WHITEPAPER

AVEVA's HMI/SCADA security approach

Mitigating cybersecurity risk through good design and implementation practices

Executive summary

Information security is a key part of AVEVA's business strategy. The security of our HMI/SCADA offerings is paramount and is achieved using a rigorous Security Development Lifecycle (SDL), and providing guidelines for secure implementation practices to our customers.

This whitepaper details how AVEVA mitigates Information Security risks in our HMI/SCADA offerings.

Introduction

AVEVA has been involved in the development and deployment of HMI/SCADA systems for over 30 years. Our HMI/SCADA systems continue to empower our customers to automate, optimize and get the most out of their industrial processes. Our customers use our products across a wide variety of industries, including Chemicals, Food and Beverage, Infrastructure, Life Sciences, Marine, Mining, Oil and Gas, Power and Utilities, Pulp and Paper, Steel Fabrication and Water and Wastewater.

Across our industrial and critical infrastructure customers, safety and reliability is the foundation of their operations ensuring safety of people (both employee and public), environmental safety and reliable operations.

At AVEVA, the safety and security of your operations including your applications and environment is our top priority and is why we follow industry best practices to continually improve the security posture of AVEVA applications.

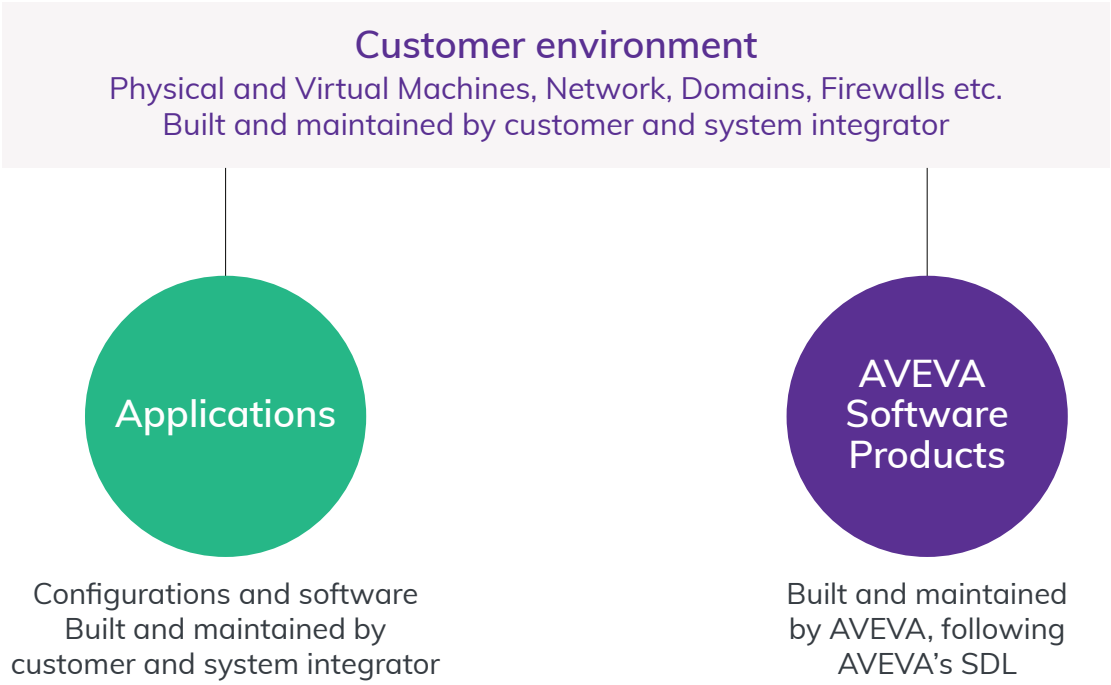
Shared responsibility

AVEVA follows a rigorous Security Development Lifecycle (SDL) to ensure our products are as secure as possible.

Our customers then install and configure these products in their environments, building applications to suit their needs. Customers and integrators must also follow good security practices to ensure that the resulting system is well designed and maintained to mitigate security vulnerabilities.

The following sections:

- Describe AVEVA's Security Development Lifecycle (SDL)
- Make recommendations for securing the customer environment
- Make recommendations for secure application development and deployment



AVEVA's Security Development Lifecycle

AVEVA's Security Development Lifecycle (SDL) is a core element of our Software Development Process (SwDP) framework. Our Quality Management System (QMS) and SwDP are regularly evaluated and maintained to incorporate process efficiencies, improved quality and security practices, and provide better value for our customers.

The SDL process applies to all product offerings and ensures that our applications are developed with security at the core from design and architecture to implementation, testing, and operations.

The SDL is focused on delivering secure software and compliance with industry best practices for designing, developing, and releasing secure software to customers. The following high-level activities occur during all development projects:

- Training
  - Software Developers are required to be trained in SDL practices.
- Requirements
  - The Security Requirements are defined and managed in a Requirements Management System.
  - Security Risk Assessments of requirements are performed.
- Design
  - Security Design Requirements are considered for all projects.
  - Tools are used to identify and mitigate potential security vulnerabilities.
  - Threat Models are developed to better understand potential risks.
- Implementation
  - Static Application Security Testing, Software Composition Analysis, and compiler options are utilized during projects.
  - Unsafe functions are deprecated to reduce risks.
  - Code Reviews ensure compliance with Security Practices.
- Verification Testing
  - Tools are utilized to monitor the application behavior of any security risks.
  - Data validation testing ensures application behavior.
  - Tools are used to determine changes in the product's surface area.
  - Penetration testing is done regularly.
- Release
  - Security Reviews are conducted before each software release.
- Response
  - Incident Response Plans are followed for any anomalies.

Our SDL process is compliant with the ISA/IEC 62443-4-1 standard for Secure Product Development Lifecycle requirements and has achieved ISASecure SDLA Certification.

Securing Industrial Control Systems

Industrial Control System (ICS) cybersecurity programs should always be part of broader ICS safety and reliability programs at both industrial sites and enterprise cybersecurity programs because cybersecurity is essential to the safe and reliable operation of modern industrial processes. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, accidents, and natural disasters as well as malicious or accidental actions by insiders. ICS security objectives typically follow the priority of availability and integrity, followed by confidentiality.

ICS cybersecurity should be based on the NIST Cybersecurity Framework (CSF) and should also follow the guidelines in NIST SP 800-82. The ISA/IEC 62443 family of standards also contains very useful information. See reference1, 3 and 4 for details.

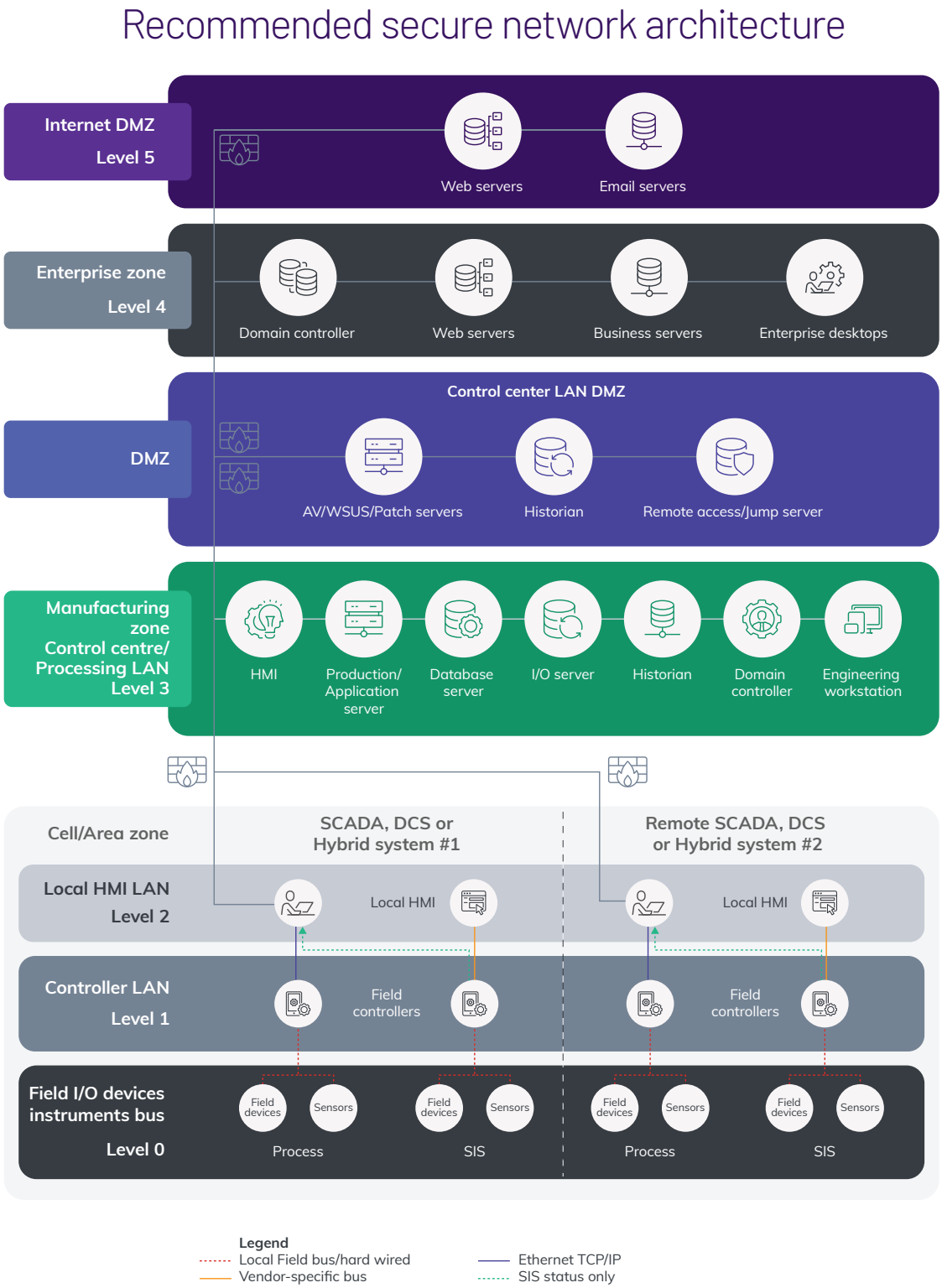
The NIST CSF consists of the following core functions:

- Identify: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect: Develop and implement appropriate safeguards to ensure the delivery of critical services.
- Detect: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident
- Recover: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Major ICS cybersecurity objectives found in NIST SP 800-82 are outlined in the following sections.

Recommended secure network architecture

Industrial Control Systems (ICS) were traditionally deployed on isolated Operational Technology (OT) networks. This is no longer the case, and convergence with IT networks is commonplace. However, unauthorized access to the OT network could result in unlimited access to the ICS. Therefore, it is important to segment the network and separate different zones using firewalls and virtual network technology. The figure below shows an integrated network architecture showing different zones/segments and mapping these to the SP-99 (Purdue) Model of Control.



Physical security

Physical access to the ICS equipment should be restricted to prevent unauthorized access.

Security patches

AVEVA performs compatibility testing for Microsoft security patches, and publishes the results on the Security Central Portal that is accessible by customers with Global Customer Support contracts.

Security patches for the host Operating System should be deployed as soon as possible after they are tested for compatibility with the ICS Software. Security patches for the ICS software should be deployed as soon as possible after release.

User privileges and security controls

Users should be given the least privilege necessary to perform their role functions. Logging and monitoring should be used to provide audit controls. Antivirus software should be installed on all endpoints.

Data integrity

Data should be restricted from unauthorized modification both in transit and at rest. Secure protocols (e.g. TLS) should be implemented wherever possible, and encryption should be used for data at rest wherever possible.

Detection of security events

Security events should be detected and monitored to help defenders break the attack chain before attackers achieve their objectives. Failed ICS components and unavailable resources or services should be detected to ensure the proper and safe functioning of the ICS.

Redundancy and resilience

The ICS should be designed so that each critical component has a redundant counterpart. It should also be designed so that it fails safely and should allow for graceful degradation such as moving from normal operation through stages to emergency manual operation with no automation.

Disaster recovery

An incident response plan needs to be in place and should include recovering from backups after an incident has occurred.

Defense in depth

A strategy of Defense in depth should be followed to limit the reach of any given failure or exploit. References #1 and #2 provide detailed guidelines for implementing defense-in-depth, but typically this strategy should include the following in addition to the above items:

- Developing security policies, procedures, training and educational material that applies specifically to the ICS.
- Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.
- Addressing security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning.
- Designing critical systems for graceful degradation (fault-tolerant) to prevent catastrophic cascading events.
- Using separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).
- Using modern technology, such as smart cards for Personal Identity Verification (PIV).
- Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
- Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate.
- Tracking and monitoring audit trails on critical areas of the ICS.
- Employing reliable and secure network protocols and services where feasible.

Cloud computing and edge devices

Cloud solutions are becoming more prevalent, and AVEVA is investing heavily in Cloud computing solutions and Edge computing.

Edge computing devices are located at the asset location, within the customer's environment. They are controlled via the Cloud and make secure connections to the AVEVA Cloud environment.

These connections are protected by TLS (Transport Layer Security) and are initiated by the Edge Device. From a networking perspective, they require a single outbound port to be open and can be routed via DMZ and network security devices and tools.

Application and solution security

AVEVA Follows a rigorous SDL process to build secure software products but this is only part of ensuring the overall solution is secure. The end customer, application developer and/or system integrator configuring and implementing the solution with these products also need to follow good security practices to ensure their networks and environments are secure. Everyone involved in the final solution needs to follow good security development lifecycle practices when building and configuring applications. These practices need to include:

- Securing the environment and network where the application development is done.
- Following good SDL practices, including
  - Security training
  - Threat Modeling
- Secure coding practices for any code that is written
- Scanning with Static Application Security Testing (SAST) tools
- Scanning with Software Composition Analysis (SCA) tools
- Verification testing
- Penetration testing
- Creating and maintaining Incident Response Plans

Essentially the system integrator needs to follow the same good SDL practices as any software developer to ensure that the solution is designed and built to be secure, and to ensure that no malicious software is introduced.

Conclusion

AVEVA offers highly scalable, robust and secure products by following industry-leading best practices in terms of secure product development.

References

1. NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
2. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies Industrial Control Systems Cyber Emergency Response Team September 2016 www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
3. NIST Cybersecurity Framework (CSF) www.nist.gov/cyberframework
4. Add 4th reference: 'ISA/IEC 62443 www.isa.org/intech/201810standards

To learn more about AVEVA's HMI/SCADA software visit: aveva.com/monitor-and-control