AVEVA

November 2021

WHITEPAPER

# AVEVA Enterprise SCADA and pipeline management security overview

Authored by:

-

**Jake Hawkes**

Senior Product Manager, AVEVA

## Executive summary:

Few industries require security more than those concerned with the management and protection of natural resources. With the security-integrated capabilities of AVEVA Enterprise SCADA, your organization can keep pace with ever-evolving security protocols and rest easier knowing that you are safely on your way to a more secure future.

# Introduction

AVEVA Enterprise SCADA brings together industry-leading pipeline control and management strategies with a powerful cybersecurity framework, delivering a flexible and secure solution to meet the needs of critical infrastructure operators. All pipeline management modules are integrated with Microsoft's Active Directory and share a unified security model, which means you can manage and monitor them all from one central location. This ensures the consistent application of security controls across your solution ecosystem as well as flexible integration with existing site infrastructure.

We designed our pipeline management software with industry standards and best practices at the forefront. Our solution arrives out of the box with a hardened configuration so that your information remains locked down and secure against whatever tomorrow's cybersecurity threat may be. The software is compatible with common security applications and tools, like multi-factor authentication and centralized log management, providing your organization strength today and a clear path to a more secure tomorrow.

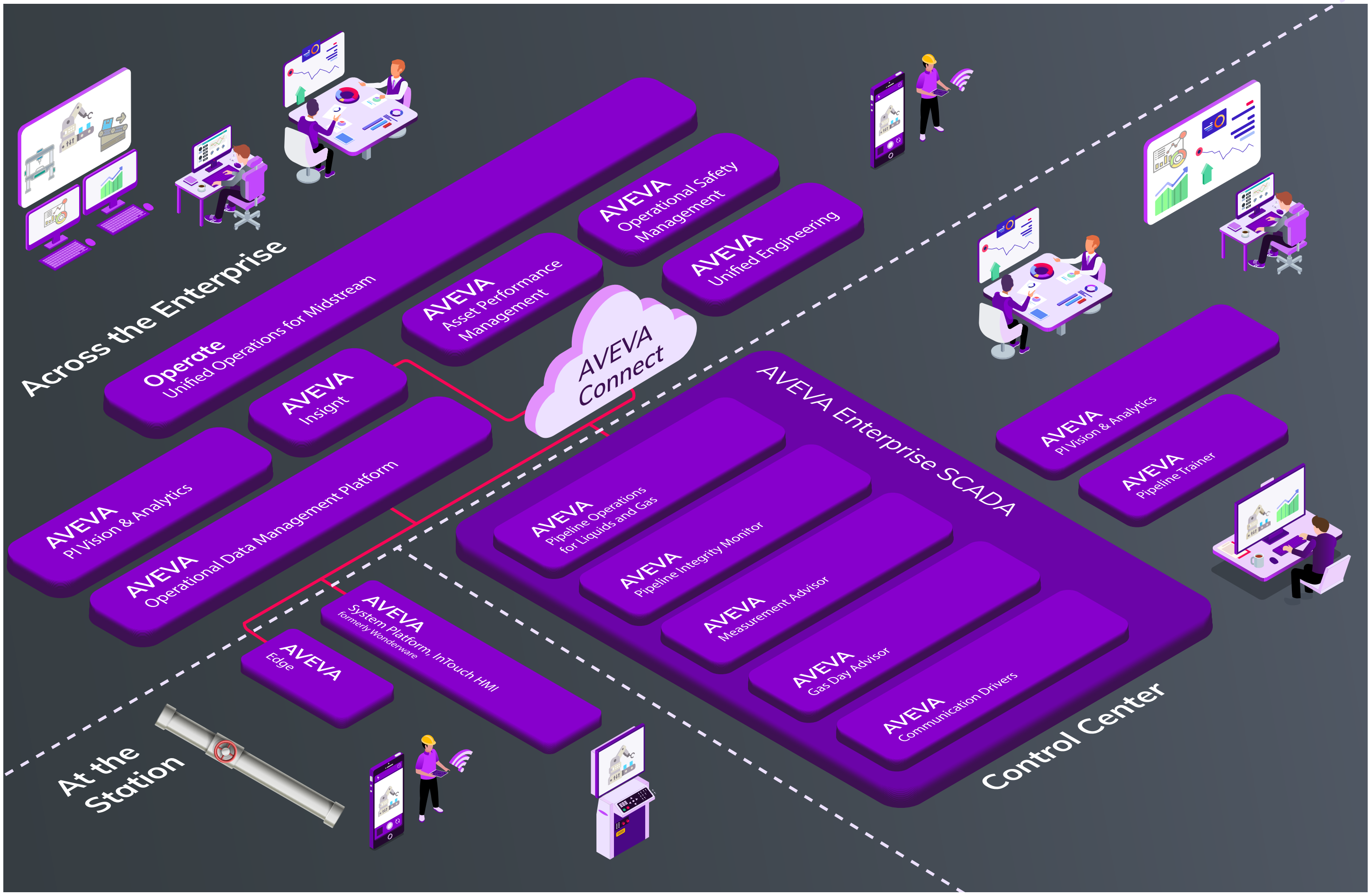


Figure 1: Pipeline management modules from edge to enterprise

# Cybersecurity

We understand the importance of incorporating robust and resilient cybersecurity controls in all our offerings. Our midstream products focus on more than meeting regulatory and standards compliance; they're aligned with industry best practices and prioritize flexibility. Flexibility is important. We want to make it easy for you to use a wide range of third-party security applications and infrastructure. With this built-in flexibility, our pipeline management system will remain secure long after you first deploy it.

By building on common platforms, such as Microsoft Windows and Microsoft SQL Server, our pipeline management solution draws on your security team's skill set to support your existing cybersecurity infrastructure.

## Multi-level security strategy

Our approach is both defense-in-depth and detection-in-depth, providing your organization protection in layers of security. We design all our products with multiple levels of security to ensure that even if a single security control fails, other controls will still provide protection.

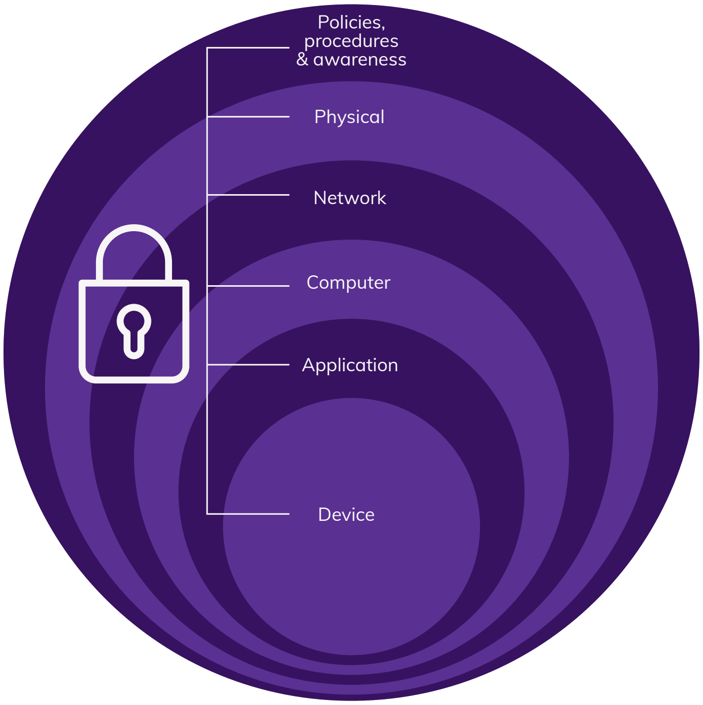
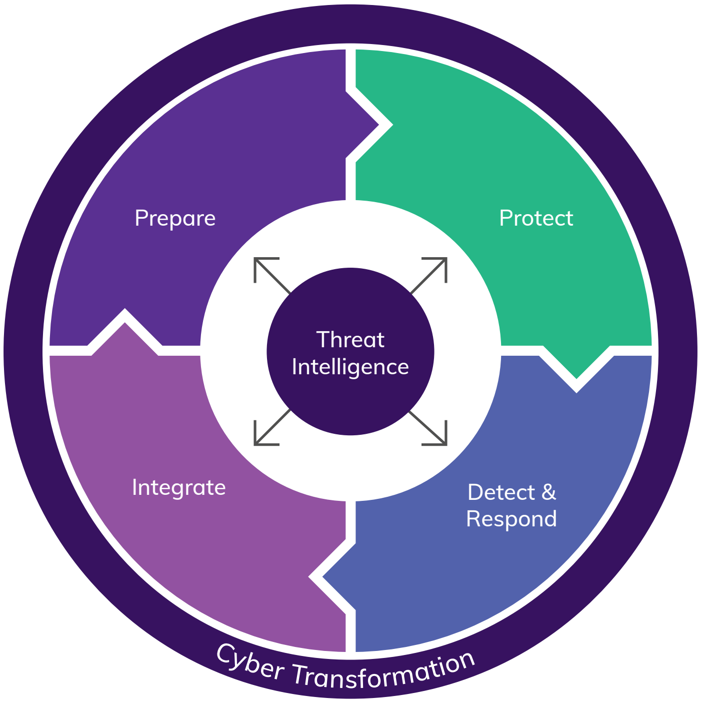


Figure 2: Defense-in-depth strategy



## Cybersecurity standards

There are a lot of different cybersecurity standards, regulations, and best practices out there in this complex security landscape we now live in. To help you navigate them, we've identified the most widely applicable of these measures and developed our pipeline management solution to satisfy all applicable technical requirements. You can rest assured knowing that our solution will provide real security for your assets and will help you meet your compliance objectives at the same time.

Key standards, regulations, and best practices followed by the pipeline management include:

- Microsoft's security recommendations
- NERC CIP
- ISA99 / IEC 62443
- API 1164
- NIST 800-53
- NIST 800-82
- Guidance from control system cybersecurity procurement language

# Security and network architecture

Our pipeline management solution includes different environments, each with different operational requirements needed to meet both business and security goals. To ensure business continuity while preventing unauthorized access to the solution components, the system architecture isolates the different environments through well-defined security zones. In general, we divide the solution into three distinct environments:

- Operational environment, consisting of pipeline management applications that support real-time control operations
- Business environment, providing non-operational access to shared information
- Test environment, for management of change facilities

Each environment, or security zone, encompasses a set of pipeline management application servers within its electronic security perimeter, allocated to serve a specific group of users. The pipeline solution software establishes security zones through:

- Active directory domains, which isolate different classes of users and data between operational and business environments
- Network segmentation, which refers to a collection of isolated networks established to reduce the network attack surface

The software architecture classifies these zones by security level, from highest to lowest, with the most critical production zone set as the highest. The architecture of our pipeline management solution only allows TCP/IP connections initiated from higher to lower security zones, which means that between the production zone and any other zone, such as the DSS or DMZ, only the production zone initiates connections. Production does not require incoming connections for the system to function.

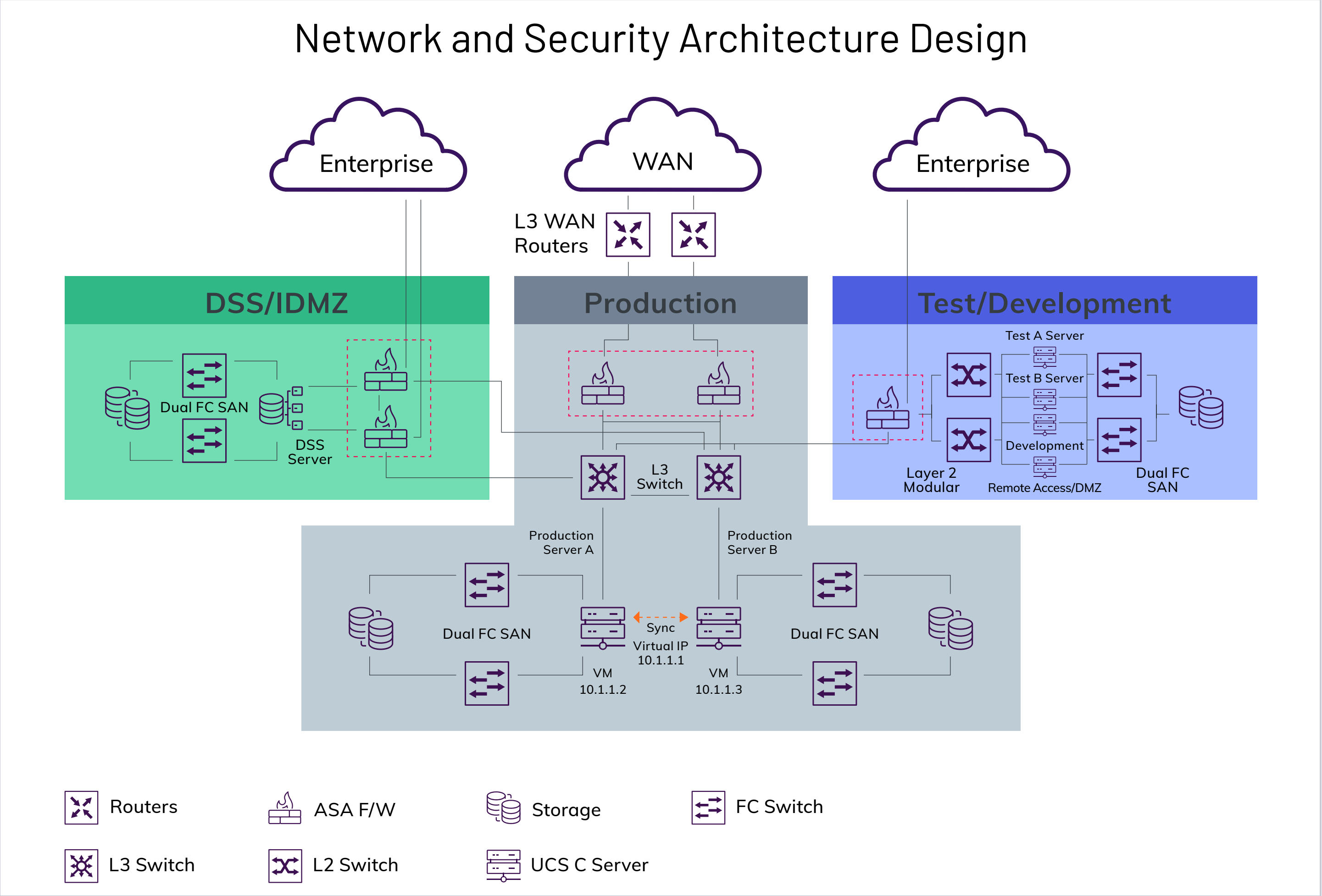

Network and Security Architecture Design

Figure 3: Network and security architecture design

### Active Directory domains

Our pipeline management solution uses Active Directory domains to segregate roles and responsibilities by providing separate authentication mechanisms and user access controls within each environment. Each environment is designated as a separate Active Directory forest, and each forest requires independent credentials for users to access the operation and business environments.

### Network segmentation

A security zone encompasses one or more network segments that represent an administrative boundary under the control of a single authority and security policy. Every pipeline management environment resides on a separate virtual local area network (VLAN) segment with an assigned IP scope. Network segmentation with VLANs creates a collection of isolated networks within the data center. Each network is a separate broadcast domain that reduces packet-sniffing capabilities and operates under the principle of least privilege, giving authorized users only as much access as they need to do their jobs. Another advantage of segmentation is protocol separation, which limits certain protocols to certain segments.

Our pipeline management solution uses a demilitarized zone (DMZ) as a perimeter network segment logically placed between two security zones, with the aim of preventing network traffic from passing directly between the corporate and operational networks. The pipeline management DMZ architecture uses firewalls placed between two networks to prevent external users from directly accessing the operational environment.

The pipeline management solution also uses switch port security to limit physical connections inside a VLAN. We configure individual switch ports to allow only a specified group of source MAC address to traverse these ports.

### Perimeter protection

Pipeline management environments interface with each other through a standby redundant pair of firewalls. The standby failover allows the redundant firewall to take over the functionality of the failed firewall partner by assuming its IP and MAC addresses to maintain the connection state.

We place network-based firewall appliances at strategic locations between trusted and untrusted networks to establish security boundaries. Trunking VLANs from these firewalls, for each environment, enables traffic segregation (admitting only tagged packets) and security restrictions through appropriate firewall rules.

Firewalls are configured to deny by default, only allowing communication between specific hosts on authorized ports. We provide customers with a least-privileged firewall ports list that should be applied within the pipeline management environment.

Administrative users can also deploy network-based intrusion detection systems (IDS) at the same security boundaries to monitor network activity between different network segments, identify suspicious patterns, and act as a security check on all transactions that take place in a specific environment.

The virtual private network (VPN) tunneling feature on the firewall devices provides secure connections to the pipeline management environment from a remote network.

## Identity and access management

We designed the pipeline management solution to integrate with Microsoft's Active Directory Domain Services (AD-DS), providing a scalable, centralized, and secure infrastructure for user and access management. Active Directory enables the pipeline management solution to merge customer business processes, security policies, and technologies to manage digital identities and control resource access.

Our pipeline management solution uses several AD features illustrated in Figure 4:

- User and group provisioning refers to the creation and management of user accounts and pipeline-management-specific authorities (security groups).
- AD ensures the consistent application of account and password policies to all computers and users across the whole environment.
- The LDAP-based user and configuration data store makes the pipeline management components compatible with any other LDAP-based security provisioning systems.

- Integrated Windows Authentication mechanisms provide mutual authentication, giving the Microsoft Windows Active Directory domain controller (DC) the role of the mutually trusted third party.
- Single-sign-on (SSO) improves user experience by allowing users to access pipeline management applications after logging in to the domain without the need to re-enter their username and password.
- Role-based access control (RBAC) enables flexible user rights configuration, which are easily adapted to a customer's organizational role structure and support user management efficiencies and secure practices.

## Account management

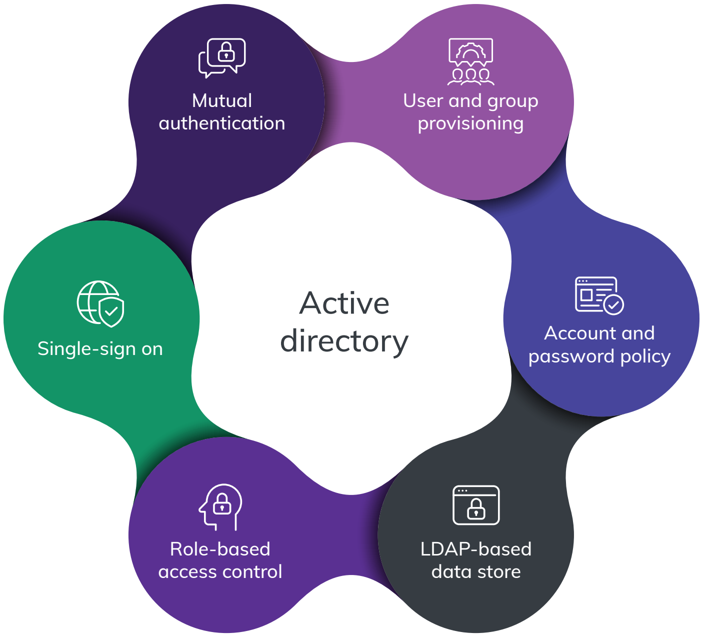

Mutual authentication
User and group provisioning
Single-sign on
Active directory
Account and password policy
Role-based access control
LDAP-based data store

Figure 4: Active Directory features used in pipeline management

Our software enables your administrators to manage accounts in the pipeline management environment centrally through Active Directory. Centralized management reduces operational complexity, improves security through accountability, and lowers the risk of misconfiguration since the software applies all changes consistently throughout each domain.

The pipeline management solution provides each user a unique account through which all access is managed, both within the operating system and the pipeline management software itself. The software prevents service accounts, used to run pipeline management services, from performing interactive logins. Service accounts operate with reduced capabilities, reducing the risk of exploitation by an attacker.

## Generic and default accounts

Our pipeline management solution does not require any generic accounts, guest accounts, development accounts, or default accounts provided by hardware components, operating systems, or database providers. All well-known default local Windows user accounts are disabled on all pipeline management workstations and servers.

During the installation process, you will create maintenance accounts to enable the setup of the pipeline management software, but these accounts are not required for the software to work. Administrative users can disable these accounts before commissioning and then enable them in the future as required (e.g. for software updates and maintenance activities). This includes an installer account, which can install the pipeline management software but cannot configure and operate the software, and a SCADA admin account, which can configure the software but has no system rights.

## Password management

The pipeline management solution enforces strong password usage throughout the environment. Password complexity is fully configurable and managed through the Active Directory password policy. Active Directory policies can enforce password requirements such as password history, age, length, and complexity.

Active Directory stores all passwords in a secure manner. When users change their account passwords, those changes automatically extend throughout the whole system without the need for system administrator intervention. The pipeline management software does not store hard-coded passwords.

## Active Directory Lightweight Directory Service

All pipeline management services use Microsoft's Active Directory Lightweight Directory Service (AD-LDS) as a locally available global database. Pipeline management services deploy, and continuously synchronize, AD-LDS instances on every machine in the pipeline management environment.

The global database stores system and security configuration information and serves as an integration point with Active Directory. It assigns user accounts in Active Directory to security groups in AD-LDS, which then define the user access rights throughout the associated pipeline management environment.

# Access management

Active Directory group policy object (GPO) definitions lock down all resource access across the pipeline management environments.

## Authentication

Our pipeline management solution uses the Active Directory-integrated Kerberos authentication protocol to provide secure authentication and single-sign-on (SSO) within a domain.

The use of Active Directory and Kerberos for authentication allows us to utilize additional security features, such as multi-factor authentication, which requires additional proof of identity during the authentication process beyond a username and password. Our pipeline management solution supports all major Microsoft Windows-supported forms of multi-factor authentication (smart cards, tokens, etc.), although they are not built into the system by default.

## Authorization

Our pipeline management solution provides a flexible and automated authorization scheme based on the principle of least privilege (no user has more privileges than are required to perform their typical operational tasks) and separation of duty (no single user has the ability to fully compromise a system or application), encouraging a system of checks and balances.

This authorization schema has two levels of control:

- Role-based access control, which assigns users permissions and authorities based on their role in the organization.
- Area of responsibility (AOR) access control, which assigns users additional application-level permissions (view, edit, and control) over a defined division of assets or region.

Administrators can assign different rights to a workstation in less secure locations outside the physical or electronic security perimeter to restrict access to any user logged onto it, (e.g. allowing a workstation to be configured as a read-only terminal independent of a user's actual permissions).

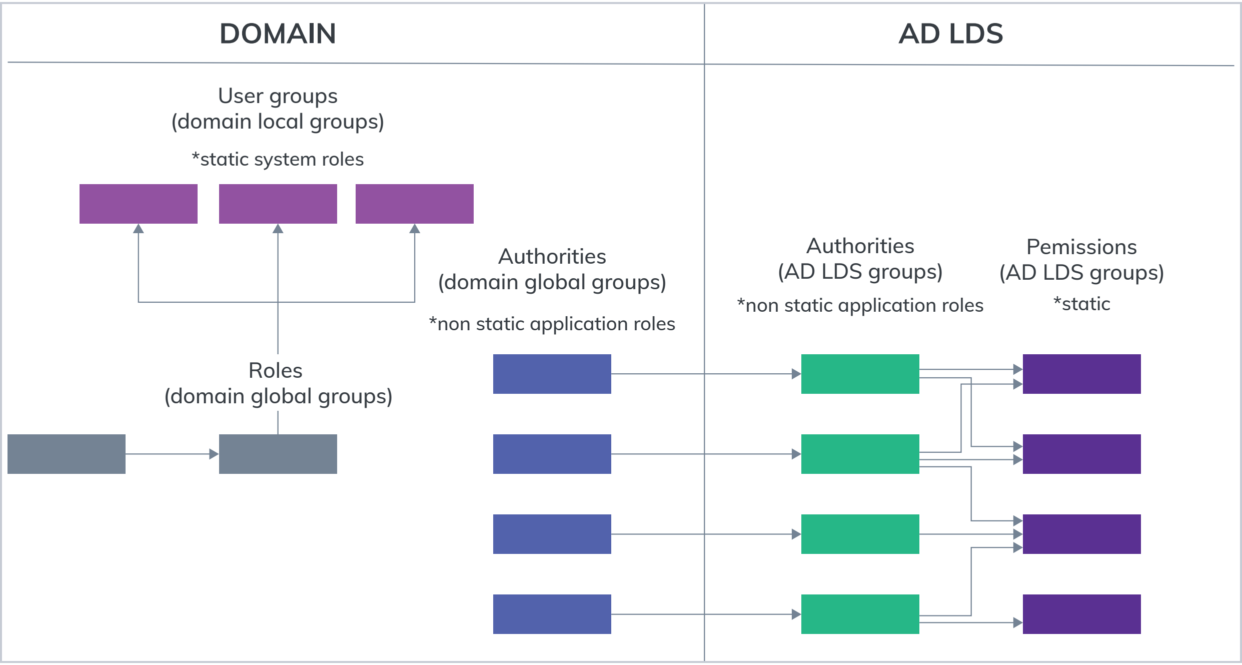


Figure 5: Role-based authorization schema

## Role-based access control

Role-based access control is based on Active Directory security group membership. Users inherit privileges from those groups they are members of. To ease administration, users should be assigned to groups that represent their role in the organization. Administrators can then assign these security groups (roles) to authorities, which define the desired level of pipeline management application access users should be allowed.

- An authority represents a set of appropriate application rights (permissions) that are checked inside the pipeline management software to restrict or allow access. Pipeline management permissions are capabilities or rights that define application-level control of the pipeline management resources and operations, thus describing an operational role (job function). Permissions are created in AD-LDS and authorities are hierarchical Active Directory security groups.
- User groups define file access restrictions (access control lists define access to objects on a file system), access to Microsoft SQL Server, and any other Active Directory-aware application.

## Area of responsibility access control

Area of responsibility (AOR) is an additional application-level (traditional SCADA construct) concept that helps to control user access based on defined boundaries. To build this access control schema, the pipeline management software defines entities called AOR areas and AOR groups:

- AOR groups represent a logical set of closely related assets or features of assets (e.g. all station equipment may have a logical grouping).
- AOR areas provide user access rights (view, edit, and control) for a set of AOR groups.

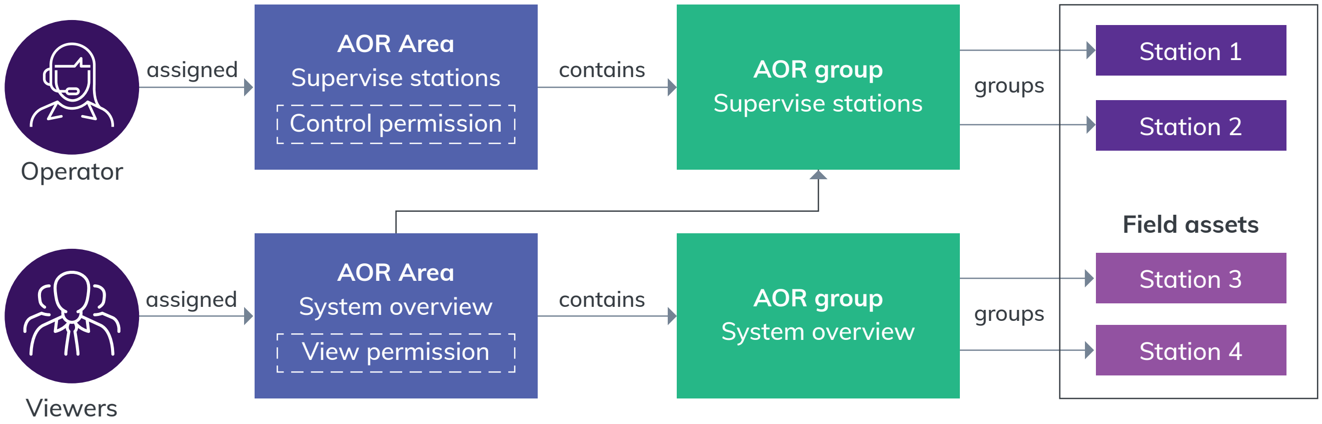


Figure 6: AOR-based authorization schema

AOR area and AOR group entities are defined as security groups in AD-LDS.

- Auditing provides the necessary evidence to explain who, what, where, when, and how resources are accessed in the pipeline management solution. The pipeline management system also provides detailed logging of the following activities:
- Authentication events
- Authorization events
- Directory object modification

All events are logged in Windows Event logs:

- Operating system events include both successful and unsuccessful account access attempts and are enforced across the domain for all users via account auditing policy settings
- Application-level events include user authorization activities on pipeline management services, along with pipeline management security configuration changes (authorization scheme changes, AOR configuration changes, etc.)

Active Directory audit policies are set to capture access success and failures, including account logins, directory service access, and privileged user access, and are enforced by Active Directory group policy objects.

## Security hardening and malware protection

Our pipeline management solution enables developers to meet compliance of all major hardening guidelines, including but not limited to Microsoft secure server hardening guidelines, NSA guidelines, and key industry standards.

To minimize the attack surface and malicious exploit exposure, we designed our pipeline management solution in accordance with security hardening best practices by making changes to the default configuration of the operating system, software applications, and required third-party software to eliminate as many security risks as possible. Our robust security hardening approach is based on:

- Security policies
- Regular scanning
- Hardening checklists that include different security practices

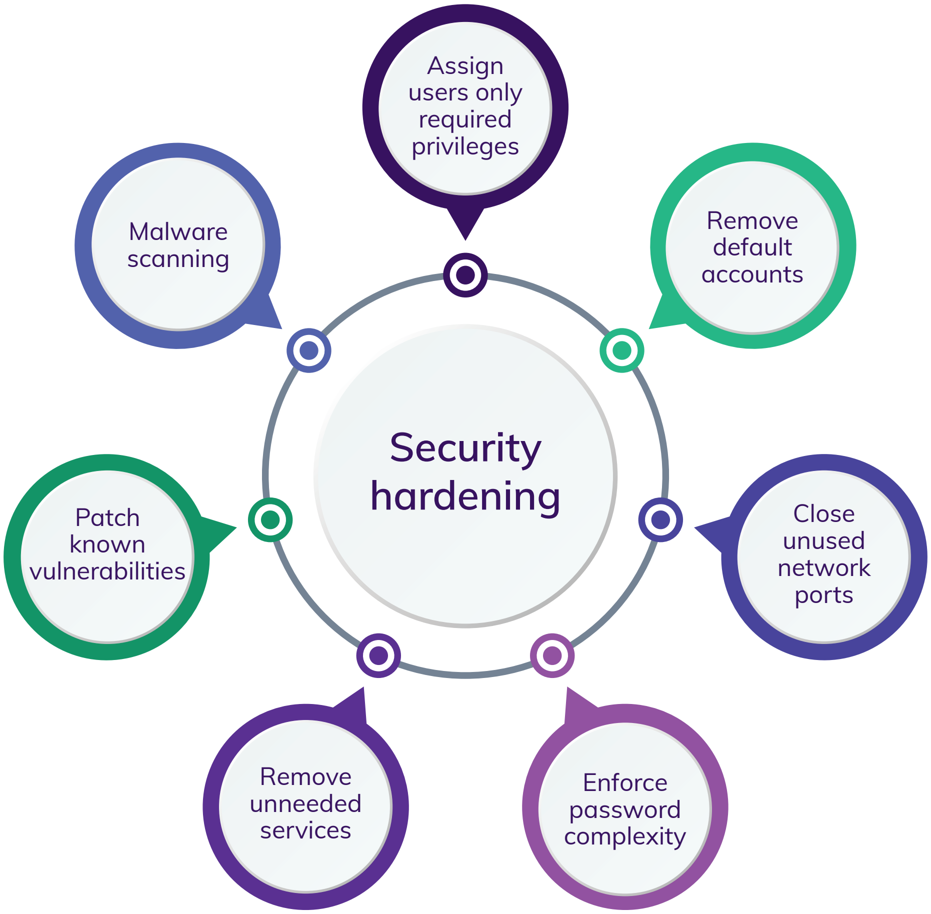

Assign users only required privileges
Remove default accounts
Close unused network ports
Enforce password complexity
Remove unneeded services
Patch known vulnerabilities
Malware scanning
Security hardening

Figure 7: Security hardening principles

## Removal of unneeded services, software, and accounts

Prior to commissioning, we disable or remove all services and software programs that are not required for operation and maintenance of the pipeline management software. While these services and programs may offer useful features to the user, we remove them to eliminate a potential threat (attack) vector. Disabled or removed items include:

- Specific Windows applications, such as games. Unprivileged users may also be restricted from installing additional software
- Device drivers not required for the delivered hardware configuration
- Hardware configuration, such as USB ports, CD and DVD drives, and other removable media devices
- Internet services
- Unused and non-secure communication protocols (e.g. HTTP, Telnet). Secure network communication protocols are enabled when required (HTTPS, SFTP, SSH, TLS, etc.) to support specific operational requirements
- Unused administrative utilities, diagnostics, network management, and system management functions
- Programs, scripts, databases, configuration files, and other files used for development and/or testing

Our pipeline management solution does not require any generic, default, or guest accounts. All unnecessary accounts are disabled or removed. Password and account hardening rules enforce strong passwords for all user accounts, as well as audit user account activities to monitor unauthorized access attempts.

The AVEVA solution also utilizes Active Directory group policies to enforce hardening configuration on appropriate servers and workstations. Additional group policy objects are created during installation to enable a higher level of security for specific services, including providing a locked-down configuration for non-administrative users. The locked-down configuration only allows users on operator workstations to control the pipeline.

Group policies enforce lockdown settings such as disallowing add/delete items, disabling Active Desktop, and preventing access to shut down, restart, sleep and hibernate commands.

## Principle of least privilege

Our pipeline management solution is configured in accordance with the principle of least privilege. No user account is assigned more privileges than required to perform their typical operational tasks. Furthermore, all hosts are configured with least-privilege file access rights (ACLs), and no pipeline management service account requires administrator privileges on the operating system.

Least-privilege firewall port configuration is also enforced. Firewalls are configured to deny access by default and open only the minimum required ports.

## Malware scanning

To remain free of malware, your system will require periodic scanning for viruses, worms, Trojan horses, and other software contaminants. Scanning, however, can impact system performance as it requires files to be locked during scanning. To achieve a balance between a secure environment and system performance and reliability, certain pipeline management files and folders that encounter the most frequent activity require exclusions. We provide configuration guidelines containing the list of folders and files that need to be excluded from scanning to ensure the anti-malware application does not pose an undue operational risk.

Administrative users will need to configure the anti-malware application to issue notifications when malicious activity is detected. We recommend that users enable automatic malware removal or quarantine behaviors.

The pipeline management system is certified for use with the CylancePROTECT anti-malware solution.

## Software updates and patch management

As part of ongoing system maintenance, AVEVA issues regular updates to the application software through our patch management and update process. Additionally, we rapidly review, test, and approve all Microsoft monthly security patches to ensure stability of our customers' pipeline systems.

We maintain an internal patch testing program to provide initial validation of all Microsoft security patches (MSXX-XXX) before approving them for use with our software. This allows us to identify problems introduced with a security patch, which builds on the additional due diligence that we perform on customers' pipeline management test environments before patch promotion.

We apply updates and patches to the pipeline management solution without affecting the normal operation of the system (no downtime). First, we apply updates to the test environment and then, following validation, we roll the update out to the other environments.

## Security development lifecycle

Our development organization follows a rigorous security development lifecycle (SDL) for all software products and projects that are delivered to our customers. The SDL is a component of our software development process (SwDP), governed by a formal quality management system (QMS) process framework. The SDL follows security best practices aligned with IEC 62443 and utilizes a selection of third-party security tools and technologies.

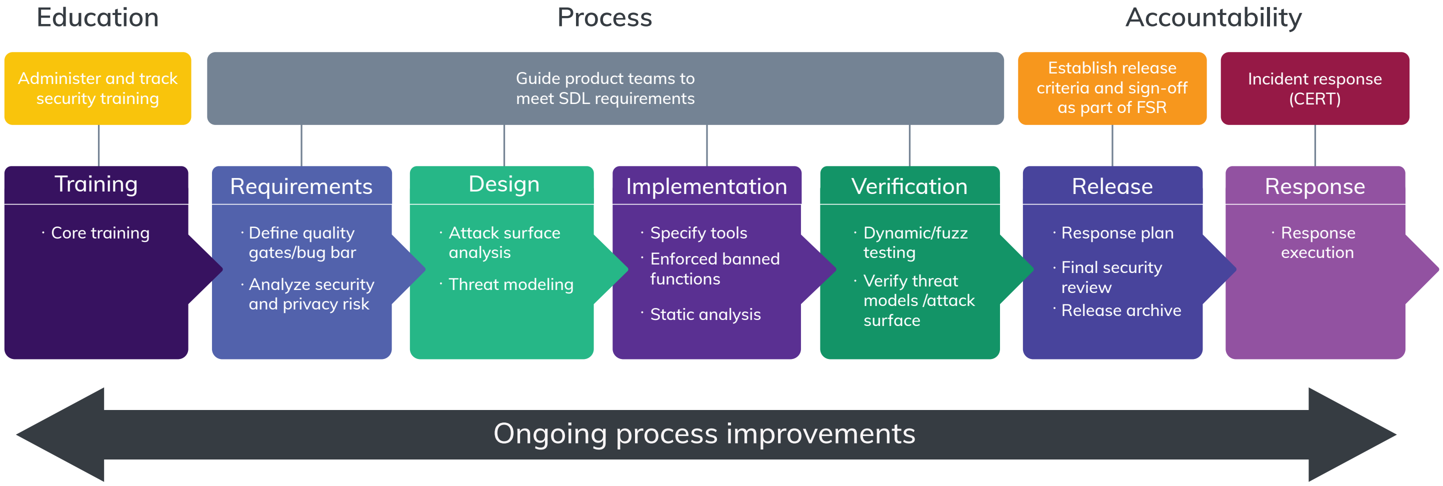

Education
Process
Accountability
Administer and track security training
Guide product teams to meet SDL requirements
Establish release criteria and sign-off as part of FSR
Incident response (CERT)
Training
· Core training
Requirements
· Define quality gates/bug bar
· Analyze security and privacy risk
Design
· Attack surface analysis
· Threat modeling
Implementation
· Specify tools
· Enforced banned functions
· Static analysis
Verification
· Dynamic/fuzz testing
· Verify threat models /attack surface
Release
· Response plan
· Final security review
· Release archive
Response
· Response execution
Ongoing process improvements

Figure 8: Security development lifecycle phases

### Details

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

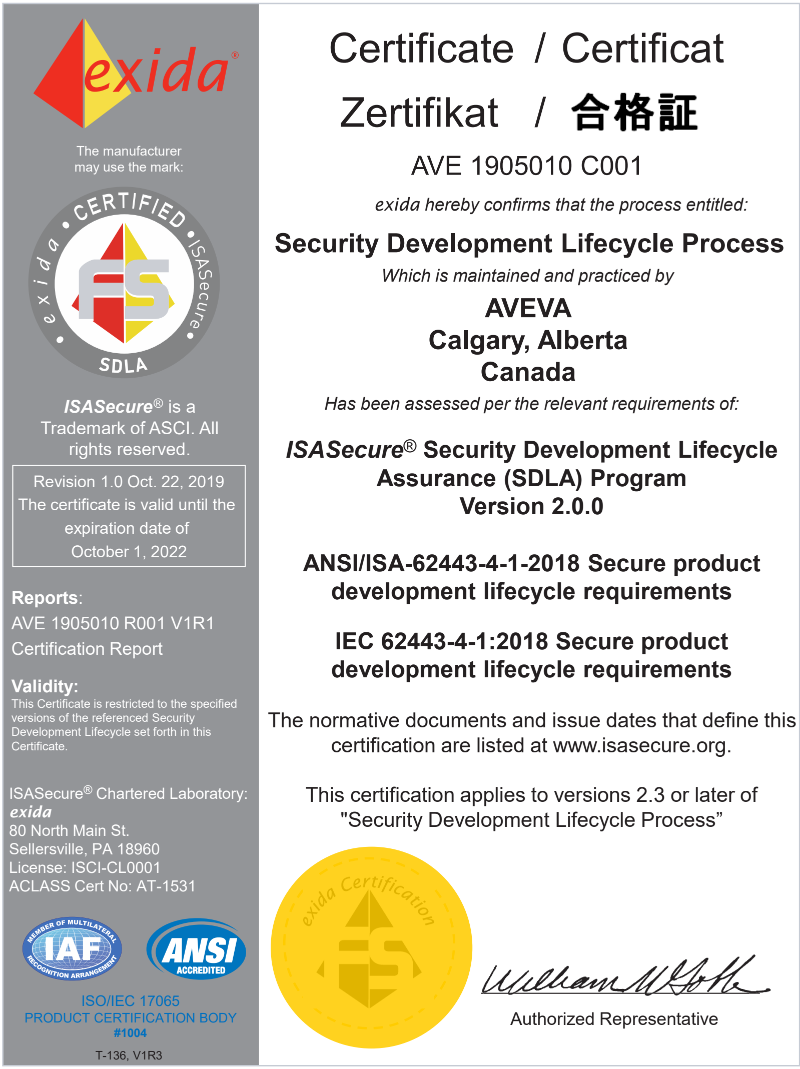
- Training
  - Software developers must train in SDL practices
- Requirements
  - Define and manage security requirements in a requirements management system
  - Perform security risk assessments of requirements
- Design
  - Consider security design requirements for all projects
  - Use tools to identify and mitigate potential security vulnerabilities
  - Develop threat models to better understand potential risks
- Implementation
  - Utilize static code analysis and compiler options
  - Deprecate unsafe functions to reduce risks
  - Code reviews ensure compliance with security practices

- Verification Testing
    - Use tools to monitor application behavior related to security risks
    - Data validation testing ensures application behavior
    - Use threat models to determine changes in the product surface area
- Release
    - Conduct final security reviews prior to a software release
- Response
    - Follow incident response plans for any encountered anomalies

## Governance

Our software product development follows a comprehensive software development life cycle process called SwDP (software development process). The SwDP process framework is based on agile development methodologies using Scrum. All products are developed using the SwDP process and the corresponding policies and procedures that comprise our quality management system (QMS).

A corporate product quality assurance (PQA) team, independent of the R&D organizations, performs oversight. The corporate PQA team audits 100% of our SwDP executed releases and approves all products prior to release, indicating that the product development process complies with the SwDP process framework and the corresponding working procedures.



exida

The manufacturer
may use the mark:

CERTIFIED • ISASecure • exida
SDLA

*ISASecure*® is a Trademark of ASCI. All rights reserved.

Revision 1.0 Oct. 22, 2019
The certificate is valid until the expiration date of
October 1, 2022

**Reports**:
AVE 1905010 R001 V1R1
Certification Report

**Validity:**
This Certificate is restricted to the specified versions of the referenced Security Development Lifecycle set forth in this Certificate.

ISASecure® Chartered Laboratory:
***exida***
80 North Main St.
Sellersville, PA 18960
License: ISCI-CL0001
ACLASS Cert No: AT-1531

IAF — MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT
ANSI ACCREDITED

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

T-136, V1R3

Certificate / Certificat

Zertifikat / 合格証

AVE 1905010 C001

*exida hereby confirms that the process entitled:*

**Security Development Lifecycle Process**

*Which is maintained and practiced by*

**AVEVA**
**Calgary, Alberta**
**Canada**

*Has been assessed per the relevant requirements of:*

***ISASecure***® **Security Development Lifecycle Assurance (SDLA) Program**
**Version 2.0.0**

**ANSI/ISA-62443-4-1-2018 Secure product development lifecycle requirements**

**IEC 62443-4-1:2018 Secure product development lifecycle requirements**

The normative documents and issue dates that define this certification are listed at www.isasecure.org.

This certification applies to versions 2.3 or later of "Security Development Lifecycle Process"

exida Certification

Authorized Representative

Figure 9: IEC 62443 – ISASecure SDLA Level 2 certification

## Conclusion

We offer highly scalable, robust, and secure products by following industry-leading best practices in secure product development.

To learn more about AVEVA Enterprise SCADA software visit: aveva.com/en/products/enterprise-scada

### About the author

Jake Hawkes is a Senior Product Manager with AVEVA with over 20 years of SCADA experience. His career started with a pipeline operator in Australia, and since then, his career has taken him all over the world, across industries such as Oil & Gas, Water, Transportation, Agriculture and Weather Systems. He started in Customer Support, then was a Software Developer, before moving into Technical Sales and Proposal Support and finally to Product Management. Jake obtained a Bachelor of Engineering Degree from the University of South Australia in Computer Systems.

AVEVA