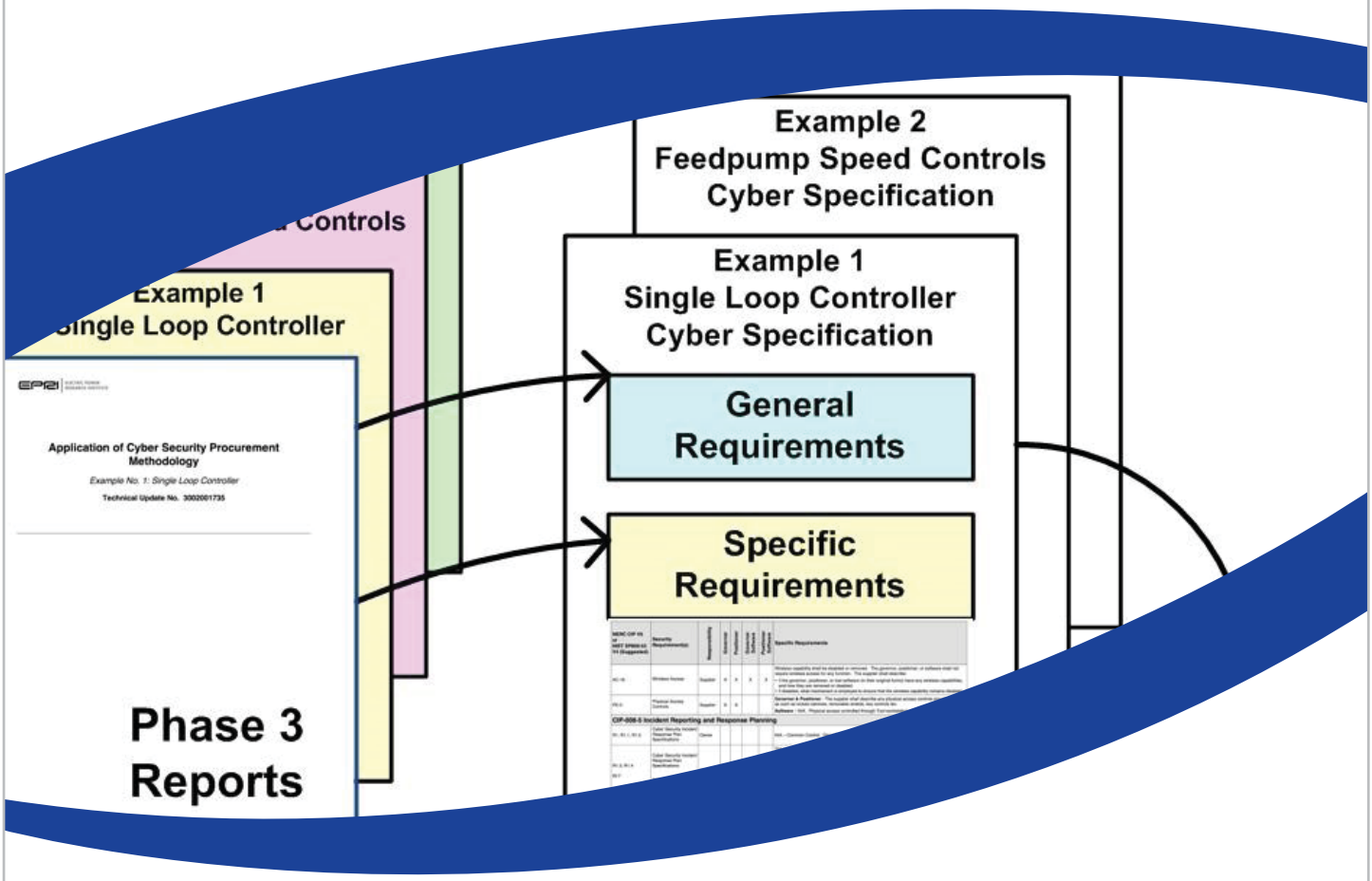
EPRI | ELECTRIC POWER RESEARCH INSTITUTE

2014 TECHNICAL REPORT

Cyber Security Procurement Methodology

Application Pilots: Lessons Learned



Cyber Security Procurement Methodology

Application Pilots: Lessons Learned

3002003255

Final Report, December 2014

EPRI Project Manager
M. Gibson

All or a portion of the requirements of the EPRI Nuclear Quality Assurance Program apply to this product.

YES  NO

ELECTRIC POWER RESEARCH INSTITUTE
3420 Hillview Avenue, Palo Alto, California 94304-1338 ▪ PO Box 10412, Palo Alto, California 94303-0813 ▪ USA
800.313.3774 ▪ 650.855.2121 ▪ askepri@epri.com ▪ www.epri.com

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS DOCUMENT WAS PREPARED BY THE ORGANIZATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED OR COSPONSORED BY THE ELECTRIC POWER RESEARCH INSTITUTE, INC. (EPRI). NEITHER EPRI, ANY MEMBER OF EPRI, ANY COSPONSOR, THE ORGANIZATION(S) BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM:

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS DOCUMENT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF EPRI OR ANY EPRI REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS DOCUMENT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS DOCUMENT.

REFERENCE HEREIN TO ANY SPECIFIC COMMERCIAL PRODUCT, PROCESS, OR SERVICE BY ITS TRADE NAME, TRADEMARK, MANUFACTURER, OR OTHERWISE, DOES NOT NECESSARILY CONSTITUTE OR IMPLY ITS ENDORSEMENT, RECOMMENDATION, OR FAVORING BY EPRI.

THE FOLLOWING ORGANIZATION, UNDER CONTRACT TO EPRI, PREPARED THIS REPORT:

Southern Engineering Services, Inc.

THE TECHNICAL CONTENTS OF THIS PRODUCT WERE **NOT** PREPARED IN ACCORDANCE WITH THE EPRI QUALITY PROGRAM MANUAL THAT FULFILLS THE REQUIREMENTS OF 10 CFR 50, APPENDIX B. THIS PRODUCT IS **NOT** SUBJECT TO THE REQUIREMENTS OF 10 CFR PART 21.

NOTE

For further information about EPRI, call the EPRI Customer Assistance Center at 800.313.3774 or e-mail askepri@epri.com.

ACKNOWLEDGMENTS

The following organization, under contract to the Electric Power Research Institute (EPRI), prepared this report:

Southern Engineering Services, Inc. (SES)
331 Allendale Drive
Canton, GA 30115

Principal Investigator
Brad Geddes

This report describes research sponsored by EPRI.

EPRI would like to express its appreciation to all members of the Cyber Security Technical Advisory Committee and to those individuals and organizations that agreed to participate in the pilots.

Brad Yeates	Southern Company
Scott Junkin	Southern Company
Mark Friedman	Southern Company
Jan Geib	SCANA
Walter Bishop	SCANA
Michael Hagen	Emerson Process Management
Steve Hagen	Emerson Process Management
Paul Hunton	Duke Energy
Jason Watts	Duke Energy
Sarosh Muncherji	Honeywell
John Connelly	Exelon
Syed Jaffery	Exelon
Hrach Minassian	Exelon
Jeff Eckdhal	Exelon
Michael Leahy	Exelon
Laura Farrell	Exelon
William Kurth	Exelon

This publication is a corporate document that should be cited in the literature in the following manner:

Cyber Security Procurement Methodology: Application Pilots: Lessons Learned. EPRI, Palo Alto, CA: 2014. 3002003255.

PRODUCT DESCRIPTION

This report describes the lessons learned and recommendations from a series of cyber security procurement pilot applications involving nuclear utilities and a controls vendor that were part of Phase 4 of a multiphase project to develop an effective cyber security procurement methodology. In order to further this research and encourage technology transfer of the Methodology, EPRI partnered with selected utilities and vendors to use the Cyber Security Procurement Methodology Revision 1 and Use Cases within their supply chain for selected pilot projects. The EPRI team worked with the utility members, and vendors to harvest the lessons learned contained in this EPRI technical report.

Background

Applying cyber security requirements for new instrumentation and control (I&C) systems in the procurement phase requires cyber security experts, I&C engineers, and procurement organizations to work together with vendors to implement and maintain cyber security controls. *Lack of proper cyber requirements and/or division of responsibilities between the utility and vendor can often result in a costly back-fit to meet the requirements.*

The Electric Power Research Institute (EPRI) has researched and developed procurement guidance to address this problem. This research has shown that generic cyber security control requirements within procurement specifications cannot effectively address the multitude of equipment types, vendors, and use cases that exist. Therefore, a methodology has been developed for determining the appropriate cyber security requirements based on specific equipment criteria and an examination of the device attack surface.

Phase 1 was a benchmarking study prior to proceeding with any new guidance. Phase 2 developed a methodology for procuring digital I&C systems with the necessary cyber security controls. Phase 3 applied the Methodology (revised in December 2013) for procuring digital I&C systems through worked examples developed in Phase 2 based on typical Use Cases. Lastly, Phase 4 developed computer based training modules and conducted workshops and mentoring sessions with EPRI utility members to pilot the Methodology. Those pilots are the subject of this technical report.

Objectives

Three objectives were identified for the project.

Objective 1

Identify and select an appropriate set of actionable pilot projects within the volunteer utility and vendor participants that can most effectively illustrate Use Cases of low and medium complexity, with a high complexity Use Case pilot as an optional objective.

Objective 2

Ensure that the pilot projects utilize the Methodology to the maximum extent possible via mentoring and coaching of the utility and vendor staff executing the Methodology throughout the procurement cycle.

Objective 3

Capture and publish the lessons learned from the pilot projects in order to validate the effectiveness and efficacy of the EPRI Cyber Security Methodology. Evaluate the potential to report the Methodology and examples based on lessons learned.

Approach

These pilots were conducted in the form of workshops, interviews, and mentoring sessions that sought to develop cyber security procurement requirements using the current EPRI Cyber Security Procurement Methodology [1], and table top applications examples [2] [3] [4] of the which cover Use Cases of low, medium, and high complexity. Lessons learned and recommendation were developed from observations and interviews during workshops. The companion Computer Based Training (CBT) [6] for the EPRI Cyber Security Procurement Methodology was used as part of the mentoring as training prior to the pilot workshops.

The project concentrated on pilot projects at the low and medium complexity level because these have the most implementation uncertainty and require the most analysis to match the appropriate requirements to the specific level of complexity. However, one high complexity project was available, providing valuable feedback from both the utility and the vendor, and is included in the report.

Results

Research results are presented in Section 2 as a short summary of each pilot from a methodology perspective. Section 3 contains the lessons learned, conclusions, and recommendations. A template spreadsheet, based on the pilot workshop experiences, for capturing the applicable cyber security control requirements, supplier responses, and evaluation is included as an MS Excel form as an external Attachment A to the report. Appendix A contains a sample of the template spreadsheet.

Applications, Value, and Use

The utility user can leverage this technical report to better understand how to effectively use the Cyber Security Application Methodology Rev 1 by informing the planning stages prior to integration of the Methodology into the local or corporate procurement procedures and processes. As a form of Operational Experience, this report can help avoid the identified circumstances that would hinder full utilization of the Methodology.

Keywords

Critical assets
Critical digital assets
Cyber security guidance
Cyber security methodology
Cyber security procurement
Cyber security standards

CONTENTS

LIST OF FIGURES

1
INTRODUCTION

1.1 Overview

The application pilots involved close interaction and observation of the pilot participants during workshops and interviews. The participants and investigators discussed the observations and lessons learned in near-real time to validate the observations and conclusion as they developed. The following sections describe the pilot scopes, activities, lessons learned, and recommendations.

1.2 Pilot Project Scope

Pilot Selection

The EPRI team conducted teleconferences, screenings, and evaluations to select prospective utilities and vendors and to evaluate their proposed projects for selection, with the goal of establishing a mix of procurement complexity opportunities. Although a number of utilities and vendors had expressed an interest, it was difficult to find volunteers to commit time and resources.

Phone interviews were conducted with six (6) volunteer utility members and one (1) vendor to gather information on their proposed projects, capabilities, and schedules. This process was repeated throughout the project as some projects were stalled and other projects were identified.

The proposed pilot projects were evaluated and six (6) projects were selected for the pilot set based on general fit for schedule, complexity, budget, and utility capability. Based on the final selection in collaboration with EPRI Staff, a schedule was established and an informal memorandum of understanding was put in place with each selected participant for execution of the pilots.

The project results include five (5) low and high complexity pilots. One existing high complexity project that was nearing completion was selected as it provided significant results. One pilot was suspended due to resource constraints, however there were lessons learned from that experience as well. A total of three (3) pilots were completed, and one pilot was started, but was not completed at the time of publication:

1. Digital Valve Controller (DVC) replacement spare(completed)
2. Distributed Control System (DCS) platform Upgrade (completed)
3. Digital Valve Controller (DVC) vendor initiated(suspended)
4. Digital Recorder replacement spare (completed)
5. Digital Recorder analog to digital upgrade(in progress)

Pilot Project Support

The EPRI team created an agenda to coordinate, train, coach and mentor each selected utility and vendor to effectively use the Methodology for the selected procurement activity. The original intent was to conduct a one and ½ day kickoff meeting with targeted training for each selectee at their facility. Following the kickoff meeting the EPRI team provided coaching as needed and periodic phone checks to answer questions, coach, and assess progress.

Following the first two pilot kick-offs the agenda was changed to a two-day workshop with all roles present that included training in the first half day and facilitation of a workshop for the balance of the workshop to create the first draft of the Project Specification and General Specification for the pilot. The workshop revealed that all knowledge roles (I&C engineering, cyber security, procurement) needed to be present and engaged.

Notes were taken from all interactions with the utilities and vendors to serve as data capture for lessons learned and recommendations.

EPRI Report Development

This EPRI technical report summarizes the pilot projects and details the lessons learned, Methodology application recommendations and conclusions, and any refinements to the Methodology. There are three categories for the lessons learned:

1. Technical Knowledge and Translation of Knowledge Domains
2. Organization, Resources, and Existing Processes and Procedures
3. Cyber Security Procurement Methodology Refinements

1.3 Report Organization

Table 1-2 from the Cyber Security Procurement Methodology [1] is included below as a reference when reviewing this report. Where appropriate, the Steps in the Methodology are indicated by (Step X.X). The reader is encouraged to have the Methodology and examples at hand as a reference.

Table 1-2
Basic Methodology Steps

STEP 1 – ALIGNMENT WITH THE CYBER SECURITY PROGRAM	
1.1	Know The Organization and Facility Cyber Security Strategy
1.2	Incorporate Cyber Security into the Existing Processes
1.3	Identify Roles and Responsibilities
STEP 2 – SPECIFICATION DEVELOPMENT	
2.1	Determine the Type of Purchase
2.2	Develop/Clarify the Use Case, Data Flow, and Access Points
2.3	Determine the Security Controls for the Use Case
2.4	Establish Owner/Operator and Supplier Responsibilities
2.5	Develop System/Component Specification based on Security Controls determined to be Supplier Responsibility
STEP 3 – GENERAL CYBER SECUIRTY SPECIFICATION DEVELOPMENT	
3.1	Confirm the Use Case and Data Flow
3.2	Map to the Required Security Controls
3.3	Identify Potential Conflicts
3.4	Identify Negotiable or Optional Security Controls or Configurations
3.5	Identify Possible Design Modifications
3.6	Identify Unused Alternate Features, Functions, and Configurations
3.7	Identify Product or Development Environment Certifications
3.8	Describe the Secure Development Environment
3.9	Consider Additional Supply Chain Considerations
3.10	Field Engineering Services
STEP 4 – EVALUATION, AND INCORPORATION WITH PROCUREMENT PROCEDURES	
4.1	Evaluate Responses and Identify Gaps
4.2	Identify Potential Conflicts
4.3	Identify Compensating Controls
4.4	Analyze Risks and Cost/Benefit
4.5	Cyber Security in Selecting the Supplier
4.6	Perform Oversight of Cyber Security
4.7	Receive the Component or System
4.8	Maintain Configuration Control.

2
PILOT SELECTION AND SUMMARY

This section describes the criteria for selection of the pilot projects and devices, and provides a brief summary of each of the pilot projects from the Methodology perspective. Whenever a step from the Methodology is referenced the step number is shown as (Step X.X).

2.1 Pilot Selection

A goal of the project was to find 3 to 5 projects to serve as pilots. The projects were targeted for procurement of simple devices or existing procurements that used the methodology.

Prior to soliciting participation of member utilities and vendors, criteria for selection of simple digital devices were developed.

- Non-networked, stand-alone application
- Single purpose I&C component, such as a digital valve controller or recorder
- Procured as a stand-alone product, not part of a larger system or procurement

The next item developed was selection criteria for utility or vendor procurement projects. This criteria was intended to insure selection of viable candidates.

- Simple device per the established criteria
- An existing or completed procurement that used the methodology
- Project scheduled for completion in 2014
- Commitment to apply the methodology in the project
- Willingness to assign appropriate resources to the project
- Allow EPRI team to observe the process and provide mentoring where warranted
- Willingness to share lessons learned and results

Once the criteria were established the EPRI project manager solicited member utilities to participate in the project and contacted vendors of simple devices that had expressed interest.

Five (5) pilot projects are summarized and the lessons learned are included in the report.

2.2 Pilot Project Summary

The following is a short summary of the projects that are included in this report. This report does not provide details on the devices and their configuration in the plant. The summary and any details provided are only those required to understand how the methodology could be applied.

One project was started and then stopped due to resource constraints, and another project was started and was unable to reach completion prior to publication of this report. Even though the two projects were not completed at the time of publication, some important insights and lessons learned were gained and are included in the report.

2.2.1 Digital Valve Controller (DVC) Spare

The pilot project was a nuclear plant procurement of a spare digital valve controller (DVC) that did not include purchase of the DVC software that runs on a separate windows Maintenance and Test Equipment (M&TE) laptop. The plant had not previously used the methodology, but recognized the need to bring cyber security into the procurement process.

Characteristics of the procurement project were:

Plant Cyber Security Strategy (Step 1.1)

The DVC, when installed, is a CDA per the plant Cyber Security Plan submitted as part of the plant's commitment to NEI 08-09 Revision 6 [5]. The DVC is subject to the cyber security controls from NEI 08-09.

Type of Purchase (Step 2.1)

Simple catalog replacement item that does not include the associated configuration software.

Use Case, Data Flow, and Access Points (Step 2.2)

Stand-alone DVC with the valve controller mounted on a wall nearby the valve positioner. The separation satisfies certain vibration requirements. Analog input and output signals with no network connectivity and no network (serial or otherwise) connections available on the DVC. The DVC has no local interface or buttons with the exception of a write protect switch.

Configuration and diagnostics data are exchanged via the HART protocol by connecting a HART hand held communicator to the terminals enclosed in the terminal box on the DVC controller. The configuration may be created by the DVC software on workstation or laptop and loaded onto the HART communicator or directly through the HART communicator interface.

Secure Development Environment (Step 3.8)

The General Requirements Specification [1] asked for a description and documentation of the vendor's secure development environment.

Project Status at Time of Publication

The procurement package was completed with additional requirements that were not developed in the workshop. The package was transmitted to the vendor, and the vendor is working to assign appropriate resources to develop a response.

2.2.2 Distributed Control System (DCS) Platform Upgrade

A nuclear fleet owner is upgrading to a common DCS platform to provide the foundation for integrating process control systems and automation software under a single, unified architecture. The project is the procurement and development of a DCS platform to be installed across the fleet. The project is a multi-year, complex, custom development, based on the vendor's existing

DCS platform. The platform is being developed as a highly collaborative development effort with the vendor and owner both contributing resources.

The project began with the recognition that cyber security is an important requirement to be included in the design and development. This project is of interest since the method used to determine the cyber security requirements was developed by the owner/vendor team at the same time that the EPRI methodology was being developed. The two approaches are nearly identical in practical application, and the opportunity to capture lessons learned from this large complex project is highly valuable.

Both the vendor and utility contributed to the lessons learned and provided valuable insight by providing two points of view for the same activities within the project.

Plant Cyber Security Strategy (Step 1.1)

The DCS platform, when installed, is a critical system with multiple CDAs per the plant Cyber Security Plan submitted as part of the owner's commitment to NEI 08-09 Revision 6 [5]. The DCS platform is subject to the cyber security controls from NEI 08-09.

Type of Procurement (Step 2.1)

Highly complex, custom integrated development.

Use Case, Data Flow, and Access Points (Step 2.2)

The DCS platform is a virtualized, distributed system architecture that is intended to integrate with specific applications such as turbine controls. It is a fully integrated and networked system that includes blade servers with virtualized Windows servers and workstations, Linux servers, SQL Server, thin clients, switches, routers, HMIs, controllers, and digital I/O modules that integrate with open fieldbus networks that support multiple communication protocols.

Active Directory manages a domain for the platform that is isolated within a cyber security logical level that has no connectivity outside of the logical level to the corporate business network or the internet. Communication protocols include unicast and multi-cast IP based Ethernet, XML based HMI protocols, as well as additional to the I/O communication protocols.

Security tools are integrated into the platform. Some of the security tools are part of the vendor's offering, such as white listing, and some tools are being purchased and integrated as part of the project, such as intrusion detection. The security tools include firewalls, Anti-Virus (AV), Intrusion Detection Systems (IDS), Security Information Event and Management (SIEM), white listing, Active Directory Account Management, and CISCO Secure Access Control System (ACS).

The project team developed a document for cyber security requirements that are mapped to NEI 08-09 [6] and developed a spreadsheet similar to the cyber security requirements table in Appendix A of the EPRI worked example report [2]. The spreadsheet is expanded to include references to the relevant paragraphs of the technical and cyber security requirements documents as well as a column that describes how the security control is implemented for the given component. The updated spreadsheet template included as Attachment A to this report includes insight gained from this project.

Secure Development Environment (Step 3.8)

As a result of the collaborative development process the vendor built a complete secure development environment based on specifications jointly developed with the owner. While there is not a strict development environment regulatory requirement as with a safety related procurement, the owner recognized the value of requiring a secure development environment. A complete set of requirements and specifications were jointly created. The requirements are complete and were derived from NIST 800-53 [7] and NEI 08-09 [6]

The secure development environment includes defense in depth with a secure physical space with physical security controls and logical boundaries using firewalls. All of the components of a complete cyber security strategy as described in NIST 800-53 were considered and implemented according to a risk based approach similar to the recommendations in NIST 800-53.

The development environment is also designed and managed to meet the requirements of NEI 08-09 Appendix E-11 System and Services Acquisition.

Project Status at Time of Publication

Nearing completion of the Factory Acceptance Test (FAT) and preparing to ship.

2.3 Digital Valve Controller (DVC) – Vendor Initiated

This project is a vendor initiated project to develop standard cyber security responses based on the most likely Use Case for their digital valve controller (DVC). The vendor was struggling with how to respond to poorly written or overly burdensome cyber security requirements and specifications. Specifications they are receiving often include cut and paste portions of NEI 08-09, or reference NEI 08-09 in entirety. The vendor realized that it is a competitive advantage to develop complete responses for an NEI 08-09 or CIP specification based on the most likely Use Cases for their product, and that the methodology could be easily applied to develop a standard response.

Characteristics of the procurement project were:

Plant Cyber Security Strategy (Step 1.1)

The pilot project assumed a nuclear procurement of both the DVC and its associated configuration software. The DVC, when installed, is a CDA per the plant Cyber Security Plan submitted as part of the plant's commitment to NEI 08-09 Revision 6 [5], while the software, when installed, will be on a laptop that is being maintained through the Portable and Mobile Device (PMD) program. The DVC is subject to the cyber security controls from NEI 08-09 and the DVC software subject to plant cyber security controls included in the PMD program.

Type of Purchase (Step 2.1)

Simple catalog replacement item that includes the associated configuration software.

Use Case, Data Flow, and Access Points (Step 2.2)

Stand-alone DVC application. Analog input and output signals with no network connectivity and no network (serial or otherwise) connections available on the DVC. The DVC has no local interface or buttons.

Configuration and diagnostics data are exchanged via the HART protocol by connecting a HART hand held communicator or maintenance laptop via HART modem to the terminals enclosed in the terminal box on the DVC controller. The configuration may be created by the DVC software on the maintenance laptop that is connected via a HART modem, or loaded onto the HART communicator, or directly through the HART communicator interface.

Secure Development Environment (Step 3.8)

The vendor has implemented physical access controls and some cyber security controls within the device development and manufacturing process as part of the corporate security program.

Project Status at Time of Publication

The project was suspended after two attempts by the technical sales team to develop a standard Use Case and specification. The technical sales team quickly realized that they would need more complete technical knowledge of the product, and cyber security knowledge, that reside in a DVC product technical expert and a cyber security expert, in order to apply the methodology. They have to source the cyber security expert from another division within the parent company. Obtaining the time and budget to bring the additional resources together for 2 days proved to be a low priority.

2.4 Digital Recorder Spare

This nuclear plant procurement of a spare digital recorder did not include purchase of the recorder software that runs on a separate windows M&TE laptop. The plant had not previously used the methodology, but recognized the need to bring cyber security into the procurement process.

Characteristics of the procurement project were:

Plant Cyber Security Strategy (Step 1.1)

The recorder, when installed, is a CDA per the plant Cyber Security Plan submitted as part of the plant's commitment to NEI 08-09 Revision 6 [5]. The recorder is subject to the cyber security controls from NEI 08-09.

Type of Purchase (Step 2.1)

Simple catalog replacement item without the associated recorder configuration software.

Use Case, Data Flow, and Access Points (Step 2.2)

Digital recorder for replacement within a main control room panel. There are a variety of optional communication and protocol functions available on the recorder, including an optional set of security functions. The project did not proceed far enough to determine the final Use Case and Data Flow, and which optional functions would be purchased.

Configuration and diagnostics data are exchanged via several available methods depending on the options purchased and Use Case and Data Flow.

Secure Development Environment (Step 3.8)

Not determined.

Project Status at Time of Publication

The project was delayed after two attempts by the procurement engineering team to develop a standard Use Case and specification. The procurement engineering team quickly realized that they would need more complete technical knowledge of the recorder its Use Case within the plant, and cyber security knowledge that reside in an I&C Engineer with the requisite recorder knowledge and a cyber security expert, in order to apply the methodology. Those limited resources were already committed to the CDA assessment project and were not available. The resources became available late in 2014 and an internal workshop was conducted to complete the project requirements cyber security control table. The recorder cyber security control table will be incorporated into a procurement package.

2.5 Digital Recorder Analog to Digital Upgrade

This was an upgrade a digital recorder to replace an analog recorder in the control room that did not include purchase of the recorder software that runs on a separate windows M&TE laptop. The nuclear plant had not previously used the methodology, but recognized the need to bring cyber security into the procurement process.

Characteristics of the procurement project were:

Plant Cyber Security Strategy (Step 1.1)

The recorder, when installed, is a CDA per the plant Cyber Security Plan submitted as part of the plant's commitment to NEI 08-09 Revision 6 [5]. The recorder is subject to the cyber security controls from NEI 08-09.

Type of Purchase (Step 2.1)

Catalog purchase, digital upgrade through an engineering change package.

Use Case, Data Flow, and Access Points (Step 2.2)

Digital recorder for replacement within a main control room panel. There are a variety of optional communication and protocol functions available on the recorder, including an optional set of security functions.

A Compact Flash (CF) memory card, USB interface, Ethernet interface, and RS-232 serial interface were specified. A stand-alone installation in a control room panel with no continuous network connections. 20 analog RTD inputs and 6 analog annunciator outputs for process data. Device history, diagnostics, and configuration can be pulled or loaded via the USB port, CF card, Ethernet connection to an M&TE laptop, or via the serial connection.

The optional security functions were not specified because the recorder is located on a continuously monitored panel in the control room and the owner decided to reduce the access and maintenance requirements by limiting the purchased functions and crediting existing compensating controls for the cyber security features of the optional security package.

Establish the Security Controls for the Use Case (Step 2.3)

The owner has developed a procedure, logic, and a software tool that performs an assessment of the CDA based on the Use Case and Data Flow. The output is in multiple forms. For the workshop a spreadsheet was used to capture the output and list the applicable controls. This was useful and efficient. The spreadsheet was then modified with additional columns in order to complete the remaining steps of the methodology.

Secure Development Environment (Step 3.8)

Not determined.

Project Status at Time of Publication

The two day workshop resulted in a draft project requirements spreadsheet and review of potential general requirements. The owner expects to review and finalize the specifications, and incorporate them into their procurement process by early 2015.

3
SUMMARY OF LESSONS LEARNED AND RECOMMENDATIONS

This section summarizes the lessons learned, conclusions, and recommendations from the pilot projects that are relevant to implementing the methodology and improving EPRI guidance. Any lessons learned that are specific to the participants and contain confidential information are not included. The results are abstracted so that the utility or vendor is not identified and the details of each procurement, device or system are not included.

The lessons learned, conclusions, and recommendations come directly from the pilot projects from both the utilities and vendors.

They are organized by 1) Technical Knowledge and Translation of Knowledge Domains, 2) Organization, Resources, and Existing Processes and Procedures, and 3) EPRI Cyber Security Procurement Methodology [1] Refinements.

3.1 Technical Knowledge and Translation of Knowledge Domains

1. **Thorough knowledge of cyber security is required (Steps 1.3, 2.5).** Just being familiar with the cyber security requirements is insufficient. How to interpret the requirements for practical application, along with knowledge of how existing cyber security controls are applied within the plant is required and is a specialized skill set. Example 1 [2] and the CBT [6] both contain good examples of this.
2. **The development of cyber security control specifications requires knowledge of more than cyber security (Steps 1.3, 2.5).** Without all of the relevant knowledge present while applying the methodology, the process quickly bogged down. It is rare that the various knowledge domains are resident in one or two people. In order to effectively determine how to apply cyber security controls the following knowledge is required:
   - Cyber security controls and how existing cyber security controls are applied within the plant.
   - Existing processes such as Engineering Design/Modification, Configuration Management, and Procurement. (Step 1.2)
   - Device and system Use Case, Data Flow, and Access Points for the intended application within the plant. (Step 2.2)
   - Detailed knowledge of how a device functions, including communication ports and protocols, firmware and software, interfaces, how a device is configured, logging and alerting capability, embedded security features, etc. (Step 2.2)
3. **Existing features and functions that are not specifically designed for cyber security can and should be used for cyber security where applicable (Steps 2.2, 2.5, 3.2, 4.1).** However, the translation of those features and functions to cyber security can be difficult.

An example is alerts and logs that are intended for operations and maintenance such as configuration change and maintenance logs. When the engineer knowledgeable about a device was asked about any cyber security logs, the answer was that there are no cyber security logs. However, when asked what logging and alerting was available, the engineer was able to answer that there are a number of alerts that are stored on the device and can be offloaded to a file external to the device. In fact, one alert that was "logged" was when the write protect switch position was changed that would be a useful cyber security event.

Understanding the logging capabilities, whether or not they are considered cyber security logs is particularly useful for determining if and how to apply the security controls from D 2.2 Auditable Events, D 2.3 Content of Audit Records, and D 2.4 Audit Storage Capacity.

Many cyber security experts are coming into generation from IT or other domain backgrounds and do not yet have the I&C knowledge that is needed and the I&C engineers do not yet have the cyber security knowledge that is needed. **The cyber security specialist and the device expert need to learn how to translate between the knowledge domains.**

4. **The application of the methodology flows quicker with familiarity and with knowledgeable resources involved (Steps 2, 3).** Even for the first time using the methodology the process moved more quickly toward the end of the pilot than at the beginning. That said, developing meaningful specifications could be time consuming for the first few iterations. See also 3.2.8. Each pilot, including the vendor initiated pilot, demonstrated that at this point in the maturity of the industry, the lack of cyber security training, knowledge, experience, and resources makes the process more difficult.

   As the industry matures, it is expected that the process will become easier and less time consuming, particularly once the vendors are able to fully document and communicate how their product features and functions meet the cyber security requirements.

   The project evaluated the problem and the methodology in light of this information to determine if the methodology could be modified to make the process less difficult and time consuming. Some improvements to the methodology were identified (see Section 3.3). The process will be streamlined through repetition for the same or similar devices and systems, **however the initial specification development requires the level of effort and knowledge as described in the methodology**.

5. **Introduction of cyber security requirements expands the traditional architectural diagrams to include Data Flows and Access Points (Step 2.2).** Engineering traditionally includes network and communication diagrams in the engineering change package, if the procurement involves an engineering change package. The typical architecture diagrams often do not contain the information needed to determine cyber security requirements. Cyber security requirements resulted in modifying the architectural and communication diagrams to capture the data flow and access point details required to apply the methodology.

6. **As discussed in Step 3.8 of the methodology, most vendors have implemented some level of security within their development environments, but do not think of the development environment as meeting a customer cyber security requirement (Step 3.8).** And in some cases, will reply that no specific secure development environment exists, or that the development environment is confidential and proprietary and cannot be shared.

   There are some exceptions. In discussions with participating owners and vendors, it was discovered that some nuclear vendors are building secure development environments as a result of nuclear requirements, or on a project basis as a result of large project requirements. These vendors are prepared to respond to requirements specifications and have supporting documentation.

7. **The Methodology can be applied by vendors to develop standard responses to cyber security specifications (Steps 2, 3).** The vendors know the most likely Use Cases for their products and can develop standard specifications and responses using the methodology. However, the vendors face the same resource availability and training constraints as the owners.

8. **A face to face workshop over two days with all roles present, greatly facilitates development of the specifications (Steps 2, 3).** Learning the methodology and how to apply it requires some training, practice, and involves multiple roles. Working through the methodology as a team for the first few times speeds up the process and establishes a dialog within the team to speed up the process in the future.

9. **Limiting product options that are purchased to only those required, may reduce the number of cyber security controls that apply, and reduce the level of effort to apply the methodology (Steps 2.1, 2.2).** It was revealed, particularly for the replacement devices, that the engineering and procurement teams wanted to purchase many or all available options for the device, "in case we need the capability in the future*"*. ***Some of these options expand the attack surface and introduce additional attack vectors***. For example, the recorder can be purchased with optional RS232 or RS485 serial ports with PROFIBUS capability that is not used in the current plant architecture. It may be more efficient to develop technical and cyber specifications concurrently.

10. **Certain configurations and tasks that are low level, disruptive, and time consuming should be locked down in early iterations of the design (Steps 2.1, 2.2).** For example, the hardware chassis and physical communication ports required. This is particularly important for more complex custom design and integration projects.

11. **Use of existing processes and tools can complement the methodology (Steps 1, 2, 4).** Approaches to analyzing assets and determining how to protect them parallel the same activities as described in the methodology. An example is the assessment tool used in the recorder digital upgrade pilot. The owner developed a procedure and software tool to determine the applicable controls for an asset and how the Cyber Security Control Implementation Strategy (SCIS) from NEI 10-09 [8] applies to an asset. The tool was applied while executing **Step 2.3**. The process was effective and saved several hours of effort to walk through the controls manually.

3.2 Organization, Resources, and Existing Processes and Procedures

1. **Cyber Security Assessment Team (CSAT) maturity and availability are an issue that requires "overhead" to educate and obtain resources (Step 1).** Similar to 3.1.1 and 3.1.2. The resources in both cyber security and engineering that have the experience and skills to apply the methodology are limited and are committed to the initial assessment of the existing plant assets. Making these resources available or to train new resources to apply the methodology requires management to make some decisions about priority. It is anticipated that this constraint will ease as the industry assigns more trained resources, and gains experience.
2. **Cyber security is not a "bolt on" (Step 1.2).** Similar to 3.1.9. Cyber security should be included as an integral part of every component and process. This is a significant lesson learned from the DCS project, however it also became apparent in each of the other pilots.
3. **The knowledge required to apply the methodology resides in multiple individuals with different roles (Step 1.3).** When working through the Use Case (Step 2.2), owner versus supplier responsibilities (Step 2.4), and the specific requirements (Steps 2.3, 2.5), if became apparent that all of the roles need to be present and engaged in a meeting room in a highly collaborative approach. Several participants attempted to work through these steps in a linear manner without all the roles present, and within a few hours realized that no progress was made and stopped the process. Similar to 3.1.1 and 3.1.2.
4. **Resource availability is a constraint (Step 1.3, Step 2).** Particularly I&C engineers and cyber security experts. With the increased use of I&C digital devices and systems that include cyber security, coupled with budget constraints, there is a shortage of qualified resources within each organization. The participating owners and vendors are in the process of implementing cyber security and have already committed the limited resources to existing projects. In all of the pilots with the exception of the large DCS procurement, the process was significantly delayed or postponed due to resource constraints.
5. **Existing Procurement and Engineering Procedures need to be modified (Step 1.2).** Although procedures exist for all aspects of the engineering modification and procurement process, the steps in the methodology need to be incorporated. The pilots were delayed while the various departments involved determined how to modify existing procedures to accommodate cyber security. In particular, incorporating the language for the General Cyber Security Specification (Step 3) and the language from the Project Specification (Step 2). Although the example Specifications provide sample language, the language needs to be reviewed and modified to fit within the existing programs and procedures. Similar to 3.2.2.
6. **Owners and Vendors have not yet developed processes and procedures for developing cyber security requirements, specifications, and responses (Step 2, 3, 4).** Several examples of procedures, requirements, and specifications that were developed without the methodology were either 1) too high level and incomplete, 2) copied directly from NEI 08-09 or, 3) simply referenced NEI 08-09. Step 2.5 describes how to take the Use Case, Data Flow, and Supplier responsibility and translate those into meaningful specifications and requirements based on the original NEI 08-09 or CIP requirements.

7. **Early use of the attack surface analysis buy the application of established device/system criteria can rapidly converge the methodology to the remaining controls of interest (Step 2.2.3.1).** The use of existing plant SCIS or other general criteria that identifies interfaces, data flows, user functions, etc. that define the attack surface can allow a large number of controls to be eliminated by demonstrating that a vulnerability does not exist.
8. **Cyber Security was not brought in at the detail level early enough in the process (Step 2.2, 2.5).** Attempts to utilize information from the cyber security assessments showed that some assessments did not include enough detail. This resulted in rework to discover the level of detail necessary. Examples include determining auditable events and what profiles exist for attack vectors.
9. **5% to 10% additional time (level of effort) was required in the DCS project for cyber specification mapping and development (All Steps).** The DCS project attempted to capture the level of effort to incorporate cyber security into the entire process. They estimate that an additional 5% to 10% level of effort is required to incorporate cyber security.
10. **A complete cyber security specification (in addition to the table of controls), that included a documented basis, helped to justify design/purchase decisions to management and leads to consistent implementation (Steps 2, 3).** The DCS project developed a thorough and complete technical requirements document for both the network and the DCS platform, as well as a cyber security requirements document. These documents greatly facilitated communication with the vendor and management and helped to justify design and purchase decisions.
11. **Procurement and Procurement Engineering are not the correct organization to apply the methodology (Step 1.3)** unless they are assigned the appropriately trained resources. Because the pilots were associated with procurement several of the owners assigned procurement and procurement engineering resources to the pilot. Procurement and procurement engineering do not have the training and experience that is required. Their experience is more relevant for the general specification, but will still require cyber security expertise to complete the general specification. Procurement expertise is required to incorporate the process and results into the procurement process.
12. **Resources for procurement of replacement components that are not part of an Engineering Change package needs to be addressed (Step 1.3).** Procurement of replacement components is typically performed by procurement and procurement engineering without the involvement of engineering or cyber security. If a standard cyber security specification has not been prepared for a like component, resources will have to be assigned to create the cyber security specifications.
13. **Involve the supplier (Steps 2, 4).** Because detailed knowledge of the asset is required in order to determine how to protect the asset, the supplier technical and cyber security resources can be an effective extension of the owner's resources. During the DVC pilot a dialog was established with vendor to answer some questions about firmware and software revisions and how alarms and events are logged. The vendor responses were appropriate and helpful.

14. **Allow time for the initial application of the methodology (All Steps).** Allow time for allocation of resources, training, revision of standard procedures and documents, and fact finding and communication with the supplier. Anticipate difficulties to ensure that the procurement does not interfere with other activities such as outage planning. This upfront effort will save time over the long run once a procurement specification is developed it can be used and or slightly altered for future procurements of like equipment.

3.3 Cyber Security Procurement Methodology [1]

1. **Consider producing another revision to the methodology (and examples) to incorporate lessons learned once the pilot projects are complete (All Steps).**
2. **Revise the methodology to describe how to look for and utilize non-cyber security device features and functions for cyber security (Steps 2.5, 3.4).** As described in 3.1.3.
3. **Add a column to the cyber security control table (Step 2.5, 4.3, 4.5) to include how the control is actually implemented including any compensating controls or exceptions to the plant cyber security strategy.** The DCS project spreadsheet added several columns that described both how the control was implemented and referenced the applicable paragraphs from the technical and cyber security requirements documents.
4. **Add a column to the cyber security controls specification table to describe how a cyber security control can be tested per NEI 08-09 E3.6 "Security Function Validation" (Step 2.5).** Likely that the method to test will be determined jointly between the vendor and the owner during finalization of the specification (Step 4.5).
5. **Revise Example 1 [2] to replace the Single Loop Controller (SLC) with a Digital Valve Controller (DVC) and revise the Project Specification to make the example more realistic (All Steps).** A revision to example 1 was published during the project. *Application of Cyber Security Procurement Methodology, Example 1: Digital Valve Controller,* Product ID 3002003257 [2] is referenced in this report.
6. **Revise methodology to discuss influence of cyber security on technical design and specifications to reduce the number of optional technical features (Steps 1.2, 2.1, 2.2).** See 3.1.9.

3.4 Overall Conclusion

The Cyber Security Procurement Methodology [1] is an effective approach assuming that certain conditions are in place when executing the methodology:

- Appropriately trained resources are available and engaged, including asset technical knowledge, cyber security, and procurement.
- The team has detailed knowledge of how the plant cyber security strategy is applied to assets of a similar type.
- Detailed technical information is known about the asset including items such as event/alert types and behavior of events/alerts, and communication protocols and ports.
- Procurement is prepared to determine how to modify existing procurement processes to incorporate aspects of the methodology.

4
REFERENCES AND BIBLIOGRAPHIES

4.1 References

1. *Cyber Security Procurement Methodology Revision 1* EPRI, Palo Alto, CA:2013 3002001824
2. *Application of Cyber Security Procurement Methodology, Example 1: Digital Valve Controller.* EPRI, Palo Alto, CA:2014. 3002003257
3. *Application of Cyber Security Procurement Methodology, Example 2: Feedpump Turbine Speed Control.* EPRI, Palo Alto, CA:2013. 3002001823
4. *Application of Cyber Security Procurement Methodology, Example 3: Digital Feedwater Control.* EPRI, Palo Alto, CA:2013. 3002002069
5. NEI 08-09, *"Cyber Security Plan for Nuclear Power Reactors"* Revision 6.
6. *Cyber Security Procurement Methodology Training Module Rev. 14.00.* EPRI Palo Alto, CA:2014, 3002002499
7. NIST SP 800-53 Revision 4, *"Security and Privacy Controls for Federal Information Systems and Organizations".*
8. NEI 13-10 Revision 0, *"Addressing Cyber Security Controls for Nuclear Power Reactors".*

4.2 Definitions and Acronyms

4.2.1 Definitions

access points: The points within the data topology and data flow where a user could feasibly access the critical data.

attack surface: The sum of all the software and hardware interface points that provide pathways for a cyber attack. These can be physical and logical interfaces and protocol connection points, as well as internal software structures that provide an executable code surface to attack.

attack vector: The channel, mechanism, means, or mode that can be exploited to conduct an attack or to circumvent the security environment and system cyber security controls of a computer, digital device, or network.

compensating control: A technical, operational, or management cyber security control employed by an organization in lieu of a required or recommended cyber security control that provides an equivalent or better level of protection for a critical asset.

component type: An I&C digital component or group of components that has similar use cases and data flows for which a common set of cyber security controls may be applied.

critical asset: A digital component of a critical system or infrastructure that, if compromised, represents a risk.

In this report, *critical asset* is interpreted to mean critical digital assets (CDA), critical cyber assets, or critical assets that are defined in various ways according to the governing standard and the buyer's cyber security policies and procedures. This report does **not** provide guidance for how a critical asset is identified. The report assumes that the buyer has a method for identifying a critical asset and that the standard or guidance listed applies to the identified critical assets.

critical data: The digital information that is contained within a critical asset and that, if compromised by a malicious attack, could affect the performance of the critical asset.

Critical data includes digital information beyond just the process data. Examples of critical data are:

- Process control data such as process variables
- Set Point data
- Tuning data
- Firmware
- Application software and operating system software and all associated files
- Security software and all associated files
- Files that contain data such as data tables, configuration, numbers, logs, security information, etc.
- Database tables and associated database files
- Network or transmission protocol data
- Test equipment files and information that could be connected to the critical asset
- Macros, formulas, and calculations whose resultant data are used as design input or to directly control plant equipment

data flow: The direction, path, method, and state (in transit or at rest) of the critical data as it flows through the data topology.

data topology: A logical and physical network, usually depicted in the form of a diagram, of the paths and connectivity with various devices and networks for the critical data.

development asset: A digital device or system that is used for the development, testing, monitoring, or maintenance of I&C components or a systems in which the I&C components or systems are intended for use as a critical asset by the facility owner/operator.

In some cases, development assets are used for monitoring or maintenance in the operational environment for troubleshooting. For example, consider a PC in a supplier's development environment that is used to configure the data in a controller that is being purchased by an owner/operator. The controller will become a critical asset when installed on site and will be

protected according to the owner/operator's policies and procedures. However, the supplier's configuration PC is never installed on site, but can be compromised by a cyber attack and, therefore, compromise the data on the controller prior to shipping; it is therefore a development asset that must be protected for nuclear safety systems and in other cases in accordance with the supplier's policies and procedures or as specified by the owner/operator.

factory acceptance test: The factory acceptance test (FAT) is necessary to verify that all features and functions, including security features, function properly and provide the expected levels of functionality. In general, prior to initiation of each FAT, the supplier shall install all operating systems and application patches, service packs, or other updates certified for use with the provided system by the time of test, and documentation of the configuration baseline. FAT is a process, not an event, and could in fact extend over several weeks or months [5].

instrumentation and control (I&C) systems: Supervisory control and data acquisition (SCADA) system, process control system (PCS), distributed control system (DCS), and industrial control system (ICS) generally refer to the systems that control, monitor, and manage the nation's critical infrastructures such as electric power generators, subway systems, dams, telecommunication systems, and natural gas pipelines. Simply stated, a control system gathers information and then performs a function based on established parameters and/or information received.

management cyber security controls: Management controls are cyber security controls that focus on the management of risk and the management of CDA security. Examples of management cyber security controls include the system and services acquisition cyber security controls.

Methodology: When used as a capitalized noun in this report, refers to the methodology published in EPRI report 3002001824, *Cyber Security Procurement Methodology, Rev. 1* [1].

operational cyber security controls: Operational cyber security controls are primarily implemented and executed by people (as opposed to systems). Examples of operational controls include cyber security awareness and training and the configuration management cyber security controls.

secure development and operational environment (SDOE): *Secure development environment* is defined as the condition of having appropriate physical, logical, and programmatic controls during the system development phases (that is, concepts, requirements, design, implementation, and testing) to ensure that unwanted, unneeded, and undocumented functionality (such as superfluous code) is not introduced into digital safety systems. *Secure operational environment* is defined as the condition of having appropriate physical, logical, and administrative controls in a facility to ensure that the reliable operation of safety systems is not degraded by undesirable behavior of connected systems and events initiated by inadvertent access to the system. RG 1.152 Revision 3, "*Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,"* defines the requirements for an SDOE for nuclear safety systems.

site acceptance test: The asset owner's site acceptance test (SAT) typically repeats a subset of an FAT after system installation with additional integrated functions. Typically, the SAT is performed before the cutover or commissioning to validate that the site installation is equivalent to the system tested at the factory. Like the FAT, the SAT may extend over several weeks or months and may occur at multiple locations.

system or software development life cycle (SDLC or SDL): Each organization is generally expected to have its own life cycle that is thoughtfully and purposefully created and followed to ensure high quality. Several standards and methodologies are available as references or for use, such as *Handbook for Verification and Validation of Digital Systems* (EPRI TR-103291-R1).

technical cyber security controls: Cyber security controls (that is, safeguards or countermeasures) for a critical asset that are primarily implemented and executed by the critical asset through mechanisms contained in the hardware, software, or firmware components of the asset.

Examples of technical cyber security controls include session lock, and audit storage capacity.

Use Case: A description of the intended functional and logical implementation and configuration of a component and its associated devices and critical data within the context of the facility cyber security strategy. A Use Case identifies, clarifies, and organizes system requirements. The Use Case is made up of a set of possible sequences of interactions between systems and users in a particular environment, related to a particular goal. The Use Case should contain all system activities that have significance to the users or the data flow that must be protected. A Use Case can be thought of as a collection of possible scenarios that are related to a particular goal.

4.2.2 Acronyms and Abbreviations

BES	Bulk Electric System
CA/CDA	critical asset/critical digital asset
CFR	code of federal regulations
CSAT	Cyber Security Assessment Team
DCS	distributed control system
DFW	digital feedwater
DHS	U.S. Department of Homeland Security
DVC	Digital Valve Controller
EPRI	Electric Power Research Institute
FAT	factory acceptance test
HSI	human system interface
HMI	human machine interface
I&C	instrumentation and control
ICS	industrial control system
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization

M&TE	measurement and test equipment
NEI	Nuclear Energy Institute
NERC	North American Electric Reliability Corporation
NERC-CIP	NERC Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
NITSL	Nuclear Information Technology Strategic Leadership
NRC	U.S. Nuclear Regulatory Commission
NSIR	U.S. Nuclear Security and Incident Response
PMD	Portable and Mobile Device
RFI	Request for Information
RFP	Request for Proposal
RFQ	Request for Quote
RG	Regulatory Guide
SAT	site acceptance test
SCIS	Cyber Security Control Implementation Strategy
SDLC/SDL	software development life cycle
SDOE	secure development and operational environment
SIEM	security information and event management
DVC	Digital Valve Controller
SME	subject matter expert
SNTP	simple network time protocol
SP	Special Publication

A
CYBER SECURITY CONTROLS WORKSHEET TEMPLATE SAMPLE

Figure A-1 below is a sample of a cyber security controls worksheet template that is provided as an MS Excel worksheet in Attachment A of the report pdf file. The worksheet includes the columns from the cyber security controls tables in the Methodology and associated examples, as well as additional columns to capture the results of evaluating the supplier responses.

NEI 08-09	Security Control	Responsibility	Device	Device Software	Specific Requirements	Supplier Response	Identified Gaps	Gap Resolution	Control Testing Methods	Final Specification
Technical Controls										
Access Controls										
D1.1	Access Control Policies and Procedures	Owner			Device: N/A Common Control Device Software:	Device: Device Software:				
D1.2	Account Management	Owner			Device: Device Software:	Device: Device Software:				
D1.3	Access Enforcement	Owner			Device: Device Software:	Device: Device Software:				
D1.4	Information Flow Enforcement	Owner			Device: Device Software:	Device: Device Software:				
D1.5	Separation of Duties	Owner			Device: Device Software:	Device: Device Software:				
D1.6	Least Privilege	Owner			Device: Device Software:	Device: Device Software:				
D1.7	Unsuccessful Login Attempts	Owner			Device: Device Software:	Device: Device Software:				
D1.8	System Use Notification	Owner			Device: Device Software:	Device: Device Software:				
D1.9	Previous Login Notification	Owner			Device: Device Software:	Device: Device Software:				
D1.10	Session Lock	Owner			Device: Device Software:	Device: Device Software:				
D1.11	Supervision and Review – Access Control	Owner			Device: Device Software:	Device: Device Software:				
D1.12	Permitted Actions Without Identification or Authentication	Shared			Device: Device Software:	Device: Device Software:				
D1.13	Automated Marking	Owner			Device: Device Software:	Device: Device Software:				
D1.14	Automated Labeling	Owner			Device: Device Software:	Device: Device Software:				
D1.15	Network Access Control	Owner			Device: Device Software:	Device: Device Software:				
D1.16	"Open/Insecure" Protocol Restrictions	Owner			Device: Device Software:	Device: Device Software:				
D1.17	Wireless Access	Owner			Device: Device Software:	Device: Device Software:				
D1.18	Insecure and Rogue Connections	Owner			Device: Device Software:	Device: Device Software:				
D1.19	Access Control for Mobile Devices	Owner			Device: Device Software:	Device: Device Software:				
D1.20	Proprietary Protocol Visibility	Owner			Device: Device Software:	Device: Device Software:				
D1.21	Third-Party Products and Controls	Owner			Device: Device Software:	Device: Device Software:				
D1.22	Use of External Systems	Owner			Device: Device Software:	Device: Device Software:				
D1.23	Public Access Access Restrictions	Owner			Device: Device Software:	Device: Device Software:				
Identification and Authentication										
D4.1	Identification and Authentication Policy and Procedures	Owner			Device: N/A (Common Control) Device Software:	Device: Device Software:				
D4.2	User Identification and Authentication	Owner			Device: Device Software:	Device: Device Software:				

Figure A-1
Sample layout of procurement specification template

Export Control Restrictions

Access to and use of EPRI Intellectual Property is granted with the specific understanding and requirement that responsibility for ensuring full compliance with all applicable U.S. and foreign export laws and regulations is being undertaken by you and your company. This includes an obligation to ensure that any individual receiving access hereunder who is not a U.S. citizen or permanent U.S. resident is permitted access under applicable U.S. and foreign export laws and regulations. In the event you are uncertain whether you or your company may lawfully obtain access to this EPRI Intellectual Property, you acknowledge that it is your obligation to consult with your company's legal counsel to determine whether this access is lawful. Although EPRI may make available on a case-by-case basis an informal assessment of the applicable U.S. export classification for specific EPRI Intellectual Property, you and your company acknowledge that this assessment is solely for informational purposes and not for reliance purposes. You and your company acknowledge that it is still the obligation of you and your company to make your own assessment of the applicable U.S. export classification and ensure compliance accordingly. You and your company understand and acknowledge your obligations to make a prompt report to EPRI and the appropriate authorities regarding any access to or use of EPRI Intellectual Property hereunder that may be in violation of applicable U.S. or foreign export laws or regulations.

The Electric Power Research Institute, Inc. (EPRI, www.epri.com) conducts research and development relating to the generation, delivery and use of electricity for the benefit of the public. An independent, nonprofit organization, EPRI brings together its scientists and engineers as well as experts from academia and industry to help address challenges in electricity, including reliability, efficiency, affordability, health, safety and the environment. EPRI also provides technology, policy and economic analyses to drive long-range research and development planning, and supports research in emerging technologies. EPRI's members represent approximately 90 percent of the electricity generated and delivered in the United States, and international participation extends to more than 30 countries. EPRI's principal offices and laboratories are located in Palo Alto, Calif.; Charlotte, N.C.; Knoxville, Tenn.; and Lenox, Mass.

Together...Shaping the Future of Electricity

Programs:

Nuclear Power

3002003255

Electric Power Research Institute
3420 Hillview Avenue, Palo Alto, California 94304-1338 • PO Box 10412, Palo Alto, California 94303-0813 USA
800.313.3774 • 650.855.2121 • askepri@epri.com • www.epri.com