AVEVA System Platform
AVEVA Operations Management Interface (OMI)
AVEVA Historian

CSPN Security Target

RnD CS 2020-0601
Authors: Manuel Meijueiro, Neville van der Merwe, Didier Collas
V1.4
1st of December, 2021

AVEVA GROUP PLC
HIGH CROSS, MADINGLEY ROAD
CAMBRIDGE CB3 0HB, UK
TEL +44 (0)1223 556655
FAX +44 (0)1223 556666

1. Contents

2. Version History

Version	Date	Comments
1.0	10/11/2020	Full new version
1.1	23/11/2020	Better definition of the TOE (chapter 11) AD (Active Directory Server) and SMS are removed from the TOE Introduction of the Gateway Communication Driver Controller simulation via OPC UA replaces real controller with OPC UA connection in the TOE
1.2	16/03/2021	Added SMC description, added administrative functions, extended Security chapter, Moved encrypted communication and moved Assumption on the environment chapter, created a chapter Security goals to conform to the ANSSI PSDN template structure Reviewed Critical Assets, Security Functions and Threat Model according to ANSSI feedback Corrected the inconsistencies in the chapter 12 tables Added the License management server
1.3	01/04/2021	Modification of chapters 7.4, 8 and 11.1 following OPPIDA comments
1.4	01/12/2021	Modifications post evaluation and ANSSI feedback. Modification of chapter 8 Assumptions on the environment: Added use of Microsoft .NET encryption functions statement. Removed software independence assumption. Modifications on paragraph 11.1 Security functions. Added link to readme file as reference document.

3. Introduction

This document describes the CSPN security target for System Platform/OMI SCADA, as a basis for agreement between AVEVA and the potential consumer of the product.

This document specifies the scope for the CSPN evaluation and describes the security properties of the product in an abstract manner, so potential consumer can rely on this description since the product has been evaluated to meet this security target.

4. References

[CSPN]	ANSSI-CSPN-CER-P-01 - First level security certification V2.1 anssi-cspn-cer-p-01-certification_de_securite_de_premier_niveau_v2.1
[CSPN Criteria]	ANSSI-CSPN-CER-P-02 – Criteria for Evaluation anssi-cspn-cer-p-02-criteres_pour_evaluation_en_vue_dune_cspn_v3.0
[CSPN Method]	ANSSI-CSPN-NOTE-03 - Methodology for evaluation ANSSI-CSPN-NOTE-03-Methodologie-pour-évaluation
[ICS-Classif]	ANSSI - Cybersecurity for ICS - Classification Method and Key Measures
[ICS-Detailed Measure]	ANSSI - Cybersecurity for ICS - Detailed Measures
[PP-SCADA SERVER ST]	ANSSI Protection Profile for a SCADA Server short-term 20151005_NP_ANSSI_SDE_4067_PJ3_serveur_scada_court_terme_PJ3
[PP-Historian ST]	ANSSI Protection Profile for an Historian Server mid-term 20151005_NP_ANSSI_SDE_4067_PJ7_historian_moyen_terme_PJ7.vf
[PP-SCADA Client MT]	ANSSI Protection Profile for a SCADA Client mid-term 20151005_NP_ANSSI_SDE_4067_PJ9_client_scada_mes_moyen_terme_P
[PP-ENGIN MT]	ANSSI Protection Profile for a SCADA Engineering mid-term 20151005_NP_ANSSI_SDE_4067_PJ10_ingenierie_moyen_terme_PJ10.v
[ANSSI-Healthy IS V2]	ANSSI – Guideline for a healthy information system in 42 measures V2
[SP Install Guide]	SP2020R2_Install_Guide.pdf
[SP Getting Started]	SystemPlatform 2020 R2 GettingStarted.pdf
[IDE User Guide]	IDE.pdf (configuring security and managing security chapters)
[SP Platform User Guide]	PlatformManager.pdf
[Historian Concepts]	HistorianConcepts.pdf
[Historian Admin]	HistorianAdmin.pdf
[Licensing]	Licensing_GettingStarted.pdf
[Readme]	Readme.html

5. Glossary of terms & terminology

5.1. Glossary of terms

- **AD**: Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks.
- **ANSSI :** National Agency of Security of Information System (Agence Nationale de la Sécurité des Systèmes d'Information).
- **AOS** (Application Object Server): Computer where application objects are deployed to run on. There can be multiple application object servers for load distribution or redundancy, or both.
- **Application object:** an IT object running on the Application Object Server and in charge of managing different services like internal communications, management of Automation Objects and their inter-communication, communication with controllers, ….
- **Automation object:** an object running in Application Object Server and representing a digital twin of a physical equipment. Its state is updated using real-time information from the control. It has a physical representation (Industrial Graphic) running in the OMI Application. The user interacts with this object (visualisation of the actual state and reaction to specific situations by sending commands to the physical device).
- **AVEVA Historian**: Runs the Historian Server software and hosts the history and alarm databases. Typically, there is only one historian server per Galaxy, but there can be more than one if needed, such as in largely distributed Galaxies hosting local historian servers per location.
- **AVEVA Operation Management Interface**: (also called AVEVA OMI or OMI in this document) is the visualization engine of System Platform that eliminates the need for complex scripting and programming.
- **AVEVA System Platform**: (Also called AVEVA SP or SP in this document). AVEVA System Platform is a scalable solution for supervisory, SCADA, HMI, and IIOT applications that integrates the process with the enterprise.
- **CSPN** : First Level Security Certification (Certification de Sécurité de Premier Niveau).
- **DAS** (Data Acquisition Server): Computer connected to the control network and running the corresponding drivers, such as a OI Sever or legacy IO Server. A single device integration server can run multiple drivers, but there can also be multiple device integration servers, depending on the control network topology. The 3 acronyms DAS, OI Server and IO Server are used indifferently to name the industrial communications servers.
- **DCOM**: Distributed Component Object Model (DCOM) is a proprietary Microsoft software component that allows COM objects to communicate with each other over the network.
- **Galaxy:** We refer to a Galaxy as a set of computers on a network with specific roles for a SCADA application and a configuration describing the architecture (network nodes and roles), the application objects and their associated graphics, the communications with the

controllers and the external applications, the users and their roles. A Galaxy is also used as the name of a SCADA project.

- **GATEWAY**: The GATEWAY Communication Driver is part of the DAS and acts as a communication protocol converter, to link clients and data sources that communicate using different protocols (OPC UA, Classic OPC, Suitelink, MQTT, ArchestrA Message Exchange and DDE/FastDDE).

- **GR** (Galaxy Repository): Runs the Galaxy Repository service and hosts the configuration project relational SQL database. There is only one Galaxy Repository per Galaxy.

- **IDE** (Engineering Station): Runs the tools necessary to develop and configure the application, like the automation objects or OMI graphic components. There can be multiple engineering stations for multi-user development teams.

- **IIOT**: Industrial Internet of Things (IIOT) is the use of smart sensors and actuators to enhance manufacturing and industrial processes.

- **Industrial Graphic**: graphical object used in the AVEVA OMI application to represent an automation object with a graphical representation of a physical assets and Automation Object. This object is animated based on information collected from the asset sensors e.g. *status, speed, level, alarm, …* It is also used to send commands to the asset e.g. *start, stop, open, close, increase speed by 5%, …*

- **IT/OT:** Information technology / Operational technology. Terms used to distinguish the office IT world from the production environment one. More and more, IT and OT are integrated and share the same operational constraints including cyber security policies and rules.

- **License Server:** An application providing the functionality to acquire, store, maintain and serve licenses to the installed AVEVA software.

- **MQTT:** Message Queuing Telemetry Transport protocol. It is an open OASIS and ISO standard (ISO/IEC 20922) lightweight, publish-subscribe network protocol that transport messages between devices. It is one of the preferred choices for protocols in IIOT architectures.

- **OMI App:** is an application which runs inside the OMI environment. It can be an AVEVA product delivered with OMI like a geographical map application or alarm grid. It can also be an external application developed and provided by an AVEVA business partner (like ALPANA dashboarding tool). It uses a specific toolkit to provide the right interface to OMI.

- **OMI Application**: This is the user interface application developed to run in OMI. It is a set of graphic objects (called Industrial Graphics) and OMI Apps running in panes on the screen. The graphics are animated with real-time information coming from AVEVA System Platform.

- **OPC**: OLE for Process Control or Open Platform Communications is a series of standards and specifications for industrial communications based on the OLE, COM, and DCOM technologies developed by Microsoft.

- **OPC DA**: OPC Data Access specification used for reading and writing real-time data.

- **OPC UA:** OPC Unified Architecture (UA) is a platform independent service-oriented architecture that integrates all the functionality of the individual OPC Classic specifications into one extensible framework.
- **PLC**: Programmable Logic Controller.
- **RTU**: Remote Terminal Unit. Specialized programmable controller used for remote process control of geographically distributed assets. Communicates with the SCADA using telemetry protocols like DNP3, Modbus or MQTT.
- **SCADA**: Supervisory Control And Data Acquisition.
- **SMC**: System Management Console. It is an administrative tool integrated in Microsoft Management Console (MMC) providing monitoring (runtime status of some system objects), diagnosis and management capability (like Galaxy backup and restore) on a System Platform application. It includes the **ArchestrA Log Viewer**, visualizing the events (system and application) logged by the **ArchestrA Logger** service.
- **SMS** (System Management Server): The role of the System Management Server is to generate, manage, and distribute secure digital certificates used for establishing and maintaining secure and encrypted communications between all the nodes.
- **TOE**: Target of Evaluation. The product under evaluation by the ANSSI.

5.2. Terminology

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
- **Availability:** Ensuring timely and reliable access to and use of information.
- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Cybersecurity:** Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation
- **Integrity**: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

6. Target of Evaluation identification

EDITOR	**AVEVA**
ORGANIZATION URL	www.aveva.com
PRODUCTS COMMERCIAL NAMES	AVEVA System Platform Using AVEVA Application Server, AVEVA Operations Management Interface and AVEVA Historian (server & client) modules
VERSIONS	AVEVA System Platform 2020 R2
PRODUCT CATEGORY	SCADA with Process Historian

7. Product description

7.1. Overview

AVEVA System Platform/OMI is a real-time software platform to build and execute human machine interface (HMI), operations management, SCADA, production and performance management applications.

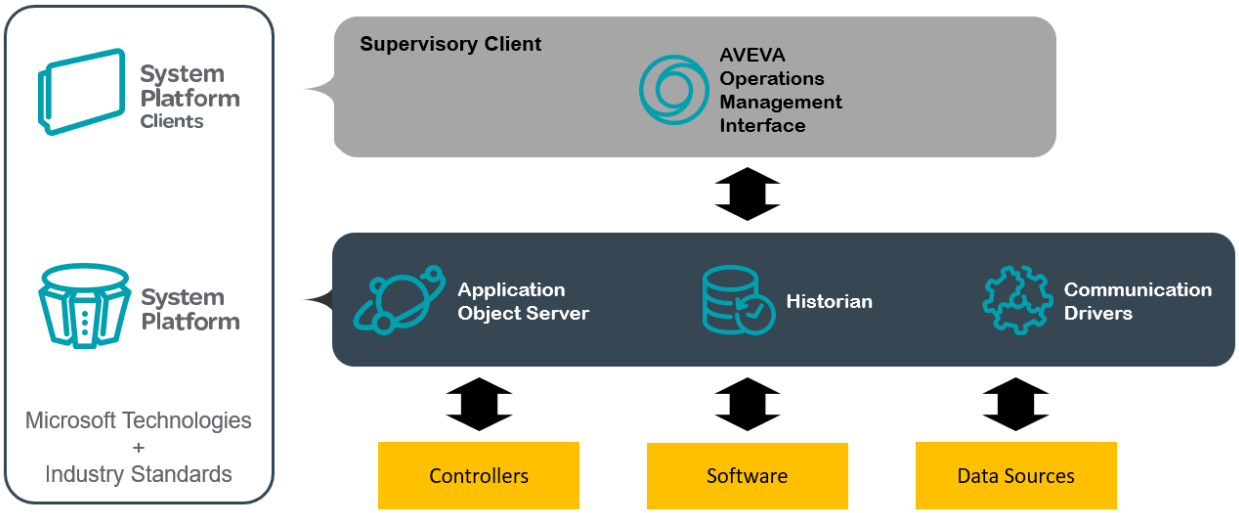
AVEVA System Platform/OMI is a SCADA application running on Microsoft Windows operating systems. Its role is to provide real-time monitoring and control of a set of physical equipment in order to operate and maintain the processes that may be utilizing the equipment in safe and optimal states. The software can be applied to a variety of equipment in order to produce goods (oil, cars, food, beverages, power, water etc.) or operate facilities (airports, railway stations, cities, tunnels etc.). It provides a view of the equipment and/or process states and allows an authenticated user to control equipment and/or processes by sending commands (e.g. start/stop, open/close etc.) or setpoints (speed, temperature, level etc.) to the equipment in order to modify the equipment or process state. The equipment is usually controlled by a PLC (Programmable Logic Controller) or local controller (RTU) and communicates with the SCADA via industrial protocols like OPC-DA, OPC UA, Modbus, DNP3 or IIOT protocols like MQTT.

AVEVA System Platform provides an integrated set of services and an extensible data model to manage plant control and information management systems. AVEVA System Platform supports the supervisory control layer and can embed the manufacturing execution system (MES) layer, presenting them to the users as a single source of information. AVEVA System Platform can integrate with other IT/OT applications like Manufacturing Execution Systems (MES), ERP, Batch management, Engineering (Computer Aided Design 1D, 2D and 3D), workflow (business process execution) and Enterprise Asset Management (EAM) via protocols like TCP/IP and different API as Web Services.

There are two phases in the use of AVEVA System Platform/OMI, one during which a development team creates, develops and tests an application (set of objects and Industrial Graphics) for a specific purpose (like managing a water treatment plant) using the IDE (development environment) and one during which AVEVA System Platform/OMI runtime runs this application in real time. The application is stored in a centralized object repository (SQL Database) called the Galaxy Repository (the IDE is not part of the TOE while the Galaxy Repository is)

The run-time environment consists of a set of servers and supervisory clients running different components of the application. A process database (AVEVA Historian) complements System Platform to record process data, alarms and events as they occur.

The following figure shows a functional architecture of AVEVA System Platform/OMI (runtime).



AVEVA System Platform components are as follows:

- **Application Object Server** is the heart of System Platform. It provides an object-oriented real-time framework running objects (pieces of code) in real-time – automation objects and application objects.
- **Historian** provides process data historization and alarm and event logging for Application Server. Data is exposed through SQL Server and/or an Open Data Protocol (oData) interface.
- **Communication Drivers** are drivers for communicating with third-party controllers (PLC and RTU). The GATEWAY Communication Driver is a communication protocol converter for OPC UA in a native format understood by Application Object Server.

The Supervisory client runs the operator interface (synoptic views and process trends) and provides real-time access to Application Object Server data, alarms and events. **AVEVA Operations Management Interface** (also called AVEVA OMI in the rest of this document) is the client chosen for the TOE (there are other clients not part of the TOE). AVEVA OMI can embed small applications (OMI Apps) to integrate different applications with the supervisory client (like an Internet Browser, a document viewer, a geographical map or a 3D visualisation tool). Some of those OMI Apps are provided by AVEVA. Some of them are developed by business partners using an AVEVA toolkit (out of the TOE).

The Historian Client is a tool for accessing and visualizing data historized with AVEVA Historian in the form of tables or curves. It can be a full independent application running on a PC or an OMI App embedded in AVEVA OMI (the TOE uses AVEVA OMI as the historian client).

Together, AVEVA System Platform and its clients provide the core services needed to safely run industrial automation applications.

Some of these services include:

- Real-time data acquisition from field devices
- Scaling, statistics, and management of data
- Process control (control loops and reaction to events)

- Alarm triggering, logging, acknowledgement and state management
- Historization, trending, and analysis of process data
- Visualization of real-time process data
- Reporting

7.2. Functional Components

7.2.1. Application Object Server

Application Object Server is the heart of AVEVA System Platform; it provides the services and tools to run an application made of multiple objects.

Some of the main functions of Application Object Server are:

- Object-oriented real-time engine to host application objects and automation objects,
- Communication with controllers via OI Servers and legacy IO Servers. OI Servers with different protocols are available from AVEVA or partners. OPC UA is the PLC communication protocol chosen for the TOE,
- Security management to prevent users from performing unauthorized activities,
- Optional redundancy capabilities for the application and for I/O communications (not part of the TOE),
- Diagnostics tools for troubleshooting the application like a data logger.

An application is called a Galaxy (kind of project) and is composed of:

- A collection of automation objects that represent all the physical and logical entities in the application; from computers and runtime engines, to all the equipment in the field
- A project relational database that holds the configuration information
- One or more networked computers running the application
- A common set of system-level policies that all components and objects comply with, such as security, alarm, and communications settings

One of the main objects in any Galaxy is the WinPlatform object, which represents a computer in the Galaxy. A WinPlatform object, when running on a computer, adds this computer to the Galaxy, providing all required services to communicate with the other Galaxy computers.

7.2.2. Data Acquisition Server

AVEVA System Platform can connect to diverse data sources to collect and manage industrial data.

Data sources include OPC DA and OPC UA Servers, databases and any application exposing data via an API such as XML, SQL, HTTP (web services) or Microsoft .NET.

The **GATEWAY Communication Driver** acts as a communication protocol converter, to link clients and data sources that communicate using different protocols (OPC UA, Classic OPC, Suitelink, MQTT, ArchestrA Message Exchange and DDE/FastDDE).

In addition, a library of device integration servers provides possible connection to any type of industrial controller through specific industrial protocols like Modbus or OPC. OI servers can be provided by either

AVEVA for the most common ones like Schneider Electric, Siemens or Rockwell Automation or by business partners using a dedicated AVEVA toolkit. The TOE will only focus on the OPC UA protocol.

7.2.3. Visualization and Analysis Clients

Visualization and analysis clients enable the authorized users to visualize real-time and historical data from AVEVA System Platform.

AVEVA OMI visualization client runs Human Machine Interface (HMI) applications made of synoptic views with animated graphical objects representing the controlled process. Those synoptic views can integrate historical and real-time trends and alarm grids, using data stored on AVEVA Historian. AVEVA OMI extends the core foundation of HMI by allowing a better integration of external application like MES, Video streams, Engineering 3D data within a SCADA application.

7.2.4. AVEVA Historian

AVEVA Historian is an optimized plant data historian. A plant data historian manages time-series data (evolution of a process variable over time) where a classical SQL database manages transactions (records of related data at a time).

AVEVA Historian:

- Acquires plant data from high-speed DA Servers, OI Servers, Application Server, and other devices
- Compresses and stores data
- Responds to SQL requests for plant data

AVEVA Historian also manages and stores events, alarms, summaries, configuration elements, security information, backup, and system monitoring information.

AVEVA Historian is tightly coupled to Microsoft SQL Server. As a real-time relational database, AVEVA Historian Server extends the functionality of Microsoft SQL Server, providing high acquisition speeds, reduction in storage volume via a specific compression algorithm, and time extensions to SQL for querying time series data.

7.2.5. AVEVA Enterprise Licensing

The AVEVA Enterprise Licensing system is a common platform that allows an administrator user to manage effectively and efficiently AVEVA software licenses. This licensing system is composed of a browser-based License Manager and a License Server that together allow an administrator to share and deliver licenses for the AVEVA software installed on the system.

The License Manager allows an administrator to quickly access and maintain licenses for certain AVEVA software products in the TOE system.

The License Server provides all the functionality to acquire, store, maintain and serve licenses to the installed AVEVA software.

7.2.6. Administrative functions

AVEVA System Platform/OMI and AVEVA Historian are providing/using a set of administrative functions, installed with the product:

SMS: System Management Server. This server manages and distributes the certificates used to protect the secrets of the application (encryption of passwords and TLS 1.2 communications). See the Cryptographic specifications document (RnD CS 2020-0702) for a detailed description.

SMC: System Management Console. The SMC is an administrative tool integrated in Microsoft Management Console (MMC) providing monitoring (runtime status of some system objects), diagnosis and management capability (like Galaxy backup and restore) on a System Platform application. It includes the **ArchestrA Log Viewer**, visualizing the events (system and application) logged by the **ArchestrA Logger** service. The SMC requires specific role permissions (typically administrator ones) to be executed in monitor only and management mode.

7.2.7. Encrypted communications

The end-to-end communication between software applications (server and client) can be encrypted and secured to prevent eavesdropping and malicious tampering (aka: Man-in-the-Middle) attacks.

To enable encrypted network communication, one of the nodes in the network must be configured to host and run the System Management Server (SMS). The role of the System Management Server is to generate, manage, and distribute secure digital certificates used for establishing and maintaining secure communications.

The SMS can be configured to generate and use self-signed certificates, or to use Domain-issued or CA-issued certificates.

All other nodes need to be configured to connect to the SMS so they all become part of the same community. The SMS is chosen during configuration of each node, and the relevant certificates are generated and copied to the node.

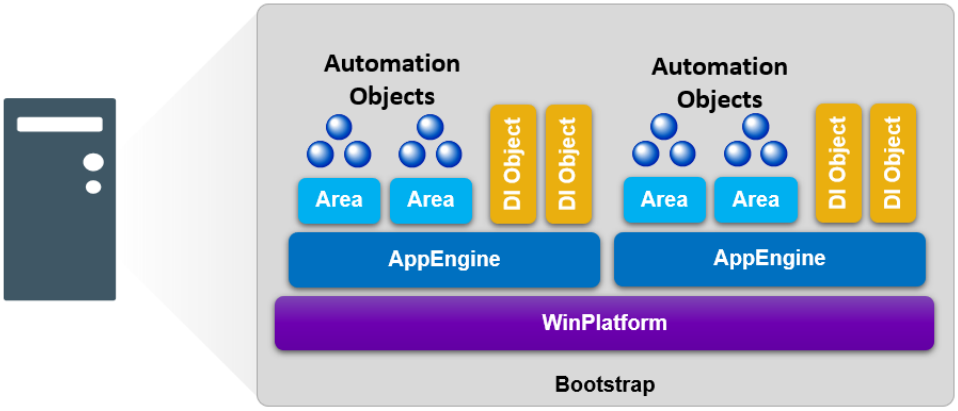
7.3. Features

7.3.1. Application Objects

Application objects, along with the relationship between each other, are the centrepiece of the object-oriented framework of Application Server. Through application objects, you can model virtually anything related to the Galaxy, from an area or section of the plant, to every equipment in the field, to the actual computers running the application.

For this, Application Server provides objects in three different categories:

- **System Objects** – Used to build the infrastructure of the application. They represent the computers that are part of the Galaxy, the runtime engines that execute the rest of the objects (including how fast the objects will run), and the layout of the plant and distribution of alarms. System objects also include the visualization applications to run in InTouch.
- **Device Integration Objects** – Represent the controllers and other I/O data sources outside the Galaxy, such as PLC, RTU, and DCS. Device integration objects are the means by which the Galaxy gets access to I/O data from the field; they connect to the drivers that access the different controllers in the application, such as OI Servers and OPC Servers.
- **Automation Objects** – Simply put: everything else. Application objects usually represent the equipment in the plant floor, such as valves, tanks, and motors; however, they can also be used to run specific runtime calculations and connections to external data sources (other than field devices), like databases or web services.



All automation objects include the following features and configuration options:

- **Inputs and Outputs** – References to real-time I/O data from the field or other objects in the Galaxy. For example, read the status of a valve and command it to open or close.
- **Scripting** – To implement custom calculations, decision-making based on equipment data, or to enhance the functionality of objects in the Galaxy. For example, calculating flow rates or defining complex alarm conditions.
- **Historical Configuration** – Specify which data points in the object will be historized by the Historian Server. It also includes configuration parameters, such as range and dead bands.

- **Security Requirements** – Permissions necessary to write values to the object. For example, command a valve to open or change the setpoint for the speed of a motor.
- **Alarms and Events Configuration** – Specify which alarms and events are to be triggered (or captured if triggered by the controller); automation objects include traditional alarm definitions built-in. For example, a HI and a LO alarm for the level of a tank.
- **Version and Documentation** – Each object keeps track of its own configuration version and includes its own help file.
- **Graphic Symbols** – Graphical representations of the object to be used in the operator's interface displayed by InTouch. Graphics can be animated to display real-time changes to values of the object; for example, a graphic for a motor object can turn green when the motor is running and gray when it is not.

7.3.2. The Deployment concept

To run the application, the automation object instances in the Galaxy must be deployed to the runtime environment. When an object is deployed, the underlying software that makes the object (from the base template) and the object's configuration (I/O references, alarms, history, scripts, and so on) are copied to the target computer; the software also gets installed or registered in that computer and the object is run, or both.

In contrast, un-deploying objects will stop them, uninstall them, and finally remove them (software and configuration) from the computer they were deployed to.

7.3.3. Symbols and Content

Industrial graphics allow you to create customized graphical representations of processes and integrate other visualization tools (Windows controls or data grids for example) in the application. They can be embedded or associated with automation objects in Application Server, so that all facets like attributes, alarms, history management, logic, graphical representations and security rules can be defined in one place within the automation object.

Industrial graphics managed in AVEVA OMI include the following:

- **Industrial Graphics** are graphics you can create to visualize data in Application Server, to be shown in a visualization application.
- **Client controls** provide functionality contained in .NET controls that can be used in symbols.
- **Screen profiles** determine where, meaning on which display screens, you want to present content in a running AVEVA OMI application.
- **Layouts** which define how you want to organize content in a running AVEVA OMI application.
- **OMI Apps** which are prebuilt, special-purpose collections of one or more controls that can be added to layouts to display content in a running AVEVA OMI application.
- **External content** refers to media content outside of a Galaxy that can be linked to an OMI App inside the application and displayed at runtime.

7.3.4. Alarms and Events

The alarm and event capabilities in the system manages the detection, notification, historization, and visualization of either industrial process alarms and events or **system/software alarms and events**. Alarms and events are occurrences in the runtime system. Events and alarms are different topics, and the system distinguishes between the two.
An event is simply an occurrence of a condition at a certain point in time. The system can detect events, store them historically and report them to various clients.
An alarm, on the other hand, is a special type of event that represents the occurrence of a condition that is considered abnormal (generally bad) in nature and requiring immediate attention from a user. The system handles the real-time reporting of alarms in a special manner and provides special clients for their visualization.

Examples of alarms include:

- A process measurement has exceeded a predefined limit, such as a high temperature alarm.
- A process device is not in the desired state, such as a pump that should be running has stopped.
- The system hardware is not operating within desired limits, for example the CPU utilization on a Platform exceeds a certain percentage for an extended time.

Examples of events include:

- A plant process has started; for example, a new batch or campaign starts.
- The operator has changed a plant operator parameter; for example, a setpoint on a temperature controller.
- The system engineer has changed the runtime system configuration; for example, deployment of a new Automation Object.

- The system engineer has started or stopped a system component; for example, stopping an engine.
- A Platform has come back online after it had a failure or shutdown.
- A user has logged into the system.

- Detection of a severe software problem; such as a failed Application Object component.

7.3.5. Trends

AVEVA Historian collects and stores process data, alarm and event data in its database.

The History feature (storage of the evolution of the value of an object attribute over time) can be enabled in Automation objects for any attributes of any type (boolean, string, analog)

Historical data can be retrieved and viewed as a real-time or historical curve using AVEVA Historian Client applications, in Industrial Graphics or OMI Apps hosted in AVEVA OMI or using Microsoft SQL Server tools.

7.4. Security

7.4.1. Network Account

The Network Account is a username and password combination that enables inter-node communication between all System Platform computers.
To enhance security, the network User Account is blocked from logging on to the Galaxy locally or through Remote Desktop Services by default. This is configured in the operating system user rights management.
See the Installation Guide for more information [SP Install Guide].

7.4.2. Users

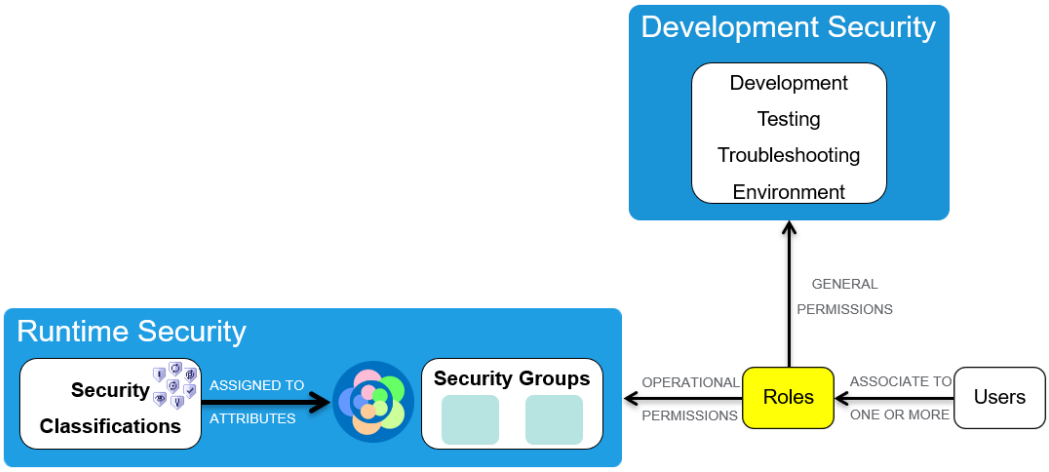
Security is designed to prevent users from performing unauthorized activities. This includes users of:

- IDE (the development environment) for configuring and managing objects (IDE is out the TOE),
- System Management Console (SMC) for performing maintenance and system administration functions,
- Any runtime operations like commands or data visualization.

The system supports operating system authentication using Active Directory. The configuration and runtime permissions are mapped to the external operating system accounts or groups. The security system is designed to support the normal operating parameters of an automation system.

The AVEVA products use Windows authentication APIs to determine user identity and group membership for authorization purposes.

See the image below for a visual hierarchical overview of our security model.

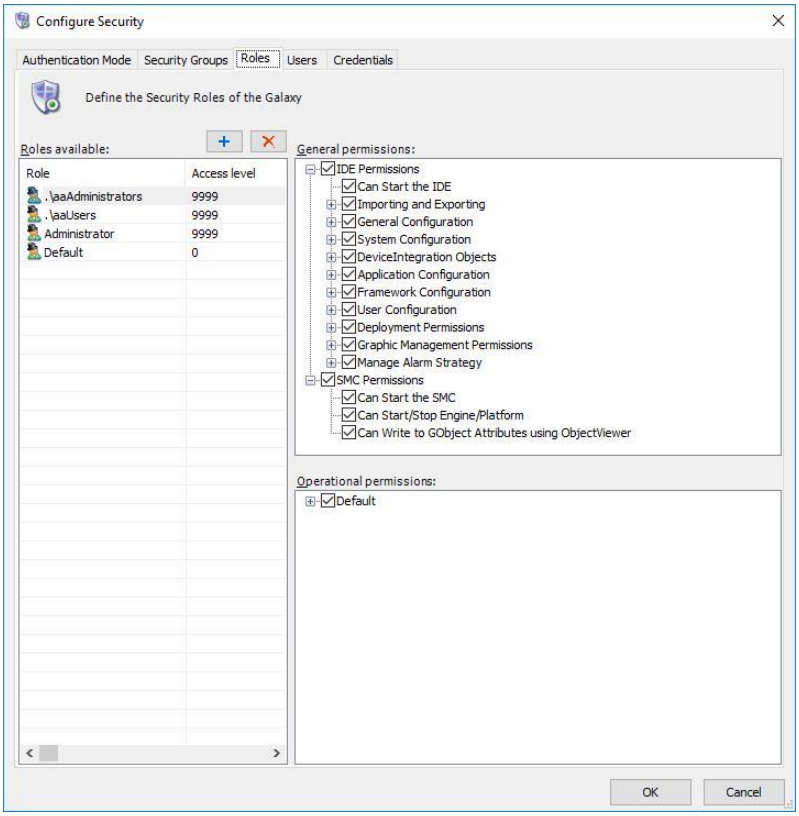


Each attribute of an Application Object is given a security classification. This provides the ability to define who can write to attributes of an object.

For example, a certain attribute of the $DiscreteDevice object may be set by the operator to change its status while a different attribute may be set by a technician. These attributes are meant for different people, Operator (operate) and Technician (tuning). Configuring access to all users for all Application Objects on individual bases would be a time-consuming and repetitive effort. Thus, configured Roles and Security Groups can be applied to Users to enable easier configuration of the Security Model.

Security Groups are simply the grouping of objects that you want to behave in the same way with respect to security. Every Application Object belongs to exactly one Security Group. By default, all new objects belong to the Default Security Group, which cannot be removed.
Roles generalize Users function, such as Intake Operator or Dispatcher. Roles are granted permissions onto a number of Security Groups. If, for instance, a Role is granted Tuning access to a Security Group, then that role has write permissions to all object attributes with a security classification of Tuning (but none other). Roles are also granted utility functions-based permissions, such as Deploy or Can Edit.

Explicit permissions are required to perform most activities. Usually only one permission is required to perform a given activity, but occasionally, two or more permissions may be required for operation-critical actions (for verify writes). This includes the access to the SMC (administration/diagnosis) and the IDE (configuration of the application and security). The security configuration screen here below shows the detailed configuration of permissions of an administrator for the SMC.



The final aspect of the Security Model is the User. This describes the access to the system allowed by a User. The User can be granted as many Roles as needed to perform their job.
There is no predefined user role like operator or administrator or auditor like recommended in the ANSSI Protection Profile for a SCADA Server mid-term document. The administrator in charge of the system configuration has to define roles and their associated permissions (like Administrator, Operator, Auditor, …) and users are then allocated one or multiple roles.

For the security model, the application uses OS Group Based authentication. This enables the Authorization for users based on which OS Groups they have been assigned to.

Examples of Operational Permissions that can be associated with a role:

- **Can Modify "Operate" Attributes:** Allows users with operational permissions to do certain normal day-to-day tasks like changing setpoints, outputs, and control modes for a PID object or commanding a $DiscreteDevice object,
- **Can Modify "Tune" Attributes:** Allows users to tune the attribute in the runtime environment; examples of tuning include attributes that adjust alarm setpoints and PID sensitivity,
- **Can Modify "Configure" Attributes:** Allows users to configure the attribute's value, which requires that the user first put the object Off scan; writing to these attributes is considered a significant configuration change, for example, a PLC register that defines a $DiscreteDevice input,
- **Can Acknowledge Alarms**: Allows users to manually acknowledge an alarm in the runtime environment,
- **Can Verify Writes:** Allows users to provide an authentication signature for attributes configured with Verified Writes security classification. Only users with this permission can verify a task performed by users with the Can Modify "Operate" Attributes permission.

7.4.3. Encrypted communications

The end-to-end communication between software applications (server and client) can be encrypted and secured to prevent eavesdropping and malicious tampering (aka: Man-in-the-Middle) attacks.

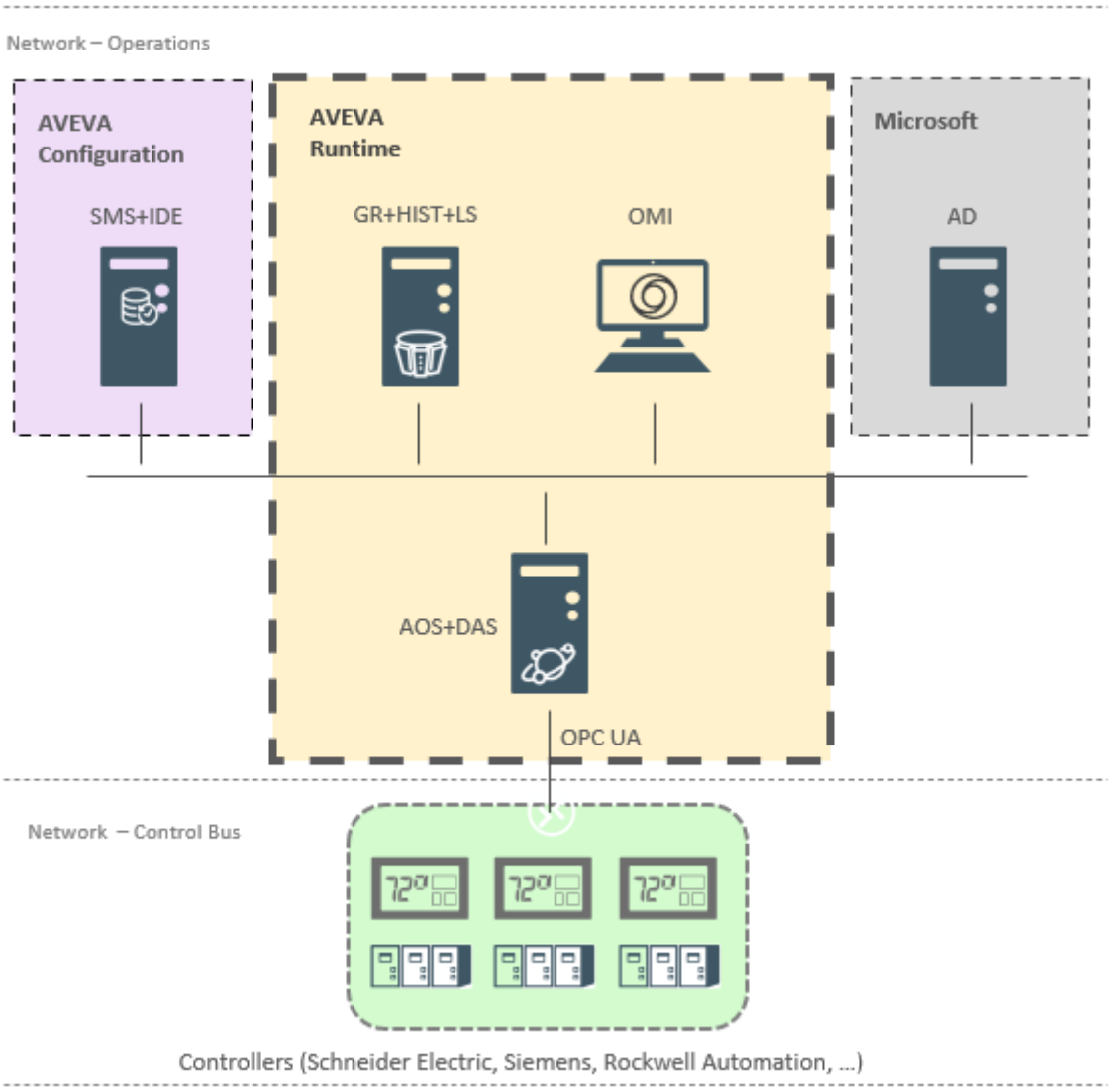
To enable encrypted network communication, one of the nodes in the network must be configured to host and run the System Management Server (SMS). The role of the System Management Server is to generate, manage, and distribute secure digital certificates used for establishing and maintaining secure communications.

The SMS can be configured to generate and use self-signed certificates, or to use Domain-issued or CA-issued certificates.

All other nodes need to be configured to connect to the SMS so they all become part of the same community. The SMS is chosen during configuration of each node, and the relevant certificates are generated and copied to the node.

7.5. Product usage

The following diagram is an example of AVEVA System Platform run-time implementation, where each computer has been assigned a single or multiple role. Keep in mind that most of these roles can be distributed in several computers or combined on a single computer, depending on the size of the application and the hardware resources available.



The possible computer roles on a System Platform implementation are:

AVEVA Configuration and Development Tools

- **IDE** (Engineering Station): Runs the tools necessary to develop and configure the application, like the automation objects or OMI graphic components. There can be multiple engineering stations for multi-user development teams. It is only used during the configuration of the application.
- **SMS** (System Management Server): The role of the System Management Server is to generate, manage, and distribute secure digital certificates used for establishing and maintaining secure and encrypted communications between all the nodes.

AVEVA Runtime

- **GR** (Galaxy Repository) – Runs the Galaxy Repository service and hosts the configuration project database.
- **HIST** - Runs the Historian Server software and hosts the history and alarm databases. Typically, there is only one historian server per Galaxy, but there can be more than one if needed, such as in largely distributed Galaxies hosting local historian servers per location.
- **LS** (License Server) - It provides the functionality to acquire, store, maintain and serve licenses to the installed software.
- **AOS** (Application Object Server) - Computer where application objects are deployed to run on. There can be multiple application object servers for load distribution or redundancy, or both.
- **DAS** (Data Acquisition Server) – Computer connected to the control network and running the corresponding drivers like the GATEWAY driver as a OPC UA client. A single device integration server can run multiple drivers, but there can also be multiple device integration servers, depending on the control network topology.
- **OMI** (Supervisory Clients) – Runs the operator's interface or HMI through OMI runtime tools. There can be multiple visualization stations.

Microsoft

- **AD** provides the Active Directory Domain Services and manages the authentication. This is a Windows service used by AVEVA System Platform, but not provided by AVEVA.

8. Assumptions on the environment

Assumptions on the environment and the use case of the TOE are the following:

- **System health rules:** ANSSI recommendations from the ANSSI "Guideline for a healthy information system in 42 measures V2" are applied when applicable. The TOE security has been setup and the TOE administrators follow the security recommendations in the Appendix A of the [IDE User Guide].
- **Infrastructure**: The network requirements, the operating system and its hardware (e.g. DNS. DHCP, Antivirus, USB ports, AD etc.) are handled securely.
- **Checking in the SMC logger**. The users will check regularly the logs produced by the TOE.
- **Architecture**: The ICS network (Network Control Bus and Network Operations) will be independent from the corporate network. If the networks must be connected, it is strongly recommended that only minimal (single if possible) connections be allowed and that the connection is through a firewall and a DMZ and using the specific products to expose data to corporate users (like InTouch Access Anywhere gateway, InSight Secure Link, … - which are not part of the TOE), according to the NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security.
- **Users:** TOE users are competent, trained and trustworthy.
- **Administrators**: TOE administrators and auditors are competent, trained and trustworthy.
- **Access:** The TOE is placed in a secured room and this room is only accessible to authorized trustworthy non hostile people. An attacker will not have access to the ports of the machine(s) of the TOE.
- **Hardware sizing:** we guess that the hardware supporting the TOE is correctly sized to support the treatments the TOE must execute.
- **Encryption functions:** the TOE uses encryption functions provided by Microsoft .NET WCF framework and Microsoft SChannel implementation. Those functions are assumed to be secure and must be trusted by the user.
- **Security**: During the installation and configuration of the system:
  - The authentication server (SMS) is safe and properly configured and the TLS 1.2 protocol for secure encrypted communications between nodes has been enabled through the SMS. TLS 1.0 and TLS 1.1 have been disabled after installation to make sure TLS 1.2 is used (cf AVEVA System Platform 2020R2 [Readme] document).
  - To avoid malicious access to the system, AD should be configured according to the ANSSI recommendation No DAT-NT-17/ANSSI/SDE/NP ("Recommandations de sécurité relatives à Active Directory") dated 10/09/2014 to avoid malicious access to the system.
  - The AVEVA System Platform security is configured to prevent users from performing unauthorized activities. Different roles will be created to apply organization's processes and work-based authorities.

- The operating system is properly set up according to AVEVA recommendations, up to date and safe. All computers run the latest published Microsoft security patches. All unnecessary services are inhibited on the Operating System. No external module except those necessary for the tests (OPC UA Server Simulator) is running on the TOE computer(s). The Windows system logger is enabled and running, and the log files are genuine and of authenticity.
- The AVEVA software makes use of Windows APIs, Windows .Net Framework, Windows SDK, Unified Automation library, Bouncy Castle library for security functions implementation.
- All computers run an up to date and properly setup anti-virus. **We recommend the use of CylancePROTECT**.

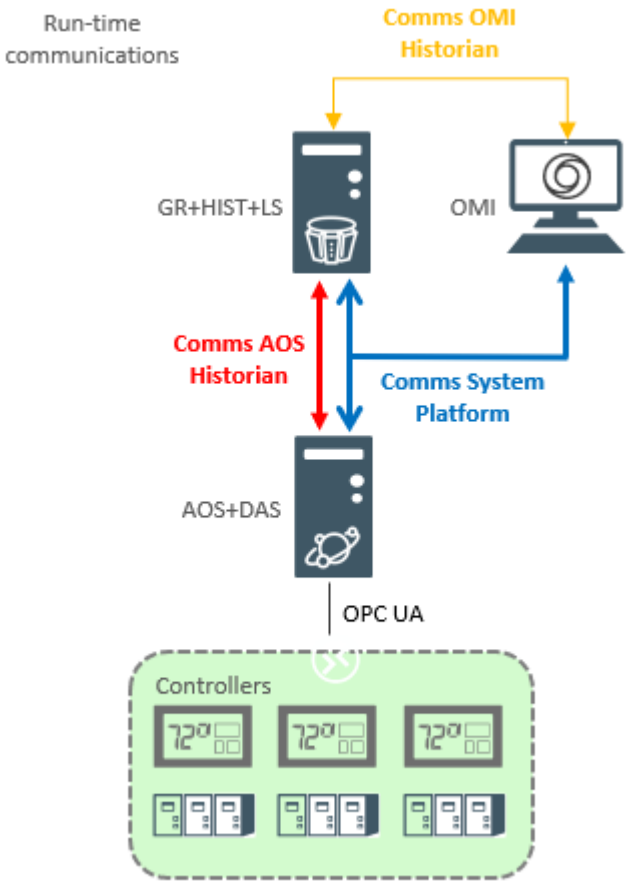
- **Documentation:** the users created by the TOE to run (services) and their default credentials are listed in the TOE documentation and have been personalized. All best practices found in the TOE documentations have been applied.

9. Critical assets

9.1. Critical assets of the environment

The critical assets of the environment are the following:

- **Comms System Platform (collaboration flow)**: Communications between the Galaxy Repository, the AOS and OMI must be protected in confidentiality, integrity and authenticity.
- **Comms AOS Historian**: Communications between the AOS and the Historian Server must be protected in integrity and authenticity.
- **Comms OMI Historian**. Communications between the Historian Server and the clients must be protected in integrity and authenticity.
- **Operating data**: Operating data consists of all the useful information for the proper functioning of the supervision system in operational phase (values, alarms, commands, …) and be must be protected in integrity and authenticity.
- **Historical data**: Historical data consists in all the information stored in the Historian (time series data, events and alarms) must be protected in integrity and authenticity.



The security requirements are as follows:

Asset	Availability	Confidentiality	Integrity	Authenticity
Comms System Platform		X	X	X
Comms AOS Historian			X	X
Comms OMI Historian			X	X
Operating data			X	X
Historical data			X	X

9.2. TOE critical assets

The critical assets of the TOE are the following:

- **Software**: in order to work properly, the software must be protected both in integrity and authenticity.
- **Configuration:** the configuration of the TOE (GR Database) must be protected in confidentiality and integrity. The attacker must not be able to discover the configuration of the TOE by other means than the TOE activity.
- **User authentication mechanism**: this mechanism should be based on AD. The TOE must ensure the integrity and authenticity of the mechanisms.
- **User secrets**: the user secrets can be passwords, certificates… They can be stored in the TOE or stored in a remote authentication server. In all cases, the TOE must ensure the integrity and confidentiality of these credentials.
- **Access control policy**: the policy (roles) can be stored locally or remotely on an authentication server. In both cases, the TOE must ensure the integrity of the access control policy.

Summary table of the TOE security requirements :

Asset	Availability	Confidentiality	Integrity	Authenticity
Software			X	X
Configuration		X	X	
User authentication mechanism			X	X
User secrets		X	X	
Access control policy			X	

10. Threat model

10.1. Attackers

The following threat agents have been identified:

- **Malicious user**: An attacker who was able to obtain a user credentials without admin rights and trying to perform activities he/she is not allowed to do.
- **Attacker inside the industrial system**: An attacker who has control of one piece of the system and tries to attack the TOE.

10.2. Threats

The following threats have been identified:

- **Flow alteration**: The attacker manages to corrupt exchanges between the TOE and a source, a destination, or a user and the administrative interface.
- **Flow compromise**: The attacker manages to fetch data by intercepting exchanges between the TOE and a source, a destination, or a user and the administrative interface.
- **Software alteration**: The attacker manages to modify, temporarily or permanently the TOE software. The attacker succeeds in executing illegitimate software code on the TOE.
- **Configuration alteration**: The attacker manages to modify, temporarily or permanently, the TOE configuration. Writing configuration settings exceeding the account privileges is also considered under this threat.
- **Configuration compromise**: The attacker manages to illegally obtain some parts of the TOE configuration. Reading configuration settings exceeding the account privileges is also considered under this threat.
- **Credentials theft**: The attacker manages to steal user credentials from the product.
- **Access control violation**: The attacker manages to obtain permissions which he does not have normally.
- **Authentication violation**: The attacker successfully bypasses authentication on the administration interface.

11. Security goals

11.1. Security functions

- **Secure communication:** The TOE allows the use of secure communications, protected in integrity, authenticity and, confidentiality with external components. The TOE uses the TLS implementation provided by the underlying Windows OS to protect communications between the different computers hosting AVEVA software: AOS, OMI clients, Historian, License manager and Galaxy Repository

- **Secure authentication:** The TOE enables connection secured with the authentication server by ensuring the authenticity of both ends, the integrity and confidentiality of the exchanges, as well as the non-replay. User Authentication uses Windows credentials and relies on the Windows/Active Directory implementation. Communication links are authenticated using the TLS implementation provided by the underlying Windows OS.

- **Secure storage of secrets:** The secrets are stored securely and compromising a file does not allow them to be recovered. Passwords are under the control of the Windows Operating System and Active Directory.

- **Secure access to administration interface (SMC):** The access is protected against theft or replay. The credentials are verified for each performed action.

- **Access control policy:** This policy guarantees the authenticity of critical operations. Windows user authentication is used to log into the SMC, and Role Based Access Control, based on Windows Groups, is used for Authorization.

- **Software signature**: The software is signed using Microsoft Authenticode digital signature (c.f. Cryptographic specifications document section 6.6) and the signature is checked on installation to guaranty the authenticity.

- **Configuration integrity and confidentiality**: User management policy does not allow an unauthorized person, either to consult, or to modify all or part of the TOE configuration. If configuration files are manually transferred during some operations (for example transfer of the configuration from the system integrator platform to the customer site), the entity transferring the file must ensure that those files are protected during transit. The configuration files are protected with ACLs (Access Control Lists) to prevent reading by unauthorized actors.

11.2. Critical Assets vs Threats

Threat coverage of assets

Asset/Threat	Flow alteration	Flow compromise	Software alteration	Configuration alteration	Configuration compromise	Credentials theft	Access control violation	Authentication violation
Comms System Platform	IA	C			C			
Comms AOS Historian	IA	C						
Comms OMI Historian	IA	C						
Operating data	IA	C						IA
Configuration data	IA	C			C			
Historical data		C						
Supervision & control availability			IA					
Historization availability								
Software								
User Program								
Configuration				I				
Execution								
User authentication mechanism							IA	
User secrets						IC		
Access control policy								
D (Availability), I (Integrity), C (Confidentiality), A (Authenticity)								

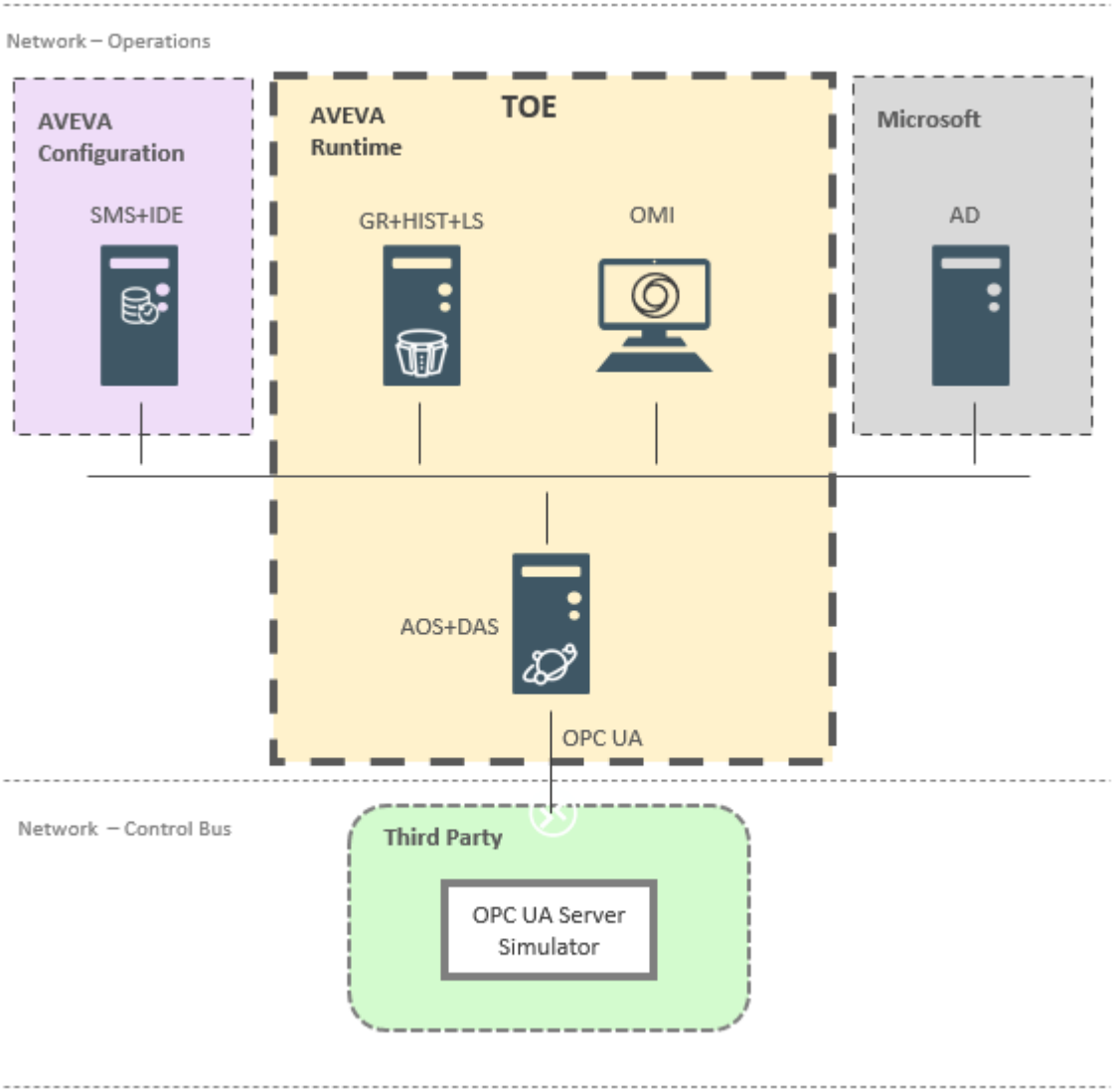
11.3. Threats coverage by Security functions

Security Functions/Threat	Flow alteration	Flow compromise	Software alteration	Configuration alteration	Configuration compromise	Credentials theft	Access control violation	Authentication violation
Secure communication	X	X						
Secure authentication							X	
Secure storage of secrets						X		
Secured access to administration interface (SMC)				X	X	X	X	
Access control policy								X
Software signature			X					
Configuration integrity and confidentiality				X	X			

12. Evaluation System (Target of evaluation/TOE)

12.1. Architecture of the evaluation system

The following diagram shows the architecture of the evaluation system



12.2. Components (computers and roles) of the evaluation system

The computer roles on the evaluation system are:

AVEVA Runtime (TOE)

- **GR** (Galaxy Repository) – Runs the Galaxy Repository service and hosts the configuration project database.

- **HIST** - Runs the Historian Server software and hosts the history and alarm databases. Typically, there is only one historian server per Galaxy, but there can be more than one if needed, such as in largely distributed Galaxies hosting local historian servers per location.
- **LS** (License Server) - It provides the functionality to acquire, store, maintain, and serve licenses to the installed software.
- **AOS** (Application Object Server) - Computer where application objects are deployed to run on. There can be multiple application object servers for load distribution or redundancy, or both.
- **DAS** (Data Acquisition Server) – Computer connected to the control network and running the corresponding drivers like the GATEWAY driver as a OPC UA client. A single device integration server can run multiple drivers, but there can also be multiple device integration servers, depending on the control network topology.
- **OMI** (Supervisory Clients) – Runs the operator's interface or HMI through OMI runtime tools. There can be multiple visualization stations.

AVEVA Configuration and Development Tools (Out of the TOE)

- **IDE** (Engineering Station): Runs the tools necessary to develop and configure the application, like the automation objects or OMI graphic components. There can be multiple engineering stations for multi-user development teams.
- **SMS** (System Management Server): The role of the System Management Server is to generate, manage, and distribute secure digital certificates used for establishing and maintaining secure and encrypted communications between all the nodes.

Third Party (Out of the TOE)

- **AD** provides the Active Directory Domain Services and manages the authentication. This is a Windows service used by AVEVA System Platform, but not provided by AVEVA.
- **OPC UA Server Simulator** simulates an OPC UA Server (Top Server V6 – OPC UA server simulator).

12.3. Base requirements

The following table provide the list of computers (physical or virtual using virtualizations tools like VMWare V6.5 or HyperV V5 or newer) and their configurations suitable for the evaluation of System Platform 2020 R2 software based on a small size application.
Three of them are part of the TOE and the three other ones are providing supporting services for the TOE like Microsoft Active Directory or the Top Server OPC UA server simulator.

ROLE	Computer Part of TOE	CPU Cores	RAM	Hard Disk Space	Screen Resolution	Network Speed	Windows Type
GR+Hist+LS	YES	6	12	150 GB	1920x1080	1Gbps	Server
AOS+DAS	YES	6	6	100 GB	1920x1080	1Gbps	Server
OMI	YES	4	8	100 GB	1920x1080	1Gbps	Client
SMS+IDE	NO	4	6	60 GB	1920x1080	1Gbps	Server
AD	NO	4	4	60 GB	1920x1080	1Gbps	Server
OPC UA Server (Top Server)	NO	4	4	60 GB	1920x1080	1Gbps	Server

The recommended versions of Windows to be used for the purpose of this evaluation are:

- Server: Windows Server 2019 LTSC (Desktop Experience)
- Client: Windows 10 1909 Pro

The recommended version of the Top Server OPC UA simulator is V6.

[DC1]