APPROACHES FOR COMPREHENSIVE SAFETY AND DIGITAL RISK MANAGEMENT FOR ADVANCED NUCLEAR TECHNOLOGY AND SMALL MODULAR REACTORS

R. ANDERSON
robert.anderson@inl.gov

J. MAHANES
joseph.mahanes@inl.gov

S. EGGERS
shannon.eggers@inl.gov
Idaho National Laboratory
Idaho Falls, Idaho

M. HEWES
International Atomic Energy Agency
m.hewes@iaea.org

M. St. JOHN-GREEN
mike@stjohn-green.co.uk

Abstract

Small Modular Reactor (SMR) designs are likely to rely on complex digital technology novel to nuclear industry applications while also leveraging passive systems and safety design simplification. The result of current approaches may lead to a safety-driven system design that lacks demonstrated robustness in the event of cyber-attacks against its digital equipment. Information and computer security should be an integral part of engineering and operational processes. Current safety and security thinking does not encourage sufficient interaction. Teams are often separate and management structures reinforce this separation. This paper provides a case for cybersecurity related safety and digital engineering security requirements to be considered together throughout design, licensing, and operation. Safety envelope boundaries may be expressed using many variables and suitably defined system theoretic models can be used to alert whether due to faults, failures, or malicious action. This provides a unifying “top down” framework for digital systems and approaches supporting and implementing safety and security requirements. This paper will identify existing work supporting this closer relationship. However, new tools, techniques, and ways of working need developing to enable SMR designers, regulators and operators to employ complex digital technology in a way that remains both safe and secure.

1. INTRODUCTION

Traditional approaches to safety, security, and information security within the nuclear industry operate in silos, with distinct teams and management structures that do not sufficiently encourage a holistic approach to risk management. This segregation leads to a fragmented understanding of threats, vulnerabilities, and responsibilities potentially overlooking the interdependencies between safety and security objectives. Risk is the common language through which these and other different engineering disciplines and stakeholders evaluate design decisions, as well as how potentially conflicting priorities are arbitrated. Digital risk encompasses both adversarial threats such as a cyber attacker and non-adversarial threats such as human performance errors and equipment failure or misconfiguration. A comprehensive consideration of the possible risks posed by maloperation of digital equipment bridges the typically threat-focused risk mitigation in security engineering, and the phenomena driven risk mitigation of safety engineering. Digital innovations introduce nuanced challenges in risk management, particularly regarding the use of new and emerging digital systems and technologies that will play integral roles

in operations, safety, and security, while potentially revealing gaps in current approaches that may lead to a system design that lacks demonstrated robustness to cyber-attacks.

A barrier to the successful deployment of SMRs is risk communication and regulatory acceptance. Many SMRs leverage mature and existing nuclear reactor design aspects to reduce the overall potential negative consequence of safety and security scenarios. These practices more effectively treat risk early in the engineering process where certain choices can eliminate or significantly reduce potential failures or attack pathways and can reduce the high operational costs associated with "bolt-on" security practices. Significant improvements in ensuring the critical functions of preserving radiological barriers, safe shutdown and continued safe shutdown,, and heat removal through advanced fuels, such as used in gas-cooled SMRs, and inherent safety features in light water cooled reactors (LWRs) with extensive natural circulation cooling capabilities. As SMR technology progress into licensing and operation, the question remains whether these designs have sufficiently demonstrated to licensing entities the due diligence, enabling a smaller safety systems footprint, physical protection guard force scaled from traditional large multi-reactor sites, and advancing the safe and secure adoption of digital technologies in ways previously not considered in the nuclear industry.

Traditional safety analysis draws a bounding envelope of operation through a series of analyses enumerating normal operation modes and expected challenges, which is then accepted by a regulatory body. These analyses utilize physics-based codes to model and understand the potential energy sources which must be contained, such as kinetic energy from high mass objects, chemical potential energy, criticality of nuclear material, radiation from radiological material, highly pressurized systems, high temperature systems and other energy sources. The challenge of the safety and security intersection can be expressed similarly as the potential for digital systems to interact adversely with these same high potential energy systems. One concern with the design and construction of new SMRs/MRs is that design teams will not address digital risk management or cybersecurity early enough in the systems engineering lifecycle. Another concern is that large, multi-teamed design projects will not bring in cybersecurity and digital risk as a separate discipline which can lead to conflicts with requirements, potentially leading to functional, safety, reliability, or security issues. Model Based Systems Engineering (MBSE) helps to bridge that gap, by bringing all disciplines together and addressing digital risk management starting early in the systems engineering lifecycle.

2. BREAKING DOWN THE SAFETY SILO

Good safety design has independently arrived at many of the same conclusions for best practice as cybersecurity, such as favouring reliance on passive systems, design simplification, layered defences and more. The result is a safety-driven system design that while often offering limited incidental robustness in event of cyber-attacks, lacks any approach to protecting the digital systems responsible for managing high energy and high potential impact consequences resulting from intentional maloperation. The ultimate reliability objective of a system for cybersecurity is the preservation of the correct performance of a vital function, even in the face of malicious compromise of one or more digital systems contributing to the performance of that function. For example, preserving a cooling loop's ability to remove heat from a system may be reliably maintained through combinations of non-digital alternative operation means, fail-safe process design, and capability to redeploy a known good configuration in an isolated mode. In this example, even if an adversary were to gain control of the system, no combination of actions can push the process outside of its safety envelope. This result requires not just a good understanding of the process and governing physics, but also the entire range of capability of the responsible control systems, and the capability of maloperation.

One such example of integrating security and engineering is Cyber-Informed Engineering (CIE), a US Department of Energy national strategy that encourages "secure-by-design" concepts to include the engineering of cyber-physical systems. This approach creates opportunities for engineering teams to secure digital systems using physics and mechanics of engineering controls [1]. This methodology to integrate security has been applied to projects across critical infrastructure sectors. Benefits have primarily been building communication pathways between different engineering teams, and incorporating cybersecurity as not only a major contributor within the entire systems engineering team, but also the awareness that cybersecurity is necessary as a major engineering

discipline during conceptual, requirements, and detailed design phases that allow for an “engineered” approach to cyber risk reduction. More importantly, projects have eliminated potential attack pathways and reduce consequence of compromise. Successful integration of cybersecurity requirements and design considerations have been applied to advanced reactor projects and ongoing research and development in support of nuclear SMRs. One example is the implementation of data encryption in OT systems. Often, encryption can be a challenge as a perceived complication in the availability of digital assets. By integrating cybersecurity into the requirements and design phase, one potential option for cryptography clearly best satisfied both functional and cybersecurity requirements. This potentially mitigated costly revisions or less effective options that would require additional controls. This example demonstrated to the safety engineers that securing digital equipment was much more efficient if security was core to the design. Other benefits of this approach include encouraging “outside the box” thinking about how an adversary could use potential digital assets in a manner not thought of for malicious goals. A standalone wireless gas supply system located outside the facility was identified as a potential jump point into the plant with or without insider help. Typically, safety does not think adversarial, however, the inclusion of security during the design process helped reduce the need for last minute bolt-on controls especially when bolt-on controls may not be possible.

The entire goal of CIE and “security-by-design” is to include all engineering disciplines, including historically siloed disciplines such as safety, to identify and design the most robust, functionally secure systems that can anticipate, as much as possible, adversarial threat tactics, techniques, and procedures (TTP). Ideally, incorporating security-by-design into the engineering process will extend the longevity of a design to, at a maximum, prevent the continuously adaptive adversary TTP’s ability to overtake a system and, at a minimum, alert operators before a security event or incident compromises nuclear security.

Additionally, recent TTPs have increasingly expanded to leverage “Living-off-the-land” (LOTL) practices, which utilize the same legitimate tools and capabilities of compromised systems to achieve adverse outcomes. While many classes of cyber-attack are utilizing specially crafted malware, LOTL techniques are highly targeted, well-informed attacks that can be difficult to detect. In this way, latent capability and intended functionality of a system can be used as a weapon that is particularly difficult to defend against. Systems engineered utilizing CIE principles or other cybersecurity design tools are best prepared to reduce both the attack surface and the potential consequence of compromise.

3. BREAKING DOWN THE SECURITY SILO

Historically, nuclear security has been applied after the safety analysis has identified systems depended on to ensure protection from theft, radiological release, and other high consequence events. Cybersecurity is applied in a graded approach dependent on the criticality of a digital system or asset, that is, its role and potential for negative consequence if compromised. Security measures are then applied to protect the identified asset. This approach can be illustrated by imagining a series of safety barriers, such as may be identified on a bow tie diagram. Consider that those safety barriers rely on the trusted operation of digital technology, e.g. to detect over-temperature or over-pressure and actuate a valve in response. It would appear to be reasonable to task the computer security team to protect that digital technology in such a way that it can be trusted to operate. However, in practice, this kind of protection cannot be easily applied to the control system without considering its engineering design. The computer security team would be limited to applying a selection of computer security measures to protect individual computer based systems, in a node-by-node approach, from rudimentary attacks. Instead, the control system needs to be designed to make attacks more intrinsically difficult, supporting the preservation of the function it’s performing and the role it contributes to in defence in depth, while maintaining its legitimate capabilities. This security-by-design approach involves a close collaboration between those designing the control system and those who understand adversarial capabilities.

Further, this node-by-node approach is insufficient because there may be multi-node attacks in which the adversary misuses the legitimate capabilities of the control system, simultaneously across multiple nodes, to create modes of operation that were never considered; for example, dynamic physical phenomena resulting from the

control system opening and closing valves as fast as possible in an orchestrated way. Multiple nodes may be induced to fail simultaneously in other ways. Digital technology is often built from commodity components, such as commonly used integrated circuits, and commodity software, such as commonly used low-level library functions. These can lead to common modes of failure but may also contain common but undiscovered security vulnerabilities. Once these are discovered by an adversary, they can create a loss of diversity or defence-in-depth, such as in independent reactor protection systems that have an unrecognised common security vulnerability.

Organisations can foster a more integrated and resilient approach to risk management by framing security measures as mechanisms to preserve these functions against malicious action. This is a profoundly different approach for many conventional cyber security teams, who are taught to defend the digital assets against recognized forms of adversary action, hunting threats, looking for indicators of compromise, etc. Arguably, in the mode prevalent understanding of cyber security, the team does not adapt their focus to be on the specific purpose, (e.g., the function of the digital technology), but rather unknowingly adopts the more widespread industry focus of securing the confidentiality, integrity, and availability of information. In a more integrated approach, the cyber security teams must help design the control systems to maintain the design function and keep the system within its design basis, given what they know about adversarial means and motives. Whereas safety analysis is concerned with the physics of interaction energy, the challenge for security-by-design engineering lies in focusing on the much wider question of “what is credible malicious intent and capability, given what I know about the design basis of the system?”

3.1. Demystifying Cybersecurity for Engineering and Operation

Early operational technology (OT) security had significant challenge of raising cybersecurity awareness and dispelling myths such as the “air gap” isolation and “security through obscurity”. As cyber-attacks become more prevalent, rising in both frequency and severity, digital security has emerged as a high priority in both design and operation. The rapidly evolving pace of both system software functionality and threat capability often places cybersecurity risk mitigation in a reactionary state, or a position where it can be difficult to allocate resources towards the risk reduction of legacy systems while addressing emerging threat and newly discovered vulnerability.

In the design of new advanced and SMR reactors, security-by-design is a driving paradigm in the process of adoption into industry best practice and regulatory requirements. Again, throughout the design process, good general cyber awareness has reinforced many good engineering practices such as limiting reliance on active systems. However, good engineering practice without cybersecurity expertise can and has led to reliance on ill-informed assumptions or poor implementation of security measures. Use of weak or improper encryption, high-impact vulnerabilities in a device’s physical security such as maintenance ports, vulnerability in the storage and protection of critical firmware, or misconfiguration in isolation implementation all represent just a few subtle digital risks that may evade due diligence while credited towards defence-in-depth by safety engineering analysis and design. Strong communication links between both safety and engineering can ensure the highest potential consequence events and critical facility functions are identified, and the selected security controls and design requirements are best tailored to mitigate those risks. Early successful efforts in this space have leveraged cybersecurity subject matter expertise within system design reviews, establishing functional requirements, and preliminary vulnerability assessment. Towards the long-term solution, greater incorporation of digital control system with engineering curricula lay a foundational skillset for engineering modern digital systems. Ongoing research and development includes enhancing the capability of commonly used engineering analysis to include modelling maloperation effects, such as improper actuation of physical equipment, including pumps, valves, or motors.

3.2. Digital Twins and Machine Learning Applications

It has been stated that some SMR designs and operating methodologies will only be financially viable if they can use more advanced digital technology than has been used in previous reactor control systems. These include greater use of sensors, in both number and granularity of the information collected, to allow the inference

of physical parameters that cannot be measured directly. Machine learning algorithms may be used to accomplish these tasks. More advanced algorithms that use digital twins with machine learning may offer improved efficiencies in reactor operation, more accurate predictive maintenance, lower demands on human operators, etc. However, design teams must consider the new opportunities for the adversary to cause loss of visibility or loss of control of physical phenomena by maliciously manipulating these algorithms. This example illustrates how far effective cyber security needs to move from simply defending the digital technology assets that support safety barriers.

While digital twins provide a valuable simulation environment, it is worth noting that without robust model training using facility-specific datasets, these may fail at capturing emergent transient behaviour. Typical training sets rely on recorded data from the real operation of nuclear power plants from sensors distributed throughout the process, or by simplified physics models coupled with powerful numerical solvers. In the case of the observed data, sufficiently off-normal conditions may push the model outside of the training data set, or even slight variations in input data might greatly reduce the likelihood the model will provide the desired capability close to the bounds established in its original training conditions. In the case of the interactive physics model, inevitably some critical boundary conditions and assumptions will be incorporated which may cause the failure to predict certain rare phenomena.

3.3. Model Based System Engineering

Many vendors use model-based systems engineering (MBSE) tools to manage the design and construction of advanced reactors. MBSE utilizes models as a central tool for designing and implementing complex systems throughout the systems engineering lifecycle, from conceptual design to decommissioning or disposal. Formal MBSE tools merge a model, systems thinking, and systems engineering to graphically represent the boundaries, context, and behaviour of interconnected systems to enable successful design, development, and use of engineered systems throughout the lifecycle.

The model represents the entire system or system of systems to provide a visual representation of requirements, structure, behaviour, and more. It can be used to integrate simulation and analysis techniques (e.g., multi-physics, computational fluid dynamics, finite element analysis, digital twins), computer-aided design (CAD), piping and instrumentation drawings (P&ID), trade-off analyses, performance testing, verification and validation, configuration management/version control, requirements management, and other project management capabilities. MBSE provides a common language for communication between all stakeholders in the development process; all disciplines involved in the project can view the complex relationships in a system to better make informed decisions. The ability to provide a holistic view of individual components as well as their interactions and dependencies enables better communication of complex ideas across diverse teams and disciplines. These tools, however, often are focused on functionality, performance, and safety and do not incorporate additional concerns introduced by use of OT.

Most, if not all, MBSE tools have the capability to add digital risk and cybersecurity requirements as additional requirements into the tool. However, it was shown through a survey of advanced reactor vendors performed by the authors that they do not currently do so or know how to do so. With the existing U.S. nuclear fleet, cybersecurity controls were ‘bolt-on’ NRC requirements after 9-11. However, we have seen with CIE and security-by-design approaches that eliminating digital risk concerns (both adversarial and non-adversarial) or designing in digital risk controls/mitigations can lead to a better security posture against adversarial threats and reduce impacts from non-adversarial threats, such as human performance errors, common cause failures, equipment degradation, and environmental issues.

4. CONCLUSIONS

Design Basis Threat, scenario development, threat hunting, and “active” cybersecurity techniques will continue to remain important components of overall security posture. However, as modern SMR design looks to deliver assurance of digitally enabled critical functions, improvement in the interface between safety and security

engineering is vitally important to reduce costly and ineffective duplication of analysis, and most effectively reduce overall risk early. This shift in perspective necessitates revaluation of current practices to provide for the development of new tools, techniques, and ways of working that encourage collaboration across traditionally separate domains to enable SMR designers, regulators, and operators to fully leverage the potential of complex digital technologies while ensuing both safety and security. The integration of digital risk management and cybersecurity-by-design capabilities into these tools will provide an improved process for ensuring reactors are built with safety and security in mind. The adoption of a security inclusive approach to nuclear digital engineering projects will support the integrated requirements, design, analysis, verification, and validation necessary to integrate safety, security, and resilience from unintentional digital incidents into the overall functional design.

5. REFERENCES

REFERENCES

[1] CIE Implementation Guide, August 2023, INL/RPT-23-74072, US Department of Energy, Office of Cybersecurity, Energy, Security, and Emergency Response.