Life Is On | Schneider Electric

Get Secure: End-to-End Cybersecurity Lifecycle Frameworks

by Gregory Strass, CISSP, CEH
Michael Pyle, CSSLP, CPT, CEH
Jesse Wiegand, CISSP, SEC+

Executive Summary

Cybersecurity has become a primary concern for building and business owners around the world. Many believe “secure” devices are all that is needed to achieve a “secure” environment. Unfortunately, this approach leaves building management system projects with unmitigated risks.

This white paper introduces and presents multiple end-to-end cybersecurity lifecycle frameworks that can be used to address security in a holistic manner.

Introduction

Business owners are becoming keenly aware that failure to have a secure infrastructure is a sure way to have a business failure. The costs associated with recovering from a security breach can be high and can pull employees off of their main functions to support the recovery effort. Additionally, legal fines for some breaches can endanger the very existence of the enterprise.

One Ponemon Institute[1] report shows the business and financial impact of a data breach, including:

- 5% drop in average stock price the day a breach is announced
- 7% loss of customers
- 31% of consumers discontinue the relationship

In 2016, Fortune Magazine[2] reported:

"On average, the cost of a breach has risen to $4 million per incident — up 29% since 2013 — according to research sponsored by IBM's (ibm, +0.34%) security division."

Figure 1

Investments in Security Operation Centers allow many enterprises to monitor and manage the continuing cybersecurity risks.

Today, statistics like these are common. They indicate the "cost of doing nothing" for cybersecurity is a cost that may be too high to afford.

While absolutely secure networks don't exist, many achieve high levels of security through cybersecurity planning best practice implementation. Most businesses focus on IT (Information Technology) networks and tend to ignore

[1] https://www.centrify.com/lp/ponemon-data-breach-brand-impact/?ls=930-011-google&utm_source=google&utm_medium=cpc&utm_campaign=Breach&utm_adgroup=Breach%20-%20Cyber%20Security&utm_term=cyber%20security%20breaches&utm_content=204448651362&utm_region=NA&utm_offer=PonemonReport&gclid=EAIaIQobChMIq_iZyp_11AIVHrnACh2TIgVAEAAYAiAAEgJ4AvD_BwE

[2] http://fortune.com/2016/06/15/data-breach-cost-study-ibm/

OT (Operational Technology) networks. This can be hazardous because many enterprises are moving toward the integration of IT and OT networks. This means that any risks on the OT network may now appear and affect the hosting IT network.

There are many sources that explain the differences in requirements between IT and OT networks, and possessing a good understanding of the difference is the first step for successful integration. The second step is evaluating to ensure the OT networks have been securely planned, implemented, and maintained.

This white paper introduces and presents multiple end-to-end cybersecurity frameworks to address security in a holistic manner. Its goal is to illuminate the many basic requirements and best practices associated with OT network security within building management projects.

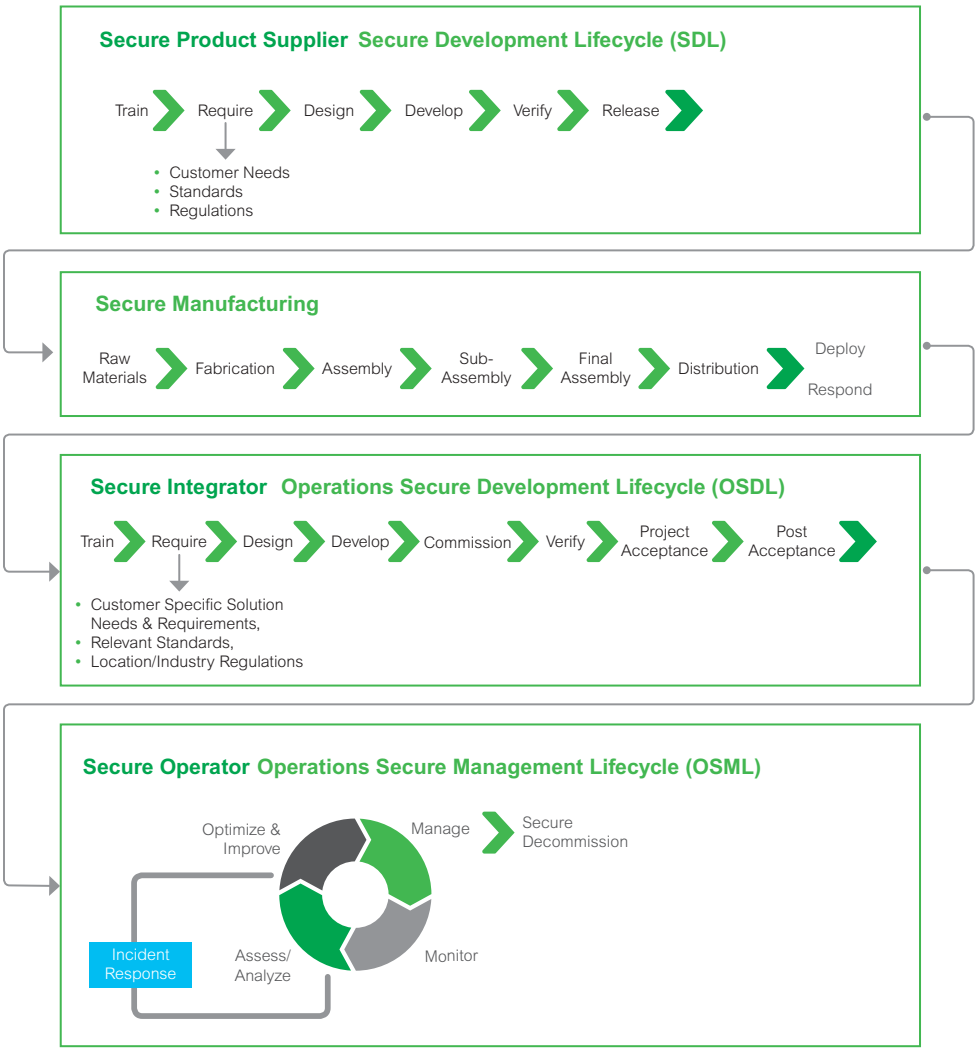
End-to-End Cybersecurity

True security begins early in the design stage of every device that connects to the OT network. The process can be long and complex, but when broken down into logical elements, it is more easily understood.

Figure 2 highlights the many steps needed to produce customer installations that meet security requirements. The process starts with product development, including manufacturing and integrator services, and is maintained by following basic secure management processes. Ultimately the security process for any customer integration only ends when it has been securely decommissioned.

Figure 2

Overall, a secure project relies upon several fundamental security frameworks as well as securely manufactured products.



From suppliers to integrators and operators, the goal of producing, installing, and maintaining secure sites is shared by all. Cybersecurity is such an encompassing issue that product suppliers must consider it from day one.

Likewise, the sales team needs to understand cybersecurity issues and how individual products handle those issues. Lastly, every installation has a "security envelope" that needs to be established and maintained.

Cybersecurity Frameworks – An Overview

The following three cybersecurity frameworks exist to help address security holistically:

- **Secure Development Lifecycle (SDL):** a key product development-based framework that helps ensure products follow secure design processes across all lifecycle stages.

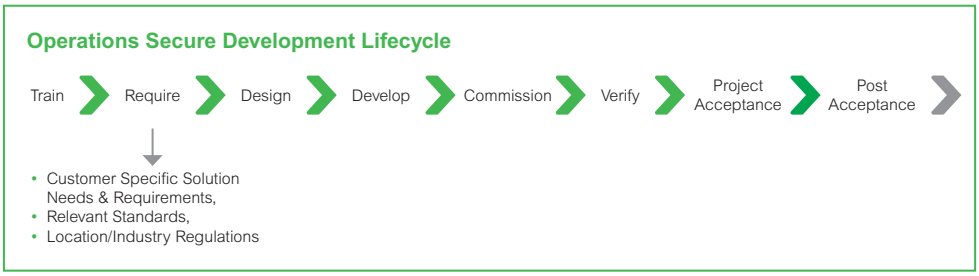
Figure 3

The Secure Development Lifecycle (SDL)

- **Operational Secure Development Lifecycle (OSDL):** relies heavily on the SDL for its structure and content. In fact, there are many similarities between designing a product and a project. This framework aims to provide a manageable security process for project creation.

Figure 4

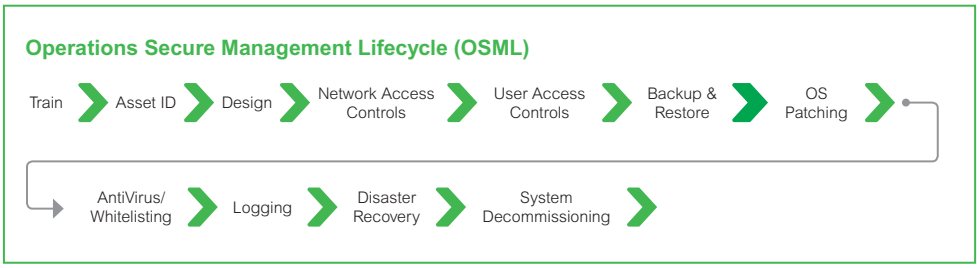
The Operations Secure Development Lifecycle (OSDL)



- **Operational Secure Management Lifecycle (OSML):** covers many of the management practices that need to be addressed over the remaining project lifecycle of the building. While it has many stages and processes, OSML needs to be incorporated into a repetitive management cycle. Unlike the other two frameworks, this one repeats until the project is redesigned or is fully decommissioned.

Figure 5

The Operations Secure Management Lifecycle (OSML)



Secure Manufacturing is Critical

While the bulk of this white paper concentrates on various best practices that work together to produce secure projects, it is also essential to understand the importance of "Secure Manufacturing" of the products which make up the system to overall cybersecurity.

In today's world of increasing security threats, it is extremely important to ensure products are genuine. While the installation of counterfeit product may raise legal concerns, integration risk is an even greater fear.

This is one of the reasons why manufacturers need to pay great attention to security in every production phase. First, purchased raw materials must be free of defect and cybersecurity issues. Then, manufacturing security throughout the Fabrication, Assembly, and Sub-Assembly processes is critical to providing assurance that products have not been compromised. This is followed by the Final Assembly process, which often includes the installation of "Device Authenticity" cryptographic keys to mark product authenticity. Lastly, distribution channels need to be secure and product packaging sealed to deliver assurance that devices have not been modified after official manufacturing.

Without secure manufacturing processes, it is impossible to guarantee products are free of corruption. This is why cybersecurity must be viewed as an end-to-end process where all sub-processes follow secure measures.

Figure 6

Secure manufacturing is a key element needed to produce secure projects

SDL Framework

Developing new, secure products requires precise attention to cybersecurity. The table below provides the basic steps needed for an SDL process.

Figure 7

SDL Framework Phases

The Secure Development Lifecycle (SDL)					
Train	Identify Development Role	Assign Courseware	Verify Completion		
Require	Research Specs, Standards, and Requirements	Evaluate and Document Requirements	Define Security Level and Refine Requirements	Define User Doc. Requirements	Develop Security Use and Misuse Cases
Design	Perform Threat Model	Prepare Mitigation Action Plan	Perform Attack Surface Evaluation	Perform Secure Design and Architecture Review	
Develop	Implement Security Features from Requirements	Ensure Approved Development Tools	Define Incremental Security Compliance Goals	Verify Secure Coding Rules	Perform Secure Code Reviews
Verify	Test Security Features	Test Overall Security	Test Network Security	Verify Security Defects are Fixed	Prepare for Security Review
Release	Document All Security Features	Ensure Patch Release Process is Ready	Conduct Final Security Review	Securely Archive Content	
Deploy	Deployments Must be Done Securely	Security Practioners to Have Appropriate Credentials	All Critical Infrastructure Solutions Require Security Practioner		
Respond	All Incidents Reported Within 24 Hours	LoB to Administer Corporate IRP for Incidents			

It all starts with a "Train" phase to ensure people are qualified to perform security related tasks. Once trained, they can begin implementing the cybersecurity functions associated with product development.

Once team members have been trained, development progresses through the Require, Design, Develop, Verify, and Release stages. After it is released, the product enters the “Deploy” stage. The Deploy stage elements lead to a secure deployment: deploying secure devices in an insecure manner will not result in secure system implementation. During Deploy, security continues to be essential.

After deployment, a product enters the “Respond” phase where device providers must be prepared to respond to field incidents. This stage requires that proper recording and tracking of all reported issues is handled in a well-defined, repeatable manner. Once issues are reported, compliance with an incident response procedure helps to ensure proper issue resolution.

OSDL: Framework

Like the SDL, implementation of a secure project requires ensuring all cybersecurity details are addressed. The OSDL derives from the SDL, with topics reinterpreted to reflect a project versus product development effort. OSDL phases follow:

Figure 8

OSDL Framework Phases

The Operation Secure Development Lifecycle (OSDL)							
Train	Identify Development Role	Assign Courseware	Verify Completion				
Require	Research Specifications, Standards, and Requirements	Asset Identification	Define Security Level and Refine Requirements	Develop Security Use and Misuse Cases	Identify Necessary Security Functions	Identify Security Policies and Procedures	Evalute and Document Requirements
Design	Perform Threat Model	Prepare Mitigation Action Plan	Perform Secure Design and Architecture Review				
Develop	Implement Security Features Found in Requirments	Define Incremental Security Compliance Goals	Perform Secure Code Reviews				
Comission	Test Security Features	Test Overall Security	Test Network Security	Verify all Security Defects are Fixed			
Verify	Ensure all Applications are Securely Installed	Verify Security of Network	Run Customer Required Network Stability and Security Tasks	Functional Test	Test, Refine, and Finalize Security Policies and Procedures		
Project Acceptance	Ensure all Items on Check-Off Sheets Have Been Completed	Instruct Users of Security Polices, Procedures and Features					
Post Acceptance	Identify Employee Role	Instruct Users on Security Policies, Procedures, and Features	Assign Courseware	Verify Courseware Completion			

OSDL: Train Phase

The OSDL "Train" phase concentrates on ensuring people assigned to system development projects are properly educated to:

1. **Identify Development Role:** This step identifies and assigns a role to each person involved in the definition, development, and implementation of systems. As people change roles, additional training may be needed.

2. **Assign Courseware:** Each person is assigned training that provides an understanding of the cybersecurity requirements for that role. Training needs to include quizzes that prove the subject was adequately understood. The amount of training will depend on the role. For instance, a technician may need to complete only 3 or 4 modules, while an architect may need to complete 12 or more.

3. **Verify Completion:** Project team members should not be allowed to assume role responsibilities until all required courseware has been successfully completed.

OSDL: Require Phase

The "Require" phase presents the following elements for consideration during project estimation prior to the start of the design:

1. **Research Specifications, Standards, and Requirements:** This can be a time-consuming step. Often the quotation request refers to international standards or local regulations. Understanding these regulations, along with customer requirements, can require a substantial effort.

   Often cybersecurity requirements are complicated and require integrated projects to be configured in compliance with those standards. These requirements need to be carefully reviewed and discussed with the customer to ensure proper understanding.

   While equipment and application suppliers may have addressed many of the typical cybersecurity concerns associated with their industry, it is likely some requirements will be "system specific" as opposed to "product specific." One must understand the distinctions and ensure appropriate planning is done.

2. **Asset Identification:** One of the first steps in establishing security requirements is identifying all assets that will exist on the network or in the system. Extra or missing assets need to be investigated.

   While there may be many different types of assets associated with a project, the primary ones affecting the security envelope will be connected devices. In addition to servers and network connected devices, there will be network control devices like routers, VPNs (Virtual Private Networks), firewalls, etc. Asset identification needs to perform the following:

   a. **Catalogue System Elements:** Keeping all devices up-to-date when it comes to security revisions can be expedited by cataloging the brand, model number, and revision level of all devices. In general, the customer's IT department wants to know about every device on the network. They need this information to proactively detect changes. This information allows for the proper investigation of unexpected changes.

One consideration that needs to be planned is the use of and presence of test and debug instruments on the network. It may be necessary to "register" these devices with the IT department to ensure they have proper access. This process also helps prevent false alarms in the IT department that may be caused by unknown test instruments operating on the network.

b. **Identify Critical Assets:** Within the list of assets, certain ones will be of critical nature. These devices may represent single points of failure that could lead to secondary failures. It is important to understand which devices are "critical" and work with the customer's IT department to develop management plans to account for device outages.

c. **Ensure Physical Access Controls are Operational:** Part of the Asset ID process is ensuring proper cataloging and tracking of devices that control physical network access. Keys to enclosures need to be cataloged and duplicates need to be securely stored for unplanned situations. Beyond simply cataloging the physical access controls, it is important to ensure all are operational.

3. **Define Security Level and Refine Requirements:** In this step, the Security Level required for the project is formally determined. There are several different security level scales; a common one follows:

   Level 1: System must protect itself and recover from "Casual or Coincidental Violations." This security level includes common user mistakes such as handling erroneous entries, inserting devices (like USB sticks) into project equipment and the like.

   Level 2: System must protect itself and recover from "Intentional Violations using Simple Means with Simple Resources, Generic Skills, and Low Motivation." This security level covers attacks performed by inexperienced hackers or people with little or no understanding of cybersecurity or hacking procedures. This security level can be associated with attacks that may be launched by a disgruntled employee or former employee.

   Level 3: System must protect itself and recover from "Intentional Violation using Moderate Resources by means of a trained Hacker with Moderate Motivation." This security level includes professional attacks for various reasons including the stealing of personal and sensitive information (names, addresses, passwords, credit card numbers) and/or sensitive corporate information or company secrets. Generally, the attacker is well trained and has a specific goal and will use advanced hacker techniques to achieve that goal.

   Level 4: System must protect itself and recover from "Intentional Violation using Extensive Resources with extensive capitalization, highly skilled hackers, and high motivation." This security level is associated with areas like Industrial Control System in the Critical Infrastructure such as banks, hospitals and airports. These routinely come under attack by foreign governments and advanced threat agents.

   Once the Security Level has been determined it is possible to understand the level of design needed to achieve the specified goal.

4. **Develop Security Use and Misuse Cases:** One of the best ways to ensure a project has achieved the required Security Level is to work through various potential use and misuse cases. During this evaluation, the planned architecture is reviewed for its ability to resist and recover from adverse actions. It is generally important to consider all known and reasonably expectable use cases in this evaluation.

5. **Identify Necessary Security Functions:** Specific security solutions will be needed to support the identified security requirements and desired security level. The need for the following items must be considered:

   - Network Access Control
   - User Access Controls
   - Intrusion Detection System (IDS)
   - Intrusion Protection System (IPS)
   - Perimeter and Segment Firewalls
   - Anti-Virus and/or Application Whitelisting
   - Backup and Restore System
   - Security Information and Event Manager (SIEM)

6. **Identify Security Policies and Procedures:** Securing a system is a continuous process that is never completed; it has to be maintained over time and adapt in response to new cyber threats. Security policies and procedures are a key element of a security system and must be incorporated into requirements and project planning.

7. **Evaluate and Document Requirements:** Often cybersecurity requirements are complicated and require the project to be configured in compliance with standards. Requirements need to be carefully reviewed and discussed with the stakeholders to ensure they are properly understood.

   While equipment suppliers may address many of the normal cybersecurity concerns associated with their industry, it is likely many integration-specific requirements will be identified. It is important to understand this distinction in the requirements and ensure you comply with all requirements.

OSDL: Design Phase

The OSDL "Design" phase uses the information generated in the Require phase as the basis for the creation of a project that meets all requirements. To incorporate adequate cybersecurity review of the design, the following steps need to be performed:

1. **Perform a Threat Model:** In cybersecurity, the Threat Model is a straightforward process that helps identify weaknesses in a design. A common tool for performing the Threat Model is the "Microsoft® Threat Modeling Tool," which is a free download from Microsoft. It provides a drawing surface for modeling and then, in the analysis phase, it presents common cybersecurity concerns. This tool helps the modeler document the intended state for each.

2. **Prepare Mitigation Action Plan:** After the Threat Model has been completed, there will be items that need to be addressed in subsequent phases. Creation of a Mitigation Action Plan ensures all Threat Model issues are addressed.

3. **Perform Secure Design and Architecture Review:** Once the design has been completed and the Threat Model exercise is completed, one last review of the project from the cybersecurity perspective can be a valuable exercise. Looking at the project as a whole may reveal issues that may have been missed in the detailed reviews. Any issues found would be added to the Mitigation Action Plan.

OSDL: Develop Phase

In the Develop phase, the project elements are pulled together into a deliverable system.

1. **Implement Security Features Found in Requirements:** In this stage, all of the design and cybersecurity requirement documents are used to create the deliverable system. There may be many requirements that will need to be verified or validated by the customer during the Project Acceptance phase. The Design phase allows those issues to be identified and handled so that the acceptance process can progress smoothly.

2. **Define Incremental Security Compliance Goals:** Projects may have significant security compliance requirements, staged for differing phases of an integration process. It is important these be identified and properly planned.

3. **Perform Secure Code Reviews:** Many customers require certification that delivered projects be free of intentionally inserted malware. This can happen when a disgruntled employee works on the project. Without a Secure Code Review process, there is no way to assure customers the delivered system is free of intentional vulnerabilities. Having an automated process that allows team members to record their review efforts can simplify this task.

OSDL: Commission Phase

In this stage of the project, sufficient functionality exists to allow review of the project from a security perspective.

1. **Test Security Features:** When customers have specific features, often derived from specification, standards or specific requirements, ensuring they have been properly addressed can significantly reduce time spent in later stages.

2. **Test Overall Security:** This is a verification procedure that confirms all issues identified in the Mitigation Action Plan have been successfully addressed. This should include verification that all use and misuse cases have been successfully addressed.

3. **Test Network Security:** In today's cybersecurity environment, many customers perform periodic network scans of OT networks. In the past, this was problematic because devices were not designed to operate in a network environment with scanners running. Today, scanning networks for unexpected changes is considered a critical security functionality, so ensuring the integration runs smoothly with these devices performing scans can greatly reduce unexplained operational field issues.

   Customers expect installed systems to be capable of operating under load. Representative testing may help locate any scanner-induced issues caused when the system is under load.

4. **Verify All Security Defects are Fixed:** Defects found during the Development process need to be recorded in a bug-tracking program. Such programs greatly simplify tracking issues through completion.

   It is critical that any security defect of high or critical rating be fixed prior to planning Project Acceptance. A growing number of customers will not accept products or project that include such cybersecurity issues.

OSDL: Verify Phase

After commissioning, the "Verify" phase helps to ensure everything has been securely implemented.

1. **Ensure All Applications are Securely Installed:** All installed packages should be verified against their supplier's signature. Software installers failing the signature verification should NEVER be installed.

2. **Verify Security of Network:** During the build-out process, various system components may be exposed to tampering. As the project nears completion, the importance of the physical security associated with sensitive systems increases. Unless all network wiring was pulled in conduits, performing a visual inspection of all networking wiring, wiring closets, and networking equipment is warranted.

   Beyond the physical wiring, it is also important to verify the secure configuration of all devices connected to the network.

   A significant issue is verifying firewall, VPN and router version, configuration, and setup. Working with the customer's IT department is recommended if there is a lack of qualified IT personnel on the team.

   While the project's network segment may be physically isolated from the rest of the IT infrastructure, any network interconnection allowing monitoring of the project represents an attack vector. Mitigating these risks is best done by someone well trained and experienced in such processes.

   The next step would be to verify all planned secure connections are in fact secure. Such connections can either be physical connections (cables and feed lines to wiring cabinets) or logical connections (Intranet and Internet connectivity). It is important to test that the communication pathway's security meets requirements.

   An important tool for performing such a verification is a product known as Wireshark. This application allows data flow on networks to be inspected. Once properly configured, it is straightforward to verify communication channels are encrypted: if you can read what's in the data packets – it's not encrypted!

   It is also important to verify no unsecured connections exist with any external systems. The connection to every external system, including the company's intranet and especially the Internet, needs to be verified as a secured connection. The use of VPNs is an excellent way to allow access to the project from the Internet in a secure manner.

   It is critical to verify that all devices and applications have had their default passwords changed. This is the SINGLE MOST IMPORTANT THING that can be done to protect the project. Often devices come from the factory only using a single credential such as "admin/admin" for the common user name/password. It is CRITICAL that these credentials are changed to conform with the system-owner's password policies.

3. **Run Customer-Required Network Stability and Security Tasks:** One result of IT/OT integration is IT departments tend to now have their own standards for devices operating on their networks. It is important to take these standards into consideration.

Cybersecurity requires network segments to be scanned to ensure all equipment on the segment is authorized to operate on the network. Such scans may be a regular process performed by the IT department on the OT network.

An additional security requirement, now being seen more regularly, is the requirement that the "system as implemented" be subjected to a Penetration Test (or PEN test for short). In this test, a qualified penetration tester is hired to evaluate the project. While this tends to be an expensive process (both monetarily and in time), it helps customers ensure all project security goals have been met.

4. **Functional Test:** This process helps ensure everything is operational and ready to proceed:

   a. **Verify all devices are connected to the network and are communicating:** When cybersecurity controls are applied, device communication is sometimes interrupted. It's critical, prior to project turnover, to ensure all devices are still communicating as expected.

   b. **Verify the database (if applicable) is receiving input and data can be retrieved:** If the database is too locked down due to cybersecurity controls being placed on the data while in the resting state, DB queries will be unsuccessful.

   c. **Verify users have the correct permissions:** All user accounts need to be verified to determine if the correct access controls are in place. If users are unable to access the data they need, their account may be worthless. If they are allowed to access information not needed by their role, then overall security is reduced.

   d. **Ensure the ports needed for communication are open:** As with user permissions, having the proper ports open so communication can take place is critical. Having more ports open than needed reduces overall security.

   e. **Create the plan of action and milestone (POAM) for any Cybersecurity issues that remain open:** Note any applied controls that lead to loss of functionality. Cybersecurity controls that cannot be applied must be documented in a POAM. All such issues need to be listed and documented as to the steps being taken to address them.

5. **Test, Refine, and Finalize Security Policies and Procedures:** Throughout the integration process, many important operational details will be derived from the operational characteristics of the integration. It is important to capture these details and incorporate proper integration of Security Policies and Procedures.

   The end product of this process should be a well-defined set of policies and procedures to be followed over the maintenance lifecycle of the integration.

OSDL: Project Acceptance Phase

Once the project has completed all required testing, the "Project Acceptance" phase is entered. Cybersecurity concerns in this phase include:

1. **Ensure All Items on Check-Off Sheets have been Completed:** Whether the check-off sheets are standard forms, or whether they are created through the prior OSDL stages, it is important the customer understands and accepts each item.

2. **Instruct Customer on Security Features:** An oft-cited weakness in project implementation is the failure to train the customer on the security features of the project and how to maintain the project's security. The depth of instruction will depend on the nature of the relationship with the customer.

OSDL: Post Acceptance Phase

The operation of the system should all begin with a cordial handoff to the people who will be using the system. A key to achieving this is training the users and managers of the system. Such a practice helps ensure understanding of the various cybersecurity functions, processes, and policies required for their roles. These activities include:

1. **Identify Employee Role:** This step allows managers to identify the specific role for each employee. As employees change roles, additional cybersecurity training may be needed.

2. **Instruct Managers and Users on Applicable Security Policies, Procedures, and Features:** The depth of instruction will depend on the nature of the relationship between the system developer and system owner.

3. **Assign Courseware:** The employee is assigned training that brings understanding of the cybersecurity requirements for that role. Training needs to include quizzes that prove the subject was adequately understood. The amount of training will depend on the role. For instance, a technician may need to complete only 3 or 4 modules while an architect may need to complete 12 or more modules.

4. **Verify Completion:** Employees should not be allowed to assume their roles until all required courseware has been successfully completed.

OSML: Framework

Like the OSDL, the OSML Framework highlights various processes and activities associated with the operation of the project over its lifecycle. Unlike the previous frameworks, the OSML is "repetitive." From a procedural standpoint, the following topics are important in securely maintaining a project over its operational lifecycle:

Figure 9

OSML Framework Phases

The Operation Secure Management Lifecycle (OSML)							
Train	Identify Development Role	Assign Courseware	Verify Completion				
Asset ID	Identify All Connected Assets	Identify Critical Assets	Ensure Physical Access Controls are Operational	Develop Security Use and Misuse Cases	Identify Necessary Security Functions	Identify Security Policies and Procedures	Evalute and Document Requirements
Design	Perform Threat Model	Prepare Mitigation Action Plan	Perform Secure Design and Architecture Review				
Network Access Controls	Upgrade NAC Firmware As Needed	Ensure Integrity of Network Connections	Verify Network Segmentation Configurations				
User Access Controls	Review List of Users	Remove or Disable Accounts No Longer In Use	Ensure Password Policy Conforms to Customer Password Policy				
Backup and Restore	Verify All Backup Schedules	Verify Backup Integrity	Verify Periodic Restore Operations	Transfer Backups to Offsite Location According to Customer Policy			
OS Patching	Schedule Maintenance Periods	Obtain Vendor List of Acceptable Patches	Obtain and Verify Patches	Apply Patches	Verify System Functionality		
AntiVirus/ Whitelisting	Ensure Antivirus Database is Up-To-Date	Verify Logs for Indications of Whitelist Violations	Escalate Any Whitelist Violations to Site Management Team				
Logging	Reivew System and Error Logs	Review System Security Logs	Review Application Logs	Verify Connection with Syslog Server	Verify Connection with SIEM		
Disaster Recovery	Designate Emergency Contact	Create Written Disaster Recovery Plan	Practice Disaster Recover Plan				
System Decommis-sioning	Inform Customer Device Will be Decommis-sioned	Ensure Viable Device Backup	Run Device's Secure Decommission-ing Procedure	Remove Power and Detach Wiring	Securely Dispose of Device in Compliant Manner		

OSML: Train Phase

As with other frameworks, it all begins with the "Train" phase because is important to ensure employees understand the various cybersecurity functions required by their role.

1. **Identify Role:** This step identifies and assigns a role to each person involved in defining, developing, and implementing the system. As people change roles, additional cybersecurity training may be needed.

2. **Assign Courseware:** Each person is assigned training that provides an understanding of the cybersecurity requirements for that role. Training needs to include quizzes that prove the subject was adequately understood. The amount of training will depend on the role. A technician may need to complete only 3 or 4 modules while an architect may need to complete 12 or more.

3. **Verify Completion:** Project team members should not be allowed to assume responsibilities until all required courseware has been successfully completed.

OSML: Design Phase

Like the previous SDL frameworks, the OSML "Design Phase" leverages information from previous stages. Like those frameworks, the design phase incorporates threat model, mitigation action plan, and design and architecture reviews. To incorporate adequate cybersecurity review of the design, the following steps need to be performed:

1. **Perform a Threat Model:** In cybersecurity, the Threat Model is a straightforward process that helps identify weaknesses in a design. A common tool for performing the Threat Model is the "Microsoft Threat Modeling Tool," a free download from Microsoft. It provides a drawing surface for modeling and then, in the analysis phase, it presents common cybersecurity concerns. This tool helps the modeler document the intended state for each.

2. **Prepare Mitigation Action Plan:** The Threat Model will find issues that need to be addressed in the subsequent phases. Creation of a Mitigation Action Plan ensures all Threat Model issues are addressed.

3. **Perform Secure Design and Architecture Review:** Once the design has been completed and the Threat Model exercise is complete, one last review of the project from the cybersecurity perspective is a valuable exercise. Looking at the project as a whole may reveal issues that have been missed in other reviews. Any issues found would be added to the Mitigation Action Plan.

OSML: Asset ID Phase

The next "Asset ID" phase identifies all assets that should exist on a network to ensure end-to-end security. The following extra or missing assets should always be investigated:

1. **Identify All Connected Assets:** In most cases, there will be a variety of device types on the network segment. In addition to servers and network-connected devices, there will be network control devices like routers, VPNs, and more.

   It is important that all devices are properly cataloged. Keeping all devices up-to-date for security revisions can be expedited by knowing the brand, model number, and revision level of all devices.

   In general, the customer's IT department wants to know about every device on the network. They need this information to proactively detect changes. This information allows for the proper investigation of unexpected changes.

   One consideration is the use of and presence of test and debug instruments on the network. It may be necessary to "register" these devices with the IT department to ensure they have proper access to prevent a security violation notification when the device is connected.

2. **Identify Critical Assets:** Within the list of assets, some will be of a critical nature. These devices may represent single points of failure that may lead to secondary failures. It is important to identify the critical devices and work with the customer's IT department to develop management plans to account for outages on these devices.

3. **Ensure Physical Access Controls are Operational:** Part of the Asset ID process is ensuring proper cataloging and tracking of the devices that control physical access to network devices. Keys to enclosures need to be cataloged and duplicates need to be securely stored for unanticipated situations. Beyond cataloging, it is important to ensure that all access controls are operational.

OSML: Network Access Controls

Long-term security for the project will be directly related to the level of effort associated with maintaining the security of the network. The following network access controls need to be considered:

1. **Upgrade Network Access Control Firmware as Needed:** Maintenance of all network access control (NAC) devices is critical to the overall security of the network. Periodically, the device's support sites and security bulletins need to be processed. These may lead to firmware upgrades. Only trained and authorized personnel should perform this process.

   An analysis of the overall impact to the running project should be performed prior to any upgrade process. Certain critically place devices may only be upgradable during maintenance periods due to the negative impact to the project due to even a temporary outage.

2. **Ensure Integrity of Network Connections:** The frequency with which network connections need to be inspected is directly related to network criticality and the amount of access non-authorized personnel have to any part of the network.

   It is important to inspect exposed wire runs and cable closets. Additional hardware may have been temporarily added to the network and then forgotten. All unauthorized network equipment must be removed as soon as possible.

   Locked enclosures should be inspected for unauthorized network devices. Debugging equipment is sometimes connected inside of them, and then forgotten. It is important to ensure only authorized equipment is inside enclosures.

3. **Verify Network Segmentation Configurations:** While OT networks are fairly static in configuration, a review is required. This allows for review of changes made to the configuration. From time to time, temporary configurations are needed for debug purposes … and then forgotten. All network segmentation configurations must be returned to a known, secure state.

OSML: User Access Controls

Probably the weakest areas associated with a project's security envelope are the maintenance and assignment of users to proper access levels.

1. **Review List of Users:** The maintenance of users for projects tends to be a significant issue. In the past, many devices only had a single user. Modern systems have the ability to have multiple users, all with varying capabilities.

   When reviewing the list of users, keep in mind the principle of "Least Privilege" that states users should only be given sufficient authority to complete their job … and nothing more. This means that as a user's role changes, assigned capabilities may also change.

   Greater user flexibility comes with higher administrative costs. Managing varying user records by project can be complicated, but must be done periodically.

2. **Remove or Disable Accounts No Longer In Use:** There are usually two options for blocking a user's rights to access a system. Some systems only allow account deletion. Others allow accounts to be deleted or disabled.

The primary advantage of disabling over deleting is that deletion results in loss of all historical user data, and this information can be critical in forensic evaluations. Unless a customer has policies to the contrary, disabling an account allows for the retention of historical user data.

When disabling a record is the chosen option, privacy laws may make it necessary to change the name of the user to something that is not directly associated with the person.

3. **Ensure Password Policy Conforms to Customers Password Policies:** Older systems are often limited to short passwords consisting of only characters. Newer systems have configurable password policies. When using a system's policy editor, make sure the policy entered matches the customer's password policy as closely as possible.

OSML: Backup and Restore Phase

Over the management lifecycle, there are many things that will occur that will require the existence and maintenance of timely backups.

1. **Verify All Backup Schedules:** Backups are things that need to be done, but often don't get done. For systems with schedulable backups, it is important to ensure there is an active backup schedule.

   Beyond active schedule verification, it is also necessary to ensure backups are actually running and there are useable backups for restores as needed.

2. **Verify Backup Integrity:** It is not uncommon for a "known good" backup to fail in a restore operation. For various reasons, the backup file is bad, which renders the restore operation useless. Because this is not uncommon, it is important to confirm the integrity of backup files.

   System backups should always be verified. In most cases, this can be an automatic function of the backup system. For other systems, the only way to ensure the backup is good is to attempt to use it. In this case, restoring a backup file to a test system may be the best solution. Doing so means the operational system will not be affected if the restore fails. It also eliminates downtime for the project.

   If a backup file is determined to be defective, it is very important to understand the source of the problem and get it fixed. Backups are critical to the overall, long-term stability of a project.

3. **Periodic Restore Operations:** It is important to perform periodic restore operations. While verification procedures can raise the confidence level that a backup is good, the only real way to know for sure is to perform a true restore. It is best if this process is done in a scheduled maintenance period.

4. **Transfer Backups to Offsite Location According to Customer Policy:** Many companies use offsite storage for critical system backups. Check with the IT department to determine if the backups of the project are considered company-critical. If they are, work with IT to establish a routine, offsite, backup process.

OSML: OS Patching Phase

Operating systems support the project's functionality and require routine patching to maintain their security envelope.

1. **Schedule Maintenance Periods:** A significant difference between IT and OT is the ease with which servers can be upgraded. For IT, performing a patch or an upgrade to a server's operating system means a given data process will be temporarily unavailable to the users. Such upgrades are usually scheduled for periods when the minimal number of employees will be affected.

   For OT networks, even a short outage can create many significant problems and increase risk. For this reason, OT projects need to planned during regular time blocks when scheduled maintenance can be performed. Due to the complexity and criticality of OT systems in the successful operation of the business, these maintenance periods may only be scheduled infrequently. This can affect the project's security in that many times, operating system defects can open the project to external attack.

   Because of this, it is important to work with the customer's IT department to define the safety issues and ensure scheduled maintenance periods meet their overall needs. There will always be stress between "the need to apply patches" and "the need to keep the business working." Working with the IT department, it may be possible to create temporary mitigating controls that will augment the system's security until patches can be applied safely.

   Ultimately, it is important that there is a well-defined "to-do" list associated with each scheduled maintenance period. This is needed to ensure sufficient time is available to accomplish all required upgrades, and that all required upgrades have been completed.

2. **Obtain Vendor List of Acceptable Patches:** Before any underlying operating system is patched, it is important to contact the application's vendor to ensure the patch will not adversely affect system performance. In cases where a patch is not recommended, it is important to work with the customer's IT department to determine what mitigations may need to be put in place to compensate.

3. **Obtain and Verify Patches:** Many patches are now available from vendor's download sites. While this would seem to be a simple and safe operation, there have been cases where threat actors have found ways to alter a vendor's upgrade files without being detected.

   For this reason, all downloaded patches need to be verified. Most vendors provide digital signatures for their packages. These signatures need to be checked. Upgrade packages that don't pass signature checks should never be loaded.

4. **Apply Patches:** Depending on many factors, some patches may be applied with no apparent affect to the operational characteristics of the project. Others will need to be postponed until scheduled maintenance periods. Again, keep the customer's IT department aware of the status of all pending patches.

5. **Verify System Functionality:** Once the patch has been applied, the upgraded system should be tested to ensure it continues to operate nominally. Issues found may require uninstalling the patch and reverting to the last known good configuration. Ensure the uninstall process is well understood prior to applying the patch.

OSML: Antivirus & Whitelisting Phase

Two of the major controls used to protect hosts are antivirus and whitelisting. Antivirus tools compare "signatures" of files against known infections. Whitelisting systems prevent unknown or non-validated applications from running. Together they provide an effective, but incomplete, protection system for hosts and endpoints. Considerations for these tools follow:

1. **Ensure Antivirus Database is Up-to-Date:** Antivirus programs are common in business and industry. Especially for Windows-based servers, antivirus provides an important function in maintaining the security envelope of the system.

   It is important that the antivirus is periodically updated. This is why many antivirus programs have automatic upgrade capabilities. There are risks with allowing these automated updates to happen and a risk/benefit analysis should always be done.

For systems that are too critical to allow automated updates, periodic manual updates need to be scheduled. Because of the time-sensitive nature associated with antivirus, it may not be possible to postpone all updates to the next scheduled maintenance period.

2. **Verify Logs for Indications of Whitelist Violations:** Whitelisting is becoming a common feature of all operating systems. Systems that use whitelisting do not allow unauthorized applications to run. While this is a good solution for many cybersecurity issues, there can be drawbacks to using whitelisting.

   For systems using whitelisting, it is important to review the logs on a periodic basis. If something stops working on the system, it is important to see if the whitelisting system is causing the problem.

3. **Escalate any Whitelist Violations to Site Management Team:** When issues are identified in the whitelisting logs, it is important to analyze and respond. It is also important to communicate all issues and findings to the IT department in that these issues may indicate an active attack against the larger company.

OSML: Logging & Monitoring Phase

It is common to expect everything to always run well. Unfortunately, this is rarely the case in the real world. When something does go wrong on a computer, the best way to determine the cause is to review the system's log files.

1. **Review System Error Logs:** The system's error log allows review of general errors that have happened on the system. Most of these errors will be associated with operating system errors. For programs that "refuse to run stably," the reason will probably be in the error log.

   Beyond diagnosing unusual runtime issues, periodic review of this log, as well as the other logs below, can help diagnose other system issues. They may also help detect attacks against the system that may indicate a larger attack in progress against the customer's business.

2. **Review System Security Logs:** These logs maintain a record of all security related events in the system. Generally, all log-in and log-out operations are recorded as well as all failed log-in attempts.

   This log can reveal attempts to discover credentials on the system.

3. **Review Application Logs:** Applications tend to put a considerable amount of information into their log files. When applications are not running correctly, reviewing this log file, as well as the error log, may greatly help in diagnosing the problem.

4. **Where Applicable – Verify Connection with Syslog Server:** A "syslog" server is a machine that concentrates all logs into a single place. Doing so allows corporate security experts to better track events throughout the company. It is important to periodically check that all systems using syslog are in fact able to transfer their data to the server.

5. **Where Applicable – Verify Connection with SIEM:** The SEIM (Security Information and Event Manager) server is similar to a syslog server in that it collects event data from across the company. It differs from a syslog server in that it performs continual analysis of all data and provides alerts to operators. It is important to periodically check that all systems that should be tied to the SIEM are, in fact, properly communicating.

OSML: Disaster Recovery Phase

Most believe disaster "will never happen." Frankly, it eventually will happen. Many volumes have been written on how to plan for disasters. While how to create a disaster recovery plan is beyond the scope of this paper, the following three concepts will help in the creation of an OT disaster recovery plan:

1. **Designate Emergency Point of Contact and Contact Information:** An important step in managing a disaster is being able to contact key vendors. When something goes wrong, really wrong, who should be called? This is a simple question with a simple answer… or is it?

   Generally, providing 24/7/365 type of support, or even just "business hour" support, can be a challenge. What happens if the contact person is ill, or on vacation, or simply not available? Disasters generally occur at the worst possible times. Often they may be part of a larger community wide disaster that also affects the customer's site. Customers need to have access to the support staff they need at those times.

   The first step in addressing disaster recovery is ensuring customers have a name and phone number that can be called that will ensure timely response. Many services exist with call lists that will eventually "find someone home" and allow emergency contact to be initiated.

2. **Create Written Disaster Recovery Plan:** There's nothing like writing it down and then going back to read it to help clarify a plan. No disaster can be adequately planned for … but all disasters should be managed by a plan.

   Larger customers may already have an IT disaster recovery plan, and maybe even a business continuation plan. These customers will understand the need to plan and can greatly assist in a plan's creation.

3. **Practice the Disaster Recovery Plan and Correct It Where Needed:** When disaster recovery plans are created, the only way to know if they work is testing. This can be done through the execution of either a "paper exercise" or a "trial run." Each form may identify plan weaknesses that should be corrected to ensure ultimate success.

OSML: System Decommissioning Phase

Most of the time spent on new products and projects is spent on creation and maintenance. Often the concept of how to securely decommission a device or a system is never considered.

There are problems associated with ignoring secure decommissioning. Devices taken out of service that have not been properly decommissioned often contain sensitive information. These devices may be resold on the Internet with sensitive information, which may lead to security problems.

As such, the following best practices are recommended for proper device decommissioning:

1. **Inform Customer the Device Will Be Removed:** As described above, when a device is being replaced, the customer's IT department needs to be informed. They will need to upgrade the asset list as well as change network configurations and assign a static IP address to the new device. Additionally, properly notifying the customer's IT department will help prevent false alarms from connected network monitoring systems.

2. **Where Applicable – Ensure Viable Device Backup:** Often a device will just fail and all data (including possibly the last backup) will be lost. This is a good reason to ensure all backups are moved to a central server or to off-site storage.

   In either case, a device replacement will need a viable recovery backup. It will be important to be aware of any changes that may have been made to the system configuration since the last backup date. Such changes may need to be manually recreated.

3. **Where Possible – Run Device Secure Decommissioning Procedure:** If the device is operational and/or just limping along, after recovering any backup file, run the decommissioning procedure. This procedure ensures data on the device is securely erased, and thus impossible to recover by the next user (if any).

4. **Remove Power and Detached Wiring from Device:** For devices requiring the removal of existing wiring, ensure this process is done is a safe manner. The old device is removed and the new device is installed, re-wired, and commissioned.

5. **Dispose of Device in Compliant Manner (DO NOT RESELL):** For devices in warranty, complete the warranty process associated with the device. Devices not returned to the factory should be physically destroyed.

The OSML

The previous section was intended to clarify the complexity associated with cybersecurity management over the lifecycle of a project. Success may rest on having adequately "qualified" practitioners for each of the various security roles.

A significant difference between OSML and the OSDL or SDL frameworks is the nature of the OSML. Managing overall project security over its lifecycle is a repetitive effort that can be represented as follows:

Figure 11

The OSML Framework Flow

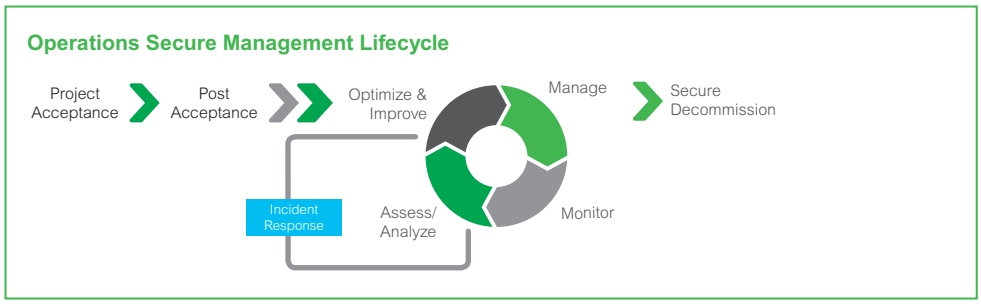


Figure 11 shows the management flow of OSML. At the far left, the OSDL's Post Acceptance phase flows into the OSML framework. Successful lifecycle management requires the performance of regular process practices. In general, these practices are performed in a the "loop" structure with the following phases:

1. **Manage:** The first phase is addressing the following functionalities:
   a. Basic system and equipment maintenance
   b. Compliance with applicable policies and procedures
   c. Reporting
   d. Backup and restore operations
   e. Backup and restore verifications and faulty device replacement
   f. Creation, management, and test of a disaster recovery plan
2. **Monitor:** The second step in verifying security is ensuring the existence of all known network assets. Extra or missing assets need investigation. It's important to stay informed on the threats affecting the system. The system owner/stakeholder must designate people to monitor the security of the system. Nominal steps to achieve this item are:
   a. Systematic review of logs
   b. Monitoring by SIEM
   c. Performing required network scans
   d. Compliance audits
3. **Assess and Analyze:** Part of the Asset ID process is ensuring proper cataloging and tracking of the devices connected to the OT network. This stage includes monitoring keys to enclosures and enclosure contents. Beyond simply cataloging the secured physical access controls, which is important, ensuring that all controls are operational is also necessary.

Long term, the overall security of the project is related to the seamless security of the network. Not all items reported by a SIEM are symptomatic of a security issue, however, some will be identified as a concern and will need to be researched. Typical steps follow:

a. Monitor findings
b. Regular compliance and performance assessments

4. **Optimize and Improve:** In this stage, the following are addressed:

a. Training
b. Policy and procedure updates
c. System patching and upgrades
d. AV and whitelisting updates
e. Maintenance of firewall rules
f. Update disaster recovery plans

This "loop" process continues until the end of the product's life is reached. The timing of each of these stages will be project dependent and may rely upon customer participation. Regular schedules need to be established to ensure all items are address as needed to maintain overall security.

5. **Decommissioning:** As the project reaches its "end of life" it will be decommissioned. When decommissioning a project, the following need to be addressed:

a. Define a replacement plan if applicable
b. Inform stakeholders of pending changes
c. Backup all system data and configurations
d. Follow all decommissioning requirements
e. Safely remove and dispose of equipment

6. **Responding to Events:** While no one wants bad things to happen, from time to time they do occur. This is where Disaster Recovery and Incident Response plans come into play. When applicable, the following should be addressed:

a. Follow the appropriate response plan
b. Perform forensics as appropriate
c. Take preventative and restorative actions
d. Work with state and federal authorities when needed

Conclusion

This discussion of the SDL, OSDL, and OSML frameworks should provide a good starting point for the creation of custom frameworks that meet end-to-end cybersecurity needs for a project. Items can be added or removed as needed.

About the authors

Gregory Strass is the Product Cybersecurity Lead for Building Management Systems (BMS) in Schneider Electric's EcoBuildings line of business. He has over 40 years of experience in embedded, application, and Cloud developments and cybersecurity. He led the effort to integrate the product development SDL process into the BMS development teams. He also works with customers to understand their requirements and needs.

Providing training to all teams associated with the successful integration of various technologies has been a special interest. Often the integration teams have only a vague understanding of how cybersecurity affects their work. For decades, BMS and physical access control systems have been considered "THE" soft target in the world. Today's products have many security features that go unused, often because of a lack of understanding of their purpose.

Michael Pyle serves as Cybersecurity Officer & Vice President of Product Cybersecurity for the Building & IT business unit of Schneider Electric. He has more than 25 years of experience in industrial control and energy management solutions and has spent the last six years in the field of cybersecurity in Operational Technology (OT)

Mike obtained his BSEE & MSEE degrees from Tennessee Technological University. He has been with Schneider Electric since 1990. During this time he has had a variety of roles and responsibilities focused on creating, developing, and maintaining industrial solutions, including leadership of R&D, Offer Creation, Operations, and Innovation.

Mike holds eight patents related to solutions for industrial control systems and has two cybersecurity patents pending.

James (Jesse) Wiegand is the Cybersecurity Compliance Leader for Schneider Electric where he manages a team of cybersecurity engineers specializing in federal government compliance. Jesse has worked in the cybersecurity industry for nearly 15 years. He currently is the Program Manager for Schneider Electric's Cybersecurity Compliance Center.

During his cybersecurity career, Jesse has worked as a penetration tester, an intrusion detection analyst, and served with Air National Guard as a red team member. Jesse has overseen the successful completion of numerous DoD Information Assurance Certification and Accreditation Process (DIACAP) projects and Risk Assessment Framework (RMF) projects.

Jesse believes, while a secure and compliant product is important to a project, it's well trained and educated personnel that are essential to the success of cybersecurity.

Contact us

For feedback and comments about the content of this white paper:

Contact your Schneider Electric representative or visit schneiderelectric.com

Schneider Electric USA
800 Federal Street
Andover, MA 01810
Telephone: 978-794-0800
www.schneider-electric.us
PN SE-998-20140821_GMA-US Rel. 12/17