CURTISS-WRIGHT

Digital Safety Systems: Deterministic Diverse Digital Solutions

Engineering, Licensing, Maintenance and Operational Solutions

For nearly 20 years, the nuclear industry and its suppliers have been working with the Nuclear Regulatory Commission (NRC) to reduce licensing uncertainty for safety-related digital systems; however, limited progress toward altering digital solutions regulations prompted the issuance of an NRC Commission directive. Issued in February of 2016, the NRC Commission directed its staff to develop an Integrated Action Plan to determine methods, processes, and practices that will permit digital systems use in safety-related applications.

Diversity eliminates Common Cause Failure licensing uncertainty. The RadICS platform is built upon internal functional and technological diversity, yielding a deterministic platform that can fulfill safety-related requirements without execution uncertainty. Built in partnership with Radics, LLC, the Curtiss-Wright Digital Safety System (DSS) is a synergistic and holistic solution that possesses the strengths of both analog and digital technologies – without their associated weaknesses. The RadICS digital platform is currently deployed and performing safety functions worldwide.

RESOLVING REGULATORY CONCERNS FOR DIGITAL SAFETY SYSTEMS

The NRC DI&C ISG-06 R2 defines a series of regulatory concerns surrounding the use of digital systems in safety-related applications:

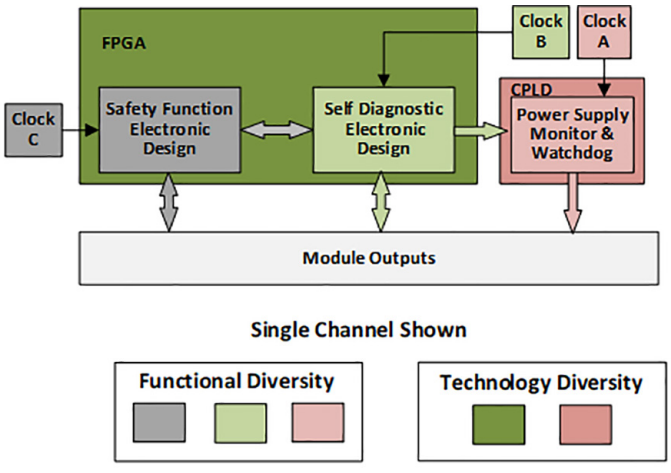
Common Cause Failure

The Common Cause Failure (CCF) risk in digital system software constitutes the principal threat to compromising predictable behavior of the system's safety function. Until the current regulatory stance is legally changed, devices that cannot be 100% tested or systems that are not approved as diverse by the regulator cannot be used in safety-related systems.

The NRC's approval of the RadICS platform credits the internal diversity of the design. Diversity removes the "risk" from the licensing process and eliminates the requirement for a diverse actuation system. The Digital Safety System is functionally and technologically diverse, and thus immune to common cause failure mechanisms that could prevent the system from performing its safety functions. It implements three separate functionally diverse asynchronous domains (function, diagnostic, and watchdog clock/power supply) to ensure execution of all safety functions.

Diversity

Per BTP 7-19, the two conditions that satisfy safety system regulatory requirements are 100% testing of the digital device or diversity. Furthermore, in NUREG/CR-7007 the NRC research identified three primary strategies of diversity in accordance with differences in technologies that serve as the basis for diverse systems, redundancies, or subsystems. These strategies involve: (a) fundamentally diverse technologies (e.g. analog and digital implementations), (b) distinctly different technology approaches (e.g. different digital technologies, such as the distinct approaches represented by programmable logic devices and general purpose microprocessors), and (c) architectural variations within a technology (e.g. different digital architectures, such as the diverse microarchitectures provided by different central processing units).



Diversity Map of the Digital Safety System

Digital Safety Systems: Deterministic Diverse Digital Solutions

The RadICS platform is credited as diverse in the NRC's Safety Evaluation Report (SER) approving its design. Architectural variations, the use of different physical devices, and the use of asynchronous clocks form the basis of the approval. No other mitigating devices, such as Diverse Actuation Systems (DAS), are required to meet diversity requirements in the safety system regulatory space. This reduces system cost, minimizes long, costly diversity evaluations, greatly simplifies the modification process, reduces system complexity, and simplifies maintenance and operation of the safety-related system.

Self-Diagnostics within a Digital I&C Platform

Modern digital systems possess the ability to perform self-diagnostics and provide real-time system health condition; however, there are concerns that system diagnostics may fail to detect an imminent failure or, alternatively, compromise system operation.

The Safety Integrity Level (SIL) certification (IEC 61508:2010) – one of the most widely accepted certification standards for safety platforms – confirms the Digital Safety System's comprehensive development controls, platform robustness and failure detection mechanisms. The SIL-3 certification level stipulates that the probability of failure on demand is less than 10^{-4}; the RadICS platform is SIL-3 certified and credited as diverse by the NRC which ensures secure and reliable execution of the safety function.

The SIL certified comprehensive diagnostics, independent watchdog clock/power supply, and functional domains, operating in separate execution paths from the safety function, continuously verify system functionality. Embedded failsafe routines automatically drive the channel outputs into a safe state upon detection of a malfunction, and maintenance personnel receive immediate notification of the location and specific failure mechanism.

Independent Verification and Validation

All program development on the RadICS platform and for the safety functions follow the verification and validation (V&V) methods and procedures set forth in IEEE 1012-20004, as endorsed by RG 1.168 R2 and IEC development standards. Additionally, Curtiss-Wright implements safety function development and independent V&V per IEEE 1012 under its 10 CFR Part 50 Appendix B program. The Digital Safety System's SER credits secure development and independent V&V of the Electronic Design (VHDL instructions) for the FPGA/CPLD design of the RadICS platform.

Management Functional Requirements Specification

Curtiss-Wright's Digital Safety System is a functional replacement for existing analog or digital installations: The safety system's original functional requirements document and its audited analog/digital safety system design documentation provide most of the information necessary to develop an equivalent digital safety-related system. The system functional requirements document is used to create the requirement's traceability matrix, as well as the resulting program and hardware requirement specifications, for creating the safety function on the approved platform.

Development & Adherence to Configuration Management

The safety function program configuration management adheres to NRC Regulatory Guide 1.169. Curtiss-Wright uses an audited, automated configuration management process to document compliance.

Use of Smart Devices

Smart sensors, instruments, and actuators can be implemented during the digital safety system deployment and system modernization where required and approved by the regulator. The RadICS platform connects directly to existing sensors and actuators in the plant, using approved actuation and voting devices.

Safety Classification Schemes

The RadICS platform that the DSS is built on is approved for use in the United States for Safety-Related, Class 1E systems. It has also been approved for use in IEC Type 1, 2, 3, 1E, 2E, SH, F1A, F1B, F2, Category A, B, C, NC and Class 1, 2, 3 systems. These safety classifications encompass all reactor protection systems, safety actuation, and safety support systems.

Cyber Security

The Digital Safety Systems are developed and tested in a Curtiss-Wright Secure Development and Operational Environment (SDOE) compliant facility that meets NRC requirements. The RadICS platform was developed in similarly protected facilities with secure, audited resources and physical barriers to improper access.

Curtiss-Wright's DSS is in full compliance with NRC Regulatory Guide 5.71, NEI 08-09 (Appendix D), 10 CFR 73.54, and NRC Regulatory Guide 1.152, Revision 3 – including all processes and procedures that regulate and protect the development and operational environment from internal and external cyber threat vectors. All diagnostic and operational data emanating from the safety system is transmitted via unidirectional fiber optic communications to the maintenance and plant interface systems.

Digital Safety Systems: Deterministic Diverse Digital Solutions

Typical Installation

Taking Credit for On-line Monitoring

The DSS automatically performs continuous on-line diagnostics on all RadICS input and output modules, logic execution hardware, programs, and actuation train devices. Failures in any portion of the system drives system outputs into their safe state, as defined in the system requirements specification. The system is stable, reliable and accurate. The recommended manual system verification interval is at scheduled refueling outage intervals. On-line, semi-automated testing can also be accommodated to minimize outage critical path interference.

Equipment Qualification of Safety System Platforms

The RadICS platform meets or exceeds NRC equipment qualification requirements, including: NRC Regulatory Guide 1.180; IEEE 323; IEEE 344-2004, and EPRI TR-107330. Additional plant-specific DSS hardware provided as part of the DSS is qualified under Regulatory Guide 1.180; IEEE 323; and IEEE 344-2004

Description Language Programmable Hardware Impact

The RadICS platform Hardware Description Language (HDL) programming techniques allowed developers to create function block code elements that are 100% testable. These elements are combined in parallel threads to perform the safety system's deterministic functional requirements. When implemented on an approved internally diverse platform, the result is a fully deterministic safety system solution that does NOT require a separate diverse actuation system.

Automated tools generate and validate the HDL based program, while the independent output validation tool validates the code that is generated from the development tools. Together, these tools deliver automated confirmation of the HDL based safety functions. Closely managed and controlled, the program elements are in use in over 100 safety-related installations worldwide.

Digital Communications

Curtiss-Wright's Digital Safety System conducts inter-channel communications using fiber optic unidirectional communications links. The DSS's RadICS components are programmed and reconfigured using secure tools in an environment protected by physical barriers and multi-level security access. All maintenance and diagnostic data are transmitted from the safety system to the maintenance and diagnostic system via independent unidirectional fiber optic links. The RadICS platform meets all requirements of the NRC DI&C ISG-04.

CONCLUSION

The NRC SER-approved RadICS platform is a functionally and technologically diverse design that eliminates licensing uncertainty.

- NRC-approved, cyber-secure and Common Cause Failure immune safety system
- Design diversity eliminates the need for costly and complex diverse actuation systems
- Fully deterministic diverse digital platform for safety-related applications
- Deployed and performing Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) safety functions worldwide
- Approved for use for Safety-Related Class 1E safety systems
- Eliminates on-line surveillance activities

DIVERSITY ELIMINATES UNCERTAINTY

Using the approved diverse RadICS safety-related platform to fulfill the low safety significant application requirements, CCF vulnerability is eliminated and the modification will invariably "screen out" under 50.59 evaluation.

LOW SAFETY SIGNIFICANT AND IMPORTANT TO SAFETY SYSTEM REPLACEMENT

Use of the RadICS platform in low safety significant and important to safety systems eliminates the risk assessment requirements under RIS 2002-12 Supplement 1 by screening out during 50.59 evaluation.

RIS 2002-22 Supplement 1 clarifies the guidance for preparing and documenting "qualitative assessments" that can be used to evaluate the likelihood of failure of a proposed digital modification, including the likelihood of failure due to a common cause failure. Licensees can use these qualitative assessments to support a conclusion that a proposed digital I&C modification has a sufficiently low likelihood of failure. This conclusion and the reasons for it can be documented, as required by 10 CFR 50.59(d)(1), as part of the evaluations of proposed digital I&C modifications against some of the criteria in 10 CFR 50.59, "Changes, tests, and experiments."

Qualitative assessments are highly subjective, time and resource consuming evaluations that only slightly reduce licensing uncertainty while opening the door for re-evaluation of a modification if a new threat vector in a digital component or design is identified; not an unlikely event in rapidly changing digital technology.

The qualitative assessment outcome is "sufficiently low" if the activity does not result in more than a minimal increase in the likelihood of the occurrence of a malfunction of an previously UFSAR evaluated SSC important to safety. In practice, no more than 10% greater than the risk is established in the UFSAR, which is vague and subjective.

CONTACT INFORMATION:
1350 Whitewater Dr., Idaho Falls, ID 83402
DSS-Sales@curtisswright.com | +1.208.497.3535