Reducing the Cyber Threat to Digital Systems: Minimizing Complexity[1]

Introduction

Cyber threats are increasingly one of the major threat facing governments and industrial facility operators. One of the foundational issues that makes protection from such attacks increasingly difficult is the complexity of today's networks and systems.

Driven by the auto industry in the early 1970s, digital automation of complex industrial environments started with comparatively simple digital devices capable of replacing hard-wired relay systems utilized on assembly lines. As much of the automotive process required annual changes, Programmable Logic Controllers (PLCs) were used to modify configurations. Compelled by a desire for flexibility, initially simple systems became increasingly complex.

The subsequent rush to digitally automate everything from component creation to facility security created a culture of solution providers and systems integrators who, driven by an enthusiastic pursuit of efficiency gains and possessing a solid belief in latent capability as a hedge against future requirements, spread their message rapidly across multiple sectors including the nuclear sector.

Significant benefits were realized through this digital expansion including reduced hardware, labor, wiring, and cabinet space, as well as quick process changes and embedded system diagnostics. While digitization and increasing levels of complexity have brought many benefits, they also increasingly represent key challenges in ensuring that critical systems are resilient under cyberattack.

The Rise of Complexity in Nuclear Systems

The first nuclear reactors were fairly simple analog systems involving a fuel, moderator, control rods, coolant, heat exchanger, containment and a mechanism to monitor the fission reaction. Driven by safety considerations, a conservative automation approach was adopted, and although digital systems quickly caught on for other industrial sectors, integrated safety systems found in Generation II nuclear reactors were primarily analog.

The comparatively advanced state of Generation III/III+[2] reactors created an increasing demand for additional fidelity around internal processes. This resulted in additional instrumentation, sensors, controls and communications, eventually including plant operations, engineering, physical security, front office forecasting, regulatory reporting, remote vendor access and even Internet gateways.[3]

[1] This paper was prepared by NTI staff with the assistance of Michael Assante, Robert Anderson and Rob Hoffman

[2] Generation III and III+ reactors are roughly defined as those designed/built since the mid-1990's and include a number of evolutionary changes compared to Generation II reactors.

[3] See, for example: http://www.neimagazine.com/features/featurescada-as-you-ve-never-seen-it-before.

Today's nuclear plants exchange information across a complex web of embedded digital devices that is all too often not fully understood by any one individual or operational entity.[4] Tens of thousands of nodes communicate across multiple media layers using a variety of protocols, operating systems and shared applications. Despite the potential liability of these critical digital resources, however, regulators and operators alike have stayed the course utilizing increasingly outdated physical security models for threat, response and deterrence.

Cyberattacks - Quiet Signals in the Noise of Complexity

As described in the 2015 article, "The Industrial Control System Cyber Kill Chain"[5], a cyber-aggressor must pass through eight primary steps (Discovery, Movement, Install/Execute, Launch, Capture, Collect, Exfiltrate, Clean/Defend) to successfully execute an attack in the ICS environment. At each of these steps the aggressor risks detection from a carefully architected defensive posture.

Generic systems designs without cybersecurity considerations as a primary requirement can include complex layers of configuration and enhanced features that are often difficult to understand. This may include internal process and communications capabilities that expand the exposure to cyberattack and raise the risk of compromise. Furthermore, the more complex the target environment, the greater the level of acceptable background "noise" against which the aggressor can operate undetected.

In addition, vendors, integrators, engineers, programmers, and subcontractors all tend to have well defined areas of expertise beyond which they may not be knowledgeable. Additional complexity thus requires the diversification of personnel responsibilities and oversight resulting in additional staff, organizational stovepipes and gaps that can be exploited.

In extreme cases, there is a resultant "expertise inequity"; the defender must be a cyber generalist, expected to deal with complexity across multiple technologies and processes whereas the attacker can act with surgical focus on a specific segment or component such as a strategic controller.

Finally, high levels of complexity make system testing and certification difficult. In many real-world systems, it is impossible to test all possible failure modes. Over time, systems can be made resilient to naturally occurring computer issues, but this is not possible for cyberattacks as they may have never been seen before.

[4] Other types of nuclear facilities are not dissimilar, and are also increasingly digitized.

[5] https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

Reducing Complexity and the Emergence of Security by Design

For the reasons described above, complexity is the enemy of security.[6] Moving to simpler systems thus makes the job of security professionals easier, enhancing security. The benefits of less complex systems have been recognized for some time, but have yet to become a major priority. In fact, the opposite is happening—systems are becoming more complex.

There have been some initial steps that take into account the benefits of reducing complexity. The United States Nuclear Regulatory Commission (NRC) recognized the challenges in modern nuclear operational technology (OT) environments and partnered with industry to publish NRC Regulatory Guide 5.71, Cyber Security Programs from Nuclear Facilities. Within this document, a section highlighted the important of defining and identifying critical digital assets (CDA), so as to prioritize cybersecurity efforts to those devices that could impact safety, security and emergency preparedness (SSEP). This allows for the application of security measures commensurate with the potential for compromise.

Nuclear security practitioners are learning that they must enhance security by focusing limited resources on high consequence related assets by severely limiting interaction and functionality, especially in those situations where the possibility of unacceptable consequence renders loss of operational control unacceptable. This process of limiting interaction and functionality is a good example of simplicity in design.

Simplicity in design is one of the element of a new discipline known as cyber informed engineering (CIE) which considers the inclusion of cybersecurity in the engineering process. CIE[7] is a body of knowledge and a methodology to characterize the risks presented by the introduction of digital computer systems in a traditionally analog environment. CIE establishes a framework of elements that are available to engineering staff as part of the mitigation strategy. Examples include: consequence/impact analysis, engineering controls, resilience planning, the control of interdependencies, and others.

One of the more promising elements of CIE is focused on removing complexity through design simplification. This concept stresses simple digital system architecture design to minimize malicious cyber access and propagation of cyber-attack limiting complexity, communications and digital integration. This approach considers architecture from the ground up, with operational requirements generating the engineering specifications for technology that delivers only required functionality with known results to all potential stimuli. Digital systems would coexist on a limited basis and only as needed to ensure critical process stability. Inherent in all designs would be the requirement to passively fail safe without the potential for cyber manipulation.

[6] Bruce Schneier was among the first to promote simplicity in the context of security. See: https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html.

[7] *Cyber-Informed Engineering: the Need for a New Risk Informed and Design Methodology*, June 2015 | https://inldigitallibrary.inl.gov/sti/6618307.pdf]

Finally, it should be recognized that technological complexity (e.g., networks and systems) is not the only concern. *Organizational* complexity can also create dangerous vulnerabilities.[8] This can take the form of organizational stove-pipes between IT and OT providers, as well as between control system engineers, nuclear safety experts and others. While cybersecurity priorities are not the only factor when developing organizational structures, going forward they must be one of the key drivers.

Conclusion

This paper has highlighted how addressing the cyber threat to high-consequence digital systems is exacerbated by the complexity of the system environment in its entirety. Motivated by features, cost, reliability and other factors, systems have been created that are more inherently complex than can be securely managed. While problematic in general, this has the potential to be catastrophic for high-consequence systems such as nuclear reactors.

This paper proposes that as part of a new strategy to protect nuclear assets from catastrophic cyberattacks, a collective of guiding priorities be established, one of which would be to reduce complexity and thereby the potential for undesired behavior in a manner commensurate with the potential consequences.

This paper has explored the impacts of complexity as it relates to cybersecurity for high consequence operational environments; it identifies and provides a basis for discussion on achieving a state of manageable risk. Others[9] have put forward related ideas, proposing that for truly critical systems (e.g., military aircraft) that there ought to be redundant systems utilizing deterministic or even analog technology.

Finally, the concept of reducing complexity to minimize the cyber threat raises a number of questions. Specifically:

- How far should reduction in design and implementation complexity be taken? For any specific proposal, what would be the implications (e.g., cost, training, component availability, performance)?

- How would the effectiveness of complexity reduction strategy be measured as it relates to cyber threat?

- What are the criteria by which processes and systems are deemed truly critical and where the potential for unpredictable system behavior due to complex interdependencies must be avoided at all costs, perhaps even calling for a return to "human in the loop" or to the placement of fully deterministic systems?

[8] See, for example: *The Need for a New IT Architecture*, available at: https://www.citrix.com/it-security/resources/ponemon-security-study.html.

[9] Defense Science Board Report "Resiliency of Military Systems", 2013.