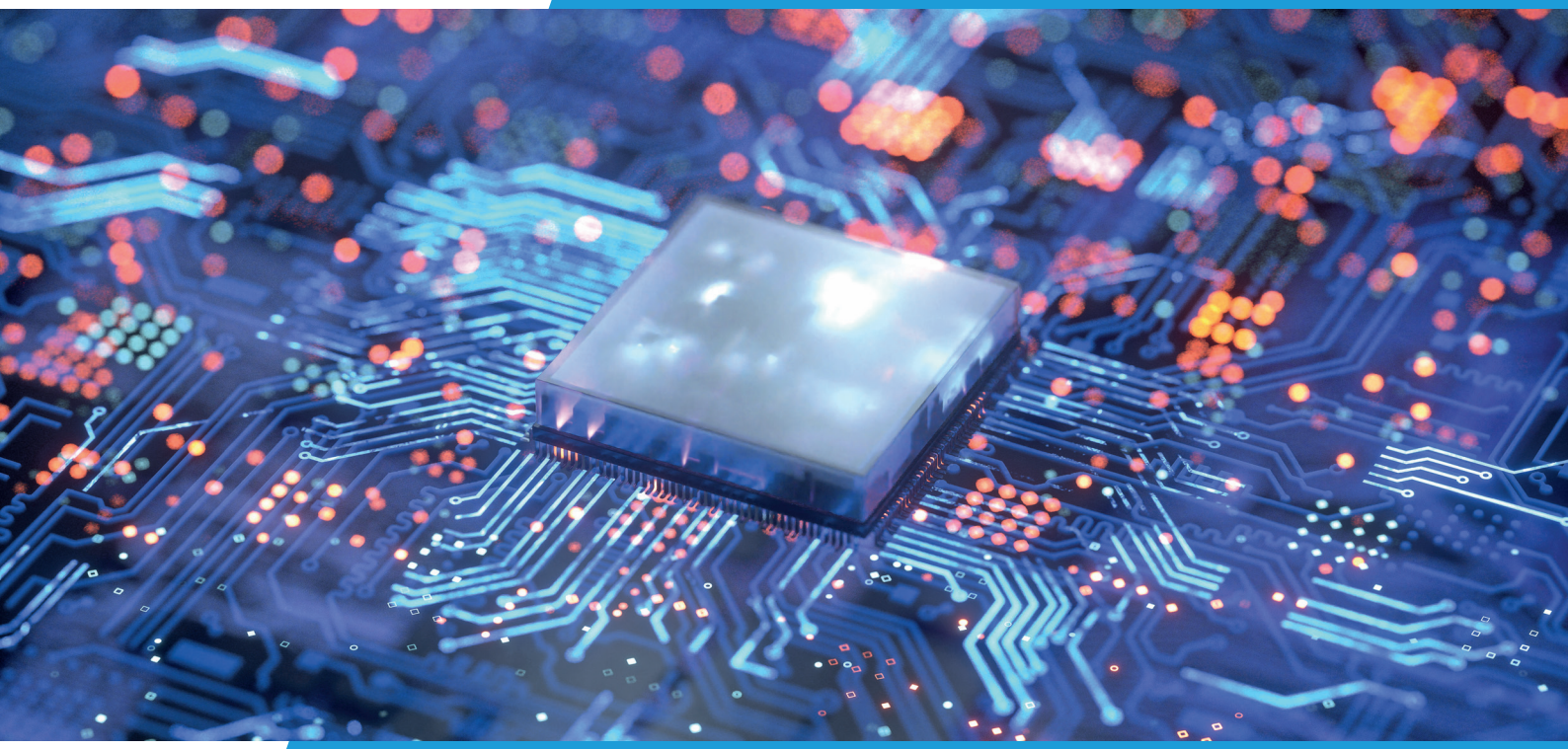
WORLD NUCLEAR ASSOCIATION



Hardware Description Language (HDL) Programmed Device (HPD) Technology in Nuclear Power Plants

Cooperation in Reactor Design Evaluation and Licensing Working Group – Digital Instrumentation & Control Task Force

Title: Hardware Description Language (HDL) Programmed Device (HPD) Technology in Nuclear Power Plants
Produced by: World Nuclear Association
Published: May 2022
Report No. 2022/002

This report reflects the views of industry experts but does not necessarily represent those of any of the World Nuclear Association's individual member organizations.

World Nuclear Association is the international organization that represents the global nuclear industry. Its mission is to promote a wider understanding of nuclear energy among key international influencers by producing authoritative information, developing common industry positions, and contributing to the energy debate.

The Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group of World Nuclear Association was created in January 2007 with the mission of establishing international standardization of individual reactor designs and harmonization of approaches to licensing. CORDEL is currently working with its six task forces covering a wide range of technical areas, while maintaining close cooperation with the OECD Nuclear Energy Agency, the International Atomic Energy Agency, and standards developing organizations (SDOs), in pursuit of the CORDEL goals.

Contents

Author

Mark Burzynski, SunPort

Technical Coordinator

Allan Carson, World Nuclear Association

Reviewers

Johannes Pickelmann, Framatome

Jean-Luc Doutre, Edvance

Hayder Haouaneb, Framatome

Warren Odess-Gillet, Westinghouse Electric Company

Nadja Joergensen, NuScale Power

Foreword

In January 2007 World Nuclear Association established the Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group with the aim of stimulating a dialogue between the nuclear industry (including reactor vendors, operators, and utilities) and nuclear regulators (national and international organizations) on the benefits and means of achieving a worldwide convergence of reactor safety standards and approaches to licensing for reactor designs.

Since its inception the CORDEL Working Group of World Nuclear Association has promoted a worldwide nuclear environment where internationally accepted standardized reactor designs can be deployed globally without major design changes. In practice, this would mean that safety evaluations of a reactor design and generic design certification approved by a recognized competent authority would be acceptable by competent authorities in other countries.

The Digital Instrumentation & Control Task Force (DICTF) of CORDEL was set up in 2013 to investigate key issues in digital instrumentation and control (I&C) related to the licensing of new and operating nuclear power plants, and to collaborate with the International Atomic Energy Agency (IAEA), the International Electrotechnical Commission (IEC) and the Multinational Design Evaluation Programme (MDEP) Digital Instrumentation and Control Working Group (DICWG)[1].

The DICTF activities to date have focused on the following issues:

- Safety classification for I&C systems in nuclear power plants.
- Defence-in-depth and diversity.
- Modernization of I&C systems.

This is the first report the DICTF has produced regarding hardware description language (HDL) programmed devices (HPDs). The report outlines the current situation in relation to the use and regulatory review of these technologies, while making recommendations for future work.

[1] The activities of MDEP's Digital I&C Working Group (DICWG) were transferred to the Working Group on Digital I&C (WGDIC) of the NEA's Committee on Nuclear Regulatory Activities (CNRA) in 2017.

Abbreviations and Acronyms

BTP	Branch Technical Position
CCF	Common cause failure
CNRA	Committee on Nuclear Regulatory Activities
CORDEL	Cooperation in Reactor Design Evaluation and Licensing
CPLD	Complex programmable logic device
DICTF	Digital Instrumentation and Control Task Force
DICWG	Digital Instrumentation and Control Working Group
EPRI	Electric Power Research Institute
ESF	Engineered safety feature
ESFAS	Engineered safety features actuation system
FPGA	Field programmable gate array
FSAR	Final safety analysis report
HDL	Hardware description language
HPD	HDL programmed device
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I&C	Instrumentation and control
IP	Intellectual property
MDEP	Multinational Design Evaluation Programme
NEA	Nuclear Energy Agency
NEI	Nuclear Energy Institute
NPEC	Nuclear Power Engineering Committee
NRC	US Nuclear Regulatory Commission
ONR	UK Office for Nuclear Regulation
RPS	Reactor protection system
SIL	Safety integrity level
SRAM	Static random-access memory

Executive Summary

Hardware description language (HDL) programmed devices (HPDs), such as field programmable gate arrays (FPGAs), used in nuclear power plant instrumentation and control (I&C) systems, offer several benefits over standard microprocessor-based I&C systems. Their capability to perform a wide range of independent functions with a high clock speed makes them well-suited to applications requiring very short response times. Furthermore, HPD's provide 'by design' separation of ancillary functions from the main safety I&C functions, therefore a postulated failure of an ancillary function will not prevent the correct execution of the safety I&C functions.

As a result, nuclear industry interest in the use of HPD-based technology has been increasing. However, despite early efforts to achieve harmonization in the requirements for HPD-based I&C platforms, efforts at harmonization have stalled. There are differences between national regulatory approaches to the treatment of HPDs, particularly in relation to the need for statistical testing and in the treatment of common cause failure (CCF) vulnerabilities. This divergence of regulatory approach is exacerbated by the lack of harmonization in nuclear industry standards. In particular, the International Electrotechnical Commission (IEC) has some standards that do not cover the full range of possible uses (*i.e.* in systems performing Category B&C safety functions), while the Institute of Electrical and Electronics Engineers (IEEE) has no corresponding standards for HPD development and use.

This report identifies the lack of consistent approach in industry standards and differences in regulatory approach relating to the use of HPD technology in nuclear power plants. The potential impacts on the future use of HPD technology are assessed and recommendations to achieve greater harmonization are provided.

To develop a consistent approach within industry standards the key recommendations from the Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group of World Nuclear Association are:

- The IEEE should address the lack of standards for the development of HPD technology in the nuclear sector through development and alignment of its own standards to those already existing or joint standard adoption of applicable IEC standards.
- The IEC standards that address the treatment of CCF in systems performing Category A functions should be updated to incorporate the various capabilities of HPD technology to address CCF vulnerabilities through internal diversity.
- A new standard should be considered for electrical systems to address the use of digital devices and data networks.

The development of consistent industry standards will support a common approach to the use of HPDs within the design of I&C systems. However, to support a consistent treatment of these devices by national regulators, CORDEL recommends:

- The Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) should consider updating its current position to include systems and components that perform Category B&C functions.
- National regulators should continue with efforts to address the commercial-grade dedication of commercial off-the-shelf digital equipment using third-party certification.

More generally CORDEL recommends that clear and consistent guidance for the treatment of CCF in relation to HPDs should be developed by the nuclear industry in collaboration with national regulators.

Harmonizing the nuclear regulatory process for HPD technology with the broader safety-critical industry sectors is a key enabler to the deployment of emerging reactor technologies, which will require greater numbers of advanced I&C components. This harmonization would provide supply chain improvements by being part of a larger market, realize process improvements through use of certified products, and improve safety by keeping up-to-date with the latest design, verification and validation techniques.

1 Introduction

The use of hardware description language (HDL) programmed devices (HPDs), such as field programmable gate arrays (FPGAs), complex programmable logic devices (CPLDs), or application-specific integrated circuits, is relatively new to the nuclear industry. The application experience has largely been focused on digital instrumentation and control (I&C) platforms for use in safety classified systems.

HPDs have characteristics of both software and hardware. As a result, applications using HPDs have many similarities with traditional software (in relation to design) and characteristics of traditional electronic design (*i.e.*, electronic-level timing). However, due to the unique nature of HPDs, there exist several differences between HPDs and traditional microprocessor software. Some key differences include:

- HPDs use parallel processing with dedicated hardware for each function instead of executing instructions sequentially as in the case of traditional software, meaning many more functions can occur simultaneously with faster response times than the sequential processing of microprocessor code.
- HPDs use declarative languages, which specify what is to be done rather than how to do it, as opposed to standard software imperative languages which specify each instruction of the program.
- The design process for HPDs is significantly different to that of standard microprocessor-based systems because certain properties, such as memory consistency after each instruction, are not inherent in HPDs.
- Translation of the HDL code to bitstreams for configuring HPDs is much more involved than the translation of source code to binary in software compilation. Whereas translating source code involves the conversion of each line of code to some bytecode, synthesizing HDL to bitstream is a process where the entire design is converted (and optimized) to a hardware implementation using the hardware resources on the HPD chip. In the HPD case, this process is not fully automatic, and therefore a designer must guide the tools, which may require additional steps or activities to ensure correct implementation. In recent years, practical methods to demonstrate the functional equivalence (*i.e.*, mathematical equivalence) of the intermediate development stages with the final configuration placed and routed on the HPD have become viable. The equivalence methods can address concerns over errors being introduced by the HPD development tools.
- High HPD clock speeds make them well-suited to applications requiring very short and static response times.
- The ability to separate ancillary functions[2] from the main safety I&C functions on the HPD chip, so that a postulated failure of an ancillary function will not prevent the correct execution of the safety I&C functions. A HPD using a finite state computer model offers the possibility to specify physically separate locations on the chip floorplan and to employ separate clock domains for additional independence of ancillary functions such as self-testing.

These differences offer unique advantages for safety-critical systems. IAEA NP-T-3.17 [1] describes current best practices and issues associated with the application of HPD-based solutions in nuclear power plants. The publication includes a description of the

[2] The words 'ancillary' and 'auxiliary' both refer to lending help or support, but ancillary implies that this support is considered subordinate in importance, while auxiliary does not have this implication.

technology and current knowledge on development processes and tools. It also includes a discussion on advantages and challenges associated with the application of HPDs, as well as licensing issues. A more detailed description of how HPDs are different and the benefits they can bring to the implementation of I&C systems is provided in EPRI 1019181 [2].

As a result of these advantages, the nuclear industry has an increasing interest in the use of HPD-based technology. Broader industry trends for HPD-based technology have implications for the nuclear supply chain. However, early efforts to achieve harmonization in the development process requirements for HPD-based I&C platforms used in safety-critical systems have stalled.

At the same time, the treatment of common cause failure (CCF) vulnerabilities in HPD-based safety systems has diverged across the international regulatory community. The regulatory treatment of HPD technology has evolved from the regulatory experience with microprocessor technology. At the initial stages of use (circa 2006), there were no specific guidance documents or standards available to support the review and acceptance implementation of HPD technology until 2012. Consequently, regulatory bodies treated HPD technology in the same manner as software.

This lack of harmonization will limit the ability of nuclear power plant designs to take full advantage of the larger market for I&C equipment used in safety-critical applications. This report identifies areas of harmonization and significant divergences in the use of HPD technology in nuclear power plants. It provides an assessment of the potential impacts on the future use of HPD technology and makes recommendations to achieve greater harmonization.

The findings and conclusions within this report are applicable to all HPD technologies, however it is recognized that to date the main use of such technologies in the nuclear industry is in relation to FPGAs. Consequently, some of the examples provided are specifically related to FPGA technology.

2 Benefits of HPD technology

One of the main areas of focus for the use of HPDs in the nuclear industry is in relation to FPGAs, a type of large-scale integrated circuit where the internal hardware architecture is configured for a specific application according to the user needs after production of the chip. The FPGA circuits are fabricated without any functionality and are entirely configured, *i.e.* their logic is programmed into the device for the given applications using HDLs.

FPGA architecture generally consists of:

- A set of logic blocks that can be configured to implement any logic functions (*i.e.*, AND, OR, XOR, NOT).
- A set of programmable input/output blocks which are the electrical interfaces between the low voltage, low current signals within the FPGA, and the higher voltages and currents required by the external electronic components connected to the FPGA.
- An internal interconnection grid. This is a set of wires to be interconnected at intersecting points when the FPGA is configured to the desired application.
- Application data memory

Some FPGA architectures contain additional elements to those mentioned above. For example, some configurations include microprocessors linked to the logic blocks through the interconnection grid. These elements will increase the complexity of the FPGA based systems, and their adoption should be carefully considered by designers regarding the overall requirements of their applications. In general, finite state computer models should be used for Category A, B or C functions; however, single platform circuits that integrate entire electronic or computer systems onto it.(system on chip) have some benefits for ancillary functions (*i.e.*, performing interface functions with non-classified systems or to accelerate data treatment for diagnosis/monitoring purposes).

There are three different types of FPGAs:

- Type 1. The static random-access memory (SRAM) type is based on static memory technology. It is reprogrammable and requires an external boot device to load contents into internal SRAM that controls routing and logic. SRAM based FPGAs are used to program both the logic cells and the interconnects and they have become quite predominant due to their re-programmability and use of complementary metal oxide semiconductor technology, which is known for its low dynamic power consumption, high speed, and tight integration.
- Type 2. The flash type is based on flash erasable programmable read-only memory technology. They are non-volatile like anti-fuse FPGAs, yet reprogrammable like SRAM FPGAs. The main advantage of flash-based programming is its non-volatile nature. Even though flash supports reprogrammability, the number of times this can be done is very small when compared to an SRAM technology.
- Type 3. The anti-fuse programming technology is an old technique of producing one-time programmable devices. The anti-fuse technology programming converts a high resistance path into a permanent electrically conductive path when the voltage across the anti-fuse exceeds a certain level. When compared to the other two technologies, the anti-fuse programming technology occupies the least amount of space but comes with the limitation of only being a one-time programmable option.

The implementation of HPD-based platforms brings the following advantages over microprocessor-based operating systems:

- Reduction in hardware complexity by requiring fewer hardware components to implement a given I&C function. This reduction in hardware complexity also results in fewer interconnections and interface points.
- The parallel hardware circuits inherent in HPD technology systems eliminate the large amount of software (*i.e.*, an operating system) required in microprocessor-based systems. This capability must be designed correctly to keep the system deterministic.
- HPD solutions based on flat hardware logic have a complexity level simply based on the complexity of the I&C function to be performed. The high complexity overhead associated with microprocessor operating system software is eliminated [3].
- The finite state machine solutions provided by HPDs eliminate the potential for operating errors associated with program execution during operation. This eliminates an important set of failure modes that are problematic within microprocessor designs.
- HPDs provide solutions for system-level common cause failure (CCF) vulnerabilities based on internal features such as independent hardware circuits, functionally diverse diagnostic logic, diverse HPD technologies, and comprehensive self-testing that can be incorporated into HPD-based I&C systems to reduce undetectable failure states.
- Portability of HDL to new chips provides good resilience to hardware obsolescence and enables ability to incorporate internal hardware diversity by using the same HDL code to program on diverse chips.
- Good resistance to cybersecurity issues.

The nuclear power industry is also increasingly interested in using industrial digital devices of limited functionality (also known as 'smart' devices) across many plant systems including safety-related systems. These devices have not been developed specifically for use in nuclear power applications, and many contain HPDs embedded in plant components and actuating devices (*i.e.*, sensing instrumentation, motors, pumps, actuators, breakers).

2.1 Design challenges

Some of the unique features of HPD-based solutions that make them attractive for use in the nuclear power industry also result in some design and regulatory challenges.

The HPD-based design should be developed with long-term support and obsolescence protection in mind. A well-designed HPD solution should be 'portable' to other circuits, even those from a different manufacturer, through use of standard languages and avoiding circuit-dependent features.

Of course, if the new HPD has a different footprint or pin-out, the circuit board will need some redesign. A greater portability of HPD designs and the degree of protection they offer against circuit obsolescence can be achieved by using available industry guidance (*i.e.*, EPRI Technical Report 1022983 [4]) in project planning, designing the architecture of the circuit, selecting the blank HPD to be used and its associated toolset, and following standardized coding rules and practices in programming the circuit. When the I&C system design incorporates proper provisions for obsolescence management, only the final HPD design steps (*i.e.*, synthesis plus place and route) are dependent on the particular HPD circuit chosen. As a result, if the HPD circuit becomes obsolete it can be replaced by another one using the currently available technology and the circuit-independent (*i.e.*, register-transfer level) representation of the design.

Cybersecurity is a concern with HPD-based systems, as it is with computer-based systems. However, HPD-based solutions have characteristics that tend to increase the level of difficulty that would be faced by a would-be attacker as compared to conventional microprocessor-based systems. HPD-based systems that directly implement the required I&C functions do not contain high-level, general-purpose components that can be easily diverted or hijacked for malicious purposes. Malicious functions must be introduced as complete designs, using technology-specific engineering tools. Once a complete HPD-based system is configured and put into a runtime state and physically secured, this virtually eliminates the threat of cyber-attacks and enhances the physical security of such systems. Adversaries would need to have physical access to the system hardware to sabotage the system. This aspect of HPD designs increases the level of difficulty a would-be attacker would face in attempting to make malicious modifications.

In addition, manufacturers now offer HPDs that incorporate features on the chips, chip loading techniques, and secure development environment methods that can be used to address the wide varieties of cybersecurity vulnerabilities that are considered of interest to broader industrial and military sector users.

3 Industry standards for HPD development and use

This section reviews the scope and limitations of the currently available international standards from the International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE) for the development and use of HPD technology.

Efficient deployment of HPD technology in nuclear power plant I&C safety systems relies on the availability of industry standards that govern the development and use of HPD-based equipment. It also requires consistent acceptance and interpretation of the industry standards by local regulatory bodies. The current state of harmonization is explored, and notable differences are identified.

This report uses the IEC 61226 [5] safety categorizations (*i.e.* Category A, B&C functions and Class 1, 2&3) in reference to systems. It should be noted that Table 2 in the CORDEL report *Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties* [6] provides a qualitative mapping of these safety categorizations to other standards and guidance.

3.1 HPD development standards

Since the initial efforts with HPD technology, international standards have been developed for HPD technology use in the nuclear sector for safety functions; these are listed in Table 1. The HDL programming standards IEC 62566 and IEC 62566-2 are used in conjunction with the software standards IEC 60880 and 62138.

These standards identify HPD-specific aspects of system integration and validation to be used in conjunction with IEC 61513 [11] for the system development process. They provide a set of requirements for the selection, qualification and use of tools for the design, verification and validation of HDL used in I&C systems implementing HPD technology. These standards do not distinguish between the requirements for different subgroups of HPD technologies (*i.e.* FPGA).

While IEEE 1012 [12] states that software can also include FPGA firmware, this standard is software-centric and not adapted to the unique aspects of validation and verification for FPGAs. Currently no comparable IEEE standards exist for the development of HPD technology in the nuclear sector, although the IEEE Nuclear Power Engineering Committee (NPEC) Working Group 6.4 is developing an update to IEEE 7-4.3.2 [13] to explicitly allow tailoring of IEEE 1012 component testing criteria for HDL devices, and IEEE NPEC Working Group 6.6 is exploring a joint standard for IEC 62671 [14] (see next section).

Table 1. International standards relevant to HPD technology use

Standard reference	Title
IEC 62566	Development of HDL-programmed integrated circuits for systems performing category A functions [7]
IEC 62566-2	HDL-programmed integrated circuits for systems performing category B or C functions [8]
IEC 60880	Software aspects for computer-based systems performing category A functions [9]
IEC 62138	Software aspects for computer-based systems performing category B or C functions [10]

3.2 Standards for use of HPD devices

Many I&C devices used for replacement at operating nuclear plants or new build projects are now only commercially available due to the loss of nuclear safety-related suppliers; this is particularly prevalent for IEC Class 1, US Nuclear Regulatory Commission (NRC) safety-related, and IEEE Class 1E components. Practical technical guidance is needed to ensure that digital components with limited functionality can be consistently implemented with minimal regulatory uncertainty.

IEC 62671 provides requirements for determining whether HPD and other digital devices of industrial quality (that are of dedicated, limited, and specific functionality and of limited configurability) are suitable for use in a safety-related nuclear application. It provides the following types of guidance:

- Criteria for functional and performance suitability.
- Criteria for dependability – evidence of correctness.
- Criteria for integration into the application (*i.e.* limits and conditions of use).
- Considerations for preserving acceptability.

However, IEEE 7-4.3.2 does not distinguish between system-level or component-level programmable digital devices when addressing commercial-grade dedication for determining suitability for use in a safety-related nuclear application. The IEEE NPEC Working Group 6.6 is considering a joint standard for the next revision to IEC 62671, which will require reconciliation with IEEE 7-4.3.2 for any conflicting requirements.

3.3 System-level industry standards

Digital technology plays a significant role in the defence-in-depth approach to the design and safety of a nuclear power plant. To satisfy the requirements of the defence-in-depth approach, digital I&C systems utilized in safety-related functions are required to have a certain level of independence (diversity) aimed at mitigating the impacts of common cause failure (CCF). The implementation of this approach can lead to diverse actuation systems with plant I&C architecture and the use of digital devices at the component level. Therefore, the susceptibility of digital devices to CCF is a critical element of the nuclear power plant safety case.

IEC standards 61513 (Section 5.4.4.2), 60880 (Section 13), and 62566 (Section 17) contain requirements for the treatment of CCF in systems performing Category A functions. IEC 61513 and 62566 also point to IEC 62340 [15] for additional requirements for the treatment of CCF in systems performing Category A functions. The purpose of IEC 62340 is to: give requirements related to the avoidance of CCF of I&C systems that perform Category A functions; and require the implementation of independent I&C systems to overcome CCF.

IEC 61226 has some ambiguity in relation to how to address CCF. In places it states that the reliability analysis for Class 1 system(s) shall consider the effects of CCF, while in other areas of the same standard it specifies that CCF be addressed for Class 1 systems. For example, Section A.3.2.1 states: "The reliability assessment shall consider the effects of common cause failures, including hardware failures, software failures, and human errors during operation, maintenance, as well as modification and repair activities." This ambiguity allows for different interpretations of what the standard is asking for and how to apply it.

IEC 61513, 62138, and 62566-2 do not address the treatment of CCF in systems performing Category B or C functions. These standards do not envision the various capabilities of HPD technology to address CCF vulnerabilities through internal diversity or comprehensive testing.

IEEE 7-4.3.2 allows for mitigation of credible CCFs through diversity and defence-in-depth. It also has criteria to determine that a programmable digital device is not considered susceptible to CCF based on rigorous testing. These requirements are consistent with the NRC evaluation criteria in Branch Technical Position 7-19 [16].

A new dual logo standard, IEC/IEEE 63160 [17], is currently under development. This standard is intended to establish requirements associated with the defence of electrical and I&C systems and their support systems against CCF in nuclear facilities. This standard (as currently written) will set out requirements for:

- Overall I&C and electrical power systems analysis.
- Analysis and defence against CCF from hazards.
- Analysis and defence against CCF from fault propagation by electrical disturbances and erroneous signal propagation.
- Analysis and defence against CCF from systematic faults.
- Documentation of the defence against CCF to allow their adequacy to be judged.

In the context of this standard, hazards are related to internal and external plant hazards (*i.e.* earthquake, flood, electromagnetic

interference). Fault propagation is related to electrical isolation and digital communication independence. Systematic faults encompass the potential for digital CCF but are not limited to CCF associated with digital I&C. The scope does encompass electrical components with embedded digital devices. Diversity is identified as a solution to CCF attributed to systematic faults and is discussed in the context of diversity between systems but does not envision the various capabilities of HPD technology to address systematic CCF vulnerabilities through internal diversity or comprehensive testing.

The draft version of IEC/IEEE 63160 provides the following statement on limitations of the standard:

> *This standard does not set requirements for determining the adequacy of the provisions to defend against CCF. This is due to the differences in national approaches to CCF; some countries treat CCF as a design basis accident requirement, others as a design extension condition and some as a deterministic requirement, and also because of the dependence on the type of facility and the plant specific details. Instead, this document identifies the process and information necessary to support a determination of adequacy.*

Draft IEC/IEEE 63160 indicates that the standard applies to CCF of redundancies of individual systems at Class 1, 2 & 3. This scope seems to contradict IEC 61226, which limits consideration of CCF to Class 1 systems. It also notes that the new standard must be used in conjunction with IEC 62340. However, certain requirements to limit fault propagation are only applied to Class 1 systems. All standards mentioned within this report are related to I&C systems; there is also a need to develop nuclear industry standards for electrical systems that are comparable to IEC 62340.

3.4 Component-level industry standards

Draft IEC/IEEE 63160 applies to systems at Class 1, 2 and 3 however is ambiguous regarding its applicability to component-level systematic CCF assessment. This standard, as currently drafted, will make it difficult for users to confidently use smart devices in Class 2 or 3 systems.

IEC 62671 mentions consideration of CCF for digital devices of limited functionality in Section 6.2.f:

> *The failure modes shall be analysed in terms of the impact of the candidate device on the system in which it will be installed, taking into account all the factors that can influence failure modes ... Particular attention should be paid to common cause failures, especially those relating to other devices (possibly in other classes) that have a role credited in the safety analysis as protecting against the same initiating events.*

IEC 62671 is a standard applied at the component level. It introduces the notion of assessment of CCFs; however, it does not give a clear sense of what is expected. It also seems to limit this assessment to Category A functions without explicitly saying it. IEEE 7-4.3.2 does not distinguish between system-level or component-level programmable digital devices when addressing credible CCFs. These standards, as written, will limit the ability of reactor designers to use smart devices in safety-related systems. IEEE NPEC Working Group 6.6 is considering a joint standard for the next revision to IEC 62671.

3.5 Use of certification for acceptance of component-level digital devices

Broader industry trends for HPD-based technology have implications for the nuclear supply chain. Other industry sectors (*i.e.* chemical process, rail transport, medical devices, and automotive) have also developed standards for use of HPD technology in safety-critical applications. These large sectors are driving the I&C market towards third-party certified HPD components (*i.e.* chips) and development tools. These same forces are also driving the market towards third-party certified products (*i.e.* IEC 61508 safety integrity level-certified devices). These market trends offer opportunities for the nuclear sector to take advantage of product, process, and methodology improvements to efficiently use HPD technology.

IEC 62671 notes that there are significant advantages to selecting a device that has been previously certified to a suitable safety standard. Such devices tend to have well-defined failure modes and have been developed under a disciplined software and/or HPD development process, and therefore supporting documentation is likely to exist, although it might be proprietary. Guidance on the evaluation and use of device certifications is found in Section 7.2 of the standard.

IEEE 7-4.3.2 does not address the use of certification when addressing commercial grade dedication of programmable digital devices for use in a safety-related nuclear applications. IEEE NPEC Working Group 6.6 is considering a joint standard for the next revision to IEC 62671, which will require a reconciliation with IEEE 7-4.3.2 for any conflicting requirements.

4 Regulatory treatment of HPD technology

The lack of harmonization continues to limit the use of HPD technology in nuclear safety applications and increases the supply chain cost for this equipment. There is also a wide variation in the treatment of CCF vulnerabilities by local regulatory authorities. The treatment of CCF in digital I&C systems and components continues to be the greatest challenge of harmonization of industry standards and regulatory guidance. The difference between the approach in the USA and some other countries is illustrated below.

4.1 Regulatory approach to HPD development standards

Nuclear industry and regulatory bodies are now learning how to treat HPD technology developed for safety system applications and how to implement the industry standards for commercial-grade smart devices for use in safety system applications. For example, several HPD-based I&C platforms have become available for use in safety-classified nuclear applications. The NRC has now approved six FPGA-based digital I&C platforms for use in safety-related systems using a combination of IEEE and IEC standards [18-23]. The NRC issued NUREG/CR-7006 [24], which describes guidance the NRC staff could use to confirm that FPGA-based safety systems are in conformance with NRC regulations; however, it was not documented as review guidance for any of the six FPGA-based digital I&C platforms. Additionally, plant protection systems at the 15 operating reactors in Ukraine have been modernized using FPGA-based digital I&C technology developed using IEC standards.

However, despite the international standards being applied by regulators, the risk of divergence between regulatory approaches remains. One such point of divergence involves the need for statistical testing to validate the development of any digital I&C platform or application using the industry standards.

This divergence can be seen explicitly in relation to IEC 62671 and MDEP Digital Instrumentation and Controls Working Group (DICWG)[3] CP-DICWG-07 [25] which addresses:

- Confirmation that devices are suitable for intended functions and designed correctly.
- Use of compensatory evidence to address identified gaps in evidence.
- Use of third-party certification as evidence.
- Specification of restrictions on use.

Both IEC 62671 and CP-DICWG-07 note that statistical testing can be used to provide supplementary evidence to support the selection and use of commercially available smart devices; however, such testing is not mandatory.

While the NRC has not required statistical testing to validate development and implementation of smart devices, the UK's Office for Nuclear Regulation (ONR) guidance NS-TAST-GD-046 [26] augments the IEC standard by requiring that statistical testing be performed as part of the 'independent confidence-building' aspects of the safety justification for use of smart devices containing HPDs in Class 1&2 systems when the source code is not available for independent review. It is of note that the ONR does not approve I&C platforms but rather approves nuclear power plant applications of digital I&C platforms. The regulatory regime is risk-informed, and the applicant must define the reliability target for the I&C application.[4]

[3] The activities of MDEP's DICWG were transferred to the Working Group on Digital I&C of the NEA's Committee on Nuclear Regulatory Activities (CNRA) in 2017.

[4] Reliability targets are derived from multiple sources including the safety categorization of the application's function and the system classification hosting the application.

In addition, the MDEP DICWG has also issued two further common positions related to the subject:

- DICWG-02 [27] – software tools for the development of software for safety systems.
- DICWG-05 [28] – treatment of HPDs for use in nuclear safety systems.

These common positions are generally consistent with the information in IEC 60880 and 62566 for Category A functions; however, they do not reflect the development guidance issued in IEC 62138, IEC 62566 and IEC 62566-2 that is more appropriate for HPD technology and Category B and C functions.

Furthermore, these common positions do not distinguish between requirements for different types of HPD or between hard and soft third-party intellectual property (IP) cores.[5] Useful guidance on this topic can be found in Section 6.4 of EPRI Technical Report 1022983 [4].

4.2 Regulatory treatment system and component-level industry standards

HPD technology can provide solutions for system-level CCF vulnerabilities based on internal diversity features. However, the treatment of CCF vulnerabilities in, for example, HPD-based systems, has some of the lowest levels of harmonization in industrial standards.

There is also a wide variation in the treatment of CCF vulnerabilities by national regulatory authorities. The treatment of CCF in digital I&C systems and components continues to be the greatest challenge of harmonization of industry standards and regulatory guidance. The lack of harmonization continues to limit the use of HPD technology in nuclear safety applications and increases the costs for this equipment.

4.2.1 HPD-based system experience in the USA

Over the last ten-year period, with the support and guidance from the NRC, various companies have illustrated the various capabilities of HPD technology to address CCF vulnerabilities through internal diversity or comprehensive analysis and testing, such as:

- The Wolf Creek main steam and feedwater isolation system modernization project was approved by the NRC in March 2009 [29]. The CCF mitigation used FPGAs with diverse logic cores designed and implemented with differing synthesis directives to achieve diverse logic paths. The NRC determined that there was sufficient diversity due to the low level of complexity and independent detailed review of core logics.
- The Areva (now Framatome) approach to CCF mitigation for the priority actuation and control system module (based on FPGA technology) was accepted by the NRC in October 2011. The CCF mitigation used 100% combinatorial testing, as outlined in D&IC-ISG-04 [30], which is achievable only for simple devices or applications.
- The Westinghouse advanced logic system generic platform was approved by the NRC in September 2013 [18]. The CCF mitigation strategy used a 'core diversity design' based on two redundant logic implementations within each FPGA. Different synthesis directives were used for each logic implementation. The NRC determined platform level diversity alone was not enough and required application-specific diversity reviews. The application

[5] Hard IP core: an IP core that is provided in the form of physical circuit layout; with a hard IP core the end-designer does not need to perform the synthesis and place-and-route process as would be required for a soft core. These are necessarily circuit technology specific.
Soft IP core: an IP core that is in the form of a netlist or HDL. A soft IP core requires verification of function following implementation (synthesis and/or place and route), unlike a hard IP core.

implementation option (called 'embedded design diversity') added additional diversity through two different versions of HDL files implemented by independent design teams.

- The NuScale highly integrated protection system generic platform was approved by the NRC in June 2017 [20]. The CCF mitigation strategy used two FPGA types (*i.e.*, one SRAM-based and the other either one-time programmable or flash-based). The FPGA types are alternated throughout redundant architecture channels. Each FPGA type has diverse development tools and programming methods.
- The Radiy RadICS generic platform was approved by the NRC in July 2019 [21]. The CCF mitigation strategy used an internal diversity strategy based on internal design features (*i.e.*, technology and functional diversity) applied at the module and platform levels to address CCF vulnerabilities [31]. The technology differences reflected the use of FPGA and CPLD chip technology for different safety functionality.

These HPD solutions may simplify the overall I&C system design by eliminating the need to add an external diverse actuation system and the associated interfaces to safety sensors and actuators. The overall integrated lifecycle costs are reduced by eliminating the need to develop and maintain a new safety analysis and I&C design basis for the external diverse actuation system and ongoing maintenance and test costs.

NRC guidance used for these CCF evaluations is found in Branch Technical Position (BTP) 7-19 [16]. It specifies that if a postulated CCF could disable a safety function, then a diverse means is required to perform either the same function or a different function that provides protection. The guidance is generally applied to I&C systems consistent with those performing Category A functions. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.[6] The guidance also notes that there are two design attributes, either of which is sufficient to eliminate consideration of software-based or software logic-based CCF:

- Diversity. If 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.
- Testability. A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested and all outputs are verified for every case.

NRC guidance available in NUREG/CR-7007 [32] provides information on what constitutes 'sufficient diversity' considering diversity attributes and attribute criteria that preclude or limit certain types of CCF.

The NRC recently updated the BTP 7-19 guidance used for these CCF evaluations to better align the testability design attribute with IEEE 7-4.3.2 and added the option to consider other alternatives (*i.e.* defensive measures that address CCF vulnerabilities).

The NRC has also issued guidance in Regulatory Issue Summary 2002-22, Supplement 1 [33], on the use of qualitative assessments that can be used to evaluate the likelihood of failure of a proposed digital modification, including the likelihood of CCF. These qualitative

[6] The NRC quality guidance for diverse actuation is between IEC 61226 Class 2 and 3 requirements.

assessments are used to support a conclusion that a proposed digital I&C modification has a sufficiently low likelihood of CCF[7]. When a sufficiently low likelihood is concluded, a CCF does not require analysis or mitigation.

The NRC guidance is:

- Not directed towards digital I&C replacements of the reactor protection system (RPS), the engineered safety features actuation system (ESFAS), or modification/replacement of the internal logic portions of these systems (*i.e.* voting logic, bistable inputs, and signal conditioning/ processing).
- Applicable to low-safety-significant I&C systems as an alternative to the defence-in-depth and diversity analysis required by BTP 7-19.
- Applicable to individual I&C components and I&C systems consistent with those performing the equivalent of IEC 61226 Category B or C functions.

The NRC guidance is considered compatible with the various capabilities of HPD technology to address CCF vulnerabilities using internal diversity as a defensive measure or comprehensive testing.

4.2.2 HPD-based system experience in other countries

MDEP DICWG-01 [34] provides limited guidance for the consideration of CCF at the system level for I&C safety systems. It notes: "Diversity is a way to reduce the potential effects of CCF (*i.e.*, incorporation of inherent diversity in the design of the I&C system, or by the use of a diverse backup system)." It also recognizes that there are different degrees of diversity. This perspective is compatible with the various capabilities of HPD technology to address CCF vulnerabilities through internal diversity or comprehensive testing. DICWG-01 does not improve the degree of harmonization for the regulatory treatment of CCF, and concedes that different "member countries may accept different methods to mitigate against the potential for CCF caused by software (*i.e.*, formal methods to prove software correctness)."

This lack of harmonization leads to significant differences in the way in which national regulators assess the need for diversity in HPD systems. For example, the UK Office for Nuclear Regulation (ONR) states:

> *Demonstrating that two complex computer-based protection systems are 'independent' and 'diverse' (i.e., will not tend to fail on the same demands) and hence that the reliability claims for each can be multiplied together remains an open question despite significant research. Hence, where a high level of risk reduction is required that is greater than the accepted common cause cut-off limit for a single computer-based safety system (i.e., 10^{-4} probability of failure on demand for a computer-based safety system where the consequence in the event of failure of the safety system could potentially involve large releases of radioactive material) then ONR's current expectation is that a simple hardware based secondary safety system should be provided.* [26]

The UK's position is the most divergent approach to the treatment for HPD technology from that of the NRC. It is presented here to illustrate the wide variation in the treatment of CCF for HPD-based systems. In addition to the preference for statistical testing discussed in Section 4.1, it does not necessarily view HPD technology as diverse from microprocessor technology.

[7] 'Sufficiently low' means much lower than the likelihood of failures that are considered in the updated final safety analysis report (FSAR) (*i.e.*, single failures) and comparable to other CCFs that are not considered in the UFSAR (*i.e.*, design flaws, maintenance errors, calibration errors).

Some countries mandate diversity on systems designs for the most important systems. In these cases, they do not use explicit CCF assessments of the system and its components; rather, the incorporation of diversity to the degree practical is simply specified.

4.2.3 Component-level regulatory guidance

NRC Regulatory Issue Summary 2016-05 [35] clarified the NRC's technical position on existing regulatory requirements for the quality and reliability of safety-related equipment with embedded digital devices (*i.e.* digital displays, motor controllers, sequencers, pumps, valve actuators, breakers, uninterruptable power supplies). It does not provide any recommended solutions; instead, it simply reiterates that the existing NRC guidance for digital I&C equipment applies, which implies that assessment of CCF is required.

NRC Regulatory Issue Summary 2002-22 Supplement 1 resolved the regulatory problems associated with implementing digital-based components and I&C systems with low safety significance. Smart devices in I&C systems with high safety significance would require CCF evaluations using the BTP 7-19 guidance.

MDEP CP-DICWG-07 guidance related to component-level CCF is as follows:

> *The rigor of the application of the positions on the selection and use of industrial digital devices of limited functionality should be commensurate with the safety classification.…*
>
> *2. Confirmation of the correctness of industrial digital devices for their intended functions should produce evidence:*
>
> *a. Potential systematic faults including those that could cause coincident failures have been evaluated and the impact of these faults on plant safety has been assessed.*

CP-DICWG-07 suggests that digital components of limited functionality can be shown to not be a credible source of CCF and can be excluded from evaluation of the CCF effects on the plant.

The accepted interpretations regarding whether sensors and actuators are to be included in the assessment of digital CCF can vary based on national regulatory perspectives (*i.e.* national regulator concern for CCF in digital I&C equipment) and the importance of the equipment to the overall safety measure for the plant (*i.e.* direct consequences or impacts on required levels of defence-in-depth).

Following discussions with nuclear operators it is clear that the rules and interpretations through the nuclear industry differs from one country to another. For example:

- The experience of nuclear power plant operator EDF is that assessment of CCF vulnerabilities for engineered safety feature (ESF) components is limited to the traditional hazards from external events (*i.e.* seismic) and internal events (*i.e.* harsh environments, electromagnetic interference, flood), which are addressed through component qualification, redundancy, independence, and separation.
- Feedback from discussions with CEZ (Dukovany nuclear plant) is that regulatory concern is mostly about CCF for digital systems, where there is a credible risk of a latent fault. For analog actuators, CCF is usually considered just for external events and not for hidden internal faults. The Dukovany RPS and ESFAS were assessed for coping with CCF in accordance with IEC 62340; however, the assessment did not specifically deal with ESF actuators, only with the digital I&C part of the system.

The UK ONR approach for assessing CCF is risk-based and considers the whole system in the context of the plant. Component-level CCFs are incorporated using standard probabilistic risk assessment techniques (*i.e.* beta factor). The ONR expects licensees to identify several layers of protection (dependent upon the consequences), each of which can independently act to prevent the hazard from taking effect. For any given failure, the ONR expects the licensee to demonstrate that the layers of protection are diverse such that a CCF cannot both cause the event and render a layer of protection ineffective.

The measures that are required to avoid CCF will differ depending on the equipment and its location, the hazards the equipment or system may be exposed to, and any other factors (*i.e.* the potential for design faults to exist). For the latter reason, the ONR expects that different I&C technologies should be used for different layers of protection at the highest safety class. However, a safety case would have to be produced to confirm that there is no CCF that could affect more than one system at the same time.

The ONR notes that support services (*i.e.* electrical power, ventilation, water, pneumatic pressure) that need to function to enable the systems that they are supporting to function are a particularly challenging area. It is necessary for the licensees to demonstrate that a CCF will not affect the support services for more

than one layer of protection. Another challenging area is the system that prioritizes the actions of the different layers of protection, as a failure here can render more than one layer of protection ineffective. For this reason, it is common (based on the risk assessment results) for there to be diverse designs of priority actuation modules.

4.3 Use of certification for acceptance of component-level digital devices

In SECY-19-0112 [36], the NRC identified its intention to endorse industry guidance being developed by the Nuclear Energy Institute (NEI) regarding commercial-grade dedication of commercial off-the-shelf digital equipment using third-party certification. The NEI has developed guidance on the use of IEC 61508 safety integrity level (SIL) certification to support the acceptance of commercial-grade digital equipment for nuclear safety-related applications [37], which was submitted to the NRC for endorsement in February 2021. This guidance is intended to be applicable to all digital I&C equipment (including digital I&C platforms), unlike IEC 62671, which is limited to digital devices of limited functionality. The NRC is interested in understanding the controls governing third-party certification and the oversight of the third-party certifiers. The NRC expects to endorse NEI 17-06 in a regulatory guide by the end of 2022.

The UK's ONR recognizes certification by an independent body (supported by evidence) as one of the suitable 'independent confidence building measures' to support justification of commercial off-the-shelf smart devices [26].
MDEP CP-DICWG-07 provides guidance related to the use of certified digital devices (in item 5):

> *Information developed during certification for safety purposes in industries other than nuclear power may be used as evidence to support device selection and use. A certificate alone is not sufficient; rather, it is the information used in the certification process (i.e., information that is generated from the device development process) that may provide value.*

5 Conclusions and recommendations

There is a lack of harmonization associated with the use of hardware description language (HDL) programmed devices (HPDs) in nuclear power plant I&C systems, both in terms of the industrial standards for development and use, as well as the regulatory assessment and requirements for implementing such equipment.

Nuclear industry standards are inconsistent or lacking; for example, the International Electrotechnical Commission (IEC) has standards for the nuclear industry that address HPD use for Category A, B&C functions, whereas no comparable standards for HPD technology have been issued by the Institute of Electrical and Electronics Engineers (IEEE).

In relation to industry standards for determining whether digital devices of industrial quality with limited functionality that contain HPD components are suitable for use in a safety-related nuclear applications, the situation is not any better. The IEC has a standard that addresses this topic, whereas the IEEE has no comparable standard but is considering a joint standard with the IEC for the next revision to its relevant standard.

There is little harmonization across industry standards that address common cause failure (CCF) for systems and components using HPD technology, resulting in confusion in this area. The IEEE standards align with US Nuclear Regulatory Commission (NRC) practices, which are reflected in its guidance documents. The IEC standards related to system design also align with NRC guidance on the treatment of CCF in Class 1 systems performing Category A functions, but do not address the treatment of CCF in systems performing Category B or C functions. The IEC standards do not envision the various capabilities of HPD technology to address CCF vulnerabilities through internal diversity or comprehensive testing.

A new joint standard being developed by the IEC and IEEE will extend the assessment of CCF to Class 1, 2&3 electrical and I&C systems and components. However, it is expected that this standard will not set requirements for determining the adequacy of the provisions to defend against CCF and therefore will not adequately address lack of clarity and harmonization.

There is some harmonization within industry standards regarding the use of certification when addressing commercial-grade dedication of programmable digital devices for use in a safety-related nuclear application. The USA is an outlier regarding the use of certification, but efforts are under way that could lead to harmonization with the international approach.

The international regulatory community is equally inconsistent in that there are generic common positions centred around the IEC standards for HPD use and the use of software development tools for the development of software for Category A functions (*i.e.* DICWG-02 and -05), but there has been no update to these common positions to address Category B&C functions.

There is limited harmonization that is consistent with IEC 62671 for digital devices of limited functionality. The national regulatory approaches significantly diverge, *i.e.* between the USA, where no statistical testing is required, and the UK, where for digital devices of limited functionality statistical testing is mandatory for use in Class 1&2 systems when the source code is not available for independent review.

There is also significant divergence in national regulatory approaches such as in the UK, where the Office for Nuclear Regulation (ONR) augments the IEC standards for HPD-based systems with statistical testing to demonstrate the numerical reliability of the safety system – something not required by the NRC, for example.

Harmonizing the nuclear regulatory process for HPD technology with the broader safety-critical industry sectors such as aviation, would provide supply chain improvements by being part of a larger market, realize process improvements through use of certified products, and improve safety by keeping up to date with the latest design, verification and validation techniques.

The regulatory practice, guidance and techniques existing today, and described in this report, to address CCF vulnerabilities in digital components are based on the undertaking of a detailed evaluation of existing components. Such evaluations are labour intensive, lengthy, expensive, and focused on 'one-off' obsolescence issues. For emerging reactor designs, developers would need to efficiently obtain the advanced sensors that will be an integral part of these new reactors.

Harmonization of the industry codes and standards and regulatory approaches to the treatment of HPD technologies would provide advanced sensor suppliers with technical criteria on how to avoid CCF vulnerability or allow them to build in the required mitigation, so that sensors could be procured with confidence without the need for lengthy review processes.

5.1 Recommendations

CORDEL recommends that the nuclear sector should take advantage of accepted safe integrated solutions for standard industry equipment (*i.e.* certified smart transmitters, integrated device controllers, circuit breakers). Standard development processes are now enforced in certified components and development tools. These devices can offer improved reliability through self-testing and diagnostics, and can reduce CCF vulnerabilities using internal diversity that can be implemented with HPD technology. They can also provide better integration into large data networks through secure communication pathways. Acceptance of these certified devices would be an alternative to the traditional regulatory practice of performing individual component reviews for each application in the nuclear power plant.

In order to increase harmonization of the use of HPD technology in nuclear power plant I&C safety systems, CORDEL makes the following recommendations:

- The IEEE should address the lack of standards for the development of HPD technology in the nuclear sector through development and alignment of its own standards to those already existing or joint standard adoption of applicable IEC standards.
- The IEEE should reconcile any conflicting requirements if a joint standard to replace IEC 62671 is pursued – IEEE 7-4.3.2 does not distinguish between system-level or component-level programmable digital devices when addressing commercial-grade dedication, CCF vulnerabilities, and use of certification for determining suitability for use in a safety-related nuclear application.
- The IEC standards that address the treatment of CCF in systems performing Category A functions should be updated to incorporate the various capabilities of HPD technology to address CCF vulnerabilities through internal diversity.

- IEC standards 61513, 62138, 62566-2, 62340 and 61226 will need to be updated to reconcile any conflicting requirements for the treatment of CCF for systems or components performing Category B or C functions when IEC/IEEE 63160 is issued.
- A new standard comparable to IEC 62340 should be considered for electrical systems to address the use of digital devices and data networks.

The following recommendations are made to help harmonize regulatory guidance in relation to HPD technology development and use in nuclear power plant I&C systems:

- The Nuclear Energy Agency's (NEA's) Committee on Nuclear Regulatory Activities (CNRA) should update Generic Common Position DICWG-05 to include systems and components that perform Category B or C functions.
- Regulators should complete efforts to address the commercial-grade dedication of 'off-the-shelf' digital equipment using third-party certification to align with Generic Common Position DICWG-07.

The lack of harmonization in the industry standards and regulatory guidance on the treatment of CCF in digital I&C systems and components requires a concerted effort by the nuclear industry and regulators to achieve harmonization. Therefore, the industry and national regulators must cooperate at the international level to align guidance and expectations that provide for the development of:

- Clear and consistent guidance for the treatment of CCF in digital I&C Class 2&3 systems.
- Clear and consistent guidance for the treatment of CCF in components with embedded digital devices in Class 1, 2&3 systems.
- Clear and consistent guidance for the consideration of HPD technology as distinct and diverse from microprocessor technology.
- Updated guidance for the use of the various capabilities of HPD technology to address systematic CCF vulnerabilities through internal diversity.

References

[1] International Atomic Energy Agency, Application of Field Programmable Gate Arrays in Instrumentation and Control Systems of Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.17, January 2016

[2] Electric Power Research Institute, Guidelines on the Use of Field Programmable Gate Arrays (FPGAs) in Nuclear Power Plant I&C Systems, 1019181, December 2009

[3] J. Mayaka and J. Cheon, *Complexity Analysis of an FPGA-based ESF-CCS*, International Symposium on Future I&C for Nuclear Power Plants, Gyeongju, Korea, 26-30 November 2017

[4] Electric Power Research Institute, Recommended Approaches and Design Criteria for Application of Field Programmable Gate Arrays in Nuclear Power Plant Instrumentation and Control Systems, Technical Report 1022983, June 2011

[5] International Electrotechnical Commission, Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems, Edition 4.0, IEC 61226, April 2020

[6] World Nuclear Association, Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties, March 2020

[7] International Electrotechnical Commission, Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions, Edition 1.0, IEC 62566, January 2012

[8] International Electrotechnical Commission, Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits – Part 2: HDL-programmed integrated circuits for systems performing category B or C functions, Edition 1.0, IEC 62566-2, May 2020

[9] International Electrotechnical Commission, Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, Edition 2.0, IEC 60880, May 2006

[10] International Electrotechnical Commission, Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions, Edition 2.0, IEC 62138, July 2018

[11] International Electrotechnical Commission, Nuclear power plants – Instrumentation and control important to safety – General requirements for systems, Edition 2.0, IEC 61513, August 2011

[12] Institute of Electrical and Electronics Engineers, IEEE Standard for System, Software, and Hardware Verification and Validation, IEEE 1012-2016, September 2017

[13] Institute of Electrical and Electronics Engineers, IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations, IEEE Std 7-4.3.2-2016, August 2016

[14] International Electrotechnical Commission, Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality, Edition 1.0, IEC 62671, February 2013

[15] International Electrotechnical Commission, Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF), Edition 1.0, IEC 62340, December 2007

[16] Nuclear Regulatory Commission, Standard Review Plan, Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems, Branch Technical Position 7-19, NUREG-0800, Revision 8, January 2021

[17] International Electrotechnical Commission, IEC/IEEE 63160, Nuclear facilities – Instrumentation, control and electrical power systems important to safety – Common cause failure, system analysis and diversity, Draft Version 2CD, June 2020

[18] Nuclear Regulatory Commission letter to Westinghouse Electric Company, U.S. Nuclear Regulatory Commission Approval Letter for Topical Report 6002-00301, "Advance Logic System Topical Report" (TAC No. ME4454), 9 September 2013

[19] Nuclear Regulatory Commission letter to Lockheed Martin Nuclear Systems and Solutions, Final Safety Evaluation of NuPAC_ED610000-47-P, Revision-, "Generic Qualification of the NuPAC Platform for Safety-Related Applications (Nonproprietary)" (TAC No. ME7900), 3 March 2017

[20] Nuclear Regulatory Commission letter to NuScale Power, Final Safety Evaluation for NuScale Power, LLC Licensing Topical Report: 1015-18653, "Design of the Highly Integrated Protection System Platform," Revision 2, CAC No. RQ6005, 6 June 2017

[21] Nuclear Regulatory Commission letter to Research and Production Company RadICS, Final Nonproprietary Safety Evaluation for "RadICS Topical Report" (CAC No. MF8411; EPID L-2016-TOP-0010), 31 July 2019

[22] Nuclear Regulatory Commission email to Doosan HF Controls Corporation, Final Safety Evaluation for HFC Topical Report RR9019-107-10, Amendment 4, 17 March 2021

[23] Nuclear Regulatory Commission letter to Toshiba America Energy Systems Corporation, Final Safety Evaluation for Toshiba "Licensing Topical Report for Toshiba NRW [Nonrewritable]-FPGA [Field Programmable Gate Array]-Based Instrumentation and Control System for Safety-Related Application," UTLA 0020P, Revision 2 (CAC No. ME9861; EPID L-201, 1 July 2020

[24] Nuclear Regulatory Commission, Review Guidelines for Field-Programmable Gate Arrays in Nuclear Power Plant Safety Systems, NUREG/CR-7006, ORNL/TM-1009/20, February 2010

[25] Nuclear Energy Agency, Multinational Design Evaluation Programme, Digital Instrumentation and Controls Working Group, MDEP Common Position CP-DICWG-07, Common Position on Selection and Use of Industrial Digital Devices of Limited Functionality, Version 3, July 2014

[26] Office for Nuclear Regulation, Nuclear Safety Technical Assessment Guide, Computer Based Safety Systems, NS-TAST-GD-046 Revision 6, April 2019

[27] Nuclear Energy Agency, Multinational Design Evaluation Programme, Digital Instrumentation and Controls Working Group, MDEP Generic Common Position No. DICWG-02, Common Position on Software Tools for the Development of Software for Safety Systems, Version B, February 2012

[28] Nuclear Energy Agency, Multinational Design Evaluation Programme, Digital Instrumentation and Controls Working Group, MDEP Generic Common Position No. DICWG-05, Common Position on the Treatment of Hardware Description Language (HDL) Programmed Devices for Use in Nuclear Safety Systems, Version A, March 2013

[29] Nuclear Regulatory Commission letter to Wolf Creek Nuclear Operating Corporation, Wolf Creek Generating Station - Issuance of Amendment Re: Modification of the Main Steam and Feedwater Isolation System Controls (TAC No. MD4389), 31 March 2009

[30] Nuclear Regulatory Commission, Task Working Group #4: Highly-Integrated Control Rooms—Communications Issues (HICRc), Interim Staff Guidance, Revision 1, DI&C-ISG-04, March 2009

[31] Anton Andrashov et al., Diversity in FPGA-Based Platform and Platform Based I&C Applications: Strategy and Implementation, Proceedings of American Nuclear Society 11th Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technolgies (NPIC&HMIT) 2019, Orlando, Florida, 9-14 February 2019

[32] Nuclear Regulatory Commission, Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems, NUREG/CR-7007, ORNL/TM-2009/302, December 2008

[33] Nuclear Regulatory Commission, NRC Regulatory Issue Summary 2002-22, Supplement 1, Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems, 31 May 2018

[34] Nuclear Energy Agency, Multinational Design Evaluation Programme, Digital Instrumentation and Controls Working Group, MDEP Generic Common Position No. DICWG-01, Common Position on the Treatment of Common Cause Failure Caused by Software Within Digital Safety Systems, Version A, June 2013

[35] Nuclear Regulatory Commission, NRC Regulatory Issue Summary 2016-05, Embedded Digital Devices in Safety-Related Systems, 29 April 2016

[36] Nuclear Regulatory Commission, Annual Update on the Integrated Strategy to Modernize the U.S. Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure, SECY-20-0100, 23 October 2020

[37] Nuclear Energy Institute, Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications, Revision 0 – Draft B, NEI 17-06, October 2021

World Nuclear Association
Tower House
10 Southampton Street
London WC2E 7HA
United Kingdom

+44 (0)20 7451 1520
www.world-nuclear.org
info@world-nuclear.org

Hardware description language (HDL) programmed devices (HPDs), such as field programmable gate arrays (FPGAs), offer several advantages over standard microprocessor based I&C systems.

These devices are able to perform a wide range of independent functions with a high clock speed making them well-suited to applications requiring very short response times. Furthermore, HPD's provide 'by design' separation of ancillary functions from the main safety I&C functions, therefore a postulated failure of an ancillary function will not prevent the correct execution of the safety I&C functions.

There is a growing trend towards the use of HPDs within nuclear I&C modernization projects and emerging reactor designs. Yet regulatory and industry guidance on these devices remains sparce and inconsistent. In order to facilitate the widespread use of HPDs and maximize the advantages they bring to I&C systems, there is an urgent need to harmonize regulatory and industry guidance on how they are to be used in nuclear plant applications.

This report has been produced by the Digital Instrumentation & Control Task Force with support from the Small Modular Reactors Task Force of World Nuclear Association's Cooperation in Reactor Design Evaluation and Licensing (CORDEL) Working Group.