATE OF TENNESSEE)
)
COUNTY OF HAMILTON)

1. I, Mark Burzynski (RPC Radics LLC US Licensing Manager), am familiar with the criteria applied by RPC Radics LLC to determine whether certain RPC Radics LLC information is proprietary. I am familiar with the policies established by RPC Radics LLC to ensure the proper application of these criteria.
2. In accordance with 10 CFR 2.390, "Public inspections, exemptions, requests for withholding," Research and Production Corporation Radics (hereafter called RPC Radics LLC) requests withholding from public disclosure of the documents listed in attached Table 1, which is attached to this affidavit. The documents contain application, product design details, and qualification process information related to the RadICS digital instrumentation and controls platform. RPC Radics LLC has expended a significant amount of money and effort involving numerous contractors over more than 5 years to develop this product.
3. As required by 10 CFR 2.390, RPC Radics LLC has included in attached Table 1 the following information:
   - Identity of the document or part sought to be withheld;
   - Declaration of the basis for proposing the information be withheld, encompassing considerations set forth in § 2.390(a);
   - Specific statement of the harm that would result if the information sought to be withheld is disclosed to the public; and
   - Locations in the documents of all information sought to be withheld.
4. As required in § 2.390(b)(4), RPC Radics LLC wishes to note that the request for withholding from public disclosure applies to pages that contain commercially sensitive information that RPC Radics LLC normally discloses only under a Non-

radICS
29 Geroyev Stalingrada Street
25009 Kirovograd, Ukraine

Disclosure Agreement (NDA). This commercially sensitive information is not available in public sources and is the type of information customarily held in confidence by RPC Radics LLC and our competitors. Some examples of categories of information which fit into the definition of proprietary information are:

a) Information which discloses process, method, or apparatus, including supporting data and analyses, where prevention of its use by competitors of RPC Radics LLC without license or contract from RPC Radics LLC constitutes a competitive, economic advantage over other companies in the industry.
b) Information, which if used by competitors, would reduce their expenditure of resources or improve •their competitive position in the design, manufacture, shipment, application, installation, assurance of quality, or licensing of a similar-product.
c) Information which reveals cost or price information, production capacities, budget levels, or commercial strategies of RPC Radics LLC, its customers, its partners, or, its suppliers.
d) Information which reveals aspects of past, present, or future RPC Radics LLC customer-funded development plans or programs, of potential commercial value to RPC Radics LLC.
e) Information which discloses patentable subject matter for which it may be desirable to obtain patent protection.
f) Information obtained through RPC Radics LLC actions which could reveal, additional insights into nuclear equipment qualification processes, customer applications, and regulatory proceedings, and which are not otherwise readily obtainable by a competitor.

5. RPC Radics LLC is transmitting this information to NRC in confidence.
6. As noted in attached Table 1, release of this information in a public forum could cause harm to RPC Radics LLC by revealing trade secrets and/or commercially sensitive design and operational details and technical processes related to designing, building, and/or operating a RadICS digital safety instrumentation and control system.

radICS
29 Geroyev Stalingrada Street
25009 Kirovograd, Ukraine

7. As RPC Radics LLC US Licensing Manager, I have been specifically delegated responsibility for reviewing the information sought to be withheld, and I am authorized to apply for its withholding on behalf of RPC Radics LLC.
8. The foregoing statements are true and correct to the best of my knowledge, information, and belief.

Mark J. Burzynski

Mark J. Burzynski
US Licensing Manager
RPC Radics LLC

Sworn to and subscribed before me
this 2nd day of August, 2018

Brittany R. Marcum

Notary Public

BRITTANY R. MARCUM
STATE OF TENNESSEE
NOTARY PUBLIC
HAMILTON COUNTY

My commission expires: November 24, 2018

Table 1. Documents requested for withholding from public disclosure

Document Title	Part of document sought to be withheld from public disclosure	Basis for proposing the information be withheld, encompassing considerations set forth in § 2.390(a)	Specific statement of the harm that would result if the information sought to be withheld is disclosed to the public
Enclosure 1: Updated Discussion on Diversity and Defense-In-Depth (Proprietary Version)	Portions of document marked by brackets **[ ]**.	Trade secrets and / or commercial information as per § 2.390(a)(4)	RPC Radics LLC would be harmed by disclosure of commercially sensitive details of how the generic hardware and software components of a RadICS Platform work, and how internal diversity features are incorporated in to the RadICS Platform design, and how such features are credited to mitigate common cause failure vulnerabilities. This would be of value to a competitor in understanding specific competitive design and operational characteristics of the RadICS Platform.

Enclosure 2

Updated Discussion on Diversity and Defense-In-Depth (Non-Proprietary Version)

The RadICS Platform contains internal diversity features that can be used to provide an acceptable regulatory solution for the digital common cause failure (CCF) vulnerabilities present in the RadICS Platform. NRC Branch Technical Position (BTP) 7-19, Revision 6, states that there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF: diversity or testability. With respect to the diversity option, BTP 7-19 specifies that when sufficient diversity exists in the protection system, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

[[

]]^{a,c,e}

The RadICS Platform diversity approach provides other benefits by simplifying the overall I&C systems designs, since a separate diverse actuation system is not required to mitigate digital CCFs. The RadICS Platform diversity strategy leads to a simpler overall I&C architecture than other platform-based diverse technology solutions. The RadICS diversity strategy eliminates the need for additional plant-level best-estimate coping or consequence analyses, since the diverse defensive measures incorporated into the RadICS Modules put the system outputs safe states consistent with the plant safety analyses. The RadICS Platform diversity strategy eliminates the complex intersystem design coordination analysis of two actuation systems controlling safety components.

The diversity of a typical application using the RadICS Platform technology was evaluated using the methodology outlined in NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems."

The impact of this expanded discussion on diversity and defense-in-depth is shown on the attached mark-up of the affected RadICS Topical Report sections.

10 Diversity and Defense-In-Depth

10.1 Overview

Digital I&C systems can be vulnerable to CCFs caused by software, firmware, or programmed logic errors, which could defeat the redundancy achieved by hardware architecture. CCFs are of particular interest for a digital I&C system designed to perform in nuclear safety-related projects like a Protection System (PS).

10.2 Digital Common Cause Failures

NRC considers CCFs in digital systems to be a beyond design basis event and specifies the special methods for providing the necessary protection for digital PS projects. These methods use a D3 assessment as the primary design tool. Defense-in-depth is a principle that ensures multiple layers of I&C systems exist to provide protection against a wide spectrum of anticipated operational occurrences and postulated accidents, both design basis and beyond design basis. Diversity is a principle that ensures digital I&C systems are protected against postulated CCFs, specifically in portions of a digital I&C system that are not fully testable (e.g., the software, firmware, or programmable logic).

Protection against CCF is primarily provided at the overall I&C architecture level by implementing different lines of defense and diversity. Regulatory guidance on performing D3 analyses is provided in two main documents: BTP 7-19 (Reference 10-1) and NUREG/CR-6303 (Reference 10-2). These guidance documents are tailored to a D3 assessment performed for a project-specific safety-related I&C system, so much of the guidance is not applicable to a generic platform qualification process.

10.3 Defense Against Common Cause Failures

Individual safety I&C systems are generally designed with identical equipment (same hardware and software) in redundant divisions, therefore raising a CCF issue at the system level.

To ensure defense against CCF at the system level, the RadICS Platform employs several defensive measures that together provide protection against and elimination of CCFs. These defensive measures are as follows:

- Software Development Process Quality
- Hardware Independence Principles
- Platform Diversity
- Defense-in-Depth

In combination, these measures work together to reduce the risks of CCF to acceptable levels within applications that utilize the RadICS Platform.

10.3.1 Software Development Process Quality

As stated in IEC 60880-2006 (Reference 10-3), Section 13.2, "Design of software against Common Cause Failure":

"The basic and most important defense against common cause failure due to software is to produce software of the highest quality (i.e., as error-free as possible)."

The following are measures taken by RadICS during the software development process as a line of defense against software CCFs (as described in Chapter 6):

- Program code volume reduction due to application of FPGA as programmable components
- Application of distributed software and separation of safety-related functions (IEC 61266 category A functions) from those of lesseer categories (i.e., IEC 61266 (Reference 10-4) Categories B and C functions) and non-safety functions
- Application of development methods and tools aimed to prevent introduction of faults into software
- Self-diagnostic testing and fault tolerant design features (validated by FIT as described in Section 7.4.2.1)
- Defensive programming
- Fail-safe design features

The RadICS Module Electronic Designs are based on life cycle processes that guarantee achievement of a robust level of quality (see Chapters 7 and 8). It aims at avoiding errors by means of:

- Adherence to a strict and phased development process
- Re-use of proven components
- Use of simple and proven design principles based on clearly defined rules
- Avoidance of unnecessary complexity
- Use of proven tools for automated code generation as much as possible to reduce risk of human errors
- Eliminating errors as soon as possible
- Documents produced during a phase are formally verified and reviewed before starting the next phase
- V&V tasks are performed by an independent team
- Static verification is performed on all manual source code and parameters
- Unit tests, integration tests, validation tests, factory acceptance tests, and site tests are planned and performed

~~10.3.1~~10.3.2Hardware Independence Principles

The steps of defense against hardware CCFs realized for both the RadICS Platform and RadICS Platform-based projects include adherence to independence principle. Generally, adherence to independence principle means that the I&C system should preserve its capacity to execute prescribed functions necessary to ensure nuclear power plant safety under failure or deliberate inactivation of one redundant channel. Radiy best practices to implement this principle are the following:

- Screening and galvanic separation of input, output circuits and power circuits in each channel using electro-optical components
- Radial ("point-to-point") structure of connections between channels to preserve the possibility and accuracy of data exchange among the rest of channels in case one of them fails

- Physical separation of redundant I&C system channels that are housed in separate cabinets and powered from different sources
- Application of technical solutions and components proven in nuclear power plant operation experience

The independence features of the RadICS Platform are described in Section 6.6.

~~10.3.2~~10.3.3RadICS Platform Diversity Assessment

As stated in NUREG/CR-6303, Section 2.6, "Diversity":

> "Diversity is a principle in instrumentation systems of sensing different parameters, using different technologies, using different logic or algorithms, or using different actuation means to provide several ways of detecting and responding to a significant event. "

The RadICS Platform employs several internal diversity features to provide sufficient protection to address CCFs that may be introduced using digital FPGA technology within the RadICS Platform. To accomplish this, the RadICS Platform addresses the following CCF vulnerabilities that are inherent in FPGA design technology used in the RadICS Modules:

II

—
—

—

]]^{a,c,e}

The validation of the independent and diverse self-tests and diagnostics, Netlist self-tests, as well as, the CPLD watchdog functions are accomplished by the RadICS Module FITs. The Module FITs demonstrate that each RadICS Module detects, reports, and performs the appropriate actions in accordance with the three defined fault types. Module FIT demonstrates that all Module Hardware Unit failures are covered by the Module self-test and diagnostic logics and the CPLD watchdog functions accordingly to place the RadICS Platform in a safe state when required and allows for these functions to mitigate any CCF vulnerabilities. The Module FIT cases were developed using the summary of the self-tests credited in the FMEDA for each Module. The validation is performed by the V&V organization as described in Section 7.4.2.1 and 7.4.5.2.

Figure 10-1 shows the diverse measures inherent to the RadICS Platform that are used to mitigate CCF vulnerabilities. The combination of these diverse measures ensure protection against the postulated CCFs.

II

]]a,c,e

Figure 10-1: Diverse Measures to Mitigate CCF Vulnerabilities

Human diversity is not specifically credited in the RadICS Platform for mitigating the potential for digital CCFs. The RadICS Platform meets requirements for having a design team and an independent verification and validation team; however, the RadICS Platform does not require an additional independent design or verification and validation team since it would provide minimal benefits in eliminating digital CCFs. The basis for not incorporating additional human diversity into the Electronic Design development process is consistent with the view that independently developed software is very likely to contain CCF modes, as discussed in a Massachusetts Institute of Technology research report on hazards analysis. It should be noted that there are additional diversity attributes (e.g., human, technological, and functional) that are implicit attributes of the FPGA and CPLD manufacturing

equipment, FPGA and CPLD chip designs, and configuration tools (e.g., Quartus II and RadICS Platform Configuration Tool); however, they are not explicitly defined nor verified for the RadICS Platform diversity strategy.

The RadICS Platform diversity strategy is based on insights drawn from recent Massachusetts Institute of Technology research report sponsored by NRC that independently developed software is very likely to still contain CCF modes. The research report noted that "almost all serious accidents caused by software have involved errors in the requirements, not in the implementation of those requirements in software code." The report noted that the software requirements have had missing cases or incorrect assumptions about the behavior of how the system operated. These problems were attributed to misunderstandings by the engineers of the requirements for safe behavior, such as an omission of what to do and circumstances that are not anticipated or considered. Software may be considered "correct" if it successfully implements its requirements, but the requirements may be unsafe in terms of the specified behavior in the surrounding system, the requirements may be incomplete, or the software may exhibit unintended (and unsafe) behavior beyond what is specified in the requirements. The report noted that redundancy or even multiple versions of the implementations of the requirements does not help in these cases.

The National Research Council was asked by the NRC to conduct a study on application of digital I&C technology to commercial nuclear power plant operations (Reference 10-6). The study has several conclusions and recommendations that are relevant to the application of diversity in the RadICS Platform design. With respect to common-mode software failure potential, the report concluded that use of different programming languages, different design approaches meeting the same functional requirements, different design teams, or different vendors' equipment used to perform the same function is not likely to be effective in achieving diversity (i.e., none of these methods is a proof of independence of failures). The report noted that there is no generally applicable, effective way to evaluate diversity between two pieces of software performing the same function. Superficial or surface (syntactic) differences do not imply failure independence, nor does the use of different algorithms to achieve the same functions.

A more effective means of addressing these types of errors is to use the appropriate system design development techniques that ensure the correctness and completeness of the system requirements (e.g., plant safety analyses, system FMEA, platform FMEDA, diversity and defense-in-depth analyses, and multidiscipline design reviews).

N-version software diversity has been proposed by some as a means of dealing with the uncertainties of design faults in a computer system implementation. One researcher looked at the question "does software diversity buy you more reliability?" (Reference 10-7) The research was motivated by the additional question from a system engineering viewpoint that there may be alternative design options at the systems engineering level that are more cost-effective. The paper noted that the Knight and Leveson experiment did a service to the computing community by showing that failure independence of design faults cannot be assumed. It further noted that from a theoretical standpoint, it has been shown that any variation in the degree of difficulty for particular inputs will result in failure dependency. The paper suggested that excessive reliance on software diversity may be a case of diminishing returns (i.e., high conformity to the wrong specification). As such, it might make more sense to utilize diversity at a higher level so that there is some defense-in-depth against faults in the requirements.

The RadICS Platform defensive measures work to limit the effects of these failures and ensures placement into safe states. These added features address the additional CCF vulnerabilities associated with digital technology and add to the defense-in-depth approach provided by the NRC hardware qualification requirements, plant design features for other licensing basis CCF vulnerabilities (e.g., fire flood, extreme weather mitigation), and the existing signal and functional diversity incorporated in the plant PS design/licensing basis.

The diversity of a typical application using the RadICS Platform technology was evaluated using the methodology outlined in NUREG/CR-7007 (Reference 10-8) is presented in Appendix D.

~~The implementation of diversity in I&C echelons of defense is based on a project-specific application. For example, a nuclear power plant could use the RadICS Platform for the RTS and a completely separate platform for the ESFAS. Alternatively, a single RadICS Platform could be used for the PS at a nuclear power plant, implementing both the RTS and ESFAS safety functions with a separate DAS. The project-specific realization of different I&C echelons of defense using the RadICS Platform is beyond the scope of this Topical Report.~~

~~The RadICS Platform can be used employ signal diversity strategies. Signal diversity is defined as the use of different sensed parameters to initiate a protective action. Signal diversity is a project-specific design decision that can be effectively implemented with the range of input module capabilities in the RadICS Platform. Signal diversity can be used to significantly improve overall PS diversity.~~

~~The RadICS Platform can also be used employ functional diversity strategies. Two signal channels are functionally diverse if they perform different physical functions or employ different algorithms. Functional diversity is a project-specific design decision that can be readily implemented by allocating functionally diverse channels to separate LMs in a RadICS Platform system. As with signal diversity, functional diversity can significantly improve overall PS diversity.~~

~~The RadICS Platform supports system architectures that employ signal diversity to defend against CCFs. The RadICS Platform also can be deployed as a diverse system as part of a project-level D3 strategy. These options do not affect the generic RadICS Platform features (i.e., the hardware, electronic design, or communications features described in Chapter 6). Instead, these options only affect certain project-specific system analysis.~~

~~10.3.3~~10.3.4Defense-in-Depth

The design principle of defense-in-depth is applied to safety-related I&C systems through the concept of echelons of defense. NUREG/CR-6303 defines four I&C echelons of defense: control system, RTS, ESFAS, and monitoring and indicator system. These four echelons are typically thought of as providing concentric barriers of protection.

The four echelons of defense described above are only conceptual and, ~~with the exception of~~except for the monitoring and indication echelon of defense (see Section B.1.4 in BTP 7-19), NRC regulations do not require nor does this guidance imply that RTS and ESFAS echelons of defense must be independent or diverse from each other with respect to a CCF. NRC accepts that the RTS and ESFAS echelons may be combined into a single digital I&C PS platform. However, plant responses to postulated CCF that could impair a safety function must be shown to meet the acceptance criteria defined in BTP 7-19 regardless

of the echelons of defense that may be affected. ~~The project-specific D3 analysis should consider the nuclear power plant's suite of safety and nonsafety I&C systems.~~ The RadICS Platform diversity strategy is implemented at the Module level and is not dependent on the echelons of defense in the plant I&C architecture.

The RadICS Platform diversity solution is an acceptable regulatory solution for the digital CCF vulnerabilities present in the RadICS Platform. NRC BTP 7-19, Revision 6, states that there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF: diversity or testability. With respect to the diversity option, BTP 7-19 specifies that when sufficient diversity exists in the PS, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

The RadICS Platform can be used employ additional signal and functional diversity strategies. Signal diversity is defined as the use of different sensed parameters to initiate a protective action. Signal diversity is a plant-specific design decision that can be effectively implemented with the range of input module capabilities in the RadICS Platform. Two signal channels are functionally diverse if they perform different physical functions or employ different algorithms. Functional diversity is a plant-specific design decision that can be readily implemented by allocating functionally diverse channels to separate LMs in a RadICS Platform system. These strategies can be used together with the existing signal and functional diversity incorporated in the plant PS design/licensing basis to further increase the overall diversity in the PS. These options do not affect the generic RadICS Platform features (i.e., the hardware, Electronic Design, or communications features described in Chapter 6). Instead, these options only affect certain plant-specific system analysis. ~~With limited exceptions, meeting the current regulatory guidance on D3 in safety-related I&C systems and replacing existing analog systems with modern digital systems requires installation of a DAS that is separate from the I&C platform (or platforms) used by the PS.~~

10.4 RadICS Diversity Summary

[[

]]^{a,c,e}

The RadICS Platform diversity solution is an acceptable regulatory solution for the digital CCF vulnerabilities present in the RadICS Platform. NRC BTP 7-19, Revision 6, states that there are two design attributes, either of which is sufficient to eliminate consideration of software based or software logic based CCF: diversity or testability. With respect to the diversity option, BTP 7-19 specifies that when sufficient diversity exists in the PS, then the potential for CCF within the channels can be considered to be appropriately addressed without further action.

The RadICS Platform diversity strategy represents a stronger diversity case (i.e., more diversity attributes) than others accepted by NRC for systems based on FPGA technology. The FPGA-based Electronic Design and CPLD-based PSWD provide CCF protection for every RadICS Module in a system. The functional diversity strategy employed for RadICS Module Electronic Designs has a greater degree of diversity than strategies that introduce functional diversity into FPGA electronic designs through the use of various degrees of development team diversity.

The RadICS Platform diversity approach provides other benefits by simplifying the overall I&C systems designs, since a separate diverse actuation system is not required to mitigate digital CCFs. The RadICS Platform diversity strategy leads to a simpler overall I&C architecture than other platform-based diverse technology solutions (e.g., addition of a separate diverse actuation system or different equipment configurations in redundant divisions in a system). The RadICS diversity strategy eliminates the need for additional plant-level best-estimate coping or consequence analyses, since the diverse defensive measures incorporated into the RadICS Modules put the system outputs safe states consistent with the plant safety analyses. The RadICS Platform diversity strategy eliminates the complex intersystem design coordination analysis of two actuation systems controlling safety components.

~~10.4~~10.5 Chapter 10 References

1 Branch Technical Position 7-19, Revision 6, "Guidance for Evaluation of Diversity and Defense- in-Depth in Digital Computer-based Instrumentation and Control Systems"

2 NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"

3 IEC 60880:2006, "Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions"

4 IEC 61226:2009, "Nuclear power plants - Instrumentation and control important to safety - Classification of instrumentation and control functions"

5 John Thomas, Francisco Luiz de Lemos, and Nancy Leveson, Research Report: NRC-HQ-11-6-04-0060, Evaluating the Safety of Digital Instrumentation and Control Systems in Nuclear Power Plants, November 2012.

6 National Research Council, "Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Final Report," Washington, DC, 1997.

7 Bishop, P. G., Adelard LLC, "*Review of Software Design Diversity*," December 1994.

8 NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems."

Appendix D: Evaluation of Diversity in an Application Using the RadICS Platform

The diversity of a typical application using the RadICS Platform technology was evaluated using the methodology outlined in NUREG/CR-7007 Reference D-1).

D.1 Evaluation Process

The NUREG/CR-7007 evaluation process consists of the following steps:

1. Classify the diversity strategy — This step involves recognition of the technology employed in the diverse systems based on the design descriptions or, if explicitly referenced, identification of the specific diversity strategy selected.
2. Confirm inherent diversity credit — This step relates to the determination of technology usage and the impact of technology difference.
3. Identify intentional diversity usage — This step consists of identification of the diversity criteria that are intentionally applied. The documentation of the proposed diversity strategy should explicitly describe the intentional diversities on which it is based.
4. Categorize diversity usage in relation to the corresponding strategy classification — This step involves capturing the combination of diversity criteria in either tabular form or a spreadsheet followed by classification in terms of a corresponding strategy and subsequent determination of the degree of adherence to one of the strategies identified in NUREG/CR-7007
5. Assess the adequacy of the diversity strategy — The activity associated with this step depends on the categorization of the proposed diversity strategy determined in Step 4.

A baseline strategy is one where the diversity usage is consistent with one of the baseline combinations of diversity criteria defined for any of the three strategy classifications in NUREG/CR-7007. The associated actions are to confirm that the diverse systems provide the specified technology difference (Step 1), the system designs do not compromise the related credit for inherent diversity (Step 2), and the explicit diversity usage employs the full set of intentional diversities (Step 3).

A variant of baseline strategy is one where the diversity is consistent with one of the alternate combinations of diversity criteria described for any of the three strategy classifications. The associated actions are to perform an assessment comparable to that described for the baseline strategy category (Step 5) with the supplemental determination of whether the conditions associated with suitability of the variant are present.

The order of steps 2 and 3 were reversed for the RadICS diversity strategy to better align the steps with the RadICS diversity strategy decisions. Specifically, the key decisions affecting the diversity strategy were chips selection and IEC 61508 Safety Integrity Level (SIL) 3 certification (i.e., functionally diverse self-tests and diagnostics). From these key decisions other inherent diversity attributes flowed from the detailed design implementation.

D.2 Diversity Strategy Classification

The RadICS Platform employs several internal diversity features to provide sufficient protection to address CCFs that may be introduced using digital FPGA technology within the RadICS Platform. The RadICS defensive measures work together to limit the effects of these failures and place the system into defined safe states. This RadICS Platform diversity strategy flows directly from the design strategy to achieve IEC 61508:2010 SIL 3 certification.

The RadICS Platform diversity strategy is a variant of the Strategy C, "Architectural Variants within a Technology."

D.3 Identification of Intentional Diversity Usage for RadICS Platform

The CPLD-based watchdog in the PSWD Unit is separate and inherently diverse from the Module FPGAs. Table 10-1 identifies the key technology differences between the FPGAs and CPLD. These inherent technology differences mitigate the consequences of common cause failure vulnerabilities associated with the FPGA and CPLD chip technologies. Other aspects of the RadICS Platform diversity strategy are discussed in Section 10.3.3

Appendix A of NUREG 7007/CR defines seven diversity attributes and related diversity criteria. The intentional diversity attributes specified for the RadICS Platform are:

- Design: Different architectures based on the intentional use the FPGA for the Electronic Design safety functions (i.e., signal acquisition, signal conversion, protection algorithms, and communications) and associated self-test and diagnostics and the CPLD for the PSWD function.
- Equipment Manufacturer: Same manufacturer of different versions of the same technology class (i.e., programmable logic device) based on the selection of FPGAs and CPLDs manufactured by Altera.
- Logic Processing Equipment: Different component integration architectures based on the allocation of Electronic Design safety function and self-test and diagnostic functions to segregated portions of the FPGA and the allocation of the PSWD functions to the CPLD.
- Function: Different purpose, function, control logic, or actuation means of same underlying mechanism based on the explicit design of the FPGA Electronic Design safety functions and functionally diverse self-test and diagnostic functions along with the separate and functionally diverse PSWD functions on the CPLD through the FMEDA process.
- Life-cycle: Different management teams within the same company based on the independence between the design team and the V&V team for the validation of the self-test and diagnostic and PSWD functions through FIT.
- Life-cycle: Different lifecycle documents for development of the FPGA self-test and diagnostics and PSWD functions on the CPLD.
- Logic: Different algorithms, logic, and program architecture based on the hardware parallelism inherent to FPGA technology for executing logic functions and control algorithms in a parallel mode and the segregation of Electronic Design safety functions and self-test and diagnostic functions on the same integrated circuit.

- Logic: Different algorithms, logic, and program architecture between the FPGA self-test and diagnostics and PSWD functions on the CPLD. No common design element or libraries used for the development of these separate functions.

D.4 Confirmation of Inherent Diversity Credit

The key decisions to use FPGA and CPLD chips along with the decision to achieve SIL 3 certification resulted in a number inherent diversity attributes for the RadICS diversity strategy. The FPGA technology allows for more deterministic performance than a microprocessor due to capability of executing logic functions and control algorithms in a parallel mode due to the hardware parallelism inherent to FPGA technology. This parallelism also provides the ability to segregate functions on the same integrated circuit (e.g., such as Electronic Design safety functions and self-test and diagnostics). The resulting circuits are pure hardware without additional layers of platform software (operating system, drivers, etc.). Dedicated separate hardware for all functions provides the advantages of computational efficiency, but from the reliability point of view, a more important aspect is the separation of functions. There is no need for resource allocation such as memory, processor time, or data transfer on a bus. This eliminates the risk of functions interfering with each other or with the operating system or other platform functions.

The inherent diversity attributes credited for the RadICS Platform are:

- Logic Processing Equipment: Different data flow architectures based on the parallel processing of the Electronic Design safety function signals and the segregation of parallel processing of the self-test and diagnostic signals.
- Function: Different response time scale based on the parallel processing of the individual Electronic Design safety function signals and the use of three separate clock domains for the Electronic Design safety functions, self-test and diagnostic functions, and the PSWD functions.
- Life-cycle: Different designers, engineers, and/or programmers by crediting the third-party IEC 61508 certification organization for its role with the validation of the self-test and diagnostics, PSWD functions, and Netlist self-tests through the FMEDA.
- Life-cycle: Different implementation/validation teams by crediting the independent Radiy validation for its role with the validation of the self-test and diagnostics, PSWD functions, and Netlist self-tests through the fault insertion testing based on test cases established by the third-party IEC 61508 certification organization.
- Logic: Different timing or order of execution based on the parallel processing of the individual Electronic Design safety function signals and the use of three separate clock domains for the Electronic Design safety functions, self-test and diagnostic functions, and the PSWD functions.
- Logic: Different runtime environments based on the parallel processing of the individual Electronic Design safety function signals and the use of three separate clock domains for the Electronic Design safety functions, self-test and diagnostic functions, and the PSWD functions.
- Logic: Different functional representations based on the fundamental differences in the functionality of Electronic Design safety functions, self-test and diagnostic features, and the PSWD Unit.

D.5 Identification of Intentional Diversity Typical of Applications Using a RadICS Platform

The intentional and inherent diversity attributes identified for the RadICS Platform augment the existing diversity features of the I&C system designs for the operating fleet. The functional and signal diversity incorporated into the protection system functional requirements is maintained. This diversity is expressed in the signal selection and protection system algorithms established and accepted for the plant design. The additional functional diversity that has been added to reactor trip systems based on operating experience (e.g., requiring both undervoltage and shunt trip features for reactor trip breakers) is maintained.[11] Additional diversity has been added to the plant I&C designs through compliance with 10 CFR 50.62 is maintained. [12]

The intentional system diversity attributes that exist in operating plants and maintained for systems modernized with the RadICS Platform are:

- Function: Different underlying mechanisms to accomplish safety function based on the existing system echelons (i.e., control reactor trip, engineered safety features actuation, and monitoring), reactor trip breaker action mechanisms, and anticipated transients without scram (ATWS) risk reduction systems.
- Signal: Different parameters sensed by different physical effects based on the existing signal diversity in the reactor trip, engineered safety features actuation, and ATWS risk reduction systems.

D.6 Comparison of RadICS Diversity to Strategy C

The RadICS Platform diversity attributes are compared to the diversity attributes for Strategy C in Table D-1. The differences are identified below:

- Equipment Manufacturer – The RadICS Platform is conservatively credited with less diversity than Strategy C by treating the FPGA and CPLD as different versions of the same product rather than different products.
- Logic Processing Equipment – The RadICS Platform is conservatively credited with less diversity than Strategy C by treating the FPGA and CPLD logic process as different logic processing versions in same architecture rather than different logic processing architectures since the FPGA and the CPLD originate from different families of devices from the same company. They have different microarchitectures and structural characteristics.
- Function – The RadICS Platform is credited with more diversity than Strategy C by recognizing the inherent diversity associated with the three separate clock domains. Additionally, the intentional diversity typical of applications using a RadICS Platform with the different underlying mechanisms to accomplish safety function present in the existing plant I&C system designs (ATWS operating experience and 10 CFR 50.62) is also recognized.

[11] NRC Generic Letter 83-28, "Required Actions Based on Generic Implications of Salem ATWS Events"
[12] 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants."

- Life-cycle – The RadICS Platform is conservatively credited with less diversity than Strategy C by treating the third-party IEC 61508 certification organization as a different management team within the same company rather than as a different design company due to its focused role with the validation of the self-test and diagnostics through the FMEDA.
- Logic - The RadICS Platform is credited with more diversity than Strategy C by recognizing the inherent diversity for different timing or order of execution based on the parallel processing of the individual Electronic Design safety function signals and the use of three separate clock domains for the Electronic Design safety functions, self-test and diagnostic functions, and the PSWD functions.
- Signal - The RadICS Platform is conservatively credited with less diversity than Strategy C by only recognizing that different are parameters sensed by different physical effects based on the existing signal diversity in the protection system utilizing the RadICS Platform. Additional diversity may be present in the existing overall plant architecture and the combination of the control, reactor trip, engineered safety features actuation, monitoring, and ATWS risk reduction systems. This additional diversity is credited in the evaluation of the RadICS diversity strategy.

Table D-1: Comparison of RadICS Diversity to Strategy C

Diversity Attribute	Strategy C	RadICS Platform
Design		
Different technologies	-	-
Different approaches within a technology	-	-
Different architectures	X	X
Equipment Manufacturer		
Different manufacturers of fundamentally different equipment designs	-	-
Same manufacturer of fundamentally different equipment designs	-	-
Different manufacturers of same equipment design	X	-
Same manufacturer—different version	-	X
Logic Processing Equipment		
Different logic processing architectures	X	-
Different logic processing versions in same architecture	-	X
Different component integration architectures	-X	-
Different data flow architectures		i
Function		
Different underlying mechanisms to accomplish safety function	-	X
Different purpose, function, control logic, or actuation means of same underlying mechanism	X	X
Different response time scale	-	i
Life-cycle		
Different design organizations/companies	X	-
Different management teams within the same company	-	X
Different designers, engineers, and/or programmers	i	i

Diversity Attribute	Strategy C	RadICS Platform
Different implementation/validation teams	i	i
Logic		
Different algorithms, logic, and program architecture	X	X
Different timing or order of execution	-	i
Different runtime environments	X	i
Different functional representations	X	i
Signal		
Different parameters sensed by different physical effects	X	X
Different parameters sensed by the same physical effects	X	-
Same parameter sensed by a different redundant set of similar sensors	X	-

D.7 Adequacy of the RadICS Diversity Strategy

The intentional and inherent diversity attributes for the RadICS Platform were entered into the NUREG/CR-7007 worksheet. The results are shown in Table D-2. The results for the RadICS Platform (i.e., 0.97 normalized score) compare favorably with the results for Strategy C (i.e., 0.98 normalized score).

D.8 Appendix A References

1 NUREG/CR-7007, "Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems"

Table D-2: NUREG/CR-7007 Worksheet Results for RadICS Platform

	ATTRIBUTE CRITERIA	Click to Clear Worksheet		RadICS Application		
		RANK	DCE WT	INT	INH	SCORE
DESIGN	Different technologies	1	0.500			0.000
	Different approaches within a technology	2	0.333			0.000
	Different architectures	3	0.167	X		0.167
	DAE WT. AND SUBTOTAL		1.000		0.167	0.167
EQUIPMENT MANUF.	Different manufacturers of fundamentally different equipment designs	1	0.400			0.000
	Same manufacturer of fundamentally different equipment designs	2	0.300			0.000
	Different manufacturers of same equipment design	3	0.200			0.000
	Same manufacturer of different versions of the same equipment design	4	0.100	X		0.100
	DAE WT. AND SUBTOTAL		0.250		0.025	0.100
LOGIC PROC. EQUIP.	Different logic processing equipment architectures	1	0.400			0.000
	Different logic processing versions in same equipment architecture	2	0.300	X		0.300
	Different component integration architectures	3	0.200			0.000
	Different data flow architectures	4	0.100		i	0.100
	DAE WT. AND SUBTOTAL		0.644		0.258	0.400
FUNCTION	Different underlying mechanisms to accomplish safety function	1	0.500	X		0.500
	Different purpose, function, control logic, or actuation means of same underlying mechanism	2	0.333	X		0.333
	Different response time scale	3	0.167		i	0.167
	DAE WT. AND SUBTOTAL		0.600		0.600	1.000
LIFECYCLE	Different design organizations/companies	1	0.400			0.000
	Different management teams within the same company	2	0.300	X		0.300
	Different designers, engineers, and/or programmers	3	0.200		i	0.200
	Different testers, installers, or certification personnel	4	0.100		i	0.100
	DAE WT. AND SUBTOTAL		0.683		0.410	0.600
SIGNAL	Different reactor or process parameters sensed by different physical effects	1	0.500	X		0.500
	Different reactor or process parameters sensed by the same physical effect	2	0.333			0.000
	The same process parameter sensed by a different redundant set of similar sensors	3	0.167			0.000
	DAE WT. AND SUBTOTAL		0.867		0.434	0.500
LOGIC	Different algorithms, logic, and logic architecture	1	0.400	X		0.400
	Different timing or order of execution	2	0.300		i	0.300
	Different runtime environments	3	0.200		i	0.200
	Different functional representations	4	0.100		i	0.100
	DAE WT. AND SUBTOTAL		0.733		0.733	1.000
	RadICS Score (x100)				263	
	Normalized Score				0.97	
	Basis for Normalizing	271				

Enclosure 3

Comments on the Draft List of Plant-Specific Action Items Related to Internal Diversity Features

RPC RadICS LLC recommends that the draft Plant-Specific Action Item 2.10 be replaced with the following:

2.10 Demonstration of Adequate Diversity - As discussed within Section #.# of this SE, an applicant or licensee referencing this "RadICS Topical Report" SE should ensure methods of providing internal diversity for the purpose of mitigating CCFs within application logic of the RadICS platform have been correctly implemented. The following should be considered:

a. **Self-Diagnostics Design Requirements** – The licensee must establish requirements for validation testing of Type III self-diagnostics features to ensure plant safety requirements are satisfied.
b. **Plant Specific Fail-Safe Behavior Requirements Definition** –The Fail-Safe state requirements shall be established by the licensee for all components actuated by the RadICS Platform to ensure plant safety is achieved when RadICS system logic failures (e.g., Type I, II, or III faults) are detected by system self-diagnostic functions.
c. **Conservation of Existing Diversity Measures** – The applicant or licensee must confirm that installation of a RadICS protection system is diverse from for the system for reducing the risk from anticipated transients without scram (ATWS), as required by 10 CFR 50.62 and existing diversity attributes of the existing protection system are preserved in the upgraded system. The existing diversity in the protection system is typically expressed in the signal selection and protection system functional algorithms established and accepted for the plant design.

Enclosure 4

Withholding Affidavit Related to the Proprietary Material in Enclosure 1