Institutionalizing Cybersecurity at Nuclear Facilities[1]

Introduction

There have been a number of recent cyberattacks on critical infrastructure, including nuclear facilities[2], which have demonstrated publicly that the cyber threat to nuclear facilities is real. Adversaries now have the ability to carry out such attacks, and incremental improvements in defenses are unlikely to be sufficient to ensure that an attack by a determined, adaptive adversary would fail.

While existing security procedures are largely effective against generic attacks and amateur hackers—the threat of greatest concern is that posed by organized, determined groups that may target specific facilities. Nation states and state-sponsored groups are developing ever more powerful cyber weapons and terrorist organizations are also becoming increasingly capable of launching damaging attacks.

For nuclear facilities in particular, a successful cyber-attack, especially if blended with a physical attack, could result in a catastrophic radiation release with serious consequences for surrounding communities.

Background and the Current Approach

The sophistication and maturity of cybersecurity programs at nuclear facilities varies widely from country to country. For example, the 2016 NTI Index found that 20 out of 47 countries with certain types of nuclear facilities have none of the most basic regulations related to cybersecurity at nuclear facilities. While this does not necessarily mean that facilities have no measures in place, it suggests that substantial opportunities for improving cybersecurity at nuclear facilities exist.[3]

Nuclear facilities have traditionally focused on physical security, which relies on physical, procedural, and electronic defences and is generally well-embedded in a facility's culture. In contrast, cybersecurity is not as well developed. Cybersecurity was initially viewed as an information technology (IT) problem, defending against viruses and other attacks from the Internet. Over time, recognition has grown that cybersecurity is also essential for what has become known as operational technology (OT), which includes all digital systems used operationally. This is distinct from IT, which deals with business systems. OT includes industrial control systems (ICS), including control and

[1] This paper was prepared by Anna Ellis and edited by NTI staff.

[2] For the purposes of this paper, "nuclear facilities" will be defined as facilities storing 1kg or more of weapons-usable nuclear materials (highly enriched uranium and plutonium) and/or facilities that, if subjected to an act of sabotage, could pose the risk of radiological release with significant off-site health consequences. Examples of these facilities include: operating nuclear power reactors, power reactors that have been shut down in the last five years, research reactors with a capacity of 2MW or greater, reprocessing facilities, and spent fuel pools with fuel that has been discharged in the past five years.

[3] With the entry into force of the 2005 Amendment to the Convention on the Physical Protection of Nuclear Materials (CPPNM), countries are now obligated to provide physical protection to nuclear materials and facilities. While this is an encouraging step for nuclear security, it is too early to evaluate the impact it will have on cybersecurity at nuclear facilities.

protection systems, human machine interfaces (HMIs), sensors and actuators. At some facilities, the electronic aspects of physical security are also included within OT.

In contrast to cybersecurity, in most countries ensuring safety at nuclear facilities is a mature discipline. For example in most countries nuclear facilities have a well-defined safety framework and a nuclear safety culture. The effects of naturally occurring safety incidents (i.e. accidents) are studied, including conditions within the "design basis" of the facility, during normal operation, under fault conditions and during (potential) severe accident conditions. Performance of the plant and its people within the 'design basis' of the plant, are well-studied, proceduralized, and evaluated. Personnel roles are well understood and personnel are suitably qualified and experienced. "Emergency planning" is in place, and response to beyond design basis conditions has been considered, and contingencies are in place.

Furthermore, for each of a range of plant states, "safety functions" and their impacts on and relationships to pre-determined safety goals are defined and explicitly stated. Many of these are partly or entirely implemented within ICS. Response to normal accidents is designed into ICS in accordance with appropriate standards and guidance. Any modification (e.g., engineering work to change the plant) preserves these design rules. A team of people analyses potential faults and updates complex models using powerful tools designed purely to implement these well-developed safety approaches. Plant staff continuously re-evaluates and updates the safety case as new operating experience is received from the plants. This sometimes leads to the requirement for a plant modification to preserve demonstrable adherence to safety targets. In addition, whether in new build, existing facilities, or decommissioning, the operator must have the organizational structures in place to remain capable through-life of maintaining safety goals. Finally, the operator must have the emergency response plans and procedures in place to respond quickly and effectively to a safety incident.

An effective and enduring cybersecurity program at nuclear facilities requires that it be treated in the same serious manner as safety. The approach taken by the nuclear sector to safety thus provides a model for a robust cybersecurity program.

Institutionalize Cybersecurity at Nuclear Facilities

Cybersecurity at nuclear facilities should be treated with the same rigor and attention paid to safety—that is, cybersecurity must be institutionalized at nuclear facilities.

Recognizing the physical consequences that can be achieved via cyberattack, cybersecurity should be treated with the same rigor and attention as other major program elements like safety and physical security. This includes acknowledging characteristics unique to cyber and embedding cybersecurity in facility design, personnel training, and processes.

Once fully institutionalized, this would be seen in the people and organizational culture, the system design, and the processes and practices. Additional details are provided below. [4]

[4] Note that this priority is focused on building *passive* defenses through design solutions, including appropriate system design, addition of controls, as well as constraints on operation and maintenance. The implementation of an *active* defense capability is the subject of another priority in this suite.

People and Organizational Culture

An organization's priorities must be embedded in an organization from top-to-bottom. While it took many years to evolve, today this is the case for safety in the nuclear industry. From the CEO to the most junior employees, everyone knows that safety is the top priority of a nuclear facility.[5] Similarly, for cybersecurity programs to be effective, everyone must know his or her role and how it fits into the larger context. Thus, within the vision of having cybersecurity treated with the same rigor as nuclear safety, all personnel would understand their role in cybersecurity. Importantly, this would also include personnel outside of the facility such as suppliers and vendors. Leadership would reinforce this priority in many ways, including through training, and in performing personnel assessments and hiring.

The end goal would be the creation of a cyber-nuclear security culture, which would exist throughout the organization.

Facility Design

This priority borrows heavily from existing models for graded application of safety and physical security at nuclear facilities in which the systems performing the most important functions are engineered to be the least likely to fail. When using a graded-approach to safety and security, systems critical to safety functions at nuclear facilities are subject to the most stringent requirements so as to minimize the likelihood of failure.

Similarly, to ensure that cyberattacks do not lead to unacceptable consequences, digital systems need to be characterized. The significance of the system would then determine how it should be designed, connected into a wider architecture, operated, maintained, modified, and upgraded. Ideally, design solutions would be robust to failure due to plant fault, fault within the ICS itself, under accident conditions and also be robust to cyberattack.

There are a number of potential approaches to identify the functions and systems that are allocated to the highest security class. The most stringent protection could be afforded to those digital systems that:

- Represent an 'ultimate backstop' system which could achieve safety and security in the event that all other systems were compromised;
- Contribute to a sequence of events which could lead to an off-site release, core damage, or consequences to the fuel pool, within existing safety analyses; and/or
- Could have consequences ***outside*** the existing safety analyses, if manipulated through cyberattack.[6]

Within the highest security class, there would likely be significant constraints on the architecture that would isolate these systems from threats or utilize 'hard to hack' technologies like hardware-based logic systems. Facilities would be constrained to select hardware, firmware, tools, and development environments from vendors who can demonstrate that their products and processes are conducive to secure design. A separate priority "Reducing the Cyber Threat to Digital Systems—Minimizing Complexity " also addresses this topic.

---

[5] See, for example: https://www.nrc.gov/about-nrc/safety-culture.html.

[6] One approach is to focus on actuators and what would need to happen for erroneous movement to be achieved. Another approach is to look with fresh eyes at sources of significant impact on stable (operating or shutdown) plant states, i.e. would lead to large transients (for example, the mis-operation of a large sized mechanical plant). This approach would identify plant dependencies on external systems to establish where a cyberattack could be disruptive. Another approach looks at internal sources of hazard; fire, flood, impact, etc. It would identify where a cyberattack could increase consequences of these events.

Processes and Practices

In addition to system design constraints, robust processes must exist to ensure that digital systems are operated and maintained appropriately. As examples, key processes would include:

- Defining a security design basis;
- Classifying digital systems;
- Providing guidance on allowable architectures and design guidance for each class of system, including restrictions on the vendor and supply chain, and including vendor audit;
- Providing guidance on rules relating to operation and maintenance of different classes of systems, and hence support the update of procedures for normal and fault conditions;
- Providing tools and techniques for collection and review of operating experience (OPEX) and guidance on the consequential improvements to be made; and
- Governing the update of procedures for emergency planning and responding to severe accidents and 'beyond design basis' events (including simulations).

Within the nuclear sector, mature process and practices currently exist for safety-relevant systems and are central elements in ensuring safety of operations. The importance of the related concept of quality management has been emphasized by Langner[7] and provides one approach to strengthening cybersecurity at nuclear facilities.

Achieving the Vision

Achieving the vision presented in this paper will not be easy or quick, may require substantial changes at the facility level and in some cases would require development of new tools and methodologies. It would almost certainly carry significant costs; though likely some of those costs could be passed on to government. After all, a blended cyber-physical attack on a nuclear facility would almost certainly be considered a "beyond-DBT" event, thus demanding some response or action at the national level.

In order to implement the changes identified, facilities would need to be convinced of the benefits or required by government authorities. In either case, successful implementation will require support by governments, regulators, vendors, research institutions and other bodies. Below an initial set of actions needed to implement the vision are identified.

People and Responsibilities

Appropriately skilled and trained personnel are essential for effective cybersecurity. While facilities can expand training programs to meet some of their needs, in many cases, the needed personnel are not readily available and will need to be recruited. For example, new cybersecurity specific roles may include:

- Specialists to implement the processes and practices to achieve the desired design solutions.
- Personnel trained to deal with cyber incidents, or incidents with a cyber element to return the plant to a safe operating condition.
- Experts in continuous improvement and cyber risk assessment, including the collection, analysis and interpretation of data on cyber incidents.

Unfortunately, there are widespread shortfalls of appropriately skilled and trained personnel. As such, there may be value in developing industry-wide efforts to identify the needed skills and establishing programs to recruit and train cyber experts.

[7] Ralph Langner has advocated for the adoption of what he has termed the Robust ICS Planning and Evaluation (RIPE) framework. For more information, please see http://www.langner.com/en/wp-content/uploads/2013/09/The-RIPE-Framework.pdf

Facility Design

The concept of security by design is a key part of protecting nuclear facilities from cyber-attacks. For many existing facilities, however, this would require migration to a new architecture, possibly implying replacement of certain systems (e.g., to separate them from others or to use a different technology). In addition, design solutions may impose constraints on technology selection and facilities may need to work with vendors and equipment providers to implement these changes.

Over the longer term, there may be a need to develop new technologies especially suited to certain classes of system and enabling modern logic systems that are able to perform complex calculations based on 'harder to hack' (e.g. hardware-based) technologies. A facility or more broadly the nuclear industry may need to work with a prospective vendor to initiate development of this. This would have consequences for the vendor and the facility, in terms of people, skills and training.

Facility Processes and Practices

Effective processes and practices are the lifeblood of safe and secure nuclear facilities. While technology has a critical role (and can amplify the effectiveness of the role played by people and processes), it is the processes and practices that are truly critical. This is especially true for cybersecurity given that much of the security is "hidden" from view, in contrast to physical security. As with safety, moving to a vision where cybersecurity is fully embedded in a facility's processes and practices will require the attention of facility management.

Moreover, analysis methodologies need to be developed that will allow facilities to assess the risk and potential consequences of cyberattacks, as well as the progress being made on strengthening facility security. Whilst facilities must drive the development of these tools and will ultimately be charged with implementing them, it may be valuable to consider a joint operator working group or a cross-industry funded working group, using resources from research establishments and other bodies.

Finally, as with safety, conducting the appropriate analyses and preparations for emergency response in the event of a cyber incident are critical to elevating cybersecurity concerns to the same level as safety and physical security concerns. Because a cyberattack could have physical consequences or be used in combination with a physical attack to facilitate an act of theft or sabotage, such preparations are of particular importance.

Actions for Governments

Finally, nuclear facilities are unlikely to take on needed changes without the support of government. The regulator, in particular, would have a key role in embracing a new strategy for protecting nuclear facilities from cyberattack. In addition, government-funded research organizations may have a key role in the development of new tools and methodologies.

Conclusions

This priority presents a vision whereby cybersecurity at nuclear facilities is treated with the same rigor and attention paid to safety. This is a key element in ensuring that cyberattacks on nuclear facilities do not have catastrophic consequences. It encompasses people and organizational culture, design solutions and processes and practices.

The vision can only start to be implemented once senior decision makers at nuclear facilities, as well as government authorities, recognize the magnitude of the cyber threat to nuclear facilities and commit to a more strategic approach.

Implementation would undoubtedly incur significant costs. These would include one-time costs to procure technologies and systems and hire additional support, and ongoing costs to implement training, and processes.

In addition to financial costs, this paper recognizes that adoption of this priority is challenged by significant hurdles to implementation, and the lengthy timescales required. Organizations will need to adapt and personnel will need to be trained and/or recruited. Implementation will pose significant constraints on architectures and design guidance, including that applicable to vendors.

There would need to be far-reaching changes to processes and practices for operations, testing and maintenance. For this to occur, government authorities may need to require its adoption, while supporting a range of cross-industry initiatives.