U.S. NUCLEAR POWER CYBER SECURITY PROGRAM IMPLEMENTATION: A BRIEF HISTORY AND A ROADMAP FOR INTERNATIONAL IMPLEMENTATION FOLLOWING THE NRC MODEL

JASON M. HOLLERN

Principal Technical Leader, Security and Digital Protection Solutions

AREVA NP.

Bachelor's degree in Mechanical Engineering and a Master's degree in Nuclear Engineering from The Ohio State University. He has also received a Graduate Certificate in Terrorism Analysis from the University of Maryland at College Park.

The cyber security program implementation at nuclear power plants in the United States has been ongoing since 2008. Over that time the nuclear power plant operators have experienced many challenges and celebrated successes. In order to better communicate those challenges and successes to the rest of the nuclear industry, many conferences, workshops, and discussions were held. Because AREVA NP has helped to implement cyber security at most of the nuclear power plants in the U.S. (over 20 nuclear utilities and over 50 reactors), many of the lessons learned and operating experience have been shared between nuclear power plant operators. Using this valuable operating experience and lessons learned, AREVA NP developed a cyber security implementation roadmap for international implementation of the Nuclear Regulatory Commission's model. The roadmap can easily be modified for other international standards such as ISO/IEC 27000 and IAEA Nuclear Security Series #17. The roadmap combines the Milestone 1-8 implementation tasks into one structured program. The roadmap streamlines implementation efforts to save up to 40% in implementation time and up to 25% in financial resources by implementing many tasks in parallel and combining programmatic efforts. The roadmap is being implemented internationally in Japan and South Korea at multiple nuclear reactor sites.

A BRIEF U.S. HISTORY

The nuclear power industry in the United States (U.S.) has been implementing cyber security programs since 2008. This year, 2017, most plants will call their interpretation of cyber security implementation complete. Over the past 9 years, there has been a large amount of money spent within the industry to meet the regulations and advance this topic. The industry and the Nuclear Regulatory Commission (NRC) has held various conferences, workshops, and discussions to try to gain alignment within the industry, share lessons learned and operating experience (OE), and discuss successes and challenges. These conferences and workshops are the perfect venue for the regulator, nuclear power plant operators, and the implementation teams to try to share their experiences and develop continuity from company-to-company and plant-to-plant.

One observation that has been noted is when the NRC released the cyber security rule, it was done in such a way that prescribed the requirements, but left it up to the nuclear power plant operator to interpret and determine how the requirements were going to be implemented. AREVA NP has noted that operators have many different interpretations throughout the industry. The goal of the conferences and workshops was to drive the industry to a unified consensus with agreement from the NRC, but many factors, such as budgets, internal company constraints, markets, shareholders, etc. have not allowed total agreement industry-wide. In addition, in some cases, the NRC has not reviewed enough nuclear operators' attempts at full implementation to express if their work is acceptable. Therefore, consistency throughout the industry is not absolute, but most nuclear plant operators are following the same general processes.

PROGRAMA DE CIBERSEGURIDAD DE LA ENERGÍA ATÓMICA DE ESTADOS UNIDOS: BREVE HISTORIA Y MAPA DE RUTA PARA SU IMPLANTACIÓN INTERNACIONAL SIGUIENDO EL MODELO DE LA NRC

"El programa de implantación de ciberseguridad en las centrales nucleares de Estados Unidos se inició en 2008. Desde ese momento, los operadores de las centrales nucleares han experimentado tanto desafíos como éxitos, que se han ido comunicando a través de diversas conferencias, workshops y coloquios al resto de la industria nuclear. Areva NP ha ayudado en la implantación de los programas de ciberseguridad a la mayoría de las plantas de los EE.UU. (más de 20 empresas propietarias nucleares y más de 50 plantas), y ha colaborado en que todos los operadores de reactores nucleares hayan tenido acceso a muchas de las lecciones aprendidas y experiencia operativa recopilada. Haciendo uso de dichas lecciones aprendidas, Areva NP ha desarrollado una hoja de ruta para la implementación internacional de los planes de ciberseguridad siguiendo el modelo de la NRC (Nuclear Regulatory Commission). Esta hoja de ruta puede ser adaptada fácilmente a otros estándares internacionales como el ISO/IEC 27000 y el *IAEA Nuclear Security Series #17* y combina en un único programa estructurado los hitos 1 al 8 de las tareas de implantación. Esto permite reducir en un 40% el tiempo de implantación y en un 25% los recursos financieros, valiéndose de la implementación de tareas en paralelo y la combinación de esfuerzos de programación. Esta hoja de ruta está siendo actualmente implementada internacionalmente en múltiples emplazamientos nucleares de países como Japón y Corea del Sur."

Cyber security implementation in the U.S. was broken into two main phases. The first phase was implementation of Milestones 1-7 and was completed by the end of 2012. These first seven milestones were implemented concurrently and included activities such as employing network segregation by installing unidirectional one-way deterministic devices, developing a portable media and mobile device program, identification of critical digital assets within the plant, training and implementing rounds to detect obvious signs of cyber tampering, etc. The second phase was the implementation of Milestone 8, which also had multiple concurrent activities. However, there was a round of inspections from the NRC after the completion of Milestones 1-7 to determine if they were implemented correctly by the nuclear power plant operators. In many cases, there were issues identified that required resolution. Therefore while the nuclear plant operators were implementing Milestone 8, they were also required to resolve the issues identified with Milestones 1-7 implementation.

As Milestone 8 implementation draws to a close this year, AREVA NP has been a major partner in the implementation of the total cyber security effort for many nuclear plant operators in the United States. AREVA NP is using these valuable lessons learned throughout the entire U.S. nuclear industry to help our partners world-wide to provide efficiencies, share the OE, and implement a cost effective and compliant program. In doing so, AREVA NP has recognized that there is an inherent cyber security implementation Roadmap and recognized that the entire cyber security program is only as effective as the individual programs and processes that comprise it.

COMPREHENSIVE SECURITY THROUGH INDIVIDUAL PROGRAMS, PROCESSES, AND PROCEDURES

There is no one single element of the cyber security program that provides total exclusive protection. There are individual elements that work together to provide a cohesive protection scheme. Because the goal of cyber security is to mitigate threats and vulnerabilities from the five attack pathways, typically there are multiple programs, processes, and procedures that make up elements of the overall cyber security program that provide these protections (Figure 1).

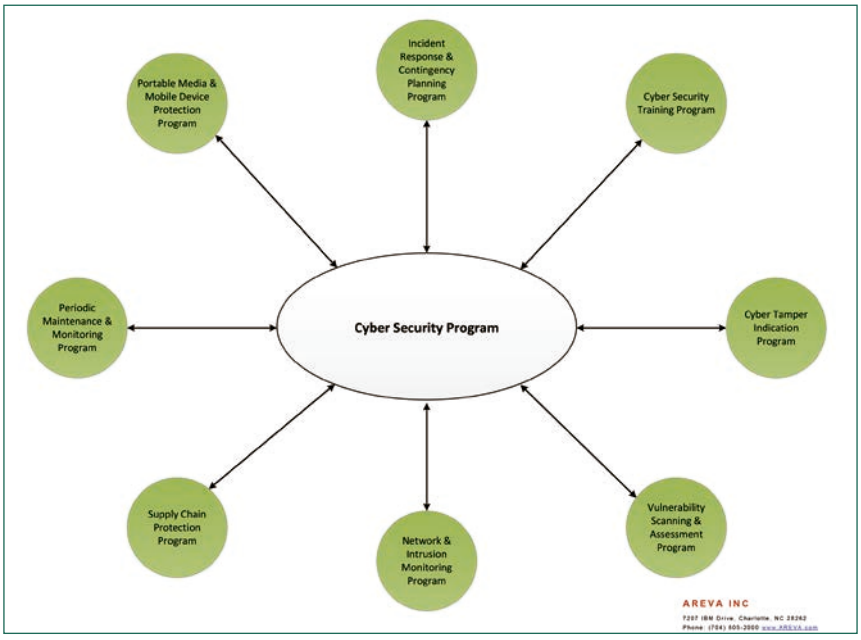

Figure 1.

For example, the nuclear power plant is required to have a portable media and mobile device (PMMD) protection program. The program consists of procedures for employees, vendors, and visitors to follow and governs the use of PMMD that is brought into the nuclear power plant. In addition, there are tools that are used to scan and detect malicious software on PMMD before use within plant systems. The nuclear power plant also has authorized equipment and PMMD that is only allowed to be used and is securely stored to prohibit intentional or accidental tampering. This program alone does not provide all of the protections necessary for cyber security, but provides an important piece of the overall comprehensive protection scheme.

As a PMMD program was developed during Milestone 4 (one of the Milestones 1-7 that was completed in parallel), the program, procedures, and tools are imported into the Milestone 8 implementation strategy to become part of the overall cohesive protection scheme. Milestone 8 is the step in the cyber security programmatic implementation that brings all of the elements together into one overarching program.

Other examples of cyber security programmatic elements that are developed as part of Milestone 8 include supply chain protections, network intrusion detection monitoring, remote monitoring, tamper indication, vulnerability scanning and assessments, wireless network connectivity protection, training programs, device risk/consequence assessments, etc. Many of the programmatic elements mentioned above are implemented in parallel during Milestone 8, but some sequencing is often required. AREVA NP has developed a simplified security program implementation Roadmap that defines the major tasks of implementation and logically outlines the sequence of program, policy, and procedure development, along with major task accomplishment.

MILESTONES 1-8 RECOMMENDED APPROACH FOR INTERNATIONAL IMPLEMENTATION

The U.S. nuclear industry took five years to implement the first seven milestones in parallel. The cyber security interim milestones include:

1. Formation and Qualification of a Cyber Security Assessment Team (CSAT).
2. One-Way Deterministic Segregation of Higher Security Levels from Lower Security Levels.
3. Identification of Critical Systems, Digital Assets, and Critical Digital Assets (CDAs).
4. Development of a Portable Media and Mobile Device (PMMD) Protection Program.

5. Implementation of Rounds to Identify Obvious Signs of Cyber Tampering.
6. Completion of Cyber Security Control Assessments of Target Set CDAs.
7. Implementation of Ongoing Monitoring of Target Set CDAs.
8. Full Cyber Security Program Implementation.

The nuclear industry in the U.S. decided to create the interim milestones to show some progress of completion, but to also determine if there would be clarification on the requirements released by the NRC. Some of the clarification and guidance came from the industry's working groups, conferences, and discussions throughout the first years.

As a new nuclear power plant ventures to implement a cyber security program for the first time, the OE and lessons learned can be applied to the milestone approach of cyber security implementation:

First, not all countries may have the concept of target set CDAs. Because these CDAs are not designated or differentiated between other safety-related or security-related CDAs, then the activities of Milestones 6-7 can be combined into Milestones 2 and 8. In addition, because the activities of Milestone 5 was largely centered around target set CDAs, those activities can also be combined in Milestone 8 when training, ongoing monitoring, and cyber tamper indication programs are developed.

Second, many of the activities in Milestones 1-7 and Milestone 8 can be collapsed into a common roadmap for parallel implementation. However, there are some activities that must be completed in series. For example, Milestone 1 is the formation and qualification of a CSAT. The CSAT is a body of professionals that has various duties that include review and approval of cyber security programmatic documentation, along with other important duties. Because the program is being developed and many of the programmatic documents that build the foundation of the entire program are developed early in the cyber security program implementation process, the CSAT must be formed and qualified early in the implementation process to avoid repeated rework, churn, and delays.

Finally, some of the larger Milestone 1-7 items, such as PMMD Protection Program development can be treated as one of the smaller individual programmatic elements that provide the overall cohesive protection scheme. These larger efforts are treated in the same way as other Milestone 8 programmatic activities, such as developing an Ongoing Monitoring capability or implementing supply chain protections. Because they are considerable efforts, they need to be conducted and treated as individual scoped, staffed, and funded projects because of their complexity and oversight requirements. However, this does not mean that they should be conducted in a vacuum, isolated from the remainder of the cyber security program implementation project because the documentation and processes developed will flow into other aspects of the overall program implementation.

THE CYBER SECURITY IMPLEMENTATION ROADMAP

AREVA NP has developed an International NRC Cyber Security Implementation Roadmap and has begun to implement it at various international utilities throughout the world. Utilities in Japan and South Korea are currently implementing the Roadmap and working toward full implementation of a cyber security program. The Roadmap was developed from AREVA NP's extensive OE implementing all phases of Milestones 1-8 within the U.S. since 2008, AREVA NP has worked with over 20 nuclear power plant operators and over 50 nuclear reactor sites in the U.S. (Figure 2).

The AREVA International NRC Cyber Security Implementation Roadmap consists of six discrete swim lanes as

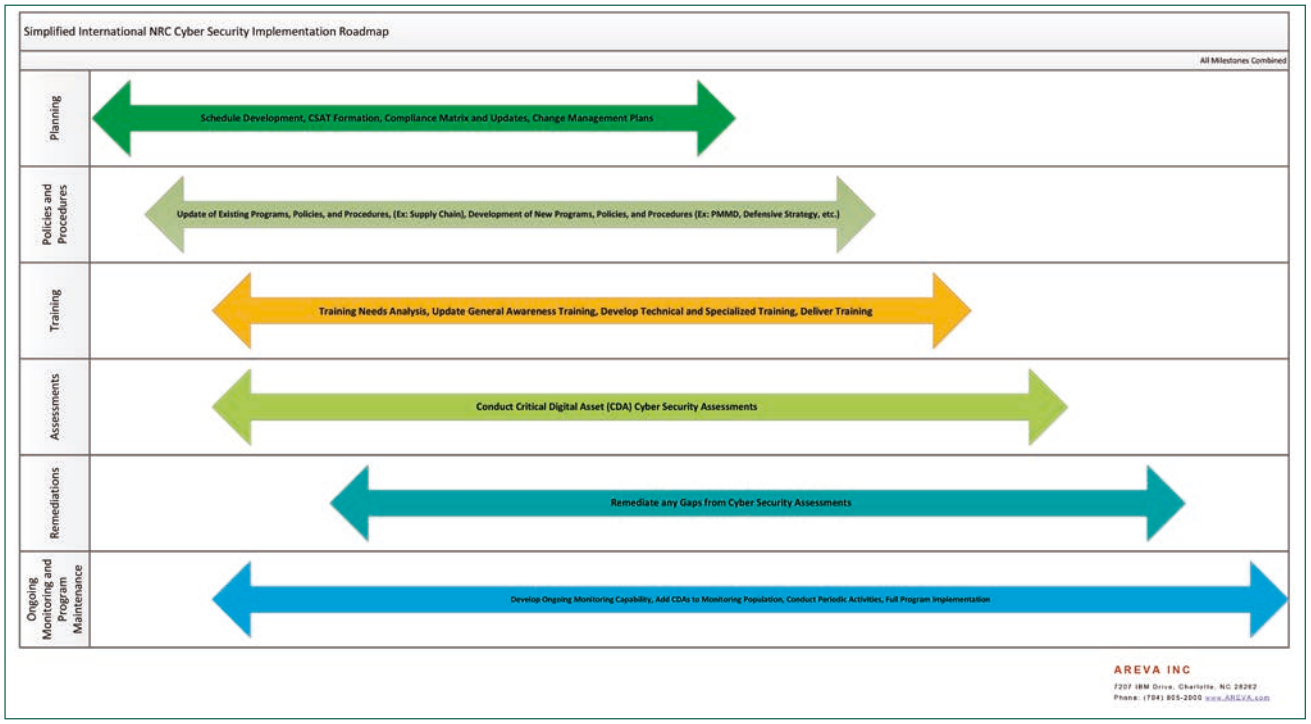

Figure 2.

seen in the figure. Each swim lane is a major implementation area and contains multiple tasks. In order to ensure that cyber security program implementation will start successfully, the planning swim lane is started by developing an overall project schedule to track all of the program implementation tasks. Because the program is built from many smaller sub-programs that all work together to provide overall protection, there are many different elements being implemented and developed in parallel. As previously noted, the CSAT is a critical predecessor that must be formed and qualified prior to many other activities' completion. In addition, a compliance matrix is developed against the regulatory requirements to ensure that the project schedule is populated with all known tasks and durations. Gaps are identified and fed back into the schedule to ensure that gap remediation can be properly tracked to completion. Once the schedule is completed, it can be resource loaded to determine the correct number of employees needed for each stage of implementation.

It is important that the project plan and project schedule be used to kick off other swim lane tasks. Many tasks in other swim lanes are dependent on the completion of the compliance matrix in order to determine if gaps exists in implementing regulatory commitments. In the beginning of the cyber security program implementation, it is expected that many gaps would be identified. Over time as gap remediation occurs, the compliance matrix is regularly updated. By the end of the cyber security implementation project as it is being transitioned to a living, ongoing program, there will be no gaps within the compliance matrix.

Robust change management plans are developed within the planning phase and can be updated throughout the cyber security program implementation. These plans are important to aid in the transition of an implementation project to a living, ongoing cyber security program. The plans aid in gaining the stakeholder ownership within various nuclear power plant departments. In order for these organizations to take an active role in the implementation of the program with respect to their responsibilities, such as developing the procedures for the tasks, training on the tasks, providing input, etc., a change management plan is used to effectively document the specific changes to responsibilities when the transition to the ongoing program is completed. Early involvement through the implementation lifecycle gives stakeholders a sense of ownership and will help accomplish successful results.

The five remaining swim lanes are major elements of the overall cyber security program implementation project. These are:

- Policy and Procedure Development,
- Training,
- CDA Assessments,
- CDA Assessment Remediations, and
- Ongoing Monitoring and Program Maintenance.

All of the remaining swim lane tasks kick off after the Planning swim lane has begun. The remediations from the gap analysis performed on the compliance matrix will generally require an update to existing nuclear power plant policies and procedures. The policies and procedures are first imported from the existing nuclear power plants processes. Policies and procedures that are updated or developed as part of compliance matrix gap analysis are typically validated by the stakeholders to ensure that they contain the necessary steps or instruction to implement the intended regulatory requirements. Because many of the milestone activities have been collapsed into the overall cyber security program implementation effort, there are gains in efficiencies of time, money, and resources. These activities are completed prior to the start of other swim lanes because many of their activities require policies and procedures to be in place and approved. While the description of this swim lane may seem like there are not many tasks for completion, the number of programs, policies, and procedures that are required to be developed and/or updated is quite significant. The gap analysis of the compliance matrix will drive this effort and the magnitude of some of the programs that are required can be large. AREVA NP's OE and lessons learned has indicated that this effort is typically underestimated by nuclear power plant operators during the implementation process. Again, the CSAT will have an active role in reviewing and approving cyber security program-related procedures and policies. Following the procedure and policy updates or development is training.

The training swim lane is important because it involves development of cyber security training for the nuclear power plant personnel. The training stakeholders at the nuclear power plant are broken into three populations:

1. All employees,
2. Personnel interacting with CDAs, and
3. Personnel implementing the cyber security program.

The NRC regulatory commitment describes three levels of training, one for each type of stakeholder mentioned above: General Awareness, Technical, and Specialized training. A training needs analysis is performed for each level of training to determine which stakeholders are in the population of each training type. In addition to the nuclear power plant employees, other populations of stakeholders commonly identified in the training needs analysis include supplemental staff, vendors, and visitors. Policies and procedures that are updated or developed in the previous swim lane are typically an input to the training modules. Stakeholders in these populations must be trained on the update or new processes in order to perform the required actions as expected. Training module development and delivery technique must follow the nuclear power plant operator's internal processes and typically the nuclear power industry's expectations.

One of the largest efforts in the implementation of the cyber security program is conducting CDA cyber security assessments and remediating any gaps discovered during this process (see the Assessments and Remediations swim lanes in the figure). There are many complex steps and activities involved with this effort and success is dependent on the thoroughness of the governing procedures and CSAT involvement in their development and approval. From AREVA NP's OE and lessons learned, the potential for rework is high when each serial predecessor activity in the swim lane is not adequately performed. For example, the first step in the assessment process is to determine the CDAs within each critical system. From that activity, a CDA list is generated and initial grouping lists are developed for pre-planning of the CDA cyber security assessments. If the CDA determination, CDA list, or CDA groups are inaccurate, the

potential for rework on the CDA cyber security assessments is high.

By completing many procedures and developing (or in process of development in parallel) many of the cyber security programmatic elements prior to completing the CDA assessments, some gaps and remediations can be avoided. For other gaps that are identified, specific remediation actions are identified and approved by the CSAT. The remediations are typically tracked to closure through the nuclear power plant's corrective action program. Some remediations may take significant time to close. CDA cyber security assessments can be approved by the CSAT with gaps and pending remediation actions that are being tracked to closure.

The final swim lane is Ongoing Monitoring and Program Maintenance. This swim lane has activities that are either very long duration or periodically recurring in nature. The development of a network monitoring capability is contained within this swim lane. It involves potentially modifying the nuclear power plant's control systems and monitoring networks to add capabilities to remotely manage the devices (by employing centralized whitelisting, centralized antivirus, centralized patching/updates, etc.), performing cyber hardening activities, installing centralized log analysis devices (Security Information and Event Management appliances), performing final network segregation activities, etc. These tasks require major nuclear power plant modifications and the need for adequate documentation and configuration information is significant. Therefore, these activities are long in duration. During the installation and configuration of the hardware, CDAs will be added to the population where these technologies can provide an additional layer of cyber security protection and monitoring.

Additionally, periodic monitoring activities are performed within this swim lane. Some activities include vulnerability scanning, discovery of rogue devices and wireless access points, routine password changes, authentication key updates, etc.

Finally, nearing completion of the implementation of all programmatic elements contained within the swim lanes, one of the final activities recommended by AREVA NP is to complete a 3rd party readiness review. The readiness review ensures that the implementation of the cyber security program has met the intent of the regulatory requirements and no gaps remain prior to transition to a full cyber security program.

CONCLUSION

AREVA NP's significant U.S. and international experience implementing cyber security programs in the nuclear industry has paved the way for capture and sharing opportunities of OE and lessons learned. AREVA NP has implemented all phases of cyber security programs in a majority of the nuclear power plants in the U.S. (over 20 utilities and over 50 nuclear reactor sites) as well as multiple international utilities. By being a trusted partner of international nuclear power plant operators, AREVA NP has developed a Cyber Security Implementation Roadmap that has proven a time savings of up to 40% and a cost savings averaging 25% from the traditional U.S. implementation. The Roadmap gains its efficiencies by combining efforts and activities into discrete swim lanes to maximize the effort toward common activities and to stream line the implementation by performing as many activities in parallel as possible.

AREVA NP's approach of active nuclear industry involvement and work with many different customers worldwide allows for the application of OE and lessons learned from many different implementations. These can be molded into a specific and customized solution that meets the need of nuclear power plant operators. While AREVA NP's Roadmap was designed with the NRC's cyber security programmatic approach, other international cyber security standards, such as IAEA Nuclear Security Series 17 or ISO 27000 series can easily be adapted and integrated into the Roadmap for a hybrid approach. Hybrid approaches have been demonstrated and are actively being implemented using the IAEA Nuclear Security Series 17 framework with the NRC's implementation guidance. No matter the approach taken, the swim lanes used to streamline the cyber security program implementation effort provide the efficiencies to minimize resources while maximizing productivity. ■