UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

June 11, 2018

Mr. Anton Andrashov, Director
Research and Production Company RadICS
29 Geroyiv Stalingradu Street
25009 Kirovohrad, Ukraine

SUBJECT: REGULATORY AUDIT REPORT FOR APRIL 2-5, 2018, RadICS DIGITAL L&C PLATFORM TOPICAL REPORT" (CAC NO. MF8411; EPID L-2016-TOP-0010)

Dear Mr. Andrashov:

By letter dated September 20, 2016 (Agencywide Documents Access and Management System Accession (ADAMS) No. ML16274A346), Research and Production Corporation RadICS (RPC RadICS) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review Topical Report (TR) "RadICS Digital I&C [Instrumentation and Control] Platform Topical Report." The TR is supported by documentation that includes plans, requirements, design specifications, programming and hardware testing, independent verification and validation, and equipment qualification testing.

From April 2, 2018, through April 5, 2018, the NRC staff performed a regulatory audit at the Kinectrics facility in Toronto, Canada. The purpose of this letter is to provide RadICS with the results of the regulatory audit. Documented in the enclosed report are the observations the NRC staff identified during the audit.

If you have any questions regarding this matter, I may be reached at 301-415-7297 or by electronic mail at Joseph.Holonich@nrc.gov.

Sincerely,

/RA/

Joseph J. Holonich, Senior Project Manager
Licensing Processes Branch
Division of Licensing Projects
Office of Nuclear Reactor Regulation

Docket No. 99902032

Enclosure:
Regulatory Audit Report

SUBJECT: REGULATORY AUDIT REPORT FOR APRIL 2-5, 2018, RadICS DIGITAL L&C PLATFORM TOPICAL REPORT" (CAC NO. MF8411; EPID L-2016-TOP-0010) DATED JUNE 11, 2018

DISTRIBUTION:
PUBLIC
RidsNrrDlp
RidsNrrDlpEicb
IJung, NRO
DMorey, NRR
RidsACRS_MailCTR
RidsNrrDlpPlpb
KMott, NRO
RidsOgcMailCenter
RidsNrrLADHarrison
JHolonich, NRR
MWaters, NRR
RidsNroOd
RidsResOd
RStattel, NRR

ADAMS Accession No.: ML18106A025 ***via e-mail** **NRR-106**

OFFICE	NRR/DLP/PLPB/PM*	NRR/DLP/PLPB/LA*	NRR/DE/EICB/BC*
NAME	JHolonich	DHarrison	MWaters
DATE	06/07/2018	06/06/2018	05/25/2018
OFFICE	NRO/DE/ICE/BC*	NRR/DLP/PLPB/BC	NRR/DLP/PLPB/PM
NAME	DTaneja for IJung	DMorey	JHolonich
DATE	06/06/2018	06/11/2018	06/11/2018

OFFICIAL RECORD COPY

U.S. Nuclear Regulatory Commission Staff RadICS Instrumentation and Control Platform Regulatory Audit Report Toronto, Canada

Background

The U. S. Nuclear Regulatory Commission (NRC) staff is evaluating the RadICS instrumentation and control (I&C) Platform License Topical Report (LTR), 2016-RPC003-TR-001, "RadICS Topical Report," Revision 0 (Agencywide Documents Access and Management System Accession (ADAMS) Accession No. ML16274A348). RadICS is seeking generic approval of the RadICS platform for use in safety systems in nuclear power plants.

Regulatory Audit Bases

As part of its evaluation, the NRC staff conducted an audit of the RadICS platform design and development processes. To support this review, the NRC staff visited the Kinectrics qualifications testing facility located in Toronto, Canada, where the RadICS I&C Platform testing was being performed. The basis of this audit was the RadICS LTR and the following regulations and regulatory guidance:

- Title 10 of the *Code of Federal Regulations* (10 CFR), Section 50.54 (10 CFR 50.54), "Conditions of licenses," (jj) and 10 CFR 50.55, "Conditions of construction permits, early site permits, combined licenses, and manufacturing licenses," (i), require that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

- 10 CFR 50.55a, "Codes and standards," (h), "Protection and Safety Systems," incorporates the 1991 version of Institute of Electrical and Electronics Engineers (IEEE) Std. 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," by reference, including the correction sheet dated January 30, 1995.

- 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants"
  - General Design Criterion (GDC) 1, "Quality standards and records"
  - GDC 2, "Design bases for protection against natural phenomena"
  - GDC 4, "Environmental and dynamic effects design bases"
  - GDC 13, "Instrumentation and control"
  - GDC 19, "Control Room"
  - GDC 20, "Protection system functions"
  - GDC 21, "Protection system reliability and testability"
  - GDC 22, "Protective system independence"
  - GDC 23, "Protective system failure modes"
  - GDC 24, "Separation of Protection and Control Systems"
  - GDC 25, "Protection System Requirements for Reactivity Control Malfunctions"

- GDC 29, "Protection against Anticipated Operational Occurrences" Commercial Grade Dedication," (10 CFR Part 21, "Reporting of Defects and Noncompliance," and the commercial grade dedication (CGD) processes and methods as approved by the NRC staff ADAMS Accession No. ML12205A284) in Electric Power Research Institute

- TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications” (ADAMS Accession No. ML103360462).

- Digital Safety System Software Quality and Processes, 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” as discussed in Branch Technical Position (BTP) 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation And Control Systems” (ADAMS Accession No. ML070670183) and applicable regulatory guides (RGs).

- Secure Development Environment, criterion specified in RG 1.152, Revision 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants (ADAMS Accession No. ML102870022).

- NUREG-0800, “NRC Standard Review Plan,” (SRP), Chapter 7, Table 7.1 (ADAMS Accession No. ML070460342) identifies RGs, BTPs, and industry standards that contain information, recommendations, guidance and, in general, provide an acceptable basis to implement the above requirements for both hardware and software features of safety-related (SR) digital I&C systems.

Regulatory Audit Scope

This audit was conducted in the Office of Nuclear Reactor Regulation Office Instruction LIC-111, “Regulatory Audits” (ADAMS Accession No. ML082900195). The NRC staff reviewed procedures and records related to RadICS platform development processes. The NRC staff evaluated the effectiveness of software development activities to determine the degree to which processes described in the RadICS LTR are being implemented to achieve a high-quality system for use in a nuclear facility.

A secondary purpose of the audit was to gain a better understanding of the RadICS development life-cycle processes to support the evaluation of the RadICS Platform and to assess the capabilities of the RadICS platform to determine the degree to which a RadICS based I&C safety system is capable of meeting regulatory acceptance criteria as described in Chapter 7 of the SRP. The NRC staff will use the results of this audit to support its safety conclusions.

Entrance Meeting

The NRC staff provided an overview of the audit plan and discussed the objectives for the audit. Facility logistics and the detailed schedule of audit activities were then reviewed and revised to accommodate availability of participants.

Presentations by Radics LLC

Radics LLC provided the following presentations during the course of the audit;

- Qualification Test Specimen (QTS) Overview
- Tracing Presentation
- Quality Assurance (2 Part)
- Functional Safety Management

- RadICS Product Configuration Tools (RPCT)
- Monitoring and Tuning System (MATS)
- Diversity Strategy
- Power Supply Watchdog (PSWD)
- Hardware Redundancy and Failure Detection

Equipment Demonstration

To begin its demonstration of the RadICS equipment, the vendor presented an overview of the QTS. Radics LLC then demonstrated the RadICS platform system being used for equipment qualification testing in the Kinectrics testing facility. This demonstration included performance of the following activities.

- Various system module replacements
- System start-up, reboot operations
- Attempt to insert module into an incorrect chassis slot
- Attempts to changing tuning parameters without meeting necessary prerequisites
- Insertion of an incorrectly configured Logic Module (LM)
- Performance of sample tuning adjustment
- Monitoring and tuning system use for monitoring LM performance in real time
- Low input voltage/frequency dropout test performed
- Burst of events test performed
- Fault to fail safe state demonstrated
- Reconfiguration of a LM performed

Anomaly Process Review

The NRC staff reviewed and discussed the anomaly reporting procedures used by Radics LLC during product development to confirm understanding and use of the anomaly resolution processes.

The NRC staff found that anomalies are screened and reviewed in accordance with the Radics LLC quality assurance (QA) program. When issues identify conditions adverse to quality, such as failures, malfunctions, deficiencies, deviations, defective material and equipment, and non-conformances, they must be promptly identified and corrected. Radics LLC reviews of anomaly reports include a process for identifying significant conditions adverse to quality.

The corrective measures reviewed by the NRC staff indicated that causes of the anomalous conditions are determined and corrective actions are taken to preclude recurrence of the issue. The NRC staff observed that identification of significant conditions adverse to quality including the cause of the conditions and the corrective actions taken are required to be documented and reported to appropriate levels of Radics LLC management.

Requirements Thread Reviews

To facilitate performance of requirements thread reviews, the NRC staff asked Radics LLC to prepare and discuss requirements traceability for sample RadICS platform requirements. Radics LLC presented an example Tuning Change Restriction requirement for various modes of equipment operation from the field programmable gate array (FPGA) Safety Controller (FSC)

Safety Requirements Specification. The requirements associated with this thread traced back to a perceived safety need requirement in the FSC Product Concept Document.

Radics LLC explained how the requirement had been implemented and tested during the RadICS platform development processes. Radics LLC showed how the Requirements had been traced to design development activities performed. This requirement was successfully traced to the following documents:

- Product Concept Document
- Safety Requirements Specification
- Product Architecture Document

Further thread evaluations were then conducted by the NRC staff upon return to the NRC offices using documentation made available on the RadICS SharePoint site. The following requirements were successfully evaluated by the NRC staff:

- Requirement 1 – UCR.05, “Fail Safe State Upon failure detection by diagnostic test result,”
- Requirement 2 – MTR.02a, “Continuous Indication of RadICS module status,” and
- Requirement 3 – SSC.08, “Time Interval for diagnostic self-checks.”

The NRC staff was able to trace selected requirements to implementation documents and verify that traceability was appropriately established and maintained.

Configuration Management

The NRC staff discussed the configuration management processes related to the storage and modification of the RadICS platform software, logic configuration files, and controlled documents. The NRC staff performed a tabletop exercise relating to the software check-out/check-in process. Radics LLC personnel explained that RadICS controlled files are stored in a corporate electronic repository system and a change control board approval is required to allow check-out of these files for the purpose of making changes to them.

A change implementation board decides what documents or files need to be updated for the change and only access to those files is provided to the persons responsible for making the changes. When a file is then checked out, access to the file becomes blocked to all other project team members such that simultaneous changes cannot be made to the same file. The process also includes provisions for revision control so that all versions of each managed file are retained and can be reviewed for audit purposes.

Portable media is used to transfer the software or controlled files from the controlled repository to the development environment. A change validation board determines what validation activities must be performed to complete the change process. The files are verified to ensure they match the controlled master copy. Once a change is made and the affected files have been reviewed by the validation team, the files are transferred back to the controlled repository via portable media for check-in and files are assigned a new revision number.

RadICS Configuration Management Document Review

The NRC staff reviewed the Change Request form, the Project Change Log form, and the Change Request Requirement Identification (RID) Matrix form to gain an understanding of how RadICS platform configurations were being captured and controlled in accordance with the Software Configuration Management Plan (SCMP).

The Change Request form includes information on the files affected by the change including a unique change request identifier, a description of the reason for the change, the date of the request, and other pertinent information. The change request also identifies the initiator and includes a section for evaluation of the change by the change control board. Approval of the change request is only provided upon successful performance of an impact analysis. Once approved by the change control board, the change is performed and a change verification board documents the required verification methods to be applied before closeout can be achieved. The NRC staff asked several questions on how the change request forms were used to ensure correct configurations were established and how they would be used to reflect approved configuration changes to RadICS equipment.

The Change Log form is a table that is used to track status and progress of change requests. The format of the change log form table was found to be standardized, clear, and concise.

The Change Request RID Matrix is a table used to track analyses of changed requirements resulting from the changes made. This matrix captures affected requirements Identifications for the made changes. The format of the change request RID matrix table was found to be standardized, clear, and concise.

Quality Assurance

The Radics LLC QA manager provided a two part presentation on RadICS QA. Discussions were held regarding the history of the QA programs and the relation to Radics LLC 10 CFR Part 50 Appendix B compliant QA programs. Platform component dedications are being performed by Radics LLC to bring Radiy components into compliance with Appendix B. The CGD Plans (docketed in phase 1) were reviewed and Radics LLC explained that results of the CGD processes will be provided to the NRC in the phase 2 submittal. Radics LLC also described the format in which CGD results will be provided to the NRC to document methods used to show that critical characteristics are met for each of the qualified platform components.

A deviation from the RadICS LTR was identified in that Method 3, “Source Verification,” will be used to show that certain critical characteristics have been satisfied for components of the platform. The submitted LTR states that Method 3 will not be used by Radics LLC for the RadICS Platform CGD activity. Radics LLC will make a correction to the LTR as a result of this change and this will be included in the approved version of the LTR. The NRC staff will add a new Open Item to verify that the change is made to the LTR prior to its final approval.

The NRC staff selected several QA procedures for the purpose of confirming implementation of the Radics LLC QA plan. These procedures were; Verification and Validation (V&V), Software Design Verification, Non-Conformance Reporting, Configuration Management, Secure Development and Operating Environment, and Internal and External Audit. In addition, the NRC staff reviewed work instructions for Change Control, RadICS Technology Change Evaluation Process, and Configuration Items identification.

Digital Safety System FPGA Safety Function Application Logic Development

The NRC staff reviewed several safety function application logic development documents to determine how the Radics LLC processes comply with applicable regulations. The LTR describes the FPGA safety function application FPGA electronic design (ED) lifecycle development process used to configure and implement the end user's safety function logic. The RadICS LTR platform utilizes the LM's FPGA to implement and control the end-user's specified safety function actuation application logic. Thus, the NRC staff performed a thread audit review of the LM's ED development process. This review and analysis of the LM's FPGA safety function application logic was conducted over several days during the audit week. The NRC staff requested additional, non-docketed, design documents as well as verbal explanations of the implementation of the LM's FPGA safety function logic requirements.

The NRC staff reviewed the RadICS ED development lifecycle as listed in Figures 7-4 and 8-1 of the LTR and selected several of the LM's FPGA safety function application logic development documents that are utilized according to the safety function logic lifecycle development phases. The NRC staff reviewed and sampled from the below listed safety function logic lifecycle development documents, processes, procedures, and instructions:

- 2016-RPC003-TR-001, "Figure 7-4, RadICS Platform Development Activities (including V&V)," RadICS Topical Report, Revision 0, September 19, 2016
- 2016-RPC003-TR-001, "Figure 8-1, RadICS ED Development Lifecycle and Documents," RadICS Topical Report, Revision 0, September 19, 2016
- D2.1, "FSC Functional Safety Management Plan," Version 3.0, September 13, 2016
- D1.0, "FSC Product Concept Document," Version 1.0M, April 27, 2012
- D3.1, "FSC Safety Requirements Specification," Version 3.0, September 2, 2016
- D5.1, "FSC Product Architecture Document," Version 3.3, September 2, 2016
- D8.21.1, "FSC LM Electronic Design Detailed Description," Version 3.4, December 2017
- 2016-RPC003-TR-001, "Figure 6-12: Functional Diagram of the LM," RadICS Topical Report, Revision 0, September 19, 2016
- D8.11, "FSC FBL Detailed Description," Version 1.1M, March 21, 2014
- Figure A001.C00.V01.R00.CTDM, "Logic Module LM Circuit Diagrams," Sheet 22, Revision 8045, September 2017
- D9.23.1, "FSC LM ED Logic Level Simulation & Timing Test Report," Version 3.1, September 18, 2017
- QP 03-4, "Software Design Verification," Revision 1, November 3, 2017
- D9.24.9.1, "FSC LM ED Place and Route Results Review Report," Version 3.2, December 6, 2017
- D10.1, "FSC Integration Test Plan," Version 3.0, September 2, 2016
- D6.5.1, "FSC LM HW [Hardware] Review Report," Version 3.4, November 14, 2017
- D9.22.1, "FCS LM ED VHDL [Verilog Hardware Description Language] Functional Test Report," Version 3.2, September 15, 2017
- 2017-RTS001-PO-130, "Instruction on Setup and Functional Testing of the RadICS Platform Modules," Revision 2, October 10, 2017
- D4.0, "FSC Safety Validation Test Plan," Version 3.1, August 31, 2017
- D10.4.1, "FSC LM Hardware Fault Insertion Test Report," Version 3.1, August 30, 2017
- QP 03-11, "Verification and Validation (General Procedure)," Revision 2, October 24, 2017
- D3.9, "FSC Requirements Tracing Report," Version V3, Revision R1, March 2018

- D3.9.1 “Requirements Tracing Matrix,” Version 3, Revision 1, March 2018, printout of Capture Sheet for D1.0 on 2015-12-18/8:32:45 AM
- WI 03-11/5, “Traceability Analysis,” Revision 0, February 10, 2016
- CG-24, “Quality Management System, Company Guide-24, Change Control Procedure for Radiy I&C Platform Components and Platform-based Applications,” Version 2.5 [No Date listed]

Several of the above documents are already docketed, and during the audit the NRC staff took the opportunity to examine other supporting LM safety function logic development documentation to help confirm that Radics LLC executes its safety function logic development procedures and processes as detailed in the RadICS LTR.

The NRC staff reviewed and analyzed the above listed RadICS LTR platform logic development process documents used to develop, configure, and implement, the LM’s FPGA safety function logic. The NRC staff verified that the LM’s FPGA safety function application logic lifecycle development plans audited were mutually consistent and were not ambiguous.

The NRC staff requested the specification sheet for the specific FPGA chips utilized in the LM. Radics LLC provided the RadICS platform FPGA chip device data sheets for all RadICS platform modules. In addition, Radics LLC provided the link to the FPGA manufacturer’s website that provided the listing of the FPGA specifications for the NRC staff’s review. The NRC staff discussed several FPGA specification ratings as they relate to the RadICS platform’s FPGA operation within a nuclear power plant safety-related control system application. All of the NRC staff’s questions were acceptably answered.

The NRC staff reviewed the QA documentation which provides justification for the suite of RadICS FPGA logic software tool selection, as listed in D2.3, “FSC Tool Selection and Evaluation Report,” Version 3.0, July 7, 2016. This report provides the results of the review, analysis, evaluation, and justification for selection of the RadICS FPGA development tools that are used to support the RadICS platform lifecycle development processes. The FPGA tool profile of all RadICS platform software tools utilized in the safety development process are listed in the report.

The RadICS platform refers to the suite of FPGA logic development tools as the RPCT. The RPCT is used to customize, configure, and integrate the standard logic ED functions onto the FPGA chip that are contained in the function block library (FBL). During each RadICS platform development project, and throughout all development and testing, the development team (in accordance with Company Guide-25, “Procedure to qualify a new version of software tools”) will check with the tool manufacturer for any tool updates or revisions. All RPCT tools are controlled under the configuration management.

The NRC staff found that the LM’s FPGA safety function actuation logic development documentation provides good evidence to confirm that configuration management processes are being implemented for the RadICS platform. The NRC staff confirmed that management activities (including identification of documents associated with the LM’s FPGA safety related printed circuit board components) are being implemented in accordance with the Radics LLC QA program.

Overall, the NRC staff verified that the LM's FPGA safety function application logic development lifecycle processes and procedures constitute acceptable evidence that the RadICS platform logic lifecycle development plans and processes are being performed as described in the RadICS LTR and maintain safety through the development of the LM's FPGA high quality safety actuation logic.

Diversity and Defense in Depth Discussion

Radics LLC made three presentations pertaining to the capabilities of the RadICS Platform to cope with the effects of Common Cause Failures (CCF) relating to platform logic. The first of these presentations was an overview of the internal diversity features of the RadICS platform design. The second presentation was of the PSWD functions described in the LTR. The third presentation related to the Hardware Redundancy and Failure Detection features of the RadICS platform design. The NRC staff is evaluating the methods used to establish internal diversity as a partial means of addressing CCF hazards.

The NRC staff pointed out that there are plant-specific factors that must be considered in order to completely address the effects of CCF of the platform. Because of this, it will be necessary to include one or more plant-specific action items (PSAIs) in the safety evaluation. These PSAIs will confirm internal diversity features are correctly implemented when they are to be credited for addressing effects of CCF. They will also require licensees to evaluate and define the necessary fail safe states for each safety function performed by the RadICS based safety system.

A new Open Item was initiated to determine what PSAIs will need to be addressed by licensees in order to credit RadICS internal diversity features for addressing CCF related hazards.

The NRC staff requested Radics LLC to develop a list of diversity attributes for internal self-diagnostic functions to support performance of D3 assessments. This will be used by licensees to identify the degree of diversity achieved for the plant-specific application of RadICS equipment. A new Open Item was initiated to capture this request.

Secure Development Environment Discussion

Because RadICS development activities are performed in Kirovograd, Ukraine, the NRC staff was not able to directly observe the secure development environment during the audit at the Toronto Kinectrics facility. To compensate for this limitation, a Radics LLC representative familiar with the physical attributes and network configuration of the Radics LLC/Radiy development facilities was available to discuss security measures in place to establish the secure RadICS platform development environment.

A presentation was provided to the NRC staff describing the development facilities in Kirovograd. The presentation included photographs of the secure areas and access point controls. It also included a network diagram which illustrated the network segments and devices used to implement separation between various development environment components of the network. The NRC staff questioned the configuration management measures used for network components such as firewall and network switch IOS configurations. Radics LLC referred to a document titled Development Environment Specification which provided instructions for establishing a secure RadICS development environment and additional details on how the environment is maintained during system development.

Implementation of secure development and operational requirements are dependent on the application related activities. Therefore, the NRC staff will write a Secure Development and Operational Environment related PSAIs which will be included in the RadICS platform safety evaluation.

Generic Open Items and Plant Specific Action Items Discussion

The NRC presented a draft list of PSAIs which could likely be included in the RadICS platform safety evaluation. This list is included as an Appendix to this report. Each list item was explained and NRC expectations for resolving these items during application development was discussed.

The NRC staff also presented a proposed draft Generic Open Item (GOI) to address use of RadICS components not evaluated by the NRC staff which could likely be included in the RadICS safety evaluation. This proposed GOI is as follows:

> Qualified Platform Components – This safety evaluation is limited to components of the RadICS Platform listed in Table (Qualified Components List) of this safety evaluation. Use of other components for safety related applications is not approved by the NRC and may be subject to additional evaluation and qualification testing.

The proposed GOI was explained and NRC staff expectations for resolving this GOI subsequent to issuance of the RadICS safety evaluation were discussed.

RadICS Platform Qualified Components List Discussion

The NRC staff conducted a discussion of the RadICS Qualified components list provided in the LTR as Table 6-1. Radics LLC will be revising this list to reflect all components by model number which were included in the platform qualification tests including the connectors and cables which connect to the protection units of the system. Radics LLC agreed to share the revised list with the NRC on the audit portal and will include the revised list in the approved version of the LTR. A new Open Item was created to track this activity for Radics LLC to provide advance updated Qualified Component Table 6-1 on audit portal. This will allow NRC staff to create a Qualified Component table in its safety evaluation.

Request for Additional Information Status Discussion

Radics LLC stated that responses to the NRC staffs Request for Additional Information had been drafted and these responses will be submitted to the NRC later in April.

Exit Meeting

During the exit meeting, Radics LLC personnel were provided with a summary of the NRC staff observations made during the audit. The NRC staff also provided a list of audit related documents requested to be placed onto the audit portal to support the audit report development.

Audit Objectives Achieved

During this audit, the NRC staff performed interviews with members of the Radics LLC design, V&V and QA, and information technology organizations. The NRC staff determined the level of independence that exists between these organizations and the level of technical competence established and maintained within the IV&V staff.

Software V&V – By conducting several requirements thread reviews, the NRC staff was able to confirm the degree to which RadICS Platform software V&V program meets the criteria outlined in the RadICS Software Verification and Validation Program, V&V Plan which was developed in accordance with IEEE Standard 1012, “IEEE Standard for Software Verification and Validation.”

Configuration Management – By reviewing the SCMP and the configuration management sheets for various RadICS components, the NRC staff was able to determine the degree to which the RadICS configuration management processes include control measures for both hardware and software configuration management. The configuration management programs used for the RadICS platform were found to be effectively controlling the platform components being evaluated.

Software QA (SQA) – The NRC staff reviewed several Radics LLC QA procedures and interviewed Radics LLC personnel to assess the SQA program effectiveness. The SQA Plan (SQAP) was reviewed for conformance to the requirements of 10 CFR Part 50, Appendix B, and the Radics LLC overall QA program. The RadICS SQAP identifies which QA procedures are applicable to specific software processes. It also identifies particular methods for implementing QA procedural requirements.

Software Safety – The NRC staff evaluated the effectiveness of software safety plans and procedures used for RadICS safety analysis activities in ensuring product safety. The review of the anomaly reporting process and interviews conducted with Radics LLC personnel during the audit indicated that Radics LLC personnel have an understanding of the importance of identifying issues that could affect product and plant safety and of the processes for resolving identified problems.

Secure Development Environment – The NRC staff reviewed information pertaining to the RadICS platform development environment. The results of this review activity will be used to determine conformance to the secure development environment requirements of RG 1.152, Revision 3.

List of Audit Participants:

Name	Role/Title	Organization
Ken Mott	Lead Technical Reviewer	NRC/NRO
Richard Stattel	Lead Technical Reviewer	NRC/NRR
Anton Andrashov	Director	Radics LLC
Kostiantyn Leontiiev	Technical Director	Radiy
Eugene Bulba	Validation Manager	Radics LLC
Eugene Brezhnev	QA Manager	Radics LLC
Vadim Kvasha	IT Manager (connected via Skype)	Radics LLC
Dmytro Kotov	EQ Manager (QTS lab)	Radics LLC
Yuri Shapovalov	Electrical Technician (QTS lab)	Radics LLC
Mark Burzynski	Consultant to Radics LLC	NewClear Day, Inc.
Sean Kelley	Consultant to Radics LLC	NewClear Day, Inc.
Sarah Wildman	Consultant to Radics LLC	NewClear Day, Inc.

Appendix: Draft Plant-Specific Action Item List

1.0 GENERIC OPEN ITEMS

On the basis of its review of the RadICS platform, the NRC staff has identified the following generic open items:

1.1 Qualified Platform Components – This safety evaluation is limited to components of the RadICS Platform listed in Table #.# of this safety evaluation. Use of other components for safety related applications is not approved by the NRC and may be subject to additional evaluation and qualification testing.

2.0 PLANT-SPECIFIC ACTION ITEMS

The following plant-specific actions should be performed by an applicant or licensee referencing this safety evaluation for a safety related system based on the RadICS platform.

2.1 RadICS Platform Changes – An applicant referencing this safety evaluation should demonstrate that the RadICS platform used to implement the plant-specific system is unchanged from the generic platform addressed in this safety evaluation. Otherwise, the licensee should clearly and completely identify any modification or addition to the generic RadICS platform as it is employed and provide evidence of compliance by the modified platform with all applicable regulations that are affected by the changes. In addition, the applicant must verify that modules, features, and or functions that require configuration are properly configured and tested to meet system requirements.

2.2 Application Logic Development Process – An applicant or licensee referencing this safety evaluation should provide oversight to ensure the development of its Application Logic was performed in accordance with a process that is equivalent to the one described in the RadICS Platform Electronic Design Development process as described in Section 8 of the RadICS LTR and evaluated in Section #.# of this safety evaluation.

2.3 System Cycle Time –The licensee must perform timing analyses and functional testing of the application implementation and system configuration to demonstrate that response time performance satisfies application specific requirements established in the plants safety analysis report.

2.4 Plant Specific Equipment Qualification – The licensee must demonstrate that the generic qualification envelope established for the RadICS platform bounds the corresponding plant-specific environmental conditions (i.e., temperature, humidity, radiation and Electro-Magnetic Compatibility (EMC)) for the location(s) in which the equipment is to be installed. The licensee should ensure that specific equipment configuration of RadICS components to be installed is consistent with that of the RadICS equipment used for environmental qualification tests.

2.5 Plant Specific Seismic Qualification – An applicant or licensee referencing this safety evaluation must demonstrate that the qualified seismic withstand capability of the RadICS platform bounds the plant-specific seismic withstand requirements. See Section #.# of this safety evaluation for boundary conditions established for the RadICS platform during Seismic testing.

2.6 Failure Modes and Effects Analysis (FMEA) – An applicant or licensee referencing this safety evaluation must perform a system-level FMEA to demonstrate that the application-specific use of the RadICS platform identifies each potential failure mode and determines the effects of each. The FMEA should demonstrate that single-failures, including those with the potential to cause a non-safety system action (i.e., a control function) that results in a condition requiring protective action (i.e., a protection function), cannot can adversely affect the protection functions, as applicable.

The applicant or licensee should ensure system failure states identified in the FMEA are consistent with system requirements and should review how errors and failures are indicated and managed upon being detected.

2.7 Application Specific System Reliability – An applicant or licensee referencing this safety evaluation should perform a system-level evaluation of the degree of redundancy, diversity, testability, and quality provided in a RadICS platform-based safety system to determine if the degrees provided are commensurate with the safety functions being performed. An applicant or licensee should confirm that a resultant RadICS platform-based system continues to satisfy any applicable reliability goals that the plant has established for the system.

This plant-specific action should consider the effect of possible failures, system-level design features provided to prevent or limit the failures' effects, and any application-specific inclusion of a maintenance bypass to support plant operations.

2.8 Setpoint Methodology – An applicant or licensee referencing this safety evaluation must perform an analysis of accuracy, repeatability, thermal effects and other necessary data for use in determining the contribution of the RadICS platform to instrumentation uncertainty in support of setpoint calculations.

2.9 System Testing and Surveillance – Because a combination of surveillance, RadICS platform diagnostics and automatic self-tests are necessary to provide comprehensive coverage of platform failures, the applicant or licensee referencing this safety evaluation must establish periodic surveillance testing necessary to detect system failures for which automatic detection is not provided. The applicant must also define appropriate surveillance intervals to provide acceptable comprehensive coverage of identifiable system failure modes.

2.10 Diversity and Defense-In-Depth (D3) Analysis – An applicant or licensee referencing this safety evaluation must perform a plant-specific D3 analysis for safety system applications of the RadICS platform.

Replace with the following:

Demonstration of Adequate Diversity – As discussed within Section #.# of this Safety Evaluation (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. Internal Design Diversity – RadICS application specifications should designate whether Internal Diversity is required for each safety function performed by that application.
b. Application Specific Internal Diversity Self-Diagnostics – Specifications should identify any application-specific self-diagnostic features that need to be implemented to address postulated Logic Common Cause Failures.
c. Fail Safe Behavior – Application Specifications should identify application-specific fail-safe behavior that should result from self-diagnostics identified failures.
d. Additional Diversity Measures – Specifications should identify any additional diversity measures, such as functional, signal, or additional logic diversity, that are included in the safety system for the purpose of maintaining plant safety.
e. Extent of Internal Diversity – The applicant or licensee should describe the extent that it relies upon the techniques and processes that provide defense against programming CCFs, which are described in Section #.# of the "RadICS Diversity Analysis" (Reference #.#), for its use of the RadICS platform and its application-specific Logic Module logic. Using this information, the licensee should demonstrate the application adequately addresses potential plant vulnerabilities to common-cause programming failures in consideration of BTP 7-19, as applicable.
f. Identification of Echelons of Defense – Applicant or licensee D3 Analysis should identify the echelon(s) of defense (i.e., control, RTS, ESFAS, and monitoring and display) within the plant that each RadICS platform-based I&C function is assigned.
g. Diverse Manual Control Features – When manual controls are not provided as discrete hardwired components connected to the safety equipment at a point downstream of the plant's digital I&C safety system outputs, the applicant or licensee D3 Analysis should demonstrate simple (e.g., component function can be completely demonstrated by test), dedicated, and diverse program-based digital equipment performs any coordinated system-level actuation logic, if applicable.

2.11 DI&C ISG-04 – although the NRC staff determined that the RadICS platform includes features to support satisfying various sections and clauses of DI&C ISG-04, an applicant or licensee referencing this safety evaluation must evaluate the RadICS platform based-system for compliance with this guidance. The applicant or licensee should consider its plant-specific design basis. This safety evaluation does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events along with its direct and indirect consequences.

Add internal SE references to ISG4 platform evaluations.

2.12 IEEE Std. 603 – Although the NRC staff determined that the RadICS platform is capable of satisfying various sections and clauses of IEEE Std. 603-1991, an applicant or licensee referencing this safety evaluation should identify the approach taken to satisfy each applicable clause of IEEE Std. 603-1991 with consideration of the plant-specific design basis.

This safety evaluation does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct and indirect consequences. Therefore, an applicant or licensee should demonstrate that the plant-specific and application-specific use of the RadICS platform satisfies the applicable IEEE Std. 603-1991 clauses in accordance with the plant-specific design basis and safety system application.

2.13 IEEE Std. 7-4.3.2 – Even though the NRC staff determined that the RadICS platform is capable of satisfying various sections and clauses of IEEE Std. 7-4.3.2-2003, an applicant or licensee referencing this safety evaluation should identify the approach taken to satisfy each applicable clause of IEEE Std. 7-4.3.2-2003 with consideration of the plant-specific design basis.

This safety evaluation does not address a specific application, establish a definitive safety system or protective action, or identify and analyze the impact of credible events including direct and indirect consequences. Therefore, the applicant or licensee should demonstrate that the plant-specific and application-specific use of the RadICS platform satisfies the applicable IEEE Std. 7-4.3.2-2003 clauses in accordance with the plant-specific design basis and safety system application.

2.14 Secure Development and Operational Environment – An applicant or licensee referencing this safety evaluation for a SR plant-specific application should ensure that a secure development and operational environment has been established for its plant-specific application, and that it satisfies the applicable regulatory evaluation criteria of RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."