Cybersecurity Tool Integration Challenges with IEDs in Digital Power Systems

SC, SHAYNE CASAVANT
BBA Engineering Ltd.
Canada

SUMMARY

Deploying and integrating cybersecurity technologies and tools/solutions in an industrial operating environment must be well planned and executed. These deployments are prone to risks such as the disruption/impact to business operations, people, safety, environment, and others. To mitigate these risks, cybersecurity/Digital Power System (DPS) project managers must consider implementing Proof of Concept (PoC) tests in their project execution plans, prior to full scale implementation. The approach is to identify gaps in tool/solution functionality, interoperability issues with Intelligent Electronic Devices (IEDs) or technology enhancements prior to making a purchasing commitment and ultimately the field technology deployments.

A vendor agnostic PoC methodology that is tailored to cybersecurity tool integration in DPSs is presented. Although, there can be similarities with other types of technology integration projects (i.e. IT, enterprise, or corporate), there are distinct differences and challenges when developing an integration strategy for Cybersecurity solutions for DPS, including distributed energy resources (DERs).

Typical cybersecurity tools include, but are not limited to, Universal Security Management (USM) systems, Regulatory compliance management tools, Security information and Event Management (SIEM) tools, Configuration Management tools, Electronic Access & Password Management tools, Patch Management tools, Threat Detection and Monitoring tools, and Vulnerability Assessment tools.

While these cybersecurity tools can offer impressive features and functions, a major challenge can often be linked to device integration limitations and lack of capabilities. This is more prevalent in legacy devices that were not designed with cybersecurity in mind. It is relatively common for IED manufacturers to force users to go through their vendor software (exclusively with no external integration) to perform cybersecurity related functions. Examples include user authentication and permissions, configuration changes, log and events, and backup and restoration. This vendor software restriction forces operators and maintenance personnel to rely on manual intensive tasks that can be time consuming, taking away from higher priority items.

Although the above stated challenges may seem daunting, there are integration strategies and options that can centralize and improve the efficiency of day-to-day operational/maintenance tasks. A balance must be struck between improved features/functions and integration effort. Each operator/owner of its DPSs will have specific needs and requirements and it is important to consider options that are a “right fit” for that operational environment and culture. This could include multiple cybersecurity tools that

Shayne.Casavant@bba.ca

each have a very specific purpose, one centralized tool, a hybrid, or more customized interfaces. There are a plethora of different options and therefore, it is paramount to fully understand the intricacies of cybersecurity tools available on the market and the limitations of device capabilities. This is also critical when undertaking legacy device replacements/upgrades, as certain cybersecurity related features/functions are not necessarily offered in the default builds.

Gaps have been identified in publicly available resources when it comes to cybersecurity tools integration of DPSs. Many IT based guides and playbooks are leveraging parallel production environments without impacting operations as a whole. This approach is not possible with DPS operating environments. Readers will take away unique concepts and will be able to directly apply key strategies to their next cybersecurity tools implementation project for Power Systems.

KEYWORDS

Cybersecurity Tools, Digital Power Systems, IEDs, Integration Challenges, Proof of Concept, PoC

1. INTRODUCTION

Cybersecurity tools and solutions can substantially boost an industrial operating environment's security posture, while providing automation of tasks that were predominantly manual in the past. These improvements are not without their challenges and the integration of cybersecurity tools in Digital Power System (DPS) environments requires strategic planning and careful execution. One approach to help ensure cybersecurity tools are successfully integrated in DPS, is through implementing Proof of Concept (PoC) tests, prior to full scale implementation.

PoCs are generally undertaken to prove the feasibility of a solution or specific functions of a solution and are typically executed in an off-site test environment. A vendor agnostic PoC methodology that is tailored to cybersecurity tool integration for DPS is presented. Although, there can be similarities with other types of technology integration projects (i.e. IT, enterprise, or corporate), there are distinct differences and challenges when developing an integration strategy for cybersecurity solutions for DPS, including distributed energy resources (DERs). The focus of this paper is on DPS, but many of the concepts can be applied to most Industrial Control Systems (ICS) and Operational Technology (OT).

This paper delves into the important differences between IT and DPS challenges (e.g. IEDs) when it comes to cybersecurity tool integration. By understanding these differences, potential obstacles can be better anticipated and planned for. Overall, this will reduce the risk of the PoC project and set the stage for success.

1.1. BACKGROUND

Gaps have been identified in publicly available resources when it comes to cybersecurity tools integration for DPS. Many IT based guides and playbooks are leveraging parallel production environments without impacting operations as a whole. This approach is not possible with DPS operating environments.

While a general PoC methodology can help mitigate risk, there are still several challenges:

- Defining the scope of the PoC and setting clear boundary limits
- Assembling the right team of internal resources, integrators, and subject matter experts
- Provisioning and staging of the PoC environment
- Successful completion of the PoC without hitting major roadblocks or stalling the project
    - Lack of adaptation and agility as the PoC is being executed
    - Lack of periodic assessment of the "must haves" versus the "nice to haves"

Although the above stated challenges may seem daunting, a properly structured and executed PoC can provide significant benefits to the project's success, such as:

- Demonstrations and testing of functions, features, and capabilities
- Identifying technical and integration constraints with the tools and systems prior to wide deployment
- Mitigating risks of disruptions to operational systems during large scale deployment
- A successful deployment of the cybersecurity tools/systems
- Capability to support future refresh of legacy devices
- Identification of future enhancements or integration points with existing technologies
- Reduce uncertainty and better understand the effort required for full deployment
- Understand how the various cyber technologies can integrate into the operating environment
- Communicate the return on investment (ROI) or value added of an on-site deployment

1.2. ASSUMPTIONS

This paper makes a few assumptions, and these have been summarized below. Although these are not all strict assumptions, they help provide the reader with appropriate context.

- The cybersecurity solution or technology to be demonstrated during the PoC has already been selected through an RFI (Request for Information) and/or RFP (Request for Proposal) process

to properly consider technical and functional requirements, and commercial and financial elements.

- Although the approach presented in this article is intended for a single solution or technology, the approach can still be adapted and applied for multiple solutions being considered.
- Typical cybersecurity solutions and technologies include, but are not limited to:
    - Universal Security Management (USM) systems
    - Regulatory compliance management tools
    - Security information and Event Management (SIEM) tools
    - Configuration Management tools
    - Electronic Access & Password Management tools
    - Patch Management tools
    - Threat Detection and Monitoring tools
    - Vulnerability Assessment tools
- There is a distinction between a PoC and a Pilot. For the purposes of this paper, the following definitions are used[1].
    - **Proof of Concept (PoC):** To prove the feasibility of a solution or specific functions of a solution. PoCs are typically executed in an off-site test environment.
    - **Pilot:** Refers to an initial roll-out of a solution into production, targeting a limited scope of the intended final solution.

2. METHODOLOGY/APPROACH

This section presents a PoC methodology that is tailored to cybersecurity tool integration in DPS. Although there can be similarities with other types of technology integration (i.e. IT, enterprise, or corporate), there are distinct differences and challenges when developing integration strategies for cybersecurity solutions in industrial operating environments, such as DERs. These differences will be highlighted at each major step in the PoC process, along with examples. If the PoC project manager/leader can understand these integration challenges, he/she can then anticipate these obstacles ahead of time and enable the project to be successful.

The diagram below illustrates the PoC methodology as an iterative process that will be discussed in more detail in the following sections. Normally, one of the first steps is to establish the PoC team. This is considered a one-time task in the sense that it is not typically part of the iterative process. Therefore, it is not shown in the diagram below. The next step is to define and agree upon high-level functionality. Once the desired functionality has been defined, PoC cyber asset types must be specified. After this, test objectives can be established. An extension of the test objectives is establishing clear success factors. Once who, what, and how are determined, the PoC testing environment can be staged. Before proceeding to PoC execution, it is recommended to clearly document cybersecurity solution capabilities versus device capabilities. The last step before circling back to the beginning of the iterative loop is to execute the PoC tests (let the fun begin!). Once core PoC testing has been completed, there are a few final tasks worth mentioning, but are not iterative in nature, and hence are not illustrated in the diagram below.

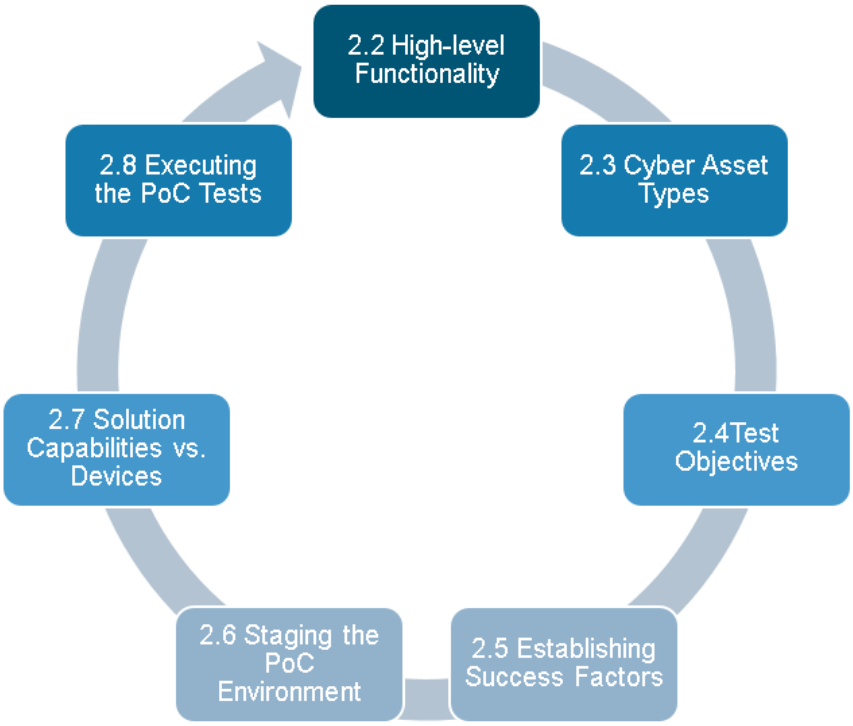

Figure 1: Iterative Process of the PoC Methodology

2.1. ESTABLISHING THE POC TEAM

Although some PoC projects may call for a change in the team part way through execution (one hopes this is not the case), this step is typically considered a one-time task. However, it can never hurt to have periodic reflection to ensure the PoC team is well equipped for the project scope.

2.1.1. INITIAL TASK – DESIGNATE LEAD INTEGRATOR

One critical element that is essential for a successful PoC, is assigning a designated Lead Integrator. This may sound obvious, but quite often companies will attempt to stack the PoC project responsibilities on top of already overloaded resources. Undeniably, this will typically lead to poor results or complete failure of the PoC. Not only can the PoC project be a failure, but this may also taint the perceived value of future PoCs. To mitigate this potential hurdle, it is recommended to designate a full-time resource(s) as the Lead Integrator. Ideally, this role is assigned to an impartial resource to minimize any bias influences on the results and outcome.

2.1.2. INITIAL TASK – ASSEMBLY OF TEAM

Once the Lead Integrator has been assigned, the remainder of the team must be assembled. Although the size and distribution of the team will vary depending on the complexity and scale of the PoC, typical team members will include internal resources, integrators, and subject matter experts (SMEs). One of the most important things to keep in mind, is leveraging the expertise of each person or group. An example is to have the client, integrator and solution vendor working closely together. Each group brings a specific expertise to the table and if coordinated properly, sets the stage for success. The diagram below illustrates the ideal PoC team triad to execute successful PoC testing and planning.

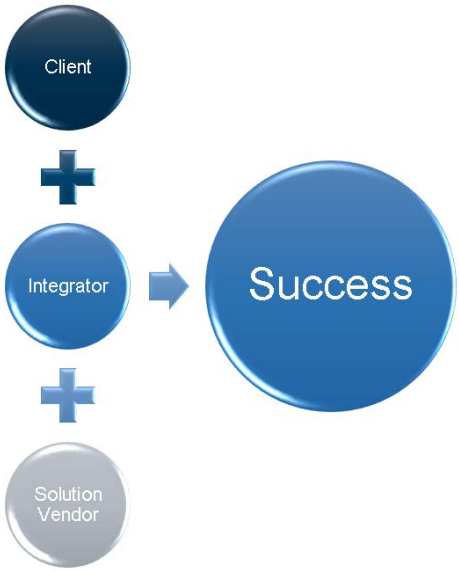

Figure 2: Ideal PoC Team Triad

2.1.3. ON-GOING TASK – DOCUMENTATION

The importance of documentation is also worth mentioning, as it is fundamental to a successful PoC. At each key task or step in the process, proper documentation is implied. Not only is it crucial to document the preparation and planning, but it is paramount to continuously update documentation as the PoC progresses.

2.2. HIGH-LEVEL FUNCTIONALITY

Defining the scope of the PoC is arguably the most important, and the most difficult, process of executing a successful PoC. Although the case may be that specific high-level functionality has already been determined, it is important to validate this with a list of commonly offered functions that are platform neutral (e.g. Asset Discovery, Access Management, Configuration Management, Patch Management, etc.). Sometimes client priorities may change when made aware of other functionalities available on the market.

The diagram below illustrates an sample list of commonly offered functions that are considered platform neutral. Note that there are still numerous subfunctions that typically fall under these high-level functions/categories. For example, baseline monitoring is a specific subfunction of configuration management.

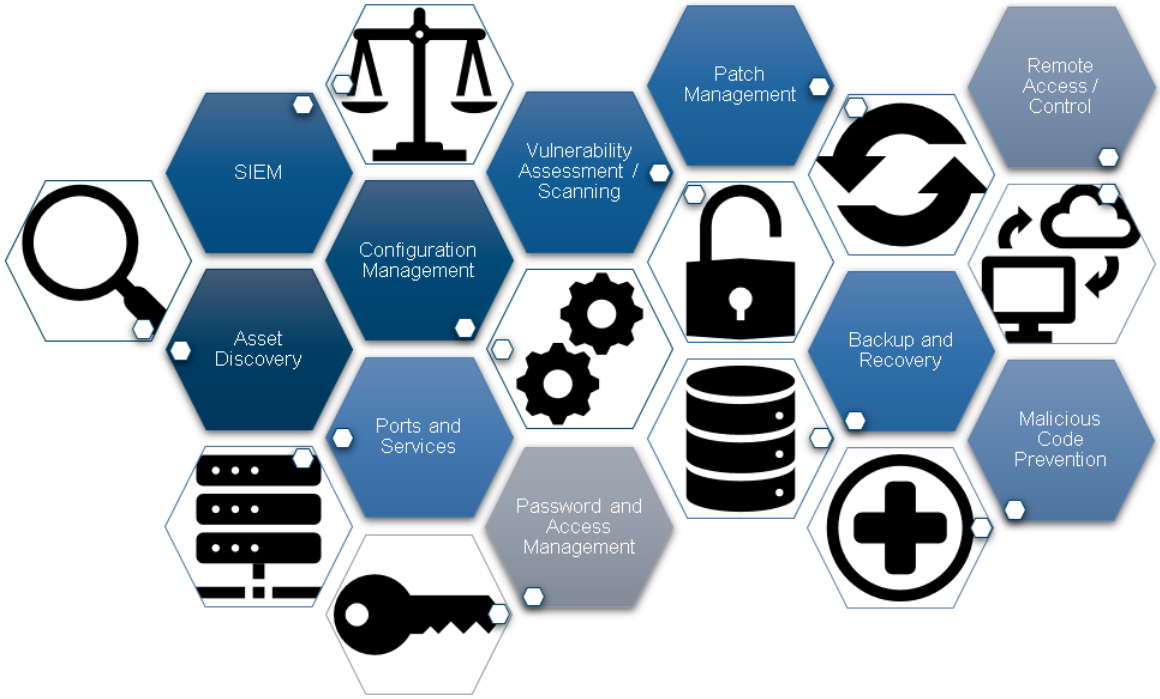

Figure 3: Common Platform Neutral Cybersecurity Tool Functions

The following table highlights key differences between Digital Power Systems (ICS) and IT at this step in the PoC process. This is by no means an exhaustive list but should provide enough detail to facilitate project specific discussions.

Table 1: Common Methods/Factors of Achieving High-Level Functionality

Cybersecurity Area	Digital Power System (ICS)	IT
Asset Discovery	-TAP or SPAN -Sometimes native active queries	-NMAP, IP sweep -Sometimes TAP or SPAN
SIEM	-Logs/events limited to Vendor software -Sometimes Syslog -Agent-less solutions common	-SNMP, Syslog, Windows Events -Agent based solutions common
Configuration Management	-Device configs limited to Vendor Software -Sometimes settings can be monitored via Modbus, SSH, Telnet -3rd party centralized management tools are still being proven and multi-vendor compatibility is rare	-SNMP, Microsoft System Center Configuration Manager (SCCM) -3rd party centralized management tools are mature and compatible with most IT assets
Vulnerability Assessment/Scanning	-Some analysis tools can rely on passive scanning. -Active vulnerability scanning not permitted -Vulnerability assessments rely on documentation, cross checking with known databases, or passive inspection of individual systems	-Active vulnerability scanning is common -Nessus, WMI, OpenVAS -Microsoft Baseline Security Analyzer (BSA) -Microsoft Security Compliance Manager (SCM) -Much of vulnerability assessment can be done by automated tools
Patch Management	-Patches and firmware must go through approved vendor software only -Patch updates are not very frequent, unless deemed critical -Patch deployment can only be done during planning outages (i.e. not during production)	-Patches and OS updates can typically be managed by 3rd party centralized management tools -Patch updates are quite frequent and can be deployed outside of office hours -WSUS

Cybersecurity Area	Digital Power System (ICS)	IT
Backup and Recovery	-Device backup file types vary drastically -Backup and recovery must go through Vendor Software	-Device backup files often leverage virtualized environments to save VM images with mature 3rd party centralized management tools -Network device backup files can be managed with mature 3rd party centralized tools
Ports and Services	-OT based protocols usually less secure by design -Modbus, OPC, Telnet, FTP,	-IT based protocols are more mature, and security has been built in by design -HTTPS, SSH, SFTP, FTPS
Malicious Code Prevention	-Agent-less solutions are common -Perimeter based tools only	-Agent based solutions common -Perimeter based tools used in conjunction with agents installed in devices
Remote Access/Control	-Remote access is not always allowed -Security management is based on devices and Vendor Software	-3rd party centralized remote access management tools are mature -Security management is typically application based only
Password and Access Management	-Access managed through Vendor Software -Passwords typically managed manually	-3rd party centralized management tools are mature -Active Directory, LDAP, Radius

2.3. CYBER ASSET TYPES

Next, and as a first pass, a list should be made of the cyber asset **types** that are to be included in the PoC tests. Note that the word "types" has been emphasized. The PoC should focus on representative samples of the client's cyber asset types to be tested. Typical information that should be included is the vendor, model, firmware, and vendor management software. If the asset type is left too generic, there will be too large of a disconnect between the PoC planning and the execution.

Three cyber asset selection criteria that should be considered are:

- Total quantities of each cyber asset type
- Criticality of each cyber asset type
- Current capabilities in terms of lack of functionality of each cyber asset type

Once a list has been drafted, consider assigning a priority value/ranking of each cyber asset type that is to be included in the PoC tests. This priority will aid in ensuring that effort is spent on the most important devices (based on client's ranking) and corresponding PoC tests.

The following table highlights key differences between Digital Power Systems (ICS) and IT at this step in the PoC process. It is important to understand that most often there are IT types of assets that are used in OT environments, such as Windows based servers and network devices. However, deploying an IT centric tool will likely not be able to integrate with the ICS types of assets. Therefore, an ICS/OT centric tool will be required to manage the ICS asset types. Depending on the ICS solution, some ICS tools provide IT features and functions and are intended to replace existing IT tools. Alternatively, a hybrid approach can be taken such that an IT based tool/solution is used to manage the IT asset types (with OT functions) and an ICS/OT based tool/solution is used to manage the ICS asset types. This typically would be used as a temporary transition if existing IT based tools are already owned. Relying on two sets of tools will be more costly in the long term because of software licensing costs and effort required to maintain and manage multiple products.

Table 2: Common Cyber Asset Types and Capabilities

Cybersecurity Area	Digital Power Systems (ICS)	IT
Asset Types	-IEDs, RTUs, PLCs, HMIs, DCS, SCADA servers	-Windows based OS, network devices, mobile devices
Security Features/Functions	-Limited or non-existent	-More commonly available
Support Life Cycle	-10 to 20 years or more	-2 to 5 years
CIA Priorities	Availability first	Confidentiality first

2.4. TEST OBJECTIVES

After the preliminary list of cyber asset types for the scope of the PoC has been defined, defining the PoC test objectives is next. Relevant requirements for the PoC test objectives are often available from technical and functional requirements that have been used previously for an RFI or RFP process. These requirements typically can be translated into test objectives, although some can be more challenging than others. This is also the stage in the process that must include any applicable regulatory requirements (e.g. NERC CIP) that need to be tested. Once the test objectives have been established, the corresponding procedures need to be defined. These will provide the necessary steps to follow and execute in order to demonstrate each test objective. Typically, these will have a device specific set of instructions and a tool/solution specific set of instructions, but this can vary depending on the project and complexity.

An example test objective is provided below that falls under an Electronic Access Management functional group. This same example will be used in the next sections.

Example Test Objective: *Centrally manage local electronic access to all capable PoC cyber asset types. This should be done by providing an interface between the tool/solution users and the local accounts of cyber assets (i.e. man in the middle solution).*

The following table highlights key differences between ICS and IT at this step in the PoC process.

Table 3: Test Objective related items

Cybersecurity Area	Digital Power Systems (ICS)	IT
Test Procedures	-Complicated integration process -Integration has often not been done before -Relevant vendor documentation and support are NOT available	-Integration process is well known or mature -Relevant vendor documentation and support are available
Regulatory Requirements	-NERC CIP Standards regulates critical infrastructure -Focus is **Reliability/Availability** of systems	-ISO 27001/02, ITL, COBIT -Focus is **Confidentiality** of information

2.5. ESTABLISHING SUCCESS FACTORS

Next, the PoC test result success factors must be defined. How does one measure the degree of success or criteria that each test objective must demonstrate? A common approach is to establish a ranked scale with specific criteria assigned to each success factor value. This can aid in removing some of the subjectivity in measuring the extent of the test's success. It is extremely important to define the success factor measures upfront (at least get this close), otherwise the outcome could be "fudged" in one direction or the other. This is not fair for any of the stakeholders involved.

Example success factor criteria is provided below that is a continuation to the example used in the previous step (test objective). Each rank represents the Level of Compatibility (LOC) and will typically require customization for each test objective. Note that the percentages (or other metric) used in the success factor criteria must be appropriate for the client requirements. It is also important to notice the word "capable devices" since the success should only be measured on the device types that can provide that feature/function.

Example Success Factor Criteria:

3 = Fully (all capable devices can be centrally managed by the tool/solution)
2 = Mostly (80% of capable devices can be centrally managed by the tool/solution)
1 = Partially (50% of capable devices can be centrally managed by the tool/solution)
0 = None (0% of capable devices can be centrally managed by the tool/solution)

For some projects, it may be appropriate to apply a weight value to the test objectives. This allows a higher weight to be associated with those test objectives that are more important to the client. The same approach can be taken for the high-level functionality groups (multiple test objectives related to the same basic function). However, adding this level of detail might not be necessary for all projects. At a minimum, this should only be applied on the second iteration to help simplify the first pass.

The following table highlights key differences between Digital Power Systems (ICS) and IT at this step in the PoC process.

Table 4: Success Factor related items

Cybersecurity Area	Digital Power Systems (ICS)	IT
Success Factors/Criteria	-Often requires customization -Examples NOT readily available via public information	-Boiler plate criteria are often acceptable (with minor tweaks) -Examples readily available via public information

2.6. STAGING THE POC ENVIRONMENT

Provisioning and staging an off-site PoC test environment are essential. It allows more flexibility for validating the PoC functions, features and capabilities, without the risk of inadvertently impacting production operations. The test environment should provide the necessary infrastructure to facilitate the PoC tests. It should be configured to emulate to some extent the production environment. It is also important to understand and document how the test environment differs from the production environment. A test environment should include various networking devices, servers, applications, and, of course, the cyber assets themselves (e.g. IEDs, PLCs, HMIs, DCS, etc.). It is paramount that this test environment be secure and isolated from the corporate IT enterprise network.

The following table highlights key differences between Digital Power Systems (ICS) and IT at this step in the PoC process.

Table 5: Staging the PoC Environment

Cybersecurity Area	Digital Power Systems (ICS)	IT
Cyber Assets	-Exact hardware and firmware for ICS devices is crucial for testing integration capabilities -Device hardware can be costly -Difficult to acquire for testing purposes	-Exact hardware and firmware for IT devices is more flexible since virtualization is common -Device hardware is typically lower cost (this can vary) -Easier to source for testing purposes
Supporting Infrastructure	-Often legacy/older versions of hardware and software	-Typically running more recent versions of hardware and software

2.7. SOLUTION CAPABILITIES VS. DEVICES

This step in the process ends up being tightly linked to the test's success factors/measures, but is worth elaborating. It especially applies to legacy devices, where it is common for such a device to have limitations in functional capabilities. It is important to clearly understand these device limitations upfront so these can be accounted for in gauging the success factors. Most cybersecurity tools/technology solutions can provide extensive features and functions, but this will not matter if the cyber asset under test is an old legacy device type and is not capable of integrating such functions. To address this, one table is required to illustrate the device capabilities or technical constraints and another table to identify the tool/solution capabilities. The tests to be performed must overlap with both tables. When a technical constraint with a device is identified, this can trigger an investigation into alternative methods to achieve a comparable result. These alternative methods are generally put

into the “nice to have” bucket for future consideration, unless this capability is considered a must have.

The following table highlights key differences between Digital Power Systems (ICS) and IT at this step in the PoC process.

Table 6: Solution Capabilities vs. Devices

Cybersecurity Area	Digital Power Systems (ICS)	IT
Solution Capabilities	-Great progress has been made by vendors, but products still evolving	-Many vendors/products are well established and mature, although new features are still released often
Device Capabilities	-Legacy devices often have very limited integration capabilities -Some newer ICS devices are offering more security by design, but is normally only practical on green field projects	-Most IT devices are considered modern and have common integration capabilities -IT devices are constantly improving with new security features/functions but can often be upgraded via software updates.

2.8. EXECUTING THE POC TESTS

Following the completion of the PoC planning and preparations, the testing can commence. The PoC test procedures must be followed and updated accordingly, and the test results must be captured and documented. There may be special exceptions or test circumstances for certain asset types, and it is important to document these as you go. For example, some tests on certain devices can only be performed using their vendor’s software with no external interface capabilities available. Finally, ensure to stay focused on in scope items. Attention can easily shift to related tasks, then to somewhat related tasks, and then finally to unrelated tasks without the initial intention of crossing the scope boundary limits. Concentrate on the “must haves” first.

The following table highlights key differences between Digital Power Systems (ICS) and IT at this step in the PoC process.

Table 7: Executing the PoC Tests

Cybersecurity Area	Digital Power Systems (ICS)	IT
Vendor Software	-Many ICS devices must be configured and managed via the Vendor Software only -Some Vendor Software use proprietary protocols that cannot be integrated to 3rd party centralized tools	-Most IT devices can be configured through the original vendor software, but also through mature 3rd party centralized tools -Most IT Vendor Software relies on open source protocols
Interface Separation	-Some ICS devices do NOT separate the management interfaces from the SCADA or operating interfaces.	-Most IT devices have a dedicated management interface that is isolated from the data/operating interfaces. This can be physical or logical separation.

2.9. ITERATE AS REQUIRED

The general process described above may have to be iterated multiple times to demonstrate the PoC observations and results to an acceptable level.

2.10. FINAL TASKS – TEST SCENARIOS FOR CLIENT WITNESSING

Normally, there are too many tests to conduct during the PoC, where having the client present to witness them is not reasonable. Therefore, test scenarios can be created to showcase key test objectives for the client to witness. Ideally, these test scenarios are demonstrated on the actual cyber assets in the PoC test environment.

Witnessing test functions and test results by the client is often an integral part of the PoC plan. One must keep in mind that some PoC tests may have requirements for client witnessing sign offs. The

actual client witnessing session must be structured based on the target audience. This could vary drastically depending on if the audience is very technical, more management level or a combination of both. Depending on the specific project details, more than one session could be offered to better accommodate the different stakeholders.

2.11. FINAL TASKS –TEST SUMMARY REPORT

The final PoC deliverables will likely vary depending on the project, but it is appropriate to provide a PoC test summary report. This report should highlight the test results in a clear and concise manner based on the previously agreed measures for success factors. This report can also provide recommendations or potential next steps. In some cases, this report can be part of the business case for an on-site pilot or full deployment.

3. CONCLUSION

The vendor agnostic PoC methodology for testing cybersecurity solutions used in Digital Power Systems environments presented in this paper provides the framework and the critical elements for the successful planning and execution of the PoC. This methodology/approach is based on successful PoC project implementations and cybersecurity expertise that have been gained by BBA over years of supporting client projects in various industries. Additionally, key differences between IT and Digital Power Systems challenges, when it comes to cybersecurity tool integration, are highlighted to provide the reader with practical insights that can be applied directly to their cybersecurity tool integration projects.

There are several key points that can be taken away from this paper:

- Deploying and integrating cybersecurity tools in Digital Power Systems must be well planned and executed in order to mitigate risks.
- Implementing vendor agnostic Proof of Concept (PoC) tests in project execution plans, prior to full scale implementation can help mitigate risks such as disruption/impact to business operations, people, safety, environment, and others.
- There are distinct differences between IT and Digital Power Systems (e.g. IEDs) when it comes to cybersecurity tool integration.
- Cybersecurity tools currently on the market can offer impressive features and functions, however a major challenge often can be linked to device integration limitations and lack of capabilities.
- It is important to validate the desired high-level functionality with a list of commonly offered functions that are platform neutral.
- There are cybersecurity tool integration strategies and options that can centralize and improve the efficiency of day-to-day operational/maintenance tasks.
- Each operator/owner of its Digital Power Systems will have specific needs and requirements and it is important to consider options that are a “right fit” for that operational environment and culture.

If you have any questions or want to learn more about this topic, feel free to contact Shayne Casavant.

BIBLIOGRAPHY

[1] Murphy, S. (2014, February 10). *Proof of Concept vs Pilot Program*. Retrieved from Nexus: http://www.nexusnet.com.au/2014/02/10/proof-of-concept-vs-pilot-program/