INL/CON-15-36958
PREPRINT

The Need for Cyber-informed Engineering Expertise for Nuclear Research Reactors

International Conference on Research Reactors: Safe Management and Effective Utilization

R. Anderson and J. Price

December 2015

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

The Need for Cyber-Informed Engineering Expertise for Nuclear Research Reactors

R. Anderson[1] **J. Price**[1]

[1]Idaho National Laboratory (INL), Idaho Falls, Idaho, United States

Robert.Anderson@inl.gov

Abstract. Personnel working in current engineering disciplines may not understand or fully embrace cybersecurity aspects as they apply to analysis, design, operation, and maintenance of nuclear research reactors. Research reactors include a wide range of diverse co-located facilities and designs necessary to meet specific operational research objectives. Because of the nature of research reactors (reduced thermal energy and fission product inventory), hazards and risks may not have received the same scrutiny as they have at power reactors. Similarly, security may not have been emphasized either. However, the lack of sound cybersecurity defenses may lead to both safety and security impacts. Risk management methodologies may not contain the foundational assumptions required to address the intelligent adversary's capabilities in malevolent cyber attacks. Although most research reactors are old and may not have the same digital footprint as newer facilities, any digital instrument and control function must be considered as a potential attack platform that can lead to sabotage or theft of nuclear material, especially for some research reactors that store highly enriched uranium.

This paper examines the need for cyber-informed engineering practices that encompass the entire engineering life cycle. Cyber-informed engineering, as referenced in this paper, is the inclusion of cybersecurity into the engineering process. This paper addresses several attributes of this process and the long-term goal of developing additional cyber-safety basis analysis and trust principles. With a culture of free information-sharing exchanges, and potentially a lack of security expertise, new risk analysis and design methodologies need to be developed to address this rapidly evolving (cyber) threatscape.

Key Words: Cyber, Engineering, Research, Security

1. Introduction

A fundamental challenge exists with modern engineering practices that do not consider cyber-attack consequences. Academia has failed to keep up with the aggressive and continuously changing cyber threats that pervade nearly all monitoring and control designs. To move forward with secure digital designs, a fundamental engineering transformation must take place that includes the analysis of one of the greatest present-day threats. That is, current security approaches may not include cyber threats to nuclear facilities, digital systems, and critical infrastructures. The majority of research reactors were not designed with security as a priority. Research reactor designs were optimized around education and training, research, or radioisotope production. These objectives often necessitated ease of access to the facility for the frequent reconfiguration of the core or for openness to facilitate ease of instruction and training [1].

Cyber-informed engineering, as referenced in this paper, is the inclusion of cybersecurity aspects into the engineering process. The desired outcome is an introductory dialog for the creation of a new cyber-informed engineering discipline that includes risk and design methodologies. Nuclear and other critical infrastructure industries are expanding the role of digital technology in the monitoring, control, and protection applications associated with the safe and secure operation of facilities. At the same time, the adversarial "cyber" threat continues to expand at an alarming rate and is challenging the existing analysis methods used to quantify the probabilistic risk associated with safe and secure operation. Where probabilistic risk assessment (PRA) or probabilistic safety assessment (PSA) analysis utilizes equipment failures or human error as initiating events for a hazard, cyber attacks use the

historical framework and functionality of a trusted system to perform operations outside the intended design and potentially without the operator's knowledge. This problem expands beyond safety to include any control measures that help prevent, detect, delay, and respond to malicious cyber initiated events. Design basis threat analyses must also incorporate the cyber threat to understand what level of protection and response an asset owner must have in place to defend against cyber threats.

The term "cyber" has taken on many definitions throughout the past few decades. The International Atomic Energy Agency uses the term "computer security" and considers cybersecurity synonymous with computer security [2]. For this paper, the term "cyber" refers to those aspects of understanding required to secure digital devices from unintended or unauthorized access with malicious intent. It encompasses subjects such as (digital) communications, processes, controls, functions, threats, attacks, analyses, risks, and mitigations. It is imperative that engineers understand that cyber (security) aspects must be incorporated into their designs and analyses in order to preserve continued safe and secure nuclear operations.

2. Modern Landscape

The 21st century relies heavily upon and operates many components and systems that embrace the rapid adoption of digital and automation technology (and its inherent state of constant evolution) in critical infrastructure. Beyond critical infrastructure is the Internet of Things [3], which will encompass nearly every aspect of modern life. Cybersecurity will inevitably be a concern for every individual. With digital communications come the added benefit of shared data and the convenience of remote access. Data are now consumed by nearly every organization and are relied upon for efficient operations and key business decisions. Organizational workforce planning often centers on the availability of remote access for monitoring, troubleshooting, upgrading, and even operation of critical infrastructure. In addition, research reactors are somewhat unique, because one of the main goals of their research partners is to share information internationally. This typically involves a high degree of openness; a constant rotation of temporary partners, clients, faculty, and students: and a transparency of and sharing of information. The problem is that digital and automation technology (including all components currently available on the market, as well as those currently installed in industrial control systems around the world) were built for functionality and reliability,[1] not integrity.

The industrial base has largely moved to digital-based systems, and vendors are gradually discontinuing support and stocking of analog spare parts. The reason for the transition to digital instrumentation and control (I&C) systems lies in the important advantages and capabilities over analog systems, such as accuracy, functionality, reliability, and efficiency. Because of the advantages of, and general shift to, digital systems in addition to waning vendor support for analog systems, it is expected that nuclear and other critical infrastructure industries will continue to replace aging analog systems with digital I&C technology. For the same reasons, designs for new, advanced research reactors will rely exclusively on digital I&C systems.

[1] In this context, reliability equals availability over a given time period within certain operating parameters; it does not imply integrity of function against malicious influence via cyber threat.

As industries continue to migrate more control functions to general-purpose digital computing platforms, cyber-informed engineering must be invoked at the earliest life-cycle stages. A new methodology must be developed requiring engagement between researchers and both government and private industry to identify the elements of critical infrastructure that falls within the national security standard and to mitigate high-consequence cyber potentials. We must assume our computing environments have been compromised and that we cannot certify any system is fully secure (even before it is turned on in its intended deployed state). With this in mind, a shift must take place beginning with the examination of fundamental assumptions and design practices.

3. Safety Analysis

Engineering is a disciplined profession with numerous checks and balances to keep a final engineered solution as robust, safe, secure, and reliable as possible. The nuclear industry demands one of the most rigorous engineering processes to make sure global catastrophic consequences are not realized. Safety is the most stringent of nuclear engineering disciplines. Safety demands that all failure modes and other initiators of misoperation be strictly analyzed. Nuclear and other critical infrastructure industries rely on I&C systems for monitoring, control, and protection. A specific plant design implements multiple independent barriers to achieve a safety envelope. These barriers include automated and operator-initiated actions utilizing I&C systems to mitigate the consequences of events. The existing technical requirements for the qualification of I&C systems for critical applications are based on traditional engineering and PRA methodologies using equipment operation and failure data. These data are based largely on non-digital I&C systems that experienced little or no cyber threat during the life span of the equipment. In addition, research reactors, due to reduced thermal energy and fission product inventory, typically do not present the hazards or risks of power reactors and, as such, are not subjected to the same stringent safety requirements. As a result, safety systems at a research reactor may be less diverse, redundant, or robust and, therefore, may also be more easily defeated than those at a nuclear power plant. The importance of research reactor safety systems must be specifically considered in the facility nuclear security regime.

The nuclear industry has a great safety track record and has been analyzing safety aspects for more than half a century. Safety analysis is required to identify and quantify the safety envelope of a given process. A safety analysis determines reliability or risk and frequencies of accident scenarios and identifies vulnerabilities in design/operations. Included in safety analyses are the possible risks to a plant that have been considered (known credible safety consequences).

Risk is the product of frequency and consequences. A PRA defines the parameters for each identified hazard and allows the risk of a hazard to be reduced by making it less likely to occur or minimizing its impact [4, 5]. These parameters become part of the technical safety requirements for the design, operation, and maintenance of a nuclear plant. The requirements are based on traditional engineering methods that consider safety factors and levels of conservatism. As systematic engineering updates are required during the lifetime of the plant to reflect new physical or cyber threats, plant operating experience, modifications, or improvements, a safety analysis must always be performed.

It is imperative that any new cyber-initiating events do not compromise or increase the likelihood of previously analyzed events or do not introduce an unanalyzed event beyond the

design basis. The question is, how can the initiating (cyber) event and/or possible responses (automatic or operator) be fully analyzed in lieu of instrument spoofing and untrusted environments from intelligent malicious attacks? Have all possible digital equipment capabilities, regardless of intended operation, been considered?

The existing safety analysis and PRA models were created with safety- and failure-mode analysis as their bases and design principles utilizing electromechanical/analog technology. With the abundant use of digital systems for both safety and non-safety functions, this model and analysis must consider incorporating cybersecurity concepts and methodologies. Safety analysis should now consider previously analyzed unlikely or highly unlikely events that could potentially change those probabilities based on an intelligent cyber aggressor. Revised analyses may yield different outcomes. Although malicious cyber-attack methods may or may not change previously analyzed safety events, the potential for reactor sabotage or damage may increase.

4. Cyber as a Unique Threat

The aspect that makes a cyber attack a unique threat is the adversary's ability to overcome the challenges of time, space, and scale while introducing intelligence behind focused system mal-operation. Digital systems are designed to improve automation, information manipulation, and communication. The advantages and trends that make digital I&C systems attractive also increase risk. The configurable capability of digital I&C provides an opportunity for exploitation for purposes other than those for which the I&C were designed. This is a direct result of a "trust model" that is a foundational design assumption in every digital implementation. The trust model assumes that the information provided or the actions taken by an individual device or user inside a boundary are trusted. This is a fort mentality that assumes a separation can be maintained between the trusted system and all other digital systems. This capability can cause the systems we depend on for reliable operation to perform unnoticed and unintended functions. The methods to maintain this separation (air gaps, unidirectional gateways, monitoring, patching) all require a real-time level of understanding of cyber threat. The very nature of modern cyber threats is a constant evolution, and no separation method can maintain the current threat state, much less predict how cyber threats will evolve.

A well-resourced and experienced cyber adversary drawing upon various skills is capable of undermining the trust model at every level. Adversaries perform targeted reconnaissance, conduct planning, develop customized tools, are goal-oriented, and test their attacks against frontline security solutions. Attackers are capable of supply-chain compromises (tampering and alterations) that can undetectably alter the digital device before it enters into the end-user's span of control. There are also cyber threats that have demonstrated the ability to autonomously impact a system with no need for a link to an attacker outside of the compromised system. The action (i.e., unanticipated behavior) can also be designed to occur simultaneously in multiple components in an orchestrated fashion. Given the existing trust model used in the design of digital I&C systems, it must be assumed that any single device or combination of devices can be compromised.

5. Critical Nuclear Systems

Safety is one of the most important aspects of nuclear engineering, including safety and safety-related systems, but other systems are equally as important. Security and emergency-

preparedness systems must perform their functions under duress. Physical-protection and emergency-preparedness systems are also susceptible to digital technology. These systems must perform their functions to physically protect personnel, systems, and nuclear material and to support emergency response/operations. Historically, these systems have not been designed with internally segregated networks, nor have they been functionally divided (more important functions isolated). Their support has been from third parties who are allowed remote virtual private network access. This arrangement is typical for these systems where minimal cyber security controls are in place.

Engineering is more than just the consideration of a single component or system and must include the interaction between all systems. The communication interconnection between digital devices has increased the complexity of design. Consideration must be given to examine consequences beyond first-order effects. There is a lack of communication analysis between those assets important to safety and those of a secondary nature. It has been shown that differential shock in a steam and condensate line can be manipulated or induced [6], potentially exceeding design specifications. Modern digital equipment is capable of producing such an event that could impact critical safety systems.

Engineers must bring a cyber-informed aspect to all digital design, operation, and maintenance. This process requires a full knowledge of not only software, firmware, and hardware, but also the techniques, tactics, and procedures (TTPs) adversaries use to defeat or abuse such systems. The knowledge gap is increasing between the attackers and the defensive security experts. Engineers must become educated on these TTPs and design around or design out those vulnerabilities. Assuming digital systems are becoming less trusted against an intelligent adversary, current methodologies may not analyze such a threat.

6. Design Basis Threat

Design basis threat (DBT) has its roots in the physical protection domain that provides the requirements a facility must meet based on a current threat assessment to protect its assets, information, and personnel. Protection must be provided against the consequences of unauthorized access, disclosure, modification, or destruction of sensitive information or sensitive information assets. This set of requirements feeds into the planning for a system design and helps establish performance requirements for the design of physical protection systems. Rigorous analysis and decision-making are essential to defining the level of protection a facility owner must meet before assistance is requested from the state. The International Atomic Energy Agency's Nuclear Security Series No. 10, *Development, Use and Maintenance of the Design Basis Threat,* states, "A DBT is a description of the attributes and characteristics of potential insider and outsider adversaries who might attempt a malicious act, such as unauthorized removal or sabotage against which a physical protection system for nuclear or other radioactive material or associated facilities is designed and evaluated." The DBT considers insiders, external adversaries, malicious acts leading to unacceptable consequences, adversary capabilities, and an evaluation of protective designs. Historically, the DBT did not address cybersecurity concerns. With the cyber threat demonstrating its ability to influence physical protections systems, including blended attacks, digital components and systems must now be considered as either part of the existing DBT or part of a separate cyber-threat assessment. Either way, cyber-informed engineering must contribute to the analysis of credible scenarios that include the adversary compromising computer systems at nuclear facilities and lead to sabotage or the blended attack to remove nuclear material.

7. Solution Discussion

It is difficult to account for a threat that is co-adaptive (i.e., an intelligent human adversary) as the technology becomes the field of contest and can be used to defeat the underlying safety basis. Cyber incidents pose unique challenges, and the appropriate response to a probabilistic failure scenario will not account for a component or system behaving in a way for which it was not intended. Given enough freedom to operate and supporting resources, attackers will find ways to be successful against a research environment where the security function is typically a secondary duty employing security staff that may lack specialized experience and knowledge of the systems or security measures necessary for adequate defense. The degree of success will be a direct function of the knowledge, forethought, and planning of system engineers, designers, and operators. Engineers must embrace training and continuing education in cybersecurity. Cyber entropy must be minimized; otherwise, the current threat trends will continue to deny, degrade, disrupt, and destroy nuclear assets and lead to a gradual decline into disorder.

7.1. Trust Environment

Cyber-informed engineering would, at its core, include fundamental paradigm shifts, such as the realization of operation in an untrusted environment and new methodologies for analyzing safety/security risks. This transformation is a huge change from years of experience in design and analysis. To design systems that must operate in an untrusted environment with an assumption that systems are owned by the adversary is daunting. However, designing such systems is not impossible, because analog or other types of non-digital solutions (biological, DNA sequencing, neural, optical) could provide backup or alternative monitoring and control. This design shift may provide resilience to I&C systems. An example may be a mechanical float installed at a critical-level measurement and hard-wired to a control room. Alternative solutions may involve deeper verification of digital code (hashes) or the creation of biometric or neural networks.

7.2. Safety and Security Risk Analysis

Safety and security risk analysis must now consider an intelligent adversary who can adapt both within the system itself and, in time, beyond controls or mitigations put in place. It is difficult to anticipate the adversary's next move or TTPs that have never been considered. However, analysis must consider the reduction of thousands or millions of combinations of scenarios that are possible with human intervention while eliminating functions that are not required. Many controllers and instruments are designed with several functions, of which only a few select ones may be required. Eliminating nonessential functions should always be applied. Merely disabling functions will not keep the determined cyber attacker from bypassing the disabled feature. This reduction of functions to the bare minimum should reduce a large set of outcomes. In addition, the focus must be kept on a small subset of monitoring and control functions that are critical to safety and support protection against a dire consequence. This process of identifying critical digital assets tries to reduce thousands of digital assets to a minimal set, so that resources can be applied without due strain on the organization. It has been suggested that this reduction of functions analysis is impossible, given a potentially endless combination of scenarios. This should be possible, however, if solid methodologies are developed with sound mathematical equations. This is probably one

of the most difficult types of analysis, because it requires a thoughtful methodology to anticipate and include many possibilities.

7.3. Detection

Detection of unwanted malicious cyber intrusion is currently difficult, especially when modern anti-virus software fails to catch nearly 80% of malware in the wild (zero-day malware). Greater detection mechanisms must be part of the cyber-informed engineering solution. The United States Industrial Control System–Cyber Emergency Response Team has investigated critical U.S. infrastructure systems that were owned by an adversary for many months without detection. As designs are created for functionality, safety, and security, they must also define requirements for the detection of such intrusions. The cyber-informed engineer must understand how an adversary can manipulate a design and must provide barriers or detection mechanisms to stop or minimally detect the intrusion. Methods for this type of engineering may include techniques or procedures that provide constant monitoring of data packets or unconventional external stimuli, such as electrical signals, heat, vibration, or other physical affects.

7.4. Human Factors

The fact that operators provide the eyes and ears of most industrial processes, including nuclear operations, implies that any cyber-informed engineering solution must consider human factors. Human involvement is one method a cyber aggressor uses to either gain unprivileged access or solicit operator actions not normally performed. Actions taken by the operator that are not part of normal operating procedures can have unanticipated consequences. The human in the loop can be manipulated, spoofed, or coerced into taking actions that can cause undue stress, damage, or other less-than-optimal operations. Some actions may even lead to outcomes that do not physically harm the facility or operation but rather cause a political ripple, effectively shutting down nuclear operations across the globe. Human-factors personnel must be included in the cyber-informed engineering discipline to verify that no new design or modification creates cyber-attack opportunities involving the operator. Operators must be strictly trained on cyber-attack TTPs so that increased awareness may help detect, and/or reduce the damage of, a cyber attack.

7.5. Resiliency

Finally, how do engineers account for digital system reliability during cyber attacks that may remain for months with or without the system owner's knowledge? Is it possible to continue to operate in spite of a cyber aggressor who owns the system? More research is required to define the landscape and parameters that must be operational during such events. Analysis must consider the impacts to separate critical functions and systems necessary for continued safe and secure operation. Do we design out digital vulnerabilities against those critical functions? Resiliency will be key to securing future digital systems and must include cyber-informed engineering analysis and practices.

8. Summary

The author proposes that new risk analysis and design methodologies be adopted to account for the co-adaptive nature of the cyber hazard and to devise potential mitigation strategies for safe and secure operations. This approach could potentially eliminate the trust model

assumption at every level of the design process. These new risk analysis methodologies could assist in development of new fundamental design processes for systems and facilities using digital I&C systems, as well as innovations in new components used within these design frameworks. New risk analysis methodologies could drive new approaches to address risks in legacy facilities that rely on inadequate or antiquated design methodologies. Competent authorities can help motivate cyber-informed engineering practices by the creation and enforcement of related regulations. What are needed are a fundamental and holistic cyber-informed engineering process and design basis that provide a framework for the application of resilience in the most critical systems and address the following core issues:

- The cyber threat is co-adaptive and intelligent, requiring new methodologies to predict and detect
- The use of current cybersecurity technologies for mitigation is only effective for the known threats at any point in time, and complete isolation does not exist
- The ability to identify how a trusted system can be manipulated is almost impossible to bound
- Cyber-design basis threat analysis must be quantified
- The supply chain for digital technology is global and complex, providing ample opportunity for the adversary outside the control of the end user
- Technology can introduce broad horizontal failures that can involve many like systems (scale)
- There may be an unsecured and uninsurable financial risk associated with cyber attacks.

From these important areas of research, engineering practices, including the full life cycle (requirements, design, procurement, installation, testing, operation, maintenance, decommissioning), must consider the cyber effects on any design to safety, security, and emergency preparedness operations utilizing digital devices. More research is necessary to protect against future adversarial advances.

Research reactors can be owned and supported by a number of different types of organizations. This influences the strength of funding support, particularly with respect to security. Where competition for government/corporate funding varies, continuing on a path of employing uninformed cyber-engineering skills may lead eventually to unsatisfactory nuclear cyber events that can delay critical nuclear research.

9. References

[1] Security Management for Research Reactor Operators – TecDoc.

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf.

[3] WIKIPEDIA, Internet of Things, http://en.wikipedia.org/wiki/Internet_of_Things.

[4] BEDFORD, T., COOKE, R., Probabilistic Risk Analysis, Foundations and Methods, 1st Edition, Cambridge University Press (2001).

[5] U.S. NUCLEAR REGULATORY COMMISSION, Probabilistic Risk Assessment (PRA), http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html.

[6] AFFILIATED STEAM EQUIPMENT COMPANY, "Water Hammer Tutorial," https://www.youtube.com/watch?v=VBa7DSSmWrE.