Operating Nuclear Power Stations in a Regulated Cyber Security Environment: A Roadmap for Success

Erik Dorman, PMP [1]
[1] Manager, Cyber Security Solutions, AREVA Inc.
(Erik.Dorman@areva.com)

Abstract

The United States Nuclear Regulatory Commission (NRC) issued 10CFR73.54 to implement a regulated Cyber Security Program at each operating nuclear reactor facility. Milestones were implemented December 31, 2012 to mitigate the attack vectors for the most critical digital assets acknowledged by the industry and the NRC. The NRC inspections have begun. The nuclear Cyber Security Plan, implemented by the site Cyber Security Program (Program), is an element of the operating license at each facility.

The Program is designed to protect critical digital assets (CDAs) by applying and maintaining defense-in-depth protective strategies to ensure the capability to detect, respond to, and recover from cyber-attacks. The Program references NEI 08-09 R. 6, the Nuclear Energy Institute Template that provides guidance for applying Cyber Security controls derived from NIST 800-53/82 and slightly modified to fit the nuclear environment. Many mature processes are in place at nuclear facilities in response to numerous regulations implemented over the past 30 years. Many of these processes such as the Physical Security Program offer protections that are leveraged to protect the functions of critical digital assets from unauthorized physical access. Other processes and technology such as engineering design control, work management and pre-job briefs, control of portable media and mobile devices, and deterministically segregated networks protect critical digital assets. By leveraging the regulated nuclear environment, integrating NIST type Cyber Security controls, and prudently deploying technology the Cyber Security posture of operating nuclear facilities supports on-demand base load electricity 24/7 with capacity factors exceeding 85%. This paper is designed to provide a glimpse into Cyber Security Programs that support safe operation and reliability in the regulated nuclear environment while supporting the on-demand base load electricity production 24/7.

1. Introduction

In today's digital age, many critical business operations take place in cyberspace, requiring companies to take measures to protect their employees and business infrastructure from cyber-attacks. Malicious individuals and groups, whether aiming to steal personal information or to completely destabilize an Internet network or critical infrastructure system, can expose sensitive personal and business information, and disrupt critical operations. Critical infrastructure, such as electrical power generation or transmission and distribution systems, experience escalated costs to protect against potential exploitation that could adversely impact operations. The processes and practices designed to protect networks, computer programs and data from attack, damage or unauthorized access is known as Cyber Security.

Cyber Security is a growing field across all facets of business operations. Our daily lives, economic vitality, critical infrastructure and national security depend on a stable, safe and resilient defense against cyber-attacks. We rely on digital technology to communicate, travel, work and power our homes,

offices and economy. The threats being launched every day have driven the need to improve upon the cybersecurity protective strategies. These improved strategies aim to protect systems and networks around the globe and across personal, business and critical infrastructure boundaries.

2. Post September 11, 2001 Regulatory Landscape

The nuclear power industry is one of the most highly regulated and safest industries in the world, and takes cyber threat seriously. After the attacks of September 11, 2001 the Nuclear Regulatory Commission (NRC) amended the plant design basis threat (DBT) to include cyber-attacks. In early 2002, the NRC issued an order to require power reactor licensees to implement interim measures to enhance Cyber Security at their sites. In 2009, the NRC amended their extensive physical protection program regulations to include a specific regulation, 10CFR73.54, for a cybersecurity program that would be a component of the operating licenses. These requirements provided high-assurance that digital computer and communication systems and networks associated with safety and important to safety functions, security functions, emergency preparedness functions (including off-site communications), and support systems would be adequately protected up to and including the DBT. Subsequently, the NRC issued COMWCO-10-0001, to clarify that its cybersecurity rule should be interpreted to include components in the Balance of Plant that contain a link to radiological health and safety at NRC-licensed nuclear power plants. Plant systems that are subject to the NRC's Cyber Security Rule are known as critical systems.

As a result, every plant submitted a Cyber Security Plan to the NRC that described how the plant would implement its cybersecurity program and the schedule for implementation. The NRC reviewed and approved each of these plans and schedules. The Cyber Security Plan provides high assurance that plant critical systems and CDAs subject to 10CFR73.54 are protected against cyber-attack up to and including the DBT. Each licensee plan includes an implementation schedule containing eight milestones. Seven of the milestones were due by December 2012. The stringent measures implemented by milestones one through seven are aimed at protecting the most sensitive critical systems by mitigating attack vectors.

By December 31, 2012, each U.S. nuclear power plant was required to:

- Isolate key control systems using either air-gaps or robust hardware-based isolation devices. As a result, the key safety, security and power generation equipment at the plants are protected from any network-based cyber-attacks originating outside the plant.
- Enhance and implement robust controls over the use of portable media and equipment. In instances where devices like thumb drives, CDs and laptops are used to interface with plant equipment, measures are in place to minimize the cyber threat. These measures include such actions as minimizing the use of devices that are not maintained at the plant; virus scanning devices both before and after being connected to plant equipment; and implementing additional security measures where the source of the data or device originates outside the plant. As a result of these actions, plants are well protected from attacks that are propagated through the use of portable media.

- Enhance defenses against insider threats. Training and insider mitigation programs (inclusive of operator and security rounds) have been enhanced to include cyber attributes. Individuals who work with digital plant equipment are subject to increased security screening, cybersecurity training and behavioral observation.
- Implement Cyber Security controls to protect equipment deemed most essential for the protection of the public health and safety.
- Implement measures to maintain the effectiveness of the program. These measures include maintaining the CDAs and the equipment subject to §73.54 in the plant configuration management program and ensuring changes to the CDAs are performed in a controlled way. A cybersecurity impact analysis must be performed before making changes to the CDAs. The effectiveness of cybersecurity controls is periodically assessed and enhancements are made where necessary. Vulnerability assessments are performed to ensure the cybersecurity posture of the CDAs is maintained.
- Establish a Cyber Security Assessment Team (CSAT) that provides a group of individuals encompassing a broad array of experience to provide oversight to the implementation and programmatic activities.
- Develop a list of Critical Systems and CDAs that are in scope of the regulatory requirements.

As nuclear plants work to enhance their Cyber Security, they are preparing for safe and reliable operation for decades into the future. The nuclear energy industry is in the midst of a renewal. Across the nation, nuclear plants are being licensed to operate for longer periods of time and are transitioning from analog to digital systems for increased safety and performance. While this transition to digital technology is increasing the capability, longevity, safety and reliability of America's nuclear energy plants, the need to integrate robust cybersecurity measures is a necessity. Proven digital protection systems are already in place at nuclear plants around the world to proactively protect against cyber threats to plant safety and control systems.

Protecting the U.S. nuclear power infrastructure from exploitation and cyber-attacks perpetrated against critical system networks is an industry challenge. As threats evolve for both nuclear infrastructure and corporate networks, there is an increased need for digital security. In addition, there is a growing need for technically knowledgeable resources that possess a combination of cybersecurity skills, plant system knowledge and nuclear regulatory experience.

For the nuclear industry, safety and security are non-negotiable, so best-in-class Cyber Security is critical to the continued operational excellence of the nuclear energy fleet.

3. AREVA's Nuclear Cyber Security Program Outline and Approach:

The AREVA Cyber Security Program is centered on our ability to manage risk for our customers and to deliver a lower overall cost to the customer in order to best meet the regulatory driven requirements which will provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the DBT.

AREVA's methodology will help drive implementation of the requirements and deliver a lower overall cost by focusing on:

- The most pragmatic approach to establish, implement, and maintain a Cyber Security program by leveraging and integrating many of the activities into existing programs, processes, and procedures.
- Optimize assessment activities by leveraging techniques such as common controls, grouping strategies, and efficient methodologies.
- Develop and maintain the supporting technical documentation which:
  - Captures the approved implementation schedule.
  - Implements a Cyber Security Plan that meets the program requirements.
  - Provides requirements traceability for validation that the requirements were met specific to each site.
  - Executes periodicity and procedural activities for:
    - ☐ Incident Detection, Response, and Recovery
    - ☐ Corrective actions, configuration management, records retention, and design control
    - ☐ Supply Chain control
- Assembling a diverse project team with significant engineering experience, specifically in instrumentation & control systems, digital plant modifications, design engineering, security, and information technology. This resource mix provides for significant nuclear plant and engineering competencies, the understanding of nuclear power plant (NPP) systems, programs, processes and procedures. In addition, this knowledge enables the team to leverage existing controls already in place and minimize the need for plant modifications that would significantly increase the overall cost of program implementation.
- Establishing partnerships with suppliers to create a toolbox of solutions that each nuclear plant licensee can leverage for expert knowledge, processes, tools, methods and cutting-edge technology to stay ahead of the evolving cybersecurity landscape

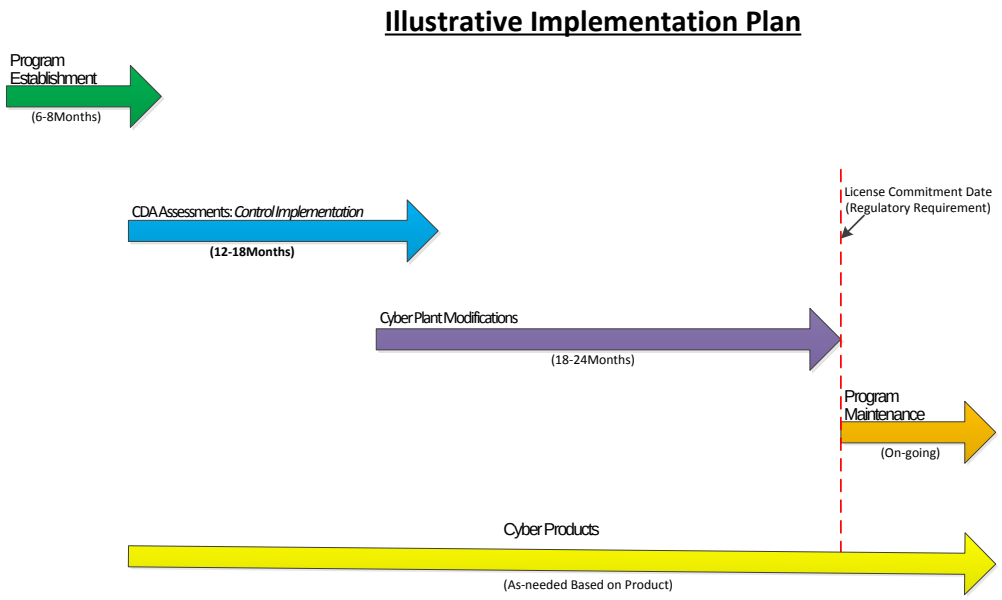

Figure 1 – Illustrative Implementation Plan

4. Conclusion

NPP Operators have challenges with managing new and existing regulatory requirements which already place a large demand on strapped operational and capital budgets. The Plan requirements add another layer of programmatic requirements that, if not managed correctly, can place additional demands on NPP resources without providing a roadmap for success.

AREVA has developed a comprehensive approach for the establishment, implementation, and management of the Program and associated requirements for our customers. AREVA has developed the resources, infrastructure, partnerships, and methodologies to provide cradle-to-grave solutions in order to most effectively and efficiently implement the regulatory requirements.

The AREVA Cyber Security Program will focus on minimizing the cost impact while providing a framework for successful implementation and on-going maintenance of the licensee's Program. Our customers will realize significant reductions in cost for Program challenges by developing an implementation roadmap which focuses on utilizing existing licensee programs, implementing prudent technical solutions, and leveraging the correct resource expertise for all phases of the Program lifecycle.

Cyber Security plays a significant role in securing the infrastructure assets for the nuclear sector. Through partnerships between the nuclear industry and Cyber Security providers who possess unique nuclear and Cyber Security experience, the industry can be confident that their critical digital assets will be protected, their Plan will be implemented most efficiently, and the Program will be

maintained with the highest level of effectiveness minimizing the regulatory and operational risks. And because of strict regulatory oversight and a culture steeped in safety and security, there is no better industry suited to address Cyber Security for the energy sector than the nuclear industry. The cutting-edge expertise brought together by the AREVA team is one example of a partnership that takes a proactive, multi-pronged approach to ensure the Cyber Security of the nuclear power sector, helping utilities meet today's missions and address tomorrow's threats.

5. References

1. NEI 08-09 Revision 6
2. NEI 10-04 Revision 2
3. 10 CFR 73.54
4. NRC Regulatory Guide 5.71