Field Programmable Gate Array-Based Reactor Protection Systems and Potential for Inclusion of Secure Elements to Improve Cybersecurity

Prepared for
US Department of Energy

Benjamin Karch, Titus Gray, Michael T. Rowland

Sandia National Laboratories

September 2024
SAND2024-14666R

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

For acceptable implementations of technologies like wireless communications, remote monitoring, etc., strong mitigations must be developed and evaluated to ensure that new attack pathways do not increase risk for Advanced Reactors. Secure Elements can be adopted and adapted for this purpose based on tamper resistance and cryptographic abilities, but research must be done to properly integrate into critical components such as FPGA-based Important to Safety systems in conjunction with current and future regulations on cyber security features in Advanced Reactors. Typically, the integration of a Secure Element happens during the POST and UEFI boot of a computing platform, performed by the Operating System, which is not possible with FPGAs because they do not include these firmware components. Work must be done to identify a reliable and secure method for integration in FPGA-based systems which lack Operating Systems and therefore complex boot procedures, system calls, etc.

ACKNOWLEDGEMENTS

This work is funded by the Department of Energy (DOE) Advanced Reactor Safety and Security (ARSS) program under milestone M3CT-24SN11030111.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

The advancement of nuclear reactor technology necessitates the adoption of innovative solutions to enhance safety, security, and operational efficiency. This report investigates the integration of secure elements (SEs) into Field Programmable Gate Array (FPGA)-based reactor protection systems (RPS), providing a detailed analysis of the technical, regulatory, and practical considerations involved. The changing needs of the nuclear industry, particularly in the development of advanced reactors (ARs), require a reduction in cybersecurity and physical security operational costs to achieve economic viability. This emphasizes the importance of integrating advanced cybersecurity technologies across the board, including safety systems such as the RPS.

FPGA-based safety systems are increasingly being adopted by AR vendors due to their ability to execute specific, optimized functions with high performance and parallelism. The report discusses four NRC-licensed FPGA reactor protection systems: Advanced Logic System (ALS), Highly Integrated Protection System (HIPS), RadICS, and HFC-FPGA. These systems are composed of multiple FPGA components that perform specific functions such as communication handling and voting. They operate on multiple groups for redundancy and incorporate modular designs and data integrity measures.

Secure elements, or smart cards, are tamper-resistant hardware components used for securely storing and processing sensitive data. They perform cryptographic operations, ensure data integrity, and manage secure authentication and access control. Widely used across various industries, secure elements offer robust security for critical operations. Integrating secure elements into FPGA-based safety systems can enhance cybersecurity, particularly for remote monitoring and control. Leveraging existing security certifications, such as Common Criteria (CC) evaluations, could facilitate the regulatory approval process and reduce associated costs. A precedent for this approach exists in the qualification of Safety Integrity Level (SIL) certifications for safety systems in nuclear reactors. However, current regulations, specifically IEEE 7-4.3.2 endorsed by the Nuclear Regulatory Commission (NRC), recommend that safety systems should not include intrusive cybersecurity measures. The inclusion of secure elements (SEs) within the operational modules of the RPS would be considered intrusive, as these elements would communicate with the modules and influence their actions based on the SEs' outputs. Furthermore, integrating SEs into the existing RPS design would constitute a significant alteration, likely incurring substantial costs to have these design changes reviewed and accepted by regulatory bodies. While changing regulations might make SEs feasible for broader applications in the future, the current regulatory landscape imposes constraints that necessitate careful consideration of the design and implementation of SEs in safety systems.

To address these constraints, a design candidate was developed where the RPS is treated as a black box, and its sensor inputs and corresponding actuation commands are authenticated using SEs. This approach could avoid the high costs associated with completely redesigning existing systems to include SEs at a fundamental level. The design candidate demonstrated that this concept is effective and offers excellent performance, considering that RPS typically poll parameters like temperature at relatively slow intervals (e.g., every second). The design candidate passed initial performance tests, running for several hours without errors. The design also considers the High-Temperature Gas-cooled Reactor (HTGR) Digital Control System Architecture (DCSA) presented in reference [1]. In this architecture, data is generated by safety systems in Security Level 4 but is allowed to be transferred to Security Level 2, where the historian is housed and security requirements are less stringent. Future ARs built and licensed under performance-based regulations may be able to extract data from the historian for completely remote monitoring, ensuring secure visibility of their most critical components.

Additionally, ARs might circumvent the IEEE standard in the future by obtaining NRC approval to operate without systems classified as safety related based on inherent reactor physics. Such systems could integrate SEs internally within modules that control voting and actuation, providing additional protections against data injection, even if an adversary physically accesses the system bus. SEs could also be integrated into Maintenance Workstations (MWS) to establish mutual authentication, thereby aiding in secure remote access.

ACRONYMS AND TERMS

Acronym/Term	Definition
ACK	Acknowledgement
ALS	Advanced Logic System
APDU	Application Protocol Data Unit
AR	Advanced Reactor
BOP	Balance of Plant
CC	Common Criteria
CDA	Critical Digital Asset
CEAS	Cyber Enabled Accident Scenarios
CM	Communications Module
CRC	Cyclic Redundancy Check
DCSA	Defensive Cyber Security Architecture
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ESFAS	Engineered Safety Features Actuation System
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HIPS	Highly Integrated Protection System
I&C	Instrumentation and Control
I^2C	Inter-Integrated Circuit
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
KDF	Key Derivation Function
LM	Logic Module
LTE	Long Term Evolution
MAC	Message Authentication Code
NEI	Nuclear Energy Institute
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCM	Optical Communication Module
PP	Protection Profile
RAB	Reliable ALS Bus
RG	Regulatory Guide

Acronym/Term	Definition
RPS	Reactor Protection System
RTS	Reactor Trip System
SCL	Serial Clock Line
SDA	Serial Data Line
SE	Secure Element
SeBD	Secure by Design
SIL	Safety Integrity Level
SMR	Small Modular Reactor
SRP	Standard Review Plan
ST	Security Target
STPA	Systems Theoretic Process Analysis
SVM	Scheduling and Voting Module
TAB	Test ALS Bus
TCA	Tiered Cyber Analysis
TLS	Transport Layer Security
TR	Topical Report
UCA	Unsafe Control Action

1. INTRODUCTION

The evolution of advanced reactors (ARs) necessitates the integration of cutting-edge technologies to enhance safety, security, and operational efficiency. Among these technologies, Field Programmable Gate Arrays (FPGAs) have emerged as a pivotal component in the development of safety systems. Unlike traditional microprocessor-based systems, FPGA-based safety systems offer significant advantages in terms of performance, parallelism, and cybersecurity. This report explores the potential for integrating secure elements (SEs) into FPGA-based reactor protection systems (RPS) for ARs, along with a specific use case and design.

FPGA-based safety systems are increasingly being considered for ARs due to their ability to execute specific, optimized functions with high performance and parallelism. These systems are designed to increase cybersecurity by avoiding the large code bases required by operating systems used in conjunction with microcontrollers, thereby reducing potential vulnerabilities. The report delves into various FPGA-based safety systems, such as the Advanced Logic System (ALS), Highly Integrated Protection System (HIPS), RadICS, and HFC-FPGA, detailing their modular designs, redundancy mechanisms, and data integrity measures.

In addition to FPGAs, SEs, also known as smart cards, offer a promising avenue for enhancing the cybersecurity of RPSs. An SE is a tamper-resistant hardware component for securely storing and processing sensitive data. It can be used to perform cryptographic operations, ensure data integrity, and manage secure authentication and access control. SEs are widely used across many industries, including payment systems, access control systems, telecommunications, and automotive industries. By integrating SEs into FPGA-based safety systems, it is possible to achieve robust security for critical operations, such as remote monitoring and control of RPSs.

There are many different places in the Tiered Cybersecurity Architecture (TCA) where an SE can be used to improve the cybersecurity of a nuclear power plant. A Tier 2 approach could involve device authentication to ensure communications are coming from approved devices and not being spoofed or tampered with. A Tier 3 approach would focus on detecting adversarial actions to assist in detection and delay of adversarial tasking. This can be done through a connection to a remote environment designed to validate plant operations by performing the same calculations and determining if the plant and remote environment agree on control actions.

The focus of this effort is on the Tier 3 approach. This is to reduce the licensing complexities that would come from implementing a Tier 2 approach, since the implementation would need to be validated to have no effect on the operations of the plant safety systems. The Tier 3 approach would be a parallel operation to the safety system, validating its decisions, instead of introducing a system that could contain a new method of potential failure in the safety system, or result in significant alterations to existing FPGA safety system designs.

The report also addresses the licensing and regulatory considerations pertinent to the potential deployment of FPGA-based safety systems with integrated SEs. It discusses the potential benefits of leveraging existing security certifications, such as Common Criteria (CC) evaluations, to streamline regulatory approval processes. By utilizing CC-certified components, vendors can demonstrate that their systems meet high security and reliability standards, potentially reducing the overall cost and time associated with the licensing process.

Furthermore, the report presents a proof of concept for integrating an SE into an FPGA-based RPS. This proof of concept aims to demonstrate the feasibility and benefits of incorporating SEs into RPSs, particularly for advanced reactors that may have less physical security compared to

existing light water reactors. The proof of concept involves testing the performance, reliability, and security of the integrated system, ensuring that it meets the stringent requirements necessary for safe and secure operation in a nuclear environment.

By addressing the technical, regulatory, and practical aspects of FPGA-based safety systems and SE integration, this report aims to provide a basis for enhancing the cybersecurity and reliability of advanced nuclear reactors. The findings and methodologies presented herein offer valuable insights for industry stakeholders, regulatory bodies, and researchers dedicated to advancing nuclear safety and security.

2. FPGA-BASED SAFETY SYSTEMS

FPGA-based safety systems are a rising trend for ARs. This trend can be seen in Table 1, which lists FPGA-based safety systems for which the NRC has reviewed and approved an associated Topical Report (TR). FPGA-based safety systems are systems made of FPGAs and have little to no microprocessor components. Microprocessors are general-purpose processors that execute a set of pre-defined instructions, to accomplish complex tasks. On the other hand, FPGAs are hardware configurable devices that execute specific, optimized functions, that need high performance and parallelism. As the market demand grows for FPGA-based safety systems, security research is needed to ensure that these systems can securely perform their jobs, while maintaining safety and security. FPGA-based safety systems are thought to increase cybersecurity by avoiding large code bases required by Operating Systems used in conjunction with microcontrollers and performing a specific and targeted function. For example, URGENT/11 is a vulnerability set that effected network packet processing functions in the VxWorks RTOS; which is commonly integrated into typical digital instrumentation and control (I&C) devices [1]. Even devices that may not require the affected packet processing function could be victim to attacks based on the exploit family. Additionally, because the FPGA operates at a low level of abstraction, overhead is reduced, allowing for increased performance and parallelization of computational functions to be achieved. These systems may also benefit from reduced licensing costs by providing modular and diverse components which perform relatively few tasks when compared to microcontroller-based systems, which include more complex software and hardware components that are designed to handle a wider variety of functions that may or may not be necessary for the target environment.

Table 1. FPGA-Based Safety Systems

FPGA-Based Safety System	System Developer	Year	Topical Report
Advanced Logic System (ALS)	Westinghouse Electric Company	2013	[2]
HFC-FPGA	Doosan	2018	[3]
Highly Integrated Protection System (HIPS)	Paragon Energy Solutions	2017	[4]
RadICS	Radiy	2020	[5]

Attacks on FPGA based systems often revolve around attacking the bitstream of an FPGA. The bitstream is where the configuration data is stored and loaded from during the initialization of the FPGA; compromise of the bitstream can lead to an attacker gaining access to the intellectual property included in the bitstream or gaining access to manipulate it and add in malicious behavior [6]. This can mean loss of confidentiality in the intellectual property, loss of data integrity for the safety system, or even a Denial-of-Service attack, causing a loss of availability. These types of attacks tend to be much more complex and specific than attacks on microprocessor-based systems since FPGAs also tend to be much more specific for each use case and have fewer general-purpose packages utilized within.

FPGAs also allow for more parallel processing as the logic blocks can perform their independent actions simultaneously, allowing for faster speeds and potential redundancy, in that FPGAs can be designed to work despite failures in a number of logic blocks. By moving functions into an FPGA, some specialized processes can be orders of magnitude faster. Parnell and Bryner (2004) conducted

a comparison of triple DES encryption and decryption speeds between Microprocessor-based software and FPGA implementations, demonstrating that utilizing FPGA coprocessing improved computation speeds from around 5500ms for 1MN of data down to around 425ms for the same data [7]. In safety critical I&C systems, the increased performance can allow faster and more frequent checks, leading to a higher confidence in the state of the systems.

2.1. Implementations of FPGA-Based Safety Systems

The four safety systems listed in Table 1 were further investigated to identify their design methodologies and common features. Each evaluated system has a published TR with the Nuclear Regulatory Commission (NRC) that details the regulatory evaluation, design process, features, and other components. Three of the systems—ALS, RadICS, and HFC-FPGA—specifically reference the use of NUREG-0800, "Standard Review Plan for the Safety Analysis Reports for Nuclear Power Plants," as guidance for evaluating the safety system [8]. The NUREG Standard Review Plan (SRP) offers guidance for safety reviews related to permits and licenses for nuclear power plants. Chapter 7 is particularly relevant to FPGA-based safety systems, providing further guidance on conforming to Institute of Electrical and Electronics Engineers (IEEE) Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which all four systems reference when discussing their regulatory evaluations [9]. These evaluations were performed at the system level, but further evaluation may be needed when integrating these systems into a plant design.

2.1.1. HIPS

A potential configuration for the HIPS system is displayed in Figure 1 below. The HIPS system is designed as a highly modular system, designed in conjunction with Nuscale for their small modular reactor (SMR). Each module has a highly specific purpose, with multiple versions of the communications module (CM) to achieve more specific goals. One example of these is the scheduling and voting module (SVM) that performs the 2-out-of-4 voting on the information received to determine trip state.

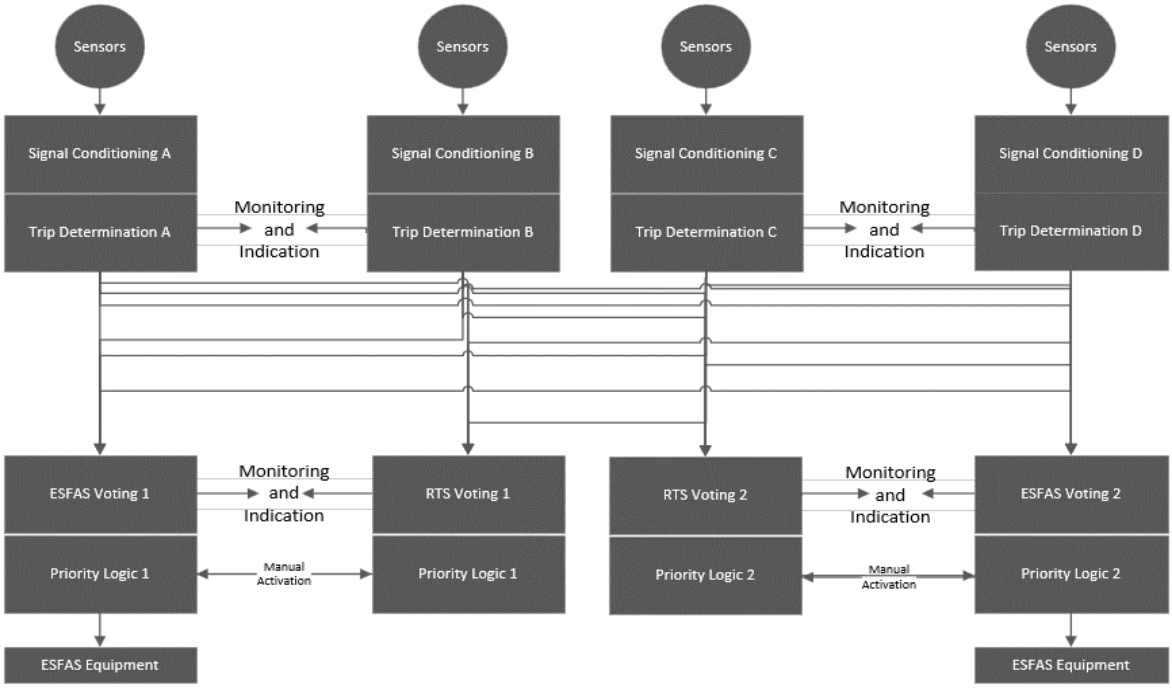

Figure 1 Potential HIPS Configuration (Adapted from [4])

2.1.2. ALS

A high-level view of the design of an ALS chassis is included in Figure 2. The ALS system utilizes more generic boards than the HIPS system, with configuration changes to achieve the various goals. The Core Logic Board is utilized for multiple goals that might include calculating average pressure and monitoring safety thresholds, the 2-out-of-4 voting that ensures redundancy and fault tolerance, and the process protection system that compares measurements to the trip thresholds to generate trips when necessary. This differs from the HIPS system that has dedicated modules for the different functions.

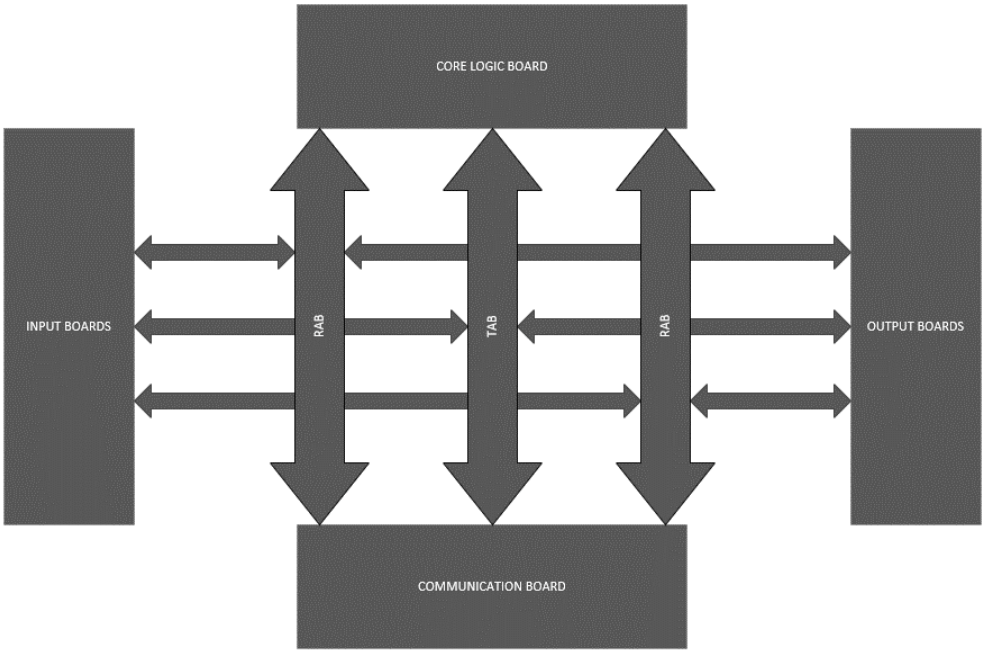

Figure 2 Generic ALS Platform Overview (Adapted from [2])

2.1.3. RadICS

The RadICS system (shown in Figure 3) modules are also more generic than that of the HIPS system, resembling the ALS. It uses one Logic Module (LM) for data exchange with other modules and the plant-specific logic. It similarly implements an Optical Communication Module (OCM) for inter-division communications. The modules are designed with smaller blocks inside, called Units; a few of these are the FPGA Unit, Input Unit, Output Unit, Communication Units, among others. This can mean that modules serve multiple purposes, based on the units contained, where the communication unit can be used for communication between two different chassis, rather than going through a dedicated module for external communication.

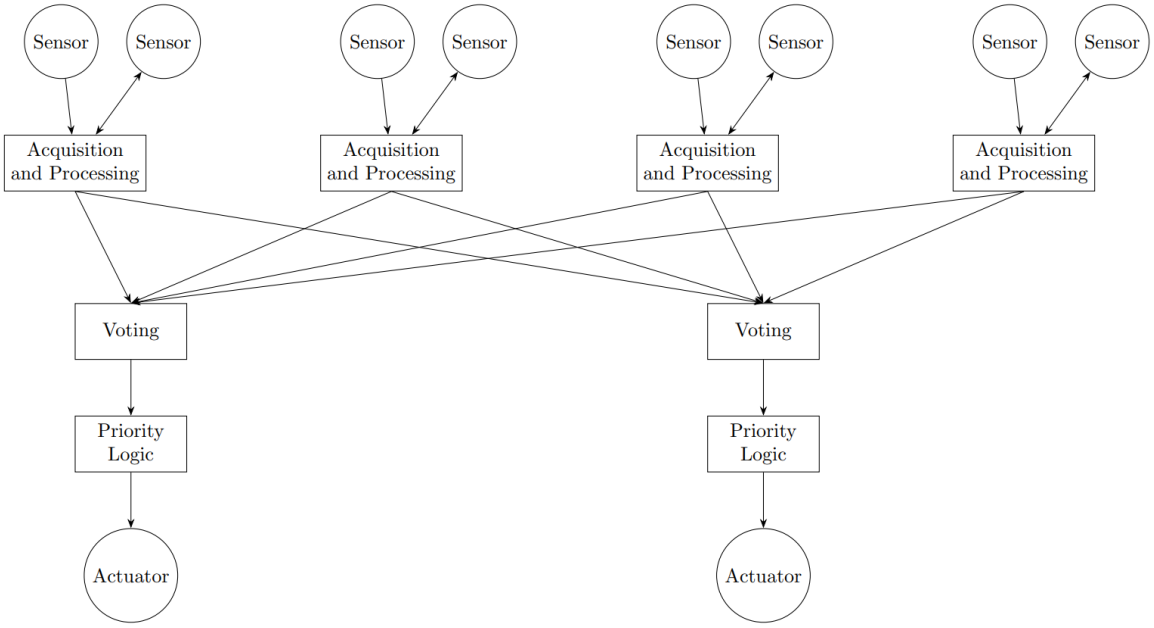

Figure 3 Potential RadICS Configuration (Adapted from [5])

2.1.4. HFC-FPGA

The primary difference for the HFC-FPGA compared to the other noted systems, is the presence of the microcontroller-based Gateway Controller. The HFC-FPGA and its components are shown below in Figure 4. Each of the other systems notes a lack of microcontroller-based components. The Gateway Controller is responsible for receiving and transmitting with external devices and the controller module; it uses a proprietary protocol that other HFC devices use called G-Link. The HFC-FPGA was designed based on, and to augment the original HFC-6000 in cases where an FPGA based system was desired over a microcontroller-based system.

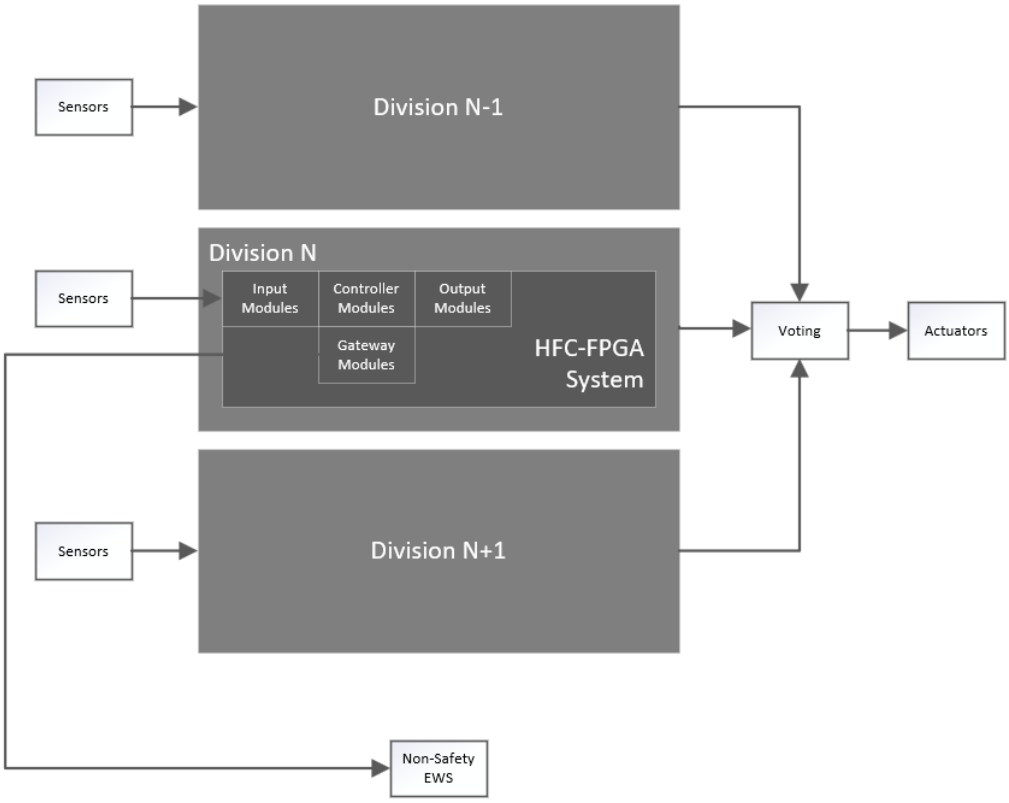

Figure 4 HFC-FPGA Platform Overview (Adapted from [3])

The vulnerability assessment for the operational phases of HFC-FPGA modules also focuses on cybersecurity-based intrusions and faults, similar to the assessment for the original HFC-6000 platform. Section 8.7 of PP901-000-01, HFC-6000 safety system TR, analyzes the security design concept and capability of the original HFC-6000 platform, which are designed to block outside cybersecurity threats. Cybersecurity of the HFC-FPGA modules at the system level is fundamentally the same as the cybersecurity for the original HFC-6000 platform. The HFC-FPGA platform uses the HFC proprietary F-Link, G-Link, and RIF as internal communication links, which have a predefined message structure, size, and timing. Any message in the link that deviates from the required size, structure, and source is logged as an error, just as the HFC-6000 ICL performs. Additionally, the only external communication link for the qualified HFC-6000 system and the HFC-FPGA modules addressed in this amendment is the C-Link.

2.2. Common Features

Many safety-critical digital control systems are being designed with a focus on use in nuclear power plants. These systems have many similarities and approaches to ensure the systems are secure and meet the requirements for use in nuclear facilities. These systems are typically made of FPGA modules with similar functions, they utilize redundancy and voting to ensure the functions of the system are not compromised by the failure or compromise of a single component and utilize common data integrity systems like checksums.

2.2.1. Modular Design

These systems are typically made up of four general types of modules: input modules, output modules, communication modules, and a main LM. The input modules are used to interpret a variety of input types, both digital and analog, and convert them to digital signals that the main logic board can then use. The main logic board is the most specialized of the four types as the logic for each facility will differ based on their requirements, parameters, and inputs. The output modules are utilized to interact with the field devices based on the determinations from the main logic board; these devices might be motors, relays, alarms, or other devices that trigger physical actions from an electrical signal. The communication modules are how the systems communicate with other parts of the system, and external devices, like a maintenance workstation, safety display, or another chassis of the same system. The modularity allows for use in many applications in a nuclear facility's safety system, as well as allowing for hardware advancements in the future without a complete ecosystem redesign being necessary.

2.2.2. Redundancy

Redundant measures are implemented across the board, throughout these safety systems. The input and output modules are responsible for ensuring one-way communication and ensuring that failure in one communication channel does not affect the other channels. The systems are designed with voting functions, where multiple separate systems evaluate the same data and then vote on whether an action is required. By implementing this voting system, the implementation can have modules fail or be compromised before it affects the safety or security of the facility. Through redundancy, the safety functions of the systems can be preserved despite software or hardware failure, or even compromise of the systems.

2.2.3. Data Integrity

Data integrity is another important piece of the safety critical I&C systems. Each of the four systems previously mentioned: ALS, HFC-FPGA, HIPS and RadICS, utilize different communication protocols and data integrity checks. The most common is CRC (Cyclic Redundancy Check) checksums. The HFC-FPGA system utilizes it in its proprietary C-Link communication protocol, when it transmits and receives payloads, and to verify the data stored in the memory of the FPGA components. The ALS and RadICS systems also reference utilizing checksums in the communication protocols implemented.

FPGA-based safety systems benefit significantly from their deployment in highly protected areas within nuclear plants, leveraging both physical and logical security measures. These systems are considered to be inherently more secure due to their non-networked nature, which minimizes exposure to external cyber threats. Unlike networked systems that are susceptible to remote attacks, FPGA-based systems operate in isolated environments, reducing the attack surface. While the specifics of data communication within these systems are not publicly disclosed, TRs indicate that integrity protections are in place. However, it is important to note that some of these protections rely on techniques that are considered insecure (e.g., CRC, which is used to detect errors rather than malicious and arbitrary alterations to communications). For instance, older cryptographic algorithms and protocols may still be in use, which could potentially expose the systems to vulnerabilities if not updated. Therefore, ongoing security research and the adoption of modern cryptographic methods are essential to ensure that FPGA-based safety systems can continue to securely perform their critical functions while maintaining the highest standards of safety and security.

3. LICENSING AND REGULATORY CONSIDERATIONS

3.1. Security Certifications

CC evaluations provide a standardized framework for assessing the security properties of information technology products, including smart cards / SEs. These evaluations involve a rigorous process where products are tested against predefined security requirements, known as Protection Profiles (PPs) and Security Targets (STs). The evaluation process includes several Evaluation Assurance Levels (EALs), ranging from EAL1 to EAL7. EAL1 involves basic functionality tests, ensuring that the product works as claimed without a thorough examination of its internal design. EAL2 through EAL4 provide increasing levels of assurance by incorporating design reviews, testing, and vulnerability analysis. EAL5 through EAL7 involve comprehensive, in-depth analyses of the product's design and implementation, including formal methods and rigorous testing to ensure the highest levels of security. These levels share common characteristics with the licensing processes for safety systems in nuclear power plants, such as the need for thorough documentation, rigorous testing, and independent verification to ensure reliability and safety.

Vendors of advanced nuclear reactors in the USA may be able to leverage the existing work performed during CC evaluations to reduce their licensing costs and streamline regulatory approval processes. By integrating smart cards that have already undergone rigorous CC evaluations, vendors might demonstrate that these components meet high security and reliability standards. This pre-existing certification could serve as a strong foundation for the safety and security assessments required by regulatory bodies such as the NRC. Specifically, compliance with regulations such as 10 CFR Part 50, which governs the licensing of production and utilization facilities, and 10 CFR Part 52, which covers the licensing, certification, and approval for nuclear power plants, might be facilitated by the use of CC-certified components.

Accrediting CC-certified smart cards could reduce testing and validation, thereby potentially lowering the overall cost and time associated with the licensing process. Similar successful efforts have been taken to accredit Safety Integrity Level (SIL) Certification IEC 61508 by the Nuclear Energy Institute (NEI) and accepted by the NRC [10], [11]. NRC staff concluded that the following benefits of leveraging international recognized standards [12]:

- Licensing efficiency
- Cost savings
- Licensing efficiency
- Cost savings

Commercial grade dedication is important for reducing costs associated with AR digital I&C systems. Many AR Vendors are minimizing reliance on Safety Related Systems, (typically custom designed) in favor of increasing use of non-safety related, but important to safety systems, and decoupling of safety systems from balance of plant (BOP)/adjacent island. The use of commercial of the shelf equipment is expected to increase, and successful efforts to accredit SIL certifications could lead to a similar effort and successful results to accredit CC certifications.

Additionally, the international recognition of CC certifications may enhance the credibility of the vendor's safety claims, potentially expediting the review and approval process. Crypto implementations are complicated, and this may be an opportunity to offset the heavy load that would be required by a vendor to establish confidence from the NRC in a custom implementation of cryptographic primitives by establishing the use of a device that is highly integrated into other

industries and with third-party validation of conformance to standards and with independent vulnerability assessments. By capitalizing on the established security assurances provided by CC evaluations, vendors might more efficiently meet regulatory requirements, ultimately facilitating the deployment of advanced nuclear technologies.

While integrating SEs and their associated cryptographic capabilities directly into safety-related systems in nuclear power plants can enhance security, it also introduces potential issues that must be carefully considered. One significant concern is the potential conflict with standards such as IEEE 7-4.3.2, which is endorsed by the NRC in regulatory guides (RGs) like RG 1.152 [9], [13]. This standard recommends that cybersecurity features should not be integrated into safety systems to avoid introducing vulnerabilities that could compromise the system's primary safety functions. Integrating SEs could inadvertently create new attack vectors or increase system complexity, making it more challenging to ensure the reliability and predictability of safety functions. Additionally, the cryptographic operations and SE management might require regular updates and patches, which could disrupt the continuous operation of safety systems. The need for specialized knowledge to manage these SEs could also complicate maintenance and emergency response procedures. Therefore, while SEs can provide robust security, their integration into safety-related systems must be approached with caution, ensuring that cybersecurity measures do not undermine the fundamental safety objectives of the nuclear power plant.

3.2. Current Approach (NEI 08-09, RG 5.71 Rev 1)

Current approaches and defensive strategies rely heavily on physical access control and secure physical boundaries, and/or deterministic controls. An example of which can be found in NEI 08-09 Rev 6 which states "Safety CDAs are isolated from all other CDAs through the use of deterministic boundary devices (i.e., data diodes, air-gaps)"[1] [14]. However, AR use cases such as remote operations and wireless will reduce the benefit of secure physical boundaries and lack deterministic logical boundaries. For example, RF signal propagation for wireless communications results in variations to where these signals can be accessed, therefore directly affecting the boundaries that limit access to the wireless communications. These use cases are prescriptively prohibited for Safety CDAs by the example Defensive Cyber Security Architecture (DCSA) in RG 5.71 Rev 1 (Section 3.2.1) and the Example 1 and 2 DCSA in NEI 08-09 Revision 6 (Section 4.3) [15], [14].

A key update to NRC RG 5.71 Revision 1, Section C.3.2 is the identification the performance-based requirements for defensive architecture, which increases the flexibility provided to achieve an acceptable defensive architecture. RG 5.71 revision 1 describes two mandatory elements for acceptable defensive strategies as [2]:

1. A defensive architecture that describes a physical and logical network design that implements successive security levels separated by boundary control devices with segmentation within each security level,
2. A defensive strategy that employs multiple, diverse, and mutually supporting tools, technologies, and processes to effectively perform timely detection of, protection against, and response to a cyberattack.

The first element details an architecture and passive defense that provides for locations to establish a capability to prevent or deny access to an adversary. SEs and their standard cryptosystems could

[1] Safety critical digital assets (CDAs) are digital technologies that perform or directly support SR or ITS functions.

benefit this element. The second aims to implement a detection and response capability designed to prevent adversaries from completing tasks needed to accomplish their aims. The integrity protections of cryptosystems could enhance detection and response capabilities to ensure that authenticity of communications from sensors are protected, and unauthorized modifications to these communications are detected.

3.3. Risk Informed Performance Based Regulation

The NRC and other international regulators are adopting a performance-based approach to cybersecurity. Performance based approaches emphasize desired outcomes and rely upon licensees and vendors to identify risks associated with cybersecurity, specify requirements on how to address these risks, and implement systems and process to reduce risk and sustain cybersecurity protections.

Specifically, the NRC has updated RG 5.71 Rev 1 considered International Atomic Energy Agency (IAEA) guidance publications NSS 17-T and NE NR-T-3.30 which detail an international consensus risk-informed performance-based approach for cybersecurity [16], [17]. The goal of the RG 5.71 "is to tailor the well-known and well-understood set of security controls (based on National Institute of Standards and Technology (NIST) cybersecurity standards) that address potential cyber risks to CDAs to provide a flexible programmatic approach in which the licensee or applicant can establish, maintain, and successfully integrate these security controls into a site-specific cybersecurity program" [15].

3.4. Draft Regulatory Guide 5075

Tiered cyber analysis (TCA) is a three-tiered cybersecurity assessment methodology derived from the requirements outlined in 10 CFR 73.110 [18]. This methodology was proposed by the U.S. NRC in the draft RG DG-5075 [19]. TCA aligns domestic standards, international standards, and technical guidance to select Secure by Design (SeBD) requirements for the development of defensive network architectures and application of effective cybersecurity controls.

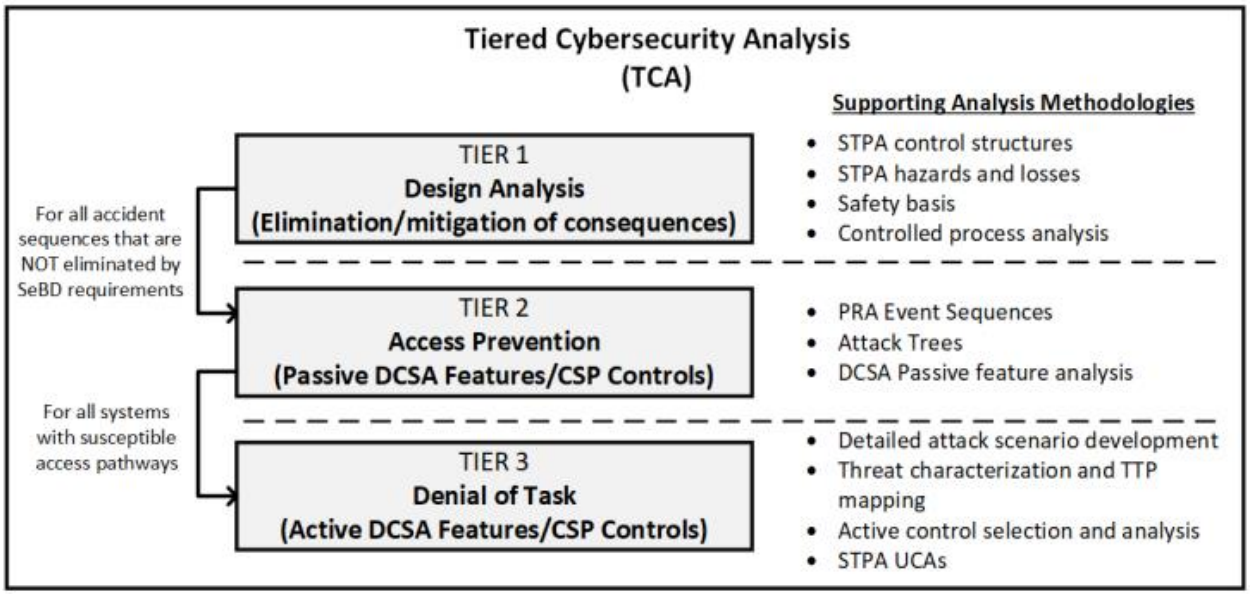

Figure 5 Tiered Cyber Analysis

Tier 1 focuses on the evaluation of the facility's design basis, passive features, and physical elements. Tier 1 prioritizes the complete avoidance of cyber enabled accident scenarios (CEAS) caused by digital compromise of the facility's entire digital footprint. This tier aims to credit the facility's design basis, passive features, and physical elements as SeBD. This accreditation identifies the features and their effects, that would prevent an adversary from implementing an attack that would cause unacceptable consequences.

Tier 2 focuses on an attack pathway analysis, which covers all attack pathways[2], except for the supply chain. Tier 2 analysis will result in identification and specification of passive or deterministic DCSA or Cybersecurity Plan elements. Tier 2 largely meets the first element of RG 5.71 Rev 1 defensive architecture [15]. SEs can be integrated to provide a by-design, always on, protection against unauthorized disclosure and unauthorized modification via cryptography. Once in place and automatically enforced by system design and operations, the cryptosystem passively secures logical communications and fortifies logical boundaries. Wide use of SEs and appropriate operations, maintenance and monitoring of their actions may provide a pathway to beneficial use cases such as remote operations and wireless networking.

Tier 3 focuses on identifying and implementing active protection measures (such as detection, delay, response, and recovery) which protect against the adversary from successfully completing all tasks needed for a successful cyber-attack. These measures are imposed upon the systems associated with the functions identified in Tier 2. Tier 3 controls should ensure that an attacker who gains access to the systems necessary to achieve their goal should encounter control measures which prevent them from being successful. This tier includes two kinds of controls: baseline controls which apply broadly and provide information security assurance, and risk-informed controls that apply to specific identified risks. Systems Theoretic Process Analysis (STPA) Unsafe Control Actions (UCAs) can assist in informing hazards and loss scenarios associated with those hazards.

Tier 3 would rely upon monitoring of the passive protections (encrypted text, secure hash, message authentication codes (MACs), digital signatures) to enhance detection and response capabilities. MACs that do not match their calculated values will be discarded and the data within the message will not be used by the digital I&C system. Prolonged corruption or manipulation of the communications may result in failure of the communication link and therefore a denial-of-service impact. However, most safety systems are designed with an expectation that a failure of the communication link would occur during the system lifetime, and the designers would have anticipated and accounted for its impact, thereby limiting consequences to an acceptable level. Nevertheless, continued failures of the communication link due to malicious actions would need to be monitored and corrective action taken upon detection of the malicious act.

Additionally, digital signatures of source files and digital I&C inputs increase confidence that recovery activities are utilizing approved software and inputs. For example, in the case of a ransomware attack, secure and unaffected archives digitally signed could be confirmed in an expeditious manner to reduce time to recover key digital I&C systems and data sets (like those in the historian) affected by the attack.

[2] The attack pathways considered are, physical, network, wireless network, removable media, mobile device, and supply chain.

4. PROOF OF CONCEPT

4.1. Description

The primary objective of this proof of concept is to demonstrate the integration of an SE or hardware root of trust into an AR nuclear power plant's RPS. This integration aims to enhance the cybersecurity of the RPS, particularly for ARs that may have less physical security compared to existing light water reactors. The proof of concept is designed to provide secure remote monitoring of the RPS, addressing the industry's shift towards remote monitoring and potentially remote control. The component layout for this system is shown in Figure 6. While protecting the FPGA bitstream is important, the immediate and direct impact on reactor safety from secure remote monitoring of the RPS is considered more critical, as the RPS is located in a highly protected area and attacks on the FPGAs' bitstreams likely requires physical access. Additionally, integration of SEs within and directly interacting with the operational FPGAs within the RPS modules would significantly increase any associated costs with licensing, as the complexity of the interactions between modules would be significantly increased. Ensuring the integrity and security of the RPS data can prevent catastrophic failures and enhance overall safety. Beginning the development of new security features on the most critical devices can setup a framework that can be expanded to future efforts, like securing the bitstream of the FPGAs.

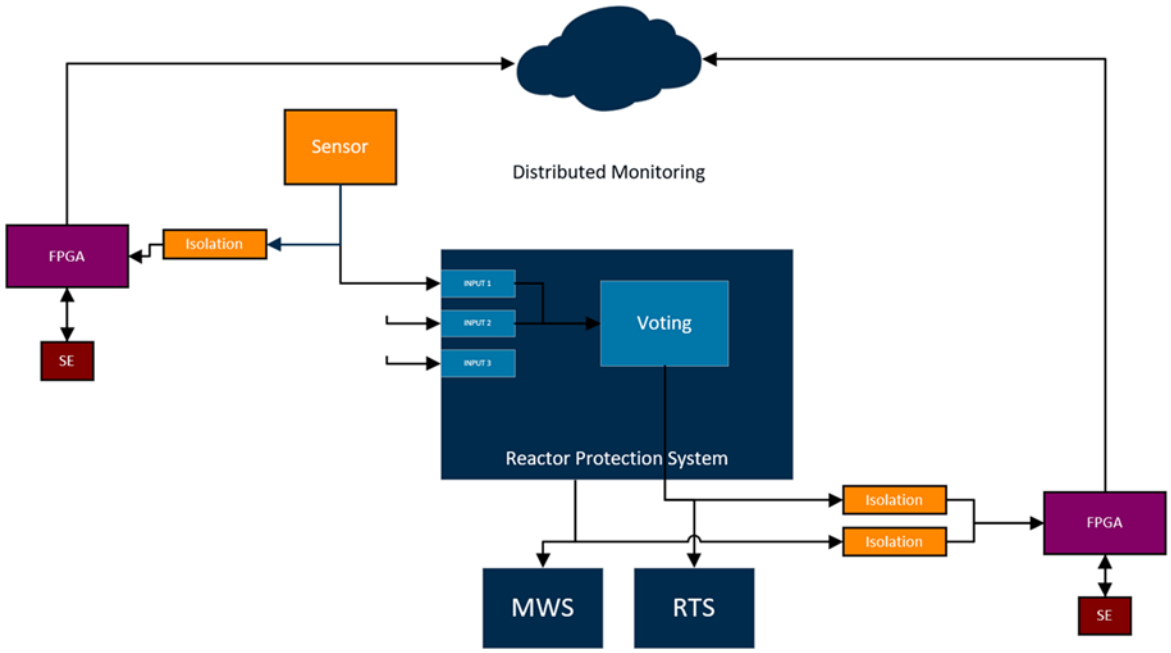

Figure 6 SE Integration for Monitoring

Existing reactor protection systems are simplistic and lack robust cybersecurity features other than those that are intrinsic to the design choices. While the inherent design choices, such as the use of hardwired logic and minimal software components, provide a basic level of security, they may not be sufficient to address the evolving landscape of cybersecurity threats specific to ARs. While current light water reactors rely on extensive physical security measures, ARs, such as microreactors, necessitate enhanced cybersecurity due to their different use cases and potentially reduced physical

security. This proof of concept addresses the need for secure communication and monitoring of the RPS in ARs.

The shift towards ARs and remote monitoring in the nuclear industry underscores the importance of integrating cybersecurity measures into RPSs. This proof of concept leverages an SE to ensure secure communication and monitoring, providing a potential solution for the evolving needs of the industry.

4.2. Equipment

The equipment used in this proof of concept includes a Raspberry Pi for I²C (Inter-Integrated Circuit) communications, logic analyzers for communication analysis, an Artix 7 FPGA, and an NXP SE050 SE. The hardware components consist of the Artix 7 FPGA, a versatile FPGA used for implementing the RPS, and the NXP SE050 SE, which provides cryptographic operations and secure storage, connected via I²C. Custom-built components include custom Verilog code for the FPGA to handle communications and cryptographic operations with the SE.

The NXP SE050 is a SE solution designed to provide a root of trust at the IC level, ensuring secure storage and cryptographic operations for critical communication and control functions. It supports RSA and ECC algorithms and holds an independent CC EAL 6+ security certification, offering robust protection against sophisticated attack scenarios. The SE050 includes a Java Card operating system and is optimized for IoT security use cases, supported by comprehensive development tools and documentation.

The Nexys A7-100T features the XC7A100T-1CSG324C Artix-7 FPGA, which provides high performance with 15,850 programmable logic slices and 4,860 Kbits of block RAM. It includes various peripherals such as DDR2 memory, Ethernet PHY, USB interfaces, and multiple I/O options, making it suitable for complex FPGA-based development. The Nexys A7-100T is compatible with Xilinx's Vivado Design Suite, facilitating efficient development and implementation.

4.3. Cryptography

The SE050 comes pre-loaded with Federal Information Processing Standards (FIPS)-compliant features that include advanced algorithms and protocols designed to provide robust security in various applications such as secure identification, payment systems, and access control. Key cryptographic capabilities of the SE050 include:

- **ECC Algorithms**: ECDSA (Elliptic Curve Digital Signature Algorithm), ECDH (Elliptic Curve Diffie-Hellman), ECDHE (Elliptic Curve Diffie-Hellman Ephemeral), and EdDSA (Edwards-curve Digital Signature Algorithm) provide strong security with smaller key sizes, making them efficient for the limited resources of smart cards.
- **MACs**: HMAC (Hash-based MAC), secure HMAC, CMAC (Cipher-based MAC), and GMAC (Galois/Counter Mode MAC) ensure data integrity and authenticity.
- **Hash Functions**: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512 are used for generating cryptographic hashes, which are essential for data integrity and digital signatures.
- **Key Derivation Functions (KDFs)**: HKDF (HMAC-based KDF), PBKDF2 (Password-Based Key Derivation Function 2), PRF (Pseudo-Random Function) for TLS-PSK (Pre-Shared Key), and MIFARE-AES-KDF are used to derive secure keys from initial secret values.

- **Symmetric Encryption Algorithms**: AES (Advanced Encryption Standard) with key sizes of 128, 192, and 256 bits in modes such as CBC (Cipher Block Chaining), EBC (Electronic Codebook), CTR (Counter), CCM (Counter with CBC-MAC), and GCM (Galois/Counter Mode) provide robust encryption for data confidentiality.
- **Triple DES (3DES)**: Available in 2-key and 3-key variants, offering an additional layer of encryption security.
- **RSA Cipher**: Supports decryption and encryption with key sizes up to 4096 bits, providing strong security for asymmetric encryption tasks.

Among these features, ECDSA is chosen for strong authentication of digital information due to its combination of security and efficiency. ECDSA leverages the mathematical properties of elliptic curves to provide high levels of security with smaller key sizes compared to traditional algorithms like RSA. This results in faster computations and reduced power consumption, which are critical for the limited processing capabilities and battery life of smart cards. Additionally, the compact key sizes of ECDSA make it ideal for the constrained storage environments of smart cards, ensuring that the device can maintain high security standards without compromising performance or efficiency.

When selecting an appropriate elliptic curve and key length for ECDSA (Elliptic Curve Digital Signature Algorithm) on a smart card, several factors need to be considered, including security, performance, and compatibility. Among the supported curves, NIST-P 256 (also known as secp256r1) is often chosen for several compelling reasons:

1. **Security**: NIST-P 256 provides a high level of security that is considered sufficient for most modern cryptographic applications. With a 256-bit key length, it offers a security level roughly equivalent to a 128-bit symmetric key, which is robust against current and foreseeable cryptographic attacks [20]. Notably, 128-bit symmetric keys are the key strength used for LTE (Long-Term Evolution) communications, further emphasizing their adequacy for securely transporting critical information in real-time systems [21]. This level of security ensures that NIST-P 256 is well-suited for applications requiring high assurance, such as the secure communication.
2. **Performance**: NIST-P 256 strikes a good balance between security and performance [22]. The 256-bit key length is efficient for computation, making it suitable for the limited processing power and energy constraints of smart cards. This ensures that cryptographic operations can be performed quickly and with minimal power consumption.
3. **Standardization and Interoperability**: NIST-P 256 is one of the most widely adopted and standardized elliptic curves. It is specified by the NIST and is included in many cryptographic standards and protocols, such as TLS (Transport Layer Security), which ensures broad compatibility and interoperability with other systems and devices.
4. **Maturity and Trust**: NIST-P 256 has been extensively studied and vetted by the cryptographic community. Its long history of use in various applications has built a high level of trust in its security properties. This maturity makes it a reliable choice for secure applications. Additionally, the licensing process could be more cost-effective by using algorithms that are more mature and widely adopted, as they are likely to be better understood by regulatory bodies and have established support in existing security frameworks. This can streamline the approval process and reduce the need for extensive validation and testing, further enhancing the economic viability of integrating advanced cybersecurity technologies into RPSs.

5. **Hardware and Software Support**: Due to its widespread adoption, NIST-P 256 is well-supported by both hardware and software implementations. This means that there are optimized libraries and hardware accelerators available, which can further enhance the performance and security of cryptographic operations on smart cards. This widespread support could allow for a reduction in cost, as there are many open-source implementations available in a variety of programming languages and hardware descriptions. Additionally, NIST-P 256 is typically available on modern SEs, making it a versatile and cost-effective choice for integrating advanced cybersecurity measures into RPSs.

While other curves like Brainpool, Twisted Edwards (Ed25519), Montgomery Curve25519, Koblitz, and Montgomery (Curve448) also offer strong security properties, NIST-P 256 is often selected because it provides a well-rounded combination of security, efficiency, and compatibility. This makes it an ideal choice for smart card applications where these factors are critical.

The key steps in testing include initial performance testing using a Raspberry Pi to test the performance of the SE050 SE, communication analysis by establishing a logic analyzer on the I²C link between the FPGA and the SE to verify communication integrity and timing, and FPGA integration by implementing and testing the custom Verilog code on the FPGA, ensuring it can handle real-time data and cryptographic operations. Success is measured by the successful integration of the SE into the FPGA, real-time data transfer and cryptographic operations performed within acceptable engineering parameters, and performance benchmarks such as digital signatures at least once every 5 seconds and continuous operation for multiple hours without errors. While specific environmental conditions for nuclear power plants are not considered in this paper, future implementations will need to address temperature requirements, seismic conditions, and other environmental factors.

One of the main engineering challenges faced was ensuring reliable response times from the SE over extended periods and handling missed responses during high-frequency requests. The NXP SE050 was chosen for its high security certification (CC EAL 6+), support for RSA and ECC cryptographic algorithms, and future-proof ECC curves. The Artyx 7 FPGA was selected for its high performance and capability to handle complex logic and communication tasks. Initially, the proof of concept aimed to provide secure monitoring based on internal FPGA communications. However, due to regulatory and licensing requirements, the focus shifted to monitoring the inputs and outputs of the RPS, treating the internal FPGA system as a black box. As discussed in Section 3, IEEE 7.4-3-2 [9] states that intrusive cybersecurity controls may not be applied while the system is in use. Additionally, alterations to RPS designs to include SE(s) that interact with voting modules and other DPGAs directly involved in decision making could result in much higher costs associated with licensing and re-qualification.

Data collected during testing includes response times and success rates of cryptographic operations, and communication integrity and timing data from the logic analyzer. Data analysis methods involve iterative analysis during development to refine performance and reliability, and benchmarking against performance requirements such as digital signature frequency and continuous operation duration.

4.4. Testing and Development

The following outlines the general testing and development procedure for integrating an SE into an AR protection system. This framework is designed to ensure an efficient and effective development lifecycle. The process is designed with the performance, reliability and security of the SE-integrated

RPS, therefore enhancing the cybersecurity posture of ARs without compromising on the efficiency of the current systems.

Initial Performance Testing begins with setting up an SE testing platform. This platform is crucial for establishing a robust environment where testing scripts can be easily developed, executed, and modified. The platform's design ensures seamless access to the SE, enabling efficient data storage and transmission.

- **Step 1.1: Set up SE Testing Platform**: Establish a system capable of developing and running testing scripts for communications with the target SE). This platform should facilitate easy development, access, data storage, and data transmission to verify that the SE meets targeted performance metrics.
- **Step 1.2: Develop Performance Test Scripts**: Create and execute performance test scripts on the SE testing platform to evaluate the SE's capabilities. These scripts should be designed to test various cryptographic operations, such as digital signatures, and assess the SE's response times and success rates.
- **Step 1.3: Measure Performance Metrics**: Collect and analyze data on the SE's performance, focusing on response times and success rates for cryptographic operations. This step ensures that the SE meets the required performance criteria for integration into the RPS.

Communication Analysis involves deploying advanced communication monitoring tools, such as logic analyzers, to observe the data exchange between the FPGA and the SE. This step is vital for capturing detailed communication data, which is then analyzed to verify the integrity and timing of the interactions.

- **Step 2.1: Set up Communication Monitoring Tools**: Deploy communication monitoring tools, such as logic analyzers, to observe the data exchange between the FPGA and the SE. These tools should be configured to capture detailed communication data for analysis.
- **Step 2.2: Capture and Analyze Communication Data**: Record and scrutinize the communication data to verify the integrity and timing of the interactions between the FPGA and the SE. This analysis helps identify any discrepancies or issues in the communication process.
- **Step 2.3: Compare Timing and Response Data**: Compare the timing and response data obtained from the FPGA with the initial performance metrics gathered from the SE testing platform. This comparison ensures consistency and reliability in the SE's performance across different platforms.

FPGA Integration is a critical phase where custom code (e.g., Verilog) is developed and implemented on the FPGA to manage communications with the SE. This code is optimized for real-time data transfer and cryptographic operations, ensuring that the FPGA can handle the required tasks efficiently.

- **Step 3.1: Implement Custom FPGA Code**: Develop and implement custom code (e.g., Verilog) on the FPGA to manage communications with the SE. This code should be optimized for real-time data transfer and cryptographic operations.
- **Step 3.2: Connect FPGA to SE**: Establish a physical connection between the FPGA and the SE via an appropriate communication protocol (e.g., I^2C). Ensure that the connection is stable and capable of handling the required data throughput.

- **Step 3.3: Conduct Real-Time Data Transfer Tests**: Perform tests to verify that the FPGA can handle real-time data transfer and cryptographic operations with the SE. These tests should simulate actual operating conditions to ensure the system's robustness.
- **Step 3.4: Verify Communication with Monitoring Tools**: Use communication monitoring tools to validate that the FPGA is correctly communicating with the SE. This step helps identify any potential issues in the data exchange process.
- **Step 3.5: Measure Performance Benchmarks**: Evaluate the system's performance by measuring key benchmarks, such as the frequency of digital signatures and the duration of continuous operation without errors. These benchmarks ensure that the system meets the necessary performance standards.

Performance Verification involves conducting extended operation tests to confirm the system's long-term reliability and stability. These tests are designed to ensure that the system can operate continuously for multiple hours without encountering errors.

- **Step 4.1: Conduct Extended Operation Tests**: Run extended tests to confirm that the system can operate continuously for multiple hours without encountering errors. These tests help verify the system's long-term reliability and stability.
- **Step 4.2: Adjust FPGA Code Based on Performance Data**: Analyze the performance data and make necessary adjustments to the FPGA code to optimize the system's performance. This iterative process ensures that the system meets all performance and reliability requirements.
- **Step 4.3: Finalize Testing Procedures and Document Results**: Complete the testing procedures and thoroughly document the results. This documentation should include detailed performance metrics, any adjustments made, and the final assessment of the system's readiness for deployment.

In summary, this testing and development procedure is designed to be agile and adaptable, allowing for rapid prototyping and iterative improvements. By following this structured approach, we ensure that the SE is effectively integrated into the RPS, enhancing the cybersecurity of advanced nuclear reactors. This comprehensive process not only validates the SE's performance but also ensures that the integrated system meets the stringent requirements necessary for safe and secure operation in a nuclear environment.

4.5. Hardware Description Language (HDL) Design

The SE communicates utilizing the I²C protocol, specifically an implementation called T=2 over I²C. I²C is a protocol that utilizes only two wires, the Serial Data Line (SDA) and the Serial Clock Line (SCL). The SDA is utilized for data transfer and the SCL is utilized to provide a clock signal that simplifies that synchronization of all devices on the I²C bus. Each slave device on the bus has a unique address that is written before each data transfer, to identify the target that the master device is communicating with. Data is transmitted in frames, with the recipient responding with an acknowledgment (ACK) or negative acknowledgement (NACK). I²C provides a low cost, low effort, simple protocol with built-in error communication and widespread support in embedded systems. T=2 over I²C is defined in the GlobalPlatform Technology specification Application Protocol Data Unit (APDU) Transport over SPI/I²C, which complies with the ISO/IEC 7816 standard for use with smart cards; the protocol adds in the structure of APDUs, establishing a structured communication between the host and an SE [23]. Each APDU has predefined fields that the manufacturer has configured to perform commands or hold data. Many sensors and other embedded devices already communicate over I²C, meaning integration of another I²C device into a plant design is trivial.

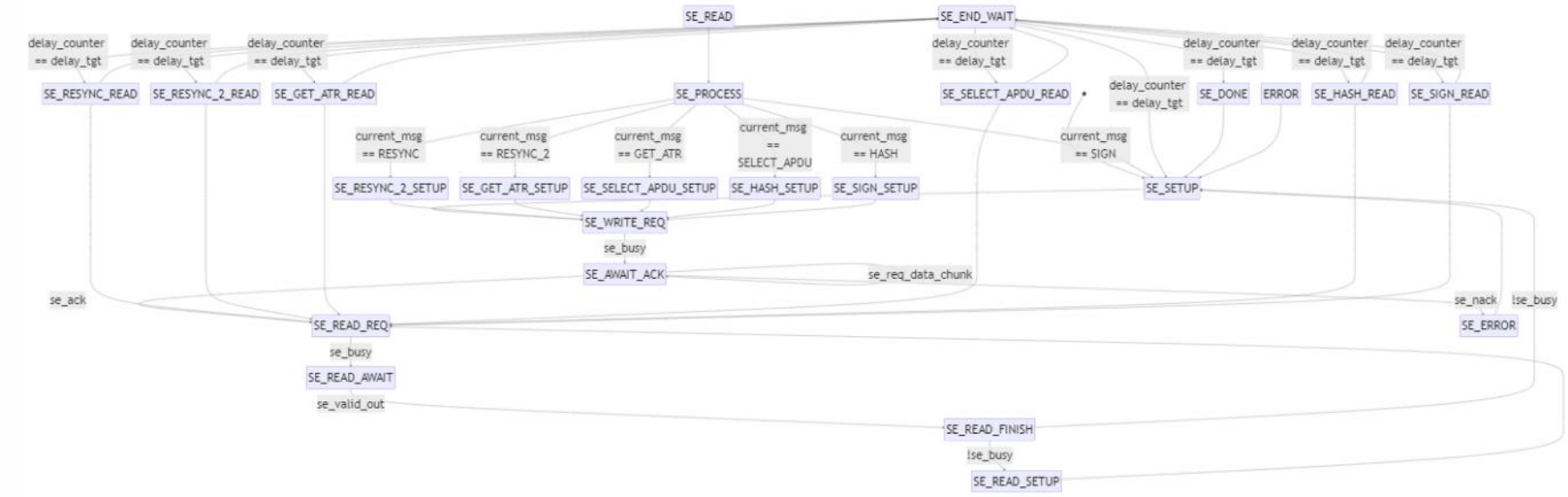

Figure 7 HDL State Machine

The state machine shown in Figure 7**Error! Reference source not found.** for the Verilog code was designed to ensure reliable communication and deterministic behavior. Each state relates to a step in the I²C communication. When the initial configuration of the I²C bus and communication lines is complete, the setup state for the first APDU command starts. This configures the parameters and any values needed to perform the communication. Following setup, the state transitions to writing each byte of the APDU in a sequential matter, awaiting the ACK at each step.

When the FPGA is waiting on an ACK from the SE, the state machine ensures deterministic behavior by checking the response from the SE. If an ACK is received the state machine sends the next byte if there is more data to send. If all bytes have been sent, it transitions to the state responsible for reading the response from the SE and sending ACKs.

If a NACK is received, the state machine transitions to the SE_ERROR state that can communicate to the operator that an ERROR has occurred. Each state has a clear transition based on the specific conditions. These clear transitions ensure there is a deterministic flow from the initial configuration of the device and communication lines, through the sending of each message, the reception of the response, and then transitioning to the next message.

The timing for reading the results from the SE was an area of focus in the development of the HDL code, due to the need for deterministic behavior in AR applications. While most I²C systems utilize a polling mechanism to continue requesting the information until it becomes available, a time needed to be selected that would have the result every time it was requested. A combination of testing with the Raspberry Pi and the FPGA/SE environment were used to observe the behavior and timing of hashing and signature requests.

4.6. Performance

The timing, performance, and reliability of nuclear power plants define the feasibility of implementing smart card cryptography. For example, if it is required for a RPS to receive and respond to flux reading or measure fuel temperature at a specific rate, the cryptographic operations must fit into that timing. If the cryptographic operations introduce a delay outside of the defined requirements, further engineering is needed to determine more efficient solutions or compensating controls. IEEE 7-4.3.2 states "Implementation of cyber security features… shall not adversely impact the performance, effectiveness, reliability or operation of safety functions" [9].

Table 2 details the observed timing figures for the I²C communication. These were measured from the time that the command to either hash or generate a signature was written to when the response is done being read back from the SE. To ensure a deterministic time to read the response, the timing needs to be comfortably above the maximum values that each process takes guaranteeing that the data will be available when a read request is sent. Each plant needs to determine appropriate delays

If a polling system were used, there would be an indeterminate amount of time spent waiting. While it might receive a response from the SE faster in some circumstances, it could also lead to significant delays in the event of an error or failure. By adhering to a deterministically set waiting time, an operator can be alerted if a device fails to respond within the expected timeframe, allowing the system to move on to the next transaction efficiently.

Table 2. Hashing and Signing

	T=2 Over I²C – EdgeLock SE050 SHA1 – Hashing	T=2 Over I²C – EdgeLock SE050 SHA256 – Hashing	T=2 Over I²C – EdgeLock SE050 SHA1/ECC – Signature	T=2 Over I²C – EdgeLock SE050 SHA256/ECC – Signature
Minimum (ms)	23.3	30.0	56.6	31.2
Maximum (ms)	34.4	47.6	82.0	46.9
Mean (ms)	27.8	35.8	62.8	40.0
Standard Deviation (ms)	0.5	0.9	0.8	0.9

Prior to the work with I²C, an investigation into smart card cryptography was performed with an NXP J2A040. There are a few differences in the previous evaluation and the new results produced by this research effort. The J2A040 signing was performed using RSA instead of ECC, the communication was done over I²C instead of USB, and the T=2 over I²C protocol used in the SE050 testing allows for extended APDUs, reducing the number of reads and writes necessary for communication.

As can be shown in Table 3, the most recent configuration results in much faster cryptographic operations, over 30 times faster on average from RSA-2048 to SHA256/ECC, with much more consistent timings. This highlights the need to have a tested and verified configuration for SE integrations, to ensure that performance requirements can be met. Smart cards can achieve many flexible goals when implemented in an efficient manner.

Table 3. Timing Results Combined

	T=2 Over I²C – EdgeLock SE050 SHA1/ECC – Hashing and Signing	T=2 Over I²C – EdgeLock SE050 SHA256/ECC – Hashing and Signing	JCOP 3 Over USB – NXP J2A040 RSA-2048
Minimum (ms)	79.9	61.2	2412
Maximum (ms)	116.4	94.5	2673
Mean (ms)	90.6	75.8	2417
Standard Deviation (ms)	0.943	1.273	25.75

4.7. Relationship to the DCSA

"Design of Defensive Cybersecurity Architectures for High Temperature, Gas-Cooled Reactors" [24] evaluates the I&C architecture and probabilistic risk assessment (PRA) of an HTGR to derive DCSA passive requirements. The DCSA template is consistent with both the RG 5.71 approach and the DG-5075 approach and is depicted in Figure 8. The DCSA template is composed of security

levels 0-4, where each security level represents an increase in both security requirements and importance of the included systems to the plants safety and functionality. As this report is concerned with SE integration for FPGA-based RPS, security level 4 is pertinent.

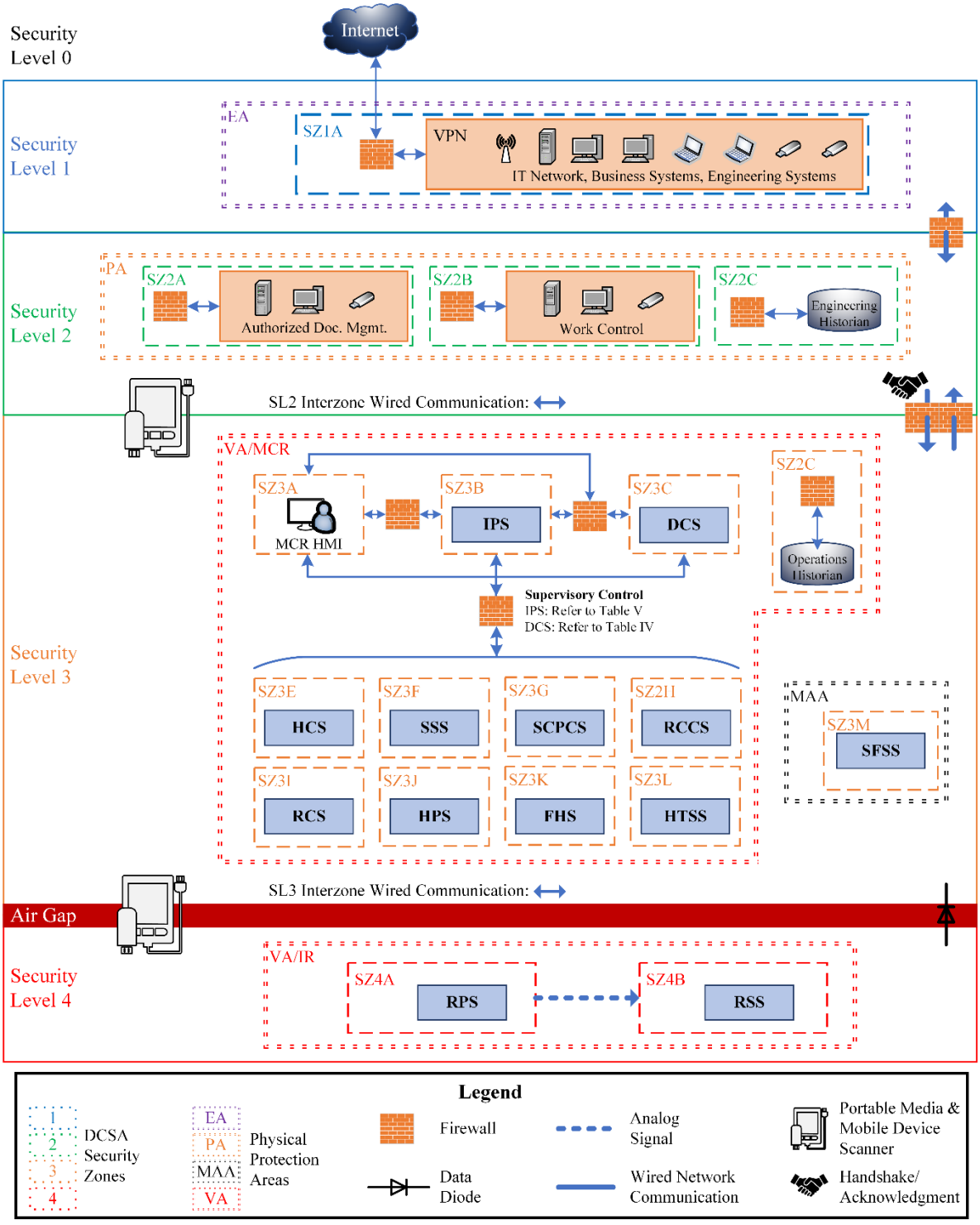

Figure 8 HTGR DCSA Template [24]

In security level 4, which contains the plant's Safety-Related (SR) systems such as the RPS and Reserve Shutdown System (RSS), the SEs are integrated into the inputs and outputs of the FPGA-based RPS. These SEs perform digital signatures on the information, ensuring that any data leaving security level 4 is authenticated and its origin is verified. This is particularly important as one-way communication from security level 4 to levels 3 and 2 is enforced by a data diode, ensuring that data flows out but not back in. By digitally signing the data at the source, the SEs provide a robust mechanism to maintain the integrity and authenticity of the data as it moves through the different security levels. Other common information protection techniques often require bidirectional communication to establish symmetric keys, complete a challenge and response, or simply are required for acknowledgement by either party.

Communications from security level 4 to security level 2 are permitted and can be stored in the engineering historian. From security level 2, data can then be communicated to the rest of the IT infrastructure, including security level 1, which has access to the Internet. The digital signatures applied by the SEs in security level 4 ensure that the authenticity and integrity of the data are maintained as it traverses these levels. This is crucial for remote monitoring and archival purposes, as it provides a verifiable chain of custody for the data, ensuring that it has not been tampered with or altered.

The SEs provide an additional layer of security for critical devices within security level 4. Given that security level 4 has the highest physical and computational security requirements, it is sensible to leverage SEs to protect the authenticity of the data originating from this level as it travels through and is stored in levels with less stringent requirements. The digital signatures not only confirm the data's origin but also authenticate the specific device within security level 4, adding an extra layer of assurance. This is particularly important as the higher security zones do not have the same stringent physical or computational security requirements as security level 4. By using SEs, the integrity and authenticity of critical data are protected, even as it moves to less secure zones.

5. CONCLUSION

The integration of advanced technologies such as FPGAs and SEs into RPSs represents a significant step forward in enhancing the safety, security, and operational efficiency of advanced nuclear reactors. FPGA-based safety systems offer numerous advantages over traditional microprocessor-based systems, including higher performance, greater parallelism, and reduced cybersecurity vulnerabilities due to their streamlined and specific implementations. These systems are increasingly being considered for ARs, as evidenced by various FPGA-based safety systems that have been reviewed and approved by the NRC.

SEs, or smart cards, provide an additional layer of security by offering tamper-resistant hardware for securely storing and processing sensitive data. Their ability to perform cryptographic operations, ensure data integrity, and manage secure authentication and access control makes them a valuable component in enhancing the cybersecurity of RPSs. By integrating SEs into FPGA-based safety systems, it is possible to achieve robust security for critical operations, such as remote monitoring and control, which are becoming increasingly important in the context of ARs.

This report has explored the potential for integrating SEs into FPGA-based RPS, addressing both the technical and regulatory considerations. The proof of concept presented demonstrates the feasibility and benefits of this integration, highlighting the importance of secure communication and monitoring in ARs. The findings suggest that SEs can significantly enhance the cybersecurity posture of FPGA-based safety systems without compromising their performance or reliability.

However, the successful deployment of these technologies requires careful consideration of licensing and regulatory requirements. Leveraging existing security certifications, such as CC evaluations, can help streamline the regulatory approval process and reduce associated costs. Additionally, adopting a performance-based approach to cybersecurity, as advocated by the NRC and other international regulators, can provide a flexible and effective framework for ensuring the security of digital I&C systems in nuclear power plants.

In conclusion, the integration of FPGAs and SEs into RPSs holds great promise for advancing the safety and security of nuclear reactors. By addressing the technical, regulatory, and practical aspects of this integration, this report provides a comprehensive framework for industry stakeholders, regulatory bodies, and researchers dedicated to enhancing nuclear safety and security. The continued development and implementation of these technologies will be crucial in meeting the evolving challenges and demands of the nuclear industry.

6. REFERENCES

[1] L. Maccarone, M. Rowland, R. Brulles and A. Hahn, "Design of Defensive Cybersecurity Architectures for High Temperature, Gas-Cooled Reactors," 2024.

[2] B. Seri, G. Vishnepolsky and D. Zusman, "URGENT/11 Critical vulnerabilities to remotely comromise VxWorks, the most popular RTOS," Armis, Inc., 2019.

[3] "Advanced Logic System Topical Report," Westinghouse Electric Company, 2013.

[4] "Amendment for HFC-FPGA System of HFC-6000 Safety Platform," Doosan HF Controls Corporation, 2021.

[5] "NuScale Topical Report TR-1015-18653-NP-A," NuScale Power, 2017.

[6] "RadICS Topical Report," Radics LLC, 2020.

[7] A. Duncan, F. Rahman, A. Lukefahr, F. Farahmandi and M. Tehranipoor, "FPGA Bitstream Security: A Day in the Life," Insitute of Electrical and Electronics Engineers, 2019.

[8] K. Parnell and R. Bryner, "Comparing and Contrasting FPGA and Microprocessor System Design and Development," Xilinix, 2004.

[9] "Guidance for Evaluating Minimum Inventory of Alarms, Controls, and Display for New Light Water Reactor Plant Designs," U.S. Nuclear Regulatory Commission, 2009.

[10] "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," IEEE Power and Energy Society, 2016.

[11] "Guidance on Using IEC 61508 SIL Certification to Suppor the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications Revision 1," Nuclear Energy Institute, 2021.

[12] "Dedication of Commercial-Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants," U.S. Nuclear Regulatory Comission, 2022.

[13] "Draft Regulatory Guide DG-1402 Dedication of Commercial-Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants," U.S. Nuclear Regulatory Comission, 2022.

[14] "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," U.S. Nuclear Regulatory Comission, 2011.

[15] "Cyber Security Plan for Nuclear Power Reactors," Nuclear Energy Institute, 2010.

[16] "Cyber Security Programs for Nuclear Power Reactors," U.S. Nuclear Regulatory Comission, 2023.

[17] "Computer Security Techniques for Nuclear Facilities," International Atomic Energy Agency, 2021.

[18] "Computer Security Aspects of Design for Instrumentation and Control Systems at Nuclear Power Plants," International Atomic Energy Agency, 2020.

[19] I. Garcia, J. Jaunitrans and M. Rowland, "U.S.A Regulatory Efforts for Cyber Security of Advanced Reactors," International Atomic Energy Agency.

[20] "Draft Regulatory Guide GD-5075," U.S. Nuclear Regulatory Commision.

[21] E. Barker, "NIST Special Publication 800-57 Part 1 Revision 5," National Institute of Standards and Technology, 2020.

[22] ETSI, "3GPP TS 33.401 version 8.2.1 Release 8".

[23] P. Dzurenda, S. Ricci, J. Hajny and L. Malina, "Performance Analysis and Comparison of Different Elliptic Curves on Smart Cards," Institute of Electrical and Electronics Engineers, 2017.

[24] "APDU Transport over SPI/I2C," GlobalPlatform Technology, 2020.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Benjamin Karch	8851	brkarch@sandia.gov
Lon Dawson	8851	ladawso@sandia.gov
Ben Cipiti	8845	bbcipit@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Katya Le Blanc	Katya.leblanc@inl.gov	Idaho National Lab

This page left blank

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.