INL/CON-15-34244
PREPRINT

Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology

International Conference on Computer Security in a Nuclear World: Expert Discussion and Exchange

R. Anderson
J. Price

June 2015

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

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

Cyber-Informed Engineering: The Need for a New Risk Informed and Design Methodology

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

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

Robert.Anderson@inl.gov

Abstract. Current engineering and risk management methodologies may not contain the foundational assumptions required to address the intelligent adversary's capabilities in malevolent cyber attacks. Current methodologies focus on equipment failures or human error as initiating events for a hazard, while cyber attacks use the functionality of a trusted system to perform operations outside of the intended design and without the operator's knowledge. These threats can bypass or manipulate traditionally engineered safety barriers and present false information, invalidating the fundamental basis of a safety analysis. Cyber threats must be fundamentally analyzed from a completely new perspective where neither equipment nor human operation can be fully trusted. A new risk analysis and design methodology needs to be developed to address this rapidly evolving threatscape.

The aspect that makes a cyber attack a unique threat in the infrastructure environment is its ability to overcome the challenges of time, space, and scale. Digital systems are designed to improve automation, manipulation of information, and/or communication. The advantages and trends that make digital instrumentation and control systems attractive also increase risk. The configurable capability of a digital instrumentation and control system provides an opportunity for exploitation for purposes other than those it was designed for. This is a direct result of a "trust model" that is a foundational design assumption in almost every digital control system implementation. The trust model assumes that the information provided or the actions taken by an individual device or user inside a boundary is trusted. This is a fort mentality that assumes a separation can be maintained between the trusted system and all other digital systems. The methods to maintain this separation (air gaps, unidirectional gateways, monitoring, patching) all require a real-time level of understanding of the state of the network and the cyber threat. The very nature of modern cyber threat is a constant evolution, and there is no separation method that can protect against all threats, much less predict how cyber threat will evolve.

A well-resourced and experienced malicious cyber actor, drawing upon various skills is capable of undermining the trust model at every level. This opponent continues to defeat defensive layers put in place to protect critical operational processes and infrastructure including nuclear instrumentation and control and physical protection systems. In a world of increasing connectivity and cyber threat innovation, it must be assumed that our computing environments have been compromised and that we cannot certify any system fully secure. It is reckless to presume historical analytical assumptions and approaches such as safety analysis, design basis threat and probabilistic risk assessment methodologies can cover the unique nuances of the cyber threat. Without a full understanding of how cyber systems are programmed, operated, and abused, we can hardly identify the threat much less establish effective analysis methods.

The rapid adoption of digital and automation technology in critical infrastructures, including nuclear facilities, has eclipsed existing methods to identify and mitigate high-consequence events. Engineering analysis is not conducted with a cyber-informed perspective. This may lead to flawed assumptions that could obscure the relevance of severe damaging scenarios. Infrastructure asset owners are beginning to recognize the potential for unmitigated risk associated with cyber attacks, but industry is looking for a model to assess and quantify risk and encourage risk reduction methods.

This paper will provide a discussion about the shortfalls of existing cyber-physical security assumptions, methods, and analysis techniques, setting up a framework or basis that can be used to launch new cyber-informed engineering analysis. Although cyber-informed engineering methods have not been fully developed or established to date, this paper will lead a discussion about how attributes of this process might be considered. Evaluating the long-term goal of developing new cyber-informed safety basis and trust principles for high consequence systems is critical.

Key Words: Cyber, Engineering, Risk, Security

1. Introduction

There exists a fundamental challenge with modern engineering practices that do not consider cyber attack consequences. Academia has not caught up to the aggressive and continuously changing cyber threats that pervade nearly all monitoring and control designs. To move forward with secure digital designs, it is imperative that, in order to move forward with secure digital designs, there must be a fundamental engineering transformation that includes the analysis of one of the greatest present-day threats. Current risk-based safety approaches may not include cyber threats to nuclear facilities, digital systems, and critical infrastructures.

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 those systems trusted to help prevent, detect, delay, and respond to the barriers put in place to protect these facilities or systems. Design basis threat analyses must also incorporate the cyber threat to understand what level of protection and response an asset owner must defend against.

The term "cyber" has taken many definitions throughout the past few decades. The International Atomic Energy Agency (IAEA) uses the term "computer security" and considers cyber security synonymous with computer security[1]. 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 how cyber (security) aspects must contribute to 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[2], which will encompass nearly every aspect of modern life. Cyber security 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 is now consumed by nearly every organization and is relied upon for efficient operations and key business decisions. Organizational workforce planning often centers around the availability of remote access for

[1] IAEA Nuclear Security Series 17 - Computer Security at Nuclear Facilities, Section 1.6
[2] Internet of Things - Wikipedia: http://en.wikipedia.org/wiki/Internet_of_Things.

monitoring, troubleshooting, upgrading, and even operation of critical infrastructure. The problem is that digital and automation technology (to include 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,[3] not integrity. As has been the case in many enterprise IT environments, security for some control systems must be "bolted on" at the system level after operation. This places the responsible defenders at a distinct disadvantage. The combinations and permutations of available options for an adversary to exploit the "implicit trust" model of modern control systems can easily prove overwhelming to any defensive effort, exposing the potential for high-consequence events.

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 I&C systems lies in the important advantages and capabilities over analog systems such as accuracy, functionality, reliability, and efficiency. Because of the advantages and because of the general shift to digital systems and 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 plants will rely exclusively on digital I&C systems.

This rapid adoption of digital technology has eclipsed existing methods to identify and mitigate high consequence events. For example, the automotive industry is embracing digital control (X-by-wire),[4] including steering, braking, accelerating, and other monitoring and control functions. New attack vectors are identified every day and must be considered. Supply chain processes are often riddled with opportunities for the adversary to inject malware or supply intelligent misinformation from the supplier before reaching the final end user or even after it is in place through corrupted vendor software updates[5]. Data confidentiality, integrity, and availability must be maintained for safe and secure operations. Air-gapped systems are not inherently secure. An isolation strategy is the starting point and a mandatory good cyber hygiene practice. However, in the context of nuclear operations, a determined adversary is undeterred due to the strategic value of the target. With sufficient money, skill, and time, the air gap can be bypassed.

As industries continue to migrate more and more control functions to general purpose digital computing platforms, cyber-informed engineering must be invoked at the earliest lifecycle 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 fall 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] In this context, reliability=availability over a given time period within certain operating parameters; it does not imply integrity of function against malicious influence via cyber threat.

[4] Automotive News - By-wire age is coming; what's missing is trust: http://www.autonews.com/article/20131202/OEM06/312029967/by-wire-age-is-coming;-whats-missing-is-trust

[5] Cyber Hackers Threaten Global Supply Chains: http://www.scmr.com/article/cyber_hackers_threaten_global_supply_chains

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 instrumentation and control (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 lifespan of the equipment.

The nuclear industry has a great track record and has been analyzing safety aspects for over 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). According to the U.S. Nuclear Regulatory Commission fact sheet on probabilistic risk assessment,[6] the PRA methodology systematically analyzes a complex system to ensure safety. PRA quantifies risk that is measurable and identifies what has the most impact on safety. To perform a PRA, analysts go through the following steps:

- Specify the **hazard(s)**—the outcome(s) to be prevented or reduced. For nuclear power plants, "core damage" is often used. The core is the first physical barrier that keeps radioactivity from release to the public.
- Identify **initiating events**—those events that could lead to the specified physical consequence (e.g., breakage of a pipe carrying reactor coolant).
- Estimate the **frequency** of each initiating event, answering questions such as, "How often do we expect a pipe of this size to break?"
- Assuming that the initiating event has occurred, identify each combination of failures (e.g., pump failure and valve failure) that lead to a specific outcome.

The likelihood of each combination is computed. The probabilities of all those sequences that lead to the same outcome are added. To determine how often this outcome might occur, these probabilities are multiplied by the frequency of the initiating event(s) that are identifiable.

Risk is the product of frequency and consequences. A PRA defines the parameters for each identified hazard and is reduced by making an undesirable event less likely or by minimizing its impact.[7] These 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 considering 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

---

[6] NRC Fact Sheet on Probabilistic Risk Assessment - http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/probabilistic-risk-asses.html.

[7] For more information on PRA, see Probabilistic Risk Analysis: Foundations and Methods, by Tim Bedford and Roger Cooke and U.S. NRC - Probabilistic Risk Assessment (PRA): http://www.nrc.gov/about-nrc/regulatory/risk-informed/pra.html.

performed.

It is imperative that any new cyber initiating events do not compromise or increase the likelihood of previously analyzed events or does 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? Has all possible digital equipment capabilities regardless of intended design operation been considered?

The existing Safety Analysis and PRA models were created with safety and failure mode analysis as its basis 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 cyber security concepts and methodologies. Safety analysis should now consider previously analyzed unlikely or highly unlikely events that could potentially change those probabilities based upon 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 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, manipulation of information, 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 it was 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 is 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 upon 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 there is no separation method that 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. The adversary performs targeted reconnaissance, conducts planning, develops customized tools, is goal-oriented, and tests 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.

The combination of trusted devices with significant configurable capabilities provides an ideal environment for the unique cyber threat associated with digital I&C. Where designs used hardwired interlocks, they now use software interlocks. This has profoundly shortened the design, installation, and maintenance processes. The focus of exploitation in the context of I&C is the application of the inherent device capabilities for purposes other than (or in addition to) the intended design function. Where the premise of historical PRA is the consideration of equipment failure modes, cyber threat is focused on the use of device capabilities outside of the intended design. Unreviewed Safety Question[8] (USQ) determinations in the future may have positive outcomes based on the cyber threat, if not previously considered. Determinations must be made to consider new probabilities of occurrence of accidents, types, consequences, and malfunctions of safety systems previously evaluated in the facility safety analysis. Margins of safety defined in basis documents must also be considered.

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

As engineering is more than just the consideration of a single component or system, it must also 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[9], 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 (TTP) the adversary uses to defeat or abuse such systems. The adversary is busy diving deep into the electronics with soldering irons while most industry cyber security experts are deploying and configuring intrusion detection systems, firewalls, and data diodes. There is an amalgamation between electronic hacking (hardware level) and typical software. In electronics, a hardware description language (HDL) is a specialized computer language used to program the structure, design, and operation of electronic circuits and, most commonly, digital logic circuits. Register-transfer-level abstraction is used in HDLs to create high-level representations of a circuit,

---

[8] 10 CFR 830.203, "UNREVIEWED SAFETY QUESTION PROCESS," http://www.gpo.gov/fdsys/granule/CFR-2011-title10-vol4/CFR-2011-title10-vol4-sec830-203.

[9] "Water Hammer Tutorial," https://www.youtube.com/watch?v=VBa7DSSmWrE.

from which lower-level representations and ultimately actual wiring can be derived[10]. The 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 links to an intelligent adversary; current methodologies may not analyze such a threat.

6. Design Basis Threat (DBT)

Design basis threat (DBT) has its roots in the physical protection domain which provides the requirements that 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 disclosure, modification, alteration, destruction, or denial of use of unauthorized access or disclosure of sensitive information or sensitive information assets. This set of requirements feed into the planning for a system design and help establish performance requirements for the design of physical protection systems. Rigorous analysis and decision-making is essential to defining the level of protection a facility owner must meet before the state is requested for assistance. The IAEA publication INFCIRC/225/Rev.4, also known as Nuclear Security Series #13, "*Recommendations for Physical Protection of Nuclear materials and Nuclear Facilities,"* states that a DBT is a description of the attributes and characteristics of potential insider and/or external adversaries who might attempt unauthorized removal of nuclear material or sabotage against which a physical protection system 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 cyber security 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 that lead to sabotage or the blended attack to remove nuclear material. Incorporation of the cyber threat must carefully consider new technologies, use of mobile computing, social media, and many more TTPs of the adversary. As these threats are considered, the engineer must design systems that reduce or remove these threats. New analysis methodologies may be necessary to accurately describe the threat as well as the mitigations necessary to contain such threats.

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 designed. Given enough freedom to operate and supporting resources, attackers will find ways to be successful. 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 of cyber security. Cyber entropy must be minimized, or the current threat trends will continue to deny, degrade, disrupt, and destroy nuclear assets towards a gradual decline into disorder.

---

[10] Wikipedia, "Hardware Description Language and Register Transfer Level," http://en.wikipedia.org/wiki/Hardware_description_language, http://en.wikipedia.org/wiki/Register-transfer_level.

7.1. Trust Environment

Cyber-informed engineering would, at its core, include fundamental paradigm shifts, including the realization of operation in an untrusted environment to 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, it is not impossible as 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. Whatever the solutions may be, heuristic techniques may be warranted. Operators have been trained to always trust their instruments first, and it will be difficult to retrain for a new operating environment with fundamental changes and prerequisites. This new operating setting will need to be carefully designed to minimize confusion.

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 TTP that has 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 non-essential 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, focus must be kept on a small subset of all monitoring and control functions to those whose functions are critical to safety or have a dire consequence. Many methods of critical digital asset (CDA) identification exist globally. Some member states use prescriptive, performance, consequence-based regulation or a combination of all three. If attention is placed primarily on these components and systems, it may be more manageable to perform the analysis. This process of identifying CDAs is core to most nuclear regulatory requirements and guides. This process 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. If solid methodologies are developed with sound mathematical equations, it should be possible. This is probably one of the most difficult types of analysis as 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 does not 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 their design and provide barriers or detection mechanisms to stop or minimally detect the intrusion. Methods for this type of engineering aspect may include techniques or procedures that provide constant monitoring of data packets or unconventional external stimuli such as electrical signal, 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 making 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 within the cyber-informed engineering discipline to verify no new design or modification creates opportunities involving the operator. Operators must be strictly trained on cyber-attack TTPs so that increased awareness may help detect and/or reduce potential 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 knowledge? Is it possible to continue to operate in spite of a cyber aggressor who owns your systems? 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 future digital systems and must include cyber-informed engineering analysis and practices.

8. Summary

It is proposed that new risk analysis and design methodologies be adopted to account for the co-adaptive nature of the cyber hazard and devise potential mitigation strategies required for safe and secure operations. At its core, this approach would 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. Do regulators enforce cyber-informed engineering practices on new designs? New risk analysis methodologies could drive new approaches to address risks in legacy facilities reliant on inadequate or antiquated design methodologies. What is needed is a fundamental and holistic cyber-informed engineering process and design basis that provides a framework for the application of resilience in the most critical systems and addresses the following core issues:

- The cyber threat is co-adaptive and intelligent, requiring new methodologies to predict and detect
- The use of current cyber security 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 lifecycle (requirements, design, procurement, installation, testing, operation, maintenance, decommissioning), must consider the cyber effects on any design utilizing digital devices as it pertains to safety, security, and emergency preparedness operations. More research is necessary to protect against future adversarial advances. Frameworks such as the RIPE framework[11] from the Langner Group and NIST's Framework for Improving Critical Infrastructure Cybersecurity[12] can help improve and strengthen the resilience of critical infrastructure towards the establishment of solid cyber-informed engineering analyses, practices, and procedures, but more research is absolutely necessary to encompass the entire cyber-informed engineering discipline.

[11] http://www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf
[12] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf