

APRIL 2023

Cybersecurity and Networking Strategies

System Design for Defensible Security

Michael Brost

Sr. Principle Technical Sales Consultant

Community of Practice Leader – America's Monitoring and Control

Basic Requirements of Defensible Control System Security

Destination Security Model Superior to Origination Security Model

- General Access be restricted and encrypted with certificates
- Each Tag/Item/Attribute/Element of the Control System, The Write Target must be able to Evaluate whom is issuing the Write
- Four **Aces's** of Control System Security (Authenticated, Authorized, Approved, Archived)
 - **Authenticated**: Gained After Authenticated Login (Identity of the Logged-in User is now known)
 - **Authorized**: Confirmed that the Logged-in User is permitted to Write. When Demanded by the Write Target
 - Reissue of User Name and Password
 - Two Factor Authentication
 - **Approved**: Write is Verified by an Authenticated Verifier, Separate from the Authenticated Writer. When Demanded by the Write Target
 - Second Actor must Approve and Sign the Write
 - Username/Password or Two Factor Approval
 - **Archived**: Action recorded into a 21 CFR Part 11 Log, By the Write Target
- All Protocols, Graphics, External APIs, External Clients must be required to enforce this model without any configuration at the origination of the Write Command

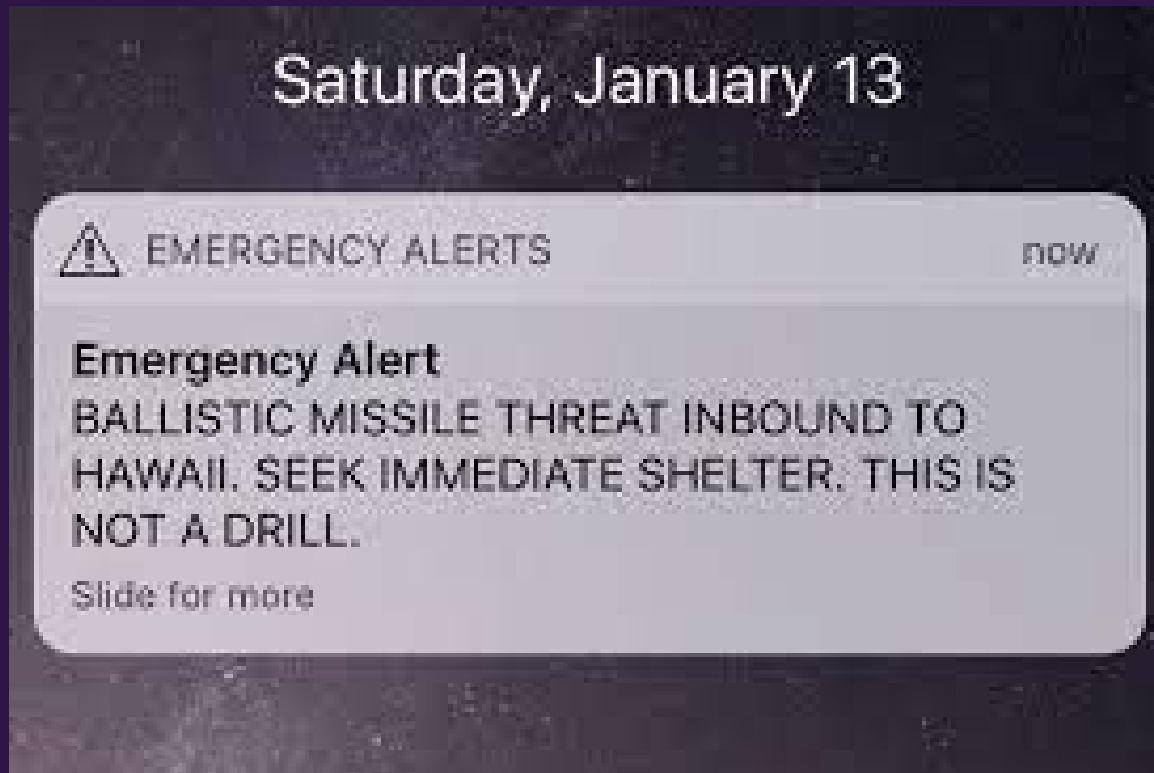


Common Threat Vectors

- Authenticated Actors Taking action inappropriately
 - Accident or Confusion
 - Disgruntled or Malicious
- Local Software inserted within the Intrusion Protection Boundary
- Business IT Domain
- Reliance on Port Restrictions
- Obscurity as a security policy
- Lack of Domain Isolation
- Open Protocols operating beneath the configured Security Model

Authenticated Actors Acting Inappropriately

On the morning of Saturday, January 13, 2018 8:07 a.m., a ballistic missile alert was accidentally issued via the Emergency Alert System and Wireless Emergency Alert System over television, radio, and cellphones in the U.S. state of Hawaii.



38 minutes and 13 seconds later...



Colonial Pipeline Ransom Ware Attack

Business IT Threat

- Business System Breached with Old VPN Account and Password
- Pipeline Control System Not Breached
- Inability to Protect the Pipeline Control System from the Business System Domain
- Pipeline Shutdown for fear of Being Breached
- \$4.5MM Ransom Paid to Hackers (Partially Recovered)

Colonial Pipeline Company System Map



Reliance on Port Restrictions

All Software needs Ports to Communicate on the Network

- Analogy to an Office Building with ~64,000 Telephones
- Restricting to only 10 phones in the building you can call
 - Who is going to Answer the Phone
 - How do you know who you are talking to
- Fewer Ports Simplifies Firewall Configuration
- Sole Reliance on Port Restrictions is a False sense of Security
- Certificates can Ensure whom/what is picking up the phone

Industrial Control System Security

Basic Guidelines for Manufacturing and Critical Infrastructure

- Never assume a system is Impregnable
- Defense in Depth is Critical
- Vigilance and Monitoring is always required
- Understand the complete set of threats
- Design to mitigate these threats
- Understand where any vulnerabilities are present
- When required have a single point of disconnection

Native Device Protocols

There are Many Industrial Protocols for Many Devices

- Sample List of Common Device Protocols
 - Modbus (Serial, RTU, TCP/IP)
 - Allen Bradley (CIP, ABTCP, ControlNet ...)
 - Siemens (S7comm, FLN P1, USS)
 - BACnet MS/TP (ASHRAE, ANSI, ISO 16484-5)
 - PROFIBUS DP (IEC 61158), PROFINET
 - MQTT
 - AS-Interface (IEC 62026-2)
 - CANopen
 - EtherNet/IP (IEEE 802.3)
- These are Access only (If Even Available). None of these protocols can change the security requirements on a Tag/Item/Attribute/Element basis

Communication Server Protocols

Normalize the Device Protocols to Industry Standards

- DDE (Intra-node only), Outdated, seldom used
- Suitelink (WinSock TCP/IP) Certificate and Non-Certificate Authentication
- OPC DA (COM, DCOM) Large Number of Ports
- OPC UA (TCP/IP) Certificate Authentication
- MQTT (OASIS) Oauth and Encryption
- Others ...

None of these protocols can restrict Access Internally, once access is granted

Security for Device Protocols and Comm Servers

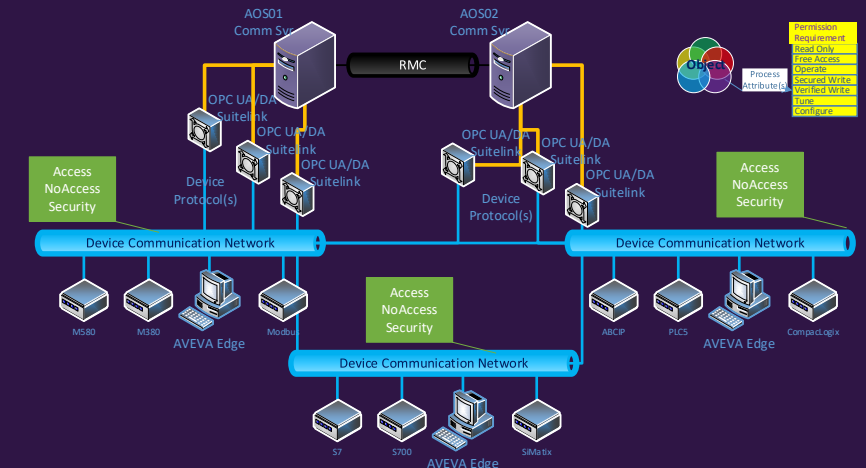
Access Level Security is ineffective and not defensible

- Access Security
 - Grant Access
 - Deny Access
 - Not Possible to Restrict Individual Data Items
- Many Actors need various types of Access
 - Once granted Access to Everything is available
 - Write Confirmation within these Protocols is Not Possible on individual Write Targets
 - Authorized Access – (Anyone, Operator, Tuner, Configurator, No One)
 - Secured Write – Authentication of Actor upon write
 - Verified Write – Authentication of Actor and Approver upon Write

Requirements of a Defensible Security Model

Securing the Devices and Communication Servers

- Devices and Comm Servers must be Restricted to Single points of Access
 - Only 1 Client should be allowed to communicate to a Device Communication Server
 - Ideally Limited to Intra-Node Connections
 - All Network Connections are Denied
 - This should only be allowed from a Service account
 - All Interactive logins should be denied access
 - Network Should be segmented apart from Process LAN
 - Device Protocols must never be allowed connectivity from the Process LAN
 - Operating Systems Executing this function should be denied interactive logins during normal operation



Requirements of a Defensible Security Model

Securing the Devices and Communication Servers

- All Access to Device and Supervisory Writes Must be Secured
 - Access must only be granted on an as needed basis
 - Write Access Only to the Item/Tag/Attribute/Element necessary per business need
 - Authorization Confirmation of writes on selected Items (Secured/Verified Writes)
 - All Writes from Interactive Sources must be Logged (21 CFR Part 11)
 - Not Configurable, No Tag level Checkboxes
 - Logged Independent of Client Technology
- Programming, Modification, and Configuration Access should only be granted when Needed
 - Only from known locations (Development Workstation)
 - Dedicated Devices/Workstations with interactive login denied during normal operation

Requirements of a Defensible Security Model

Secure the Mechanisms used to issue Command and Control Writes

- Supervisory Write Protocol Requirements
 - User Credential (Token) sent with the Write
 - Write Authorized at the Destination of Command
 - Destination Target can Demand Authentication and/or Verification before accepting Write
 - Single Point of Configuration
 - Modification does not require Deployment of HMI Application
- Graphic level security is Desirable but Not Defensible
 - Enhances Operator Experience
 - Restricts Visibility and Reduces Confusion
 - Easily bypassed from different Clients, Graphics and Access Protocols (OPC UA, MQTT, OPC DA, Suitelink)
 - Impossible to maintain or verify (Too Many Configuration Points)
 - Typically implemented by a condition placed on the Animation Link

Requirements of a Defensible Security Model

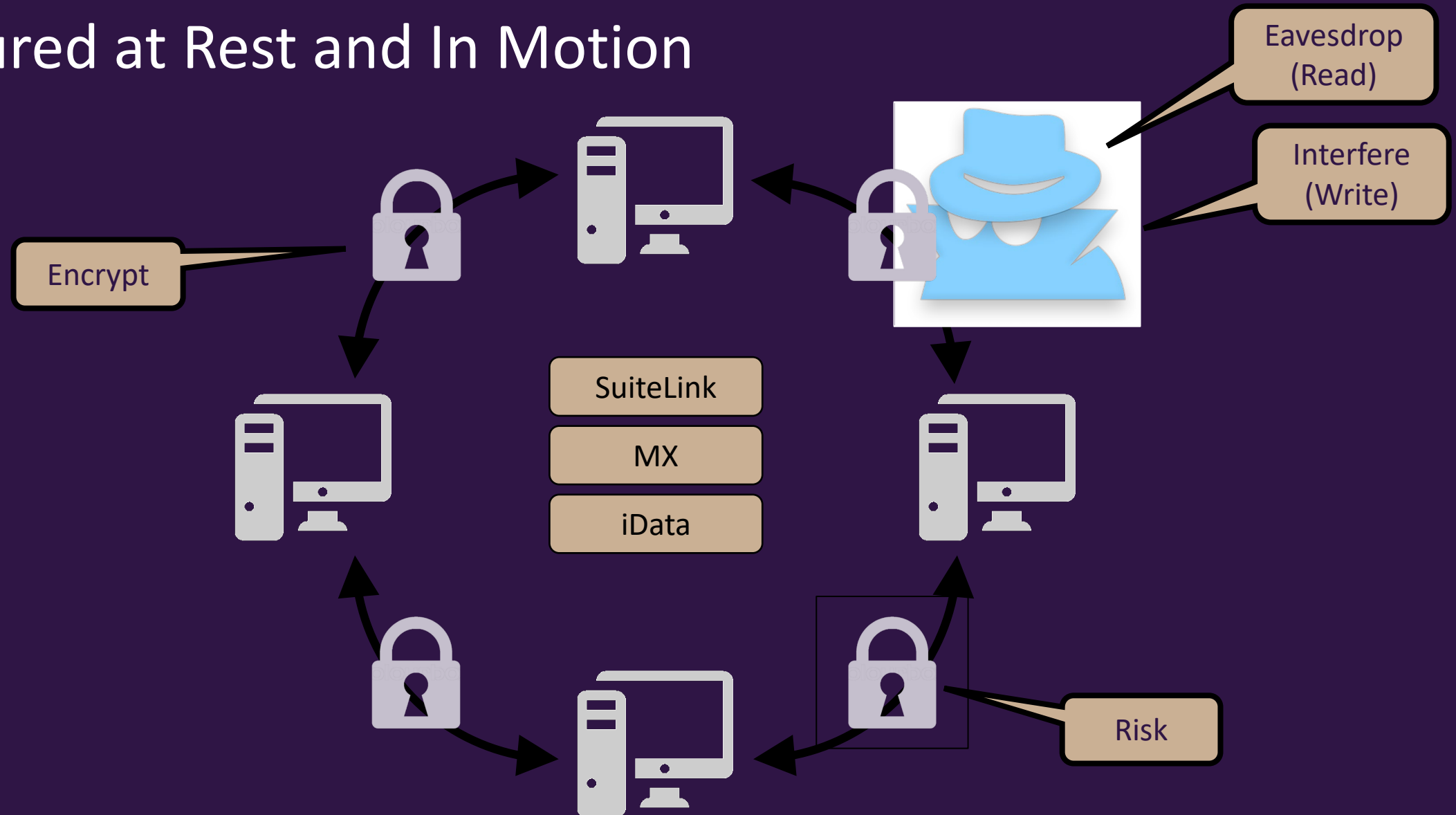
Know and Understand the Needs of Industrial Security

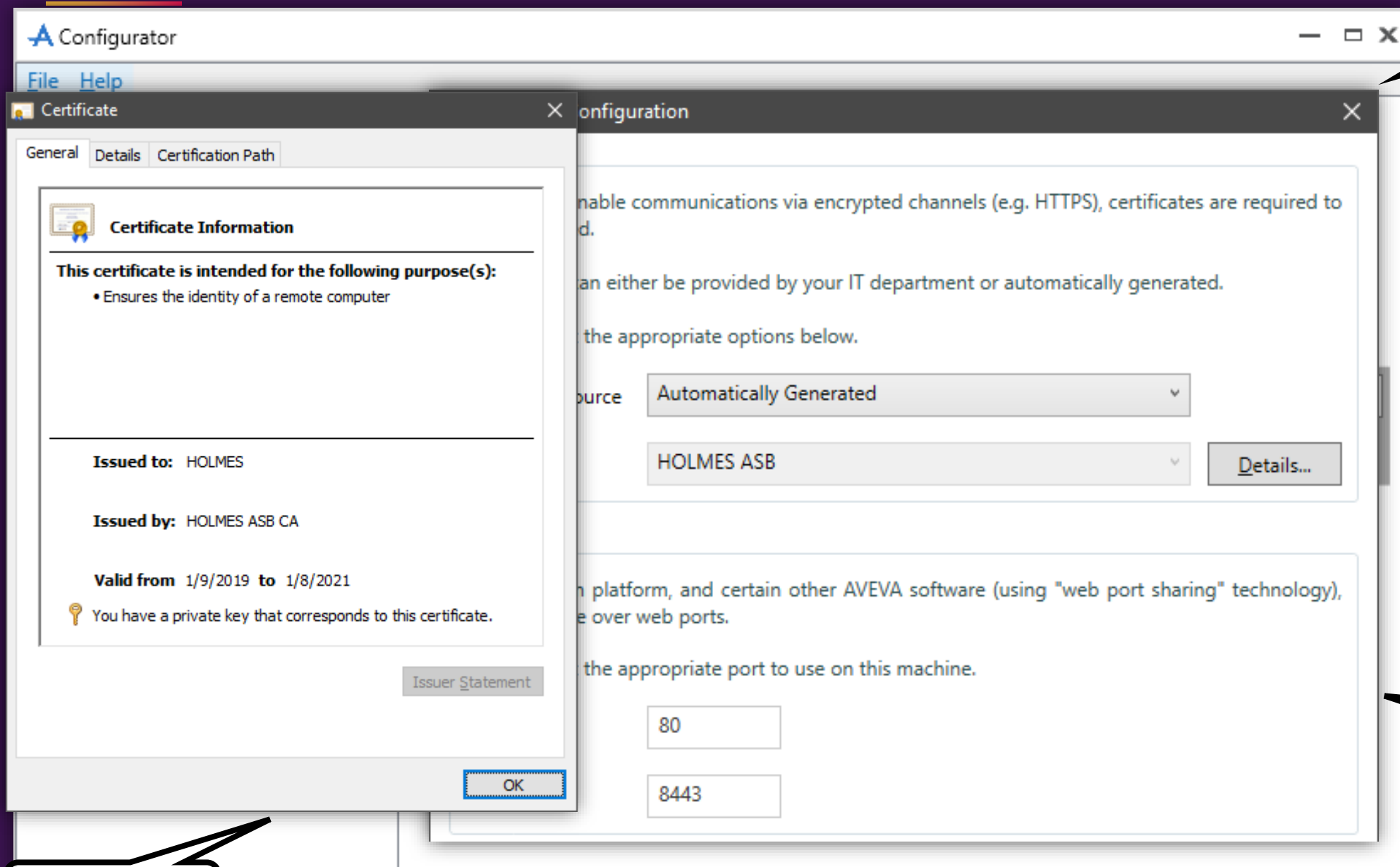
- Sharing of Industrial Data to the Cloud
 - Only Control Domain can Originate this communication
 - Tablets, Browsers, and Phones are Cloud based devices they should not be allowed to breach the Intrusion protections in place
 - What is shared cannot be changed by anyone or thing external to the Control Domain
 - Process Information must be Secured at Rest and Secured in Motion
 - Transmission must preserve the Intrusion Protections in place
 - Firewalls, DMZs, Internet Proxies, Secure Gateways, Domain Isolation must never be bypassed
 - Transmission once established should be Certificate Based locked to the Transmitting entity



AVEVA System Platform Security

Secured at Rest and In Motion





Management
Server

Reduce Risk

Cross Galaxy IDE
access

TLS 1.2
Encryption

Configure

Certificate

and its subsidiaries. All rights reserved.

AVEVA Security Central Website

Global Customer Support

+

https://softwaresupportsp.schneider-electric.com/#/securitycentral

≡

AVEVA™

User ID : 23513599

Mike Llapitan ▾

Search...

Q

Security Central

Security Central Supported Products

Cyber Security Updates

Policy & Guidelines

X

Posted ▾	Report	Status	Description
Sep 28, 2018	WW18-091	Supported	Cumulative Security update for Windows Server 2016 (KB4457131)
Sep 28, 2018	WW18-098	Supported	Security and Quality Rollup for .Net Framework (KB4457043, KB4457044, KB4457038, KB4457035, KB4457042, KB4457037, KB4457033, KB4457045, KB4457036, KB4457034, KB4457131, KB4457138, KB4457142, KB4457128, KB4457921, KB4457918, KB4457919, KB4457920)
Sep 28, 2018	WW18-095	Supported	Security-Only update for Windows (KB4457984, KB4457145, KB4457140, KB4457143)

Object and Role Based Security

User

- Default / Galaxy / OS User / OS Group

Role(s)

- Galaxy Roles / OS or AD Groups
- Development and Operational Permissions

Security Group(s)

- Grouping of Asset Object(s)

Object(s)

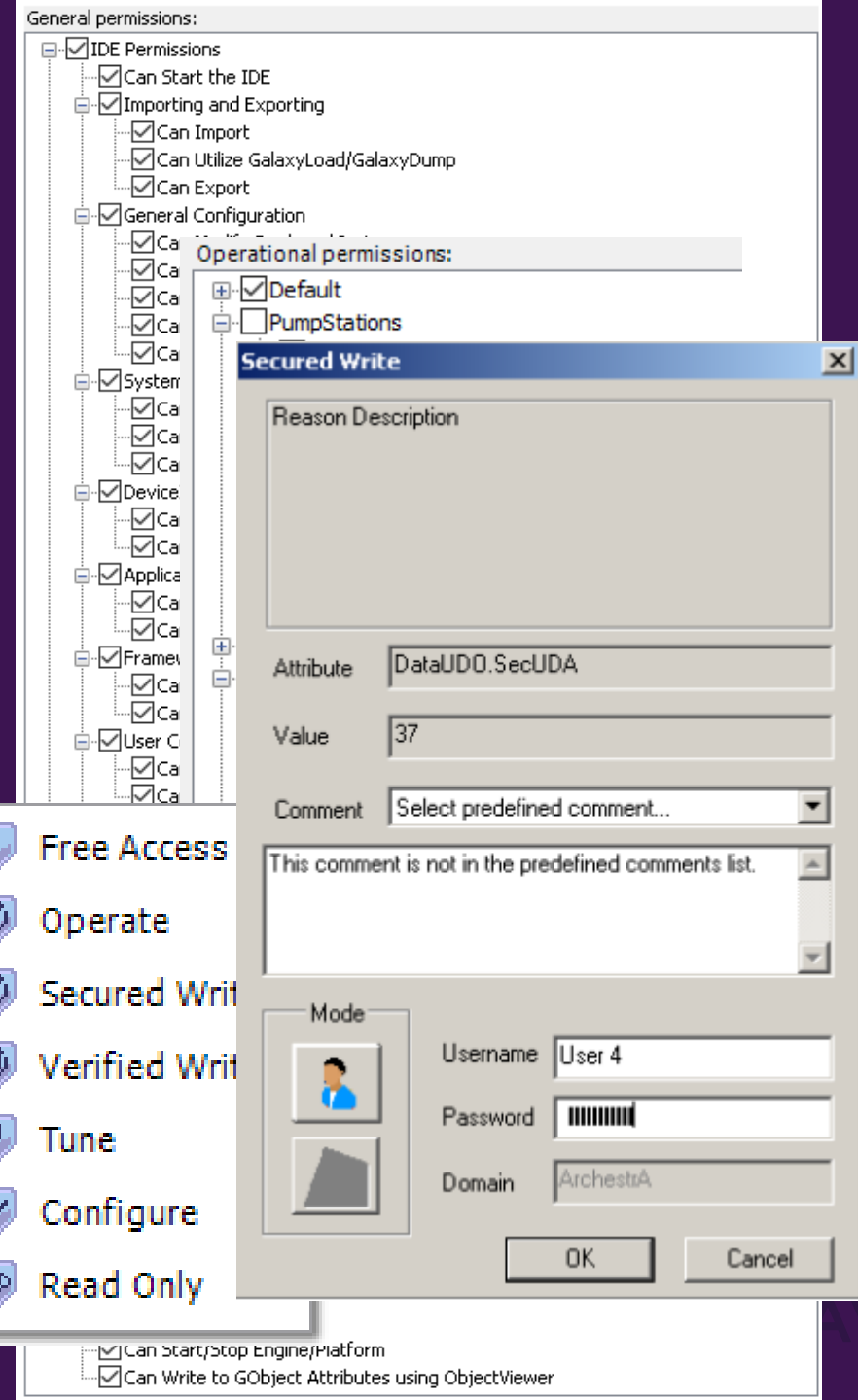
- Templates and Instances

Attributes

- User Writeable / Calculated / Locked

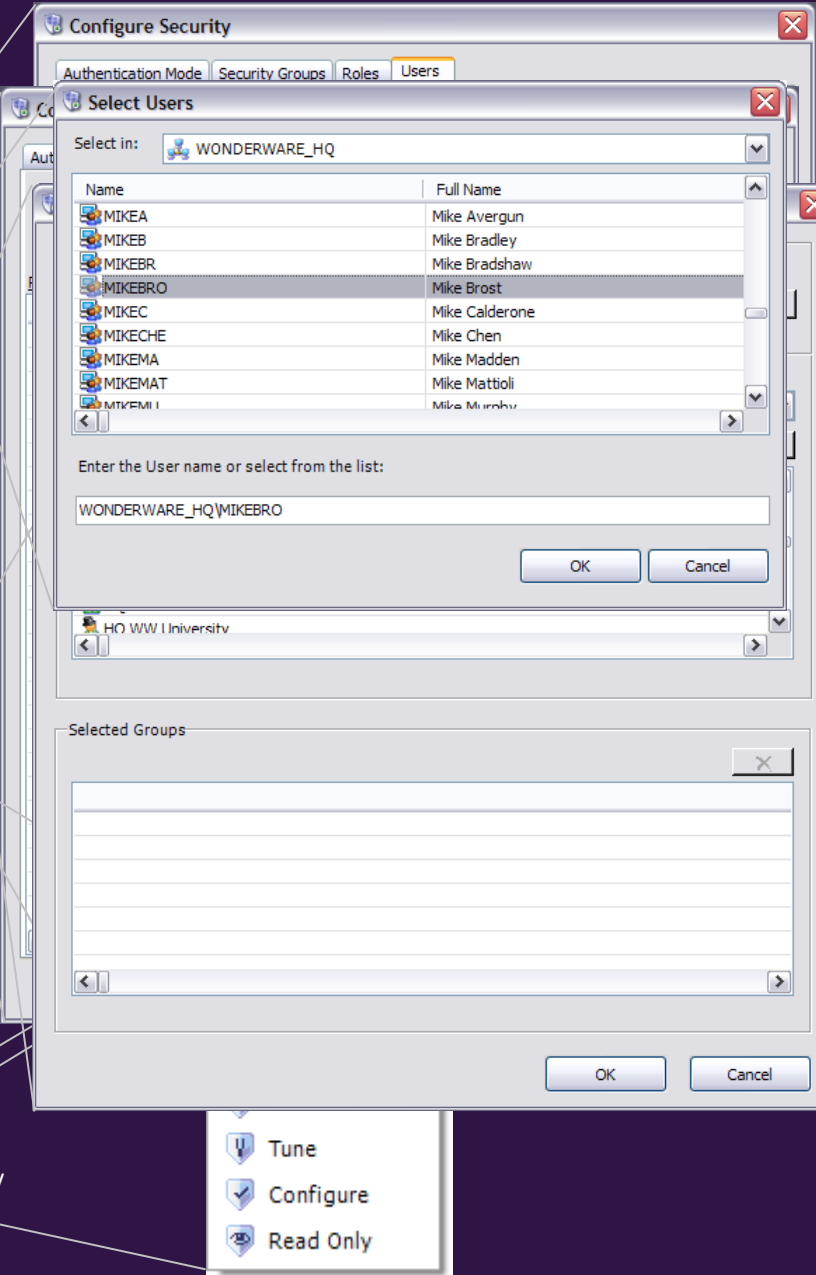
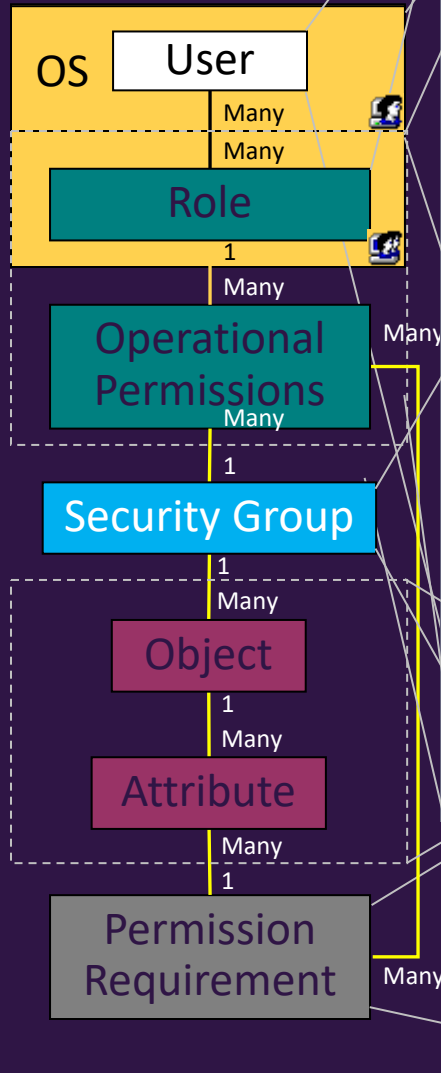
Permission

- Free Access / Operate / Tune / Configure / Read Only
- Secured Write / Verified Write



Powerful and easy to

Security model



Security can be defined down to the object attribute level.

The permission requirements can be set for each of the attributes. This can be done at the object template level.

Object instances with the same access characteristics, are grouped in Security Groups.

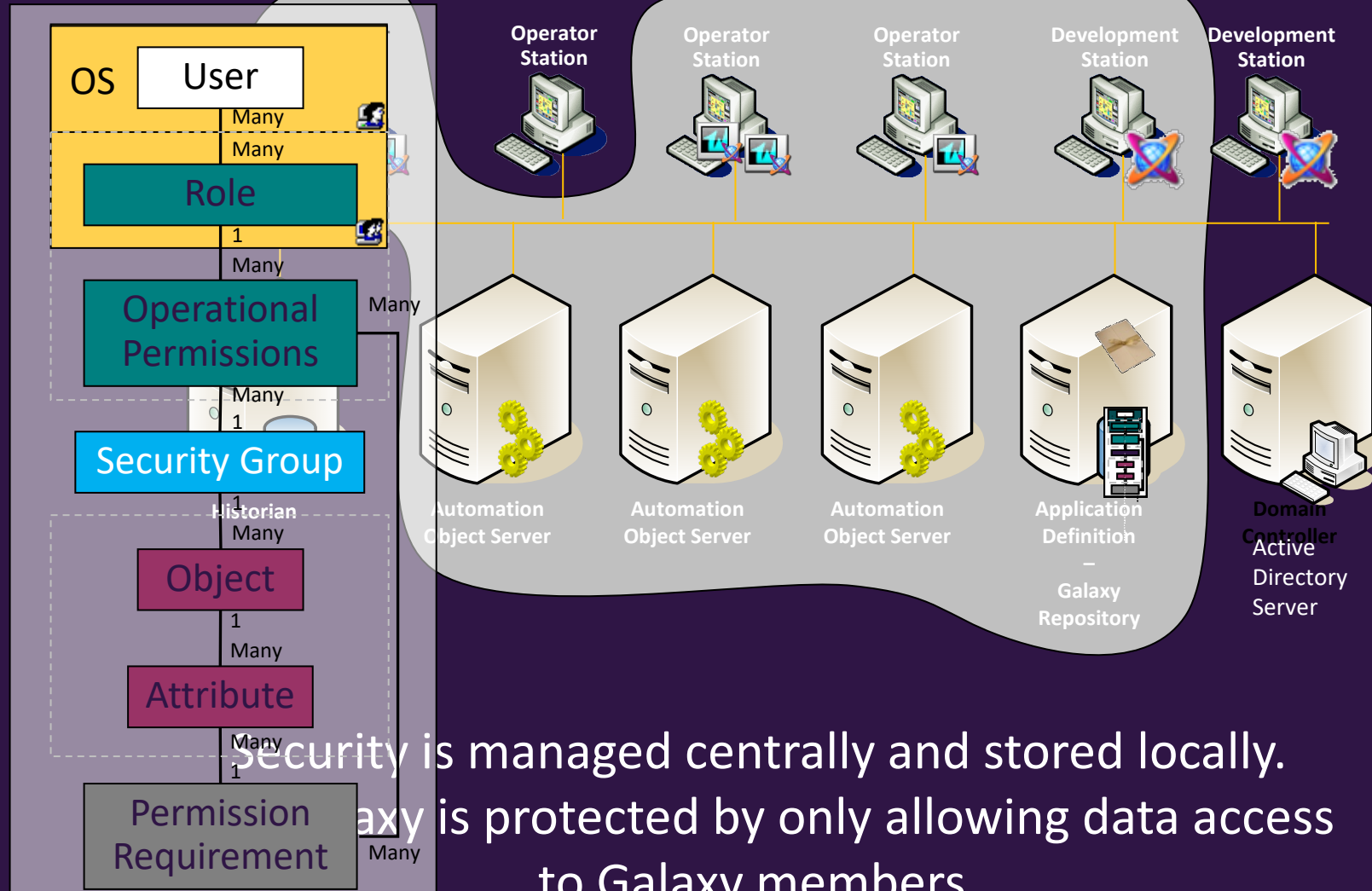
Roles can be given operational permissions for each of the Security Groups.

Users can have multiple Roles.

OS User based authentication allows user administration to be moved to the OS.

OS Group based authentication allows user groups (roles) to be administered from the OS.

Centrally managed and locally stored runtime security model



Runtime Security Model is managed centrally.

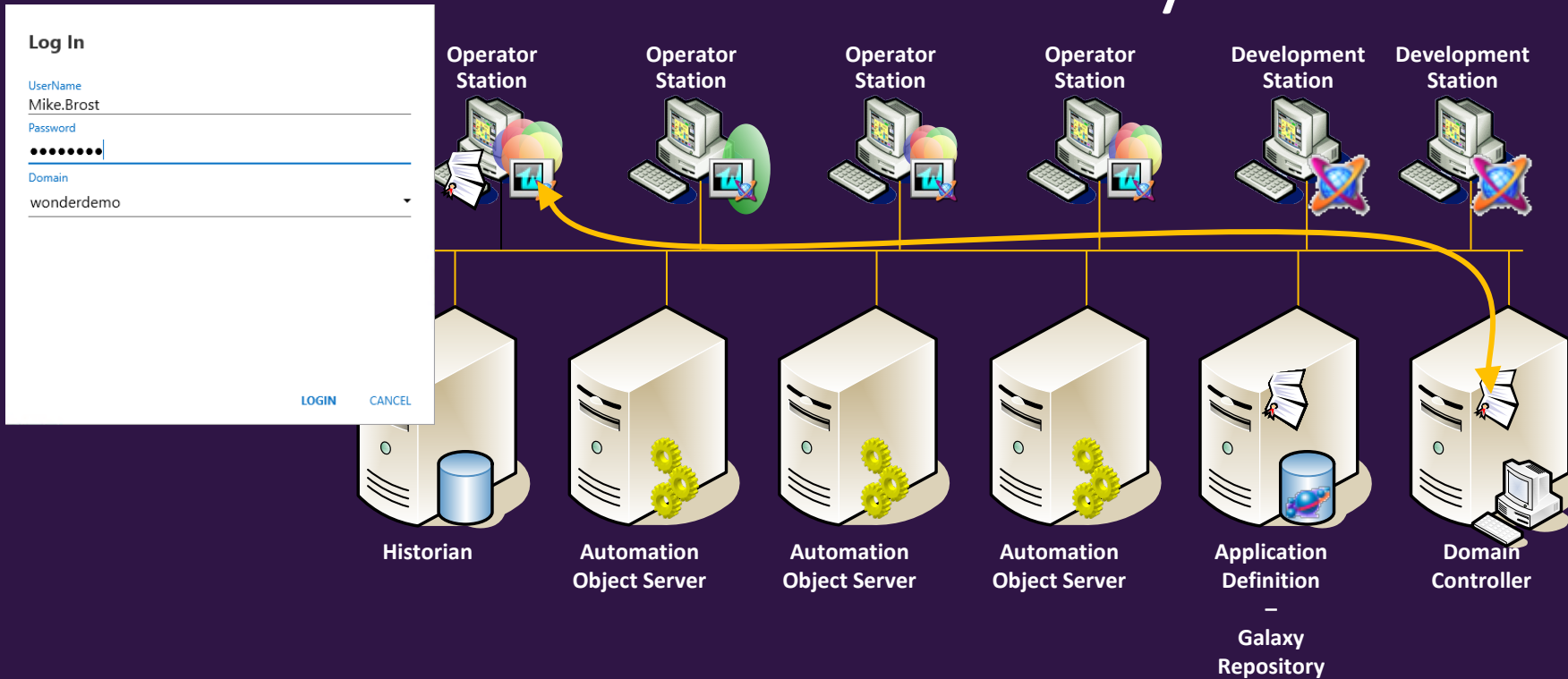
Galaxy Membership invitations can only be sent from Galaxy Repository.

Only Galaxy members get access to real time data in the Galaxy.

Runtime Security Model is stored in Global Cache and distributed to all Galaxy Members

Security is managed centrally and stored locally.
Galaxy is protected by only allowing data access to Galaxy members.

Enforcement of runtime security



Login at Node 1. Operator login independent of PC login.

Login is verified by the Global Cache or Domain Controller as required by the Security Model.

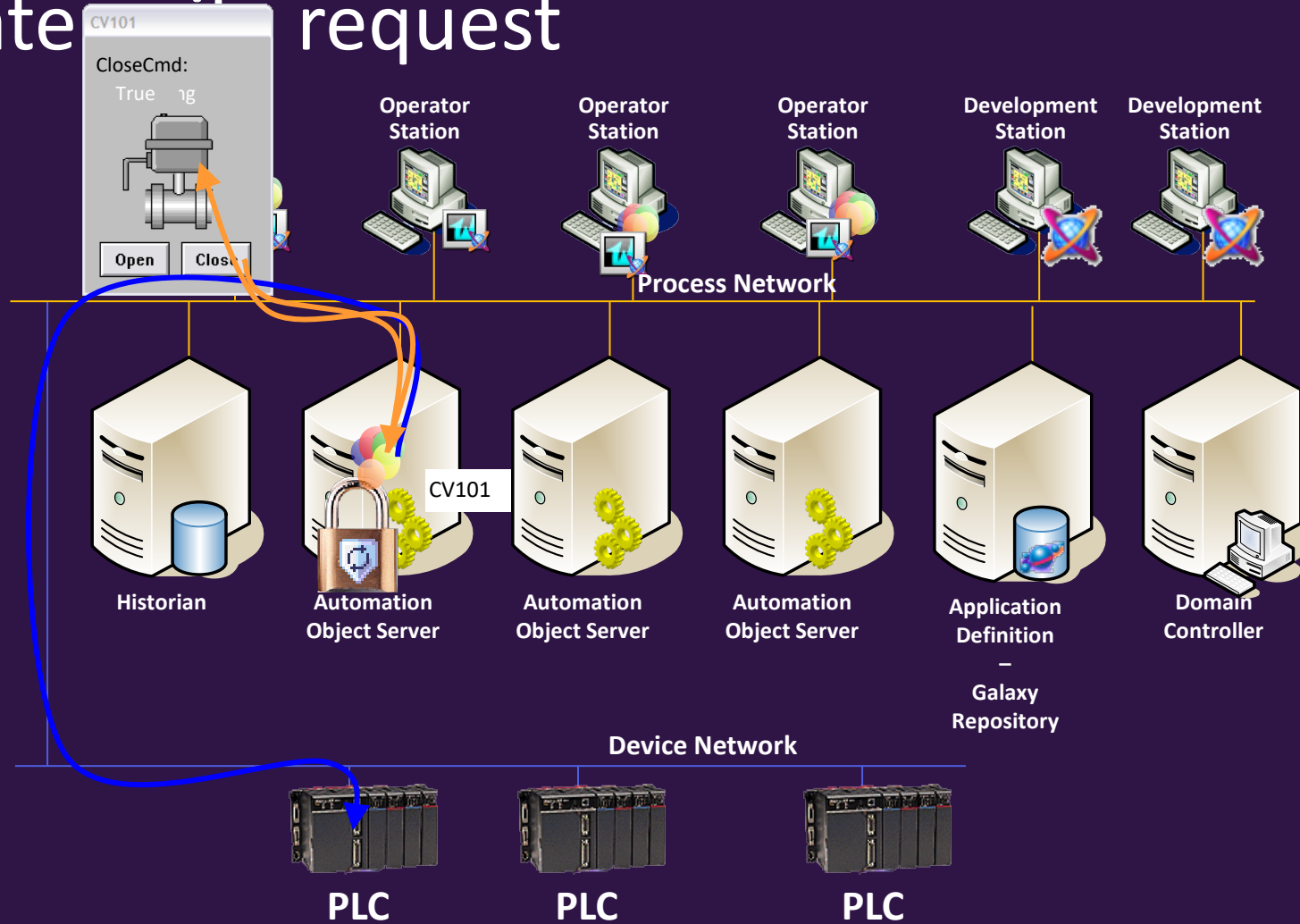
Node 1 local cache is updated with the user credentials.

Galaxy Repository reads Node 1 local cache and updates global cache.

Subsequent logins can be performed against cache if DC or GR is not available.

Can be fully integrated with OS Security.

Operate request



Unrivalled data level security protecting the control hardware layer.

User accesses CV101.

Write request and user credentials are sent to CV101.

CV101: Operate permission required. Object verifies the credentials.

The write is performed, logged in the event sub-system and reported back to the operator station.

The Security Model is not dependent on the Galaxy Repository or Domain Controller.

Secured Verified write request

User/PWD
Two Factor

CV101

Verified Write

Attribute: SecurityTest.VerifiedWrite Value: 76

Comment: This is the Reason you can log for the write

Operator Mode

Username: Mike.Brost

Password: [Redacted]

Domain: wonderdemo.net

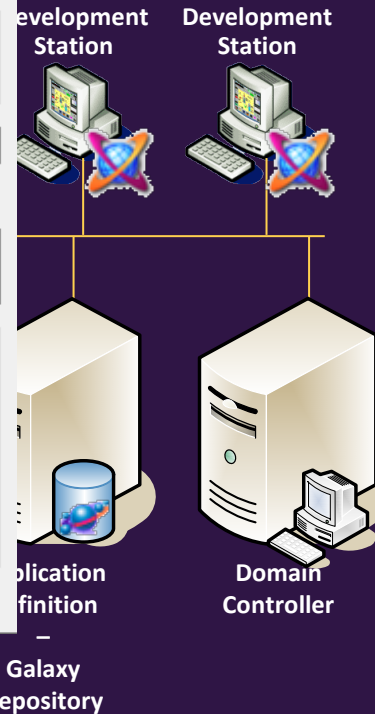
Verifier Mode

Username: Joe.Supervisor

Password: [Redacted]

Domain: wonderdemo.net

OK Cancel



PLC



PLC



PLC

Unrivalled data level security protecting the control hardware layer.

User accesses CV101.

Write request and user credentials are sent to CV101.

CV101: Secured write permissions required.

The user is requested to re-enter the password or 2-Factor.

The user credentials are sent to CV101.

CV101 verifies the credentials and performs write.

Verified write is similar, but with two signatures.



Network Architectures

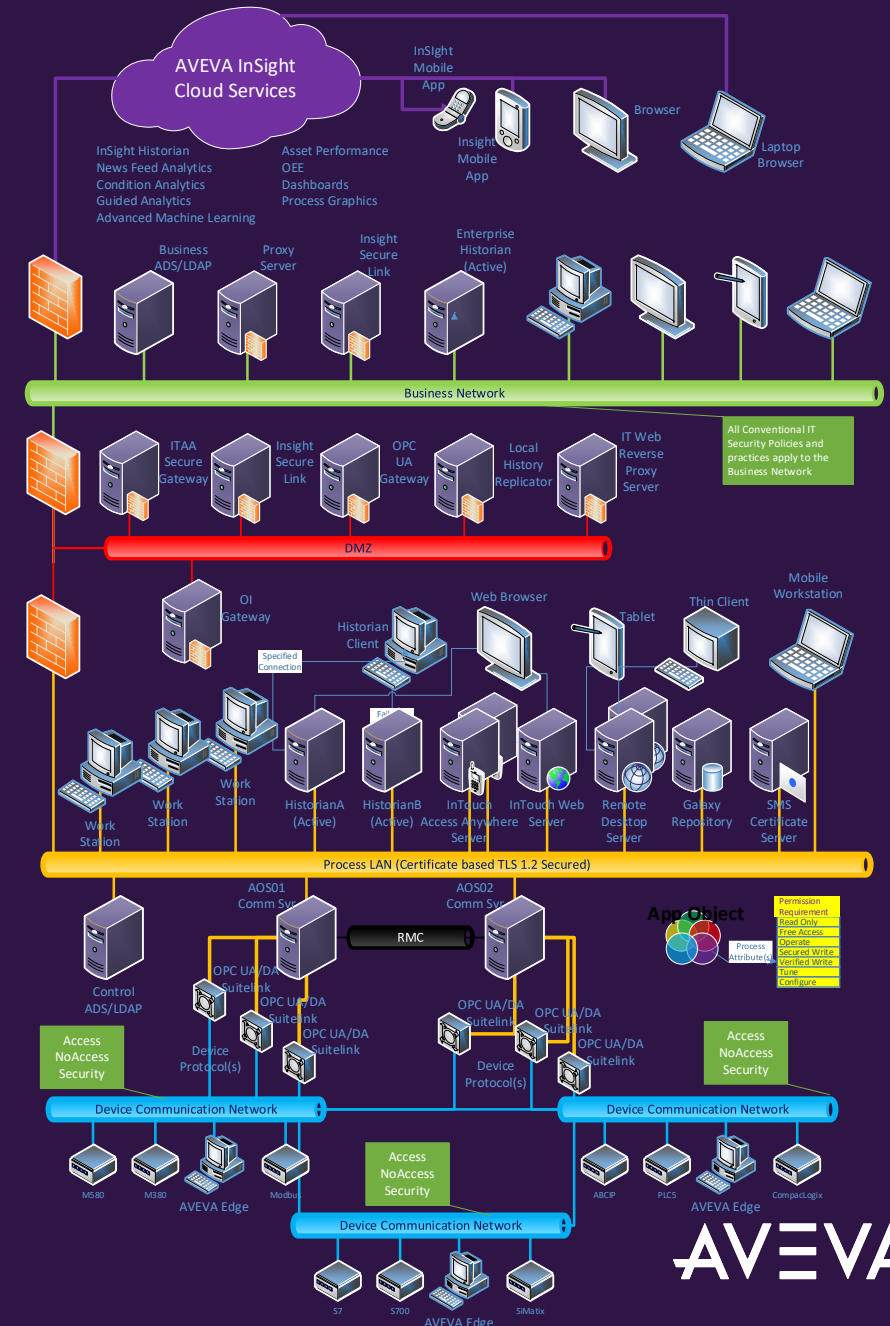


Network Architecture

Connected and Securely Isolated

- AVEVA InSight Cloud (Purple)
- Business Network (Green)
- Site DMZ Network (Red)
- Process/Control Network (Orange)
- Redundant Message Network (Black)
- Device Network (Blue)
- All Intrusion Protection Active and Enforced
- Firewalls Isolate all Traffic to Control Devices

AVEVA System Platform Network Architecture





Securing Device Connectivity

Practical and Effective Security Guidelines



Isolating Device Connectivity

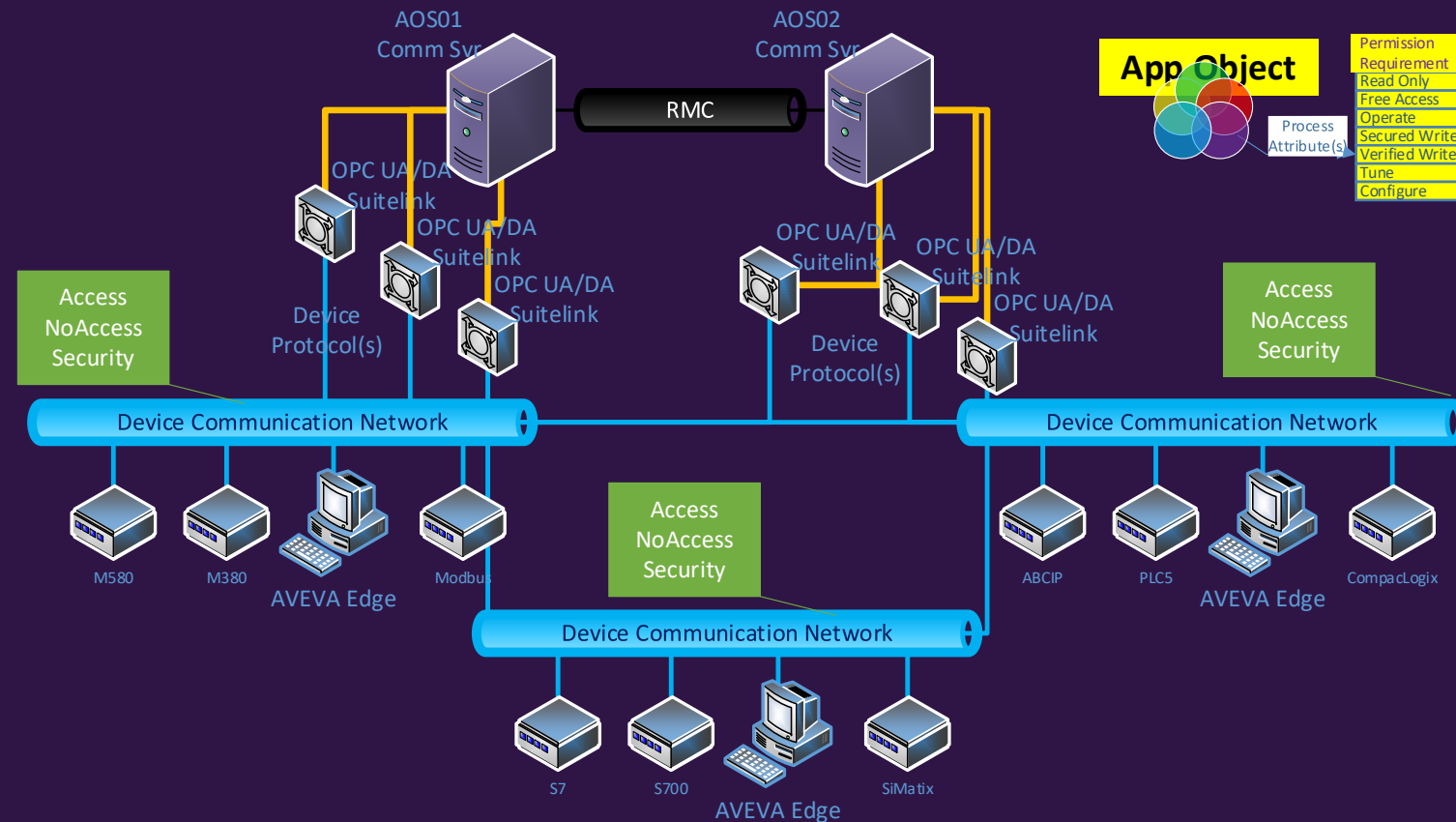
Restricting Connectivity to the Vulnerable

- Dedicated Networks
 - Ethernet (Wired, Wireless, Ethernet Radio)
 - Non-Ethernet (MBPlus, DataHighway, ProfiBus, AS-Interface, Serial, Telemetry, Cellular...)
- Switch Isolation
 - Network Restricted Connections
- Account Restrictions
 - Service Accounts
 - No Interactive Logins
- Programmability Access by exception

Device Level Network (Blue Network)

Least Secure and Most Vulnerable Network

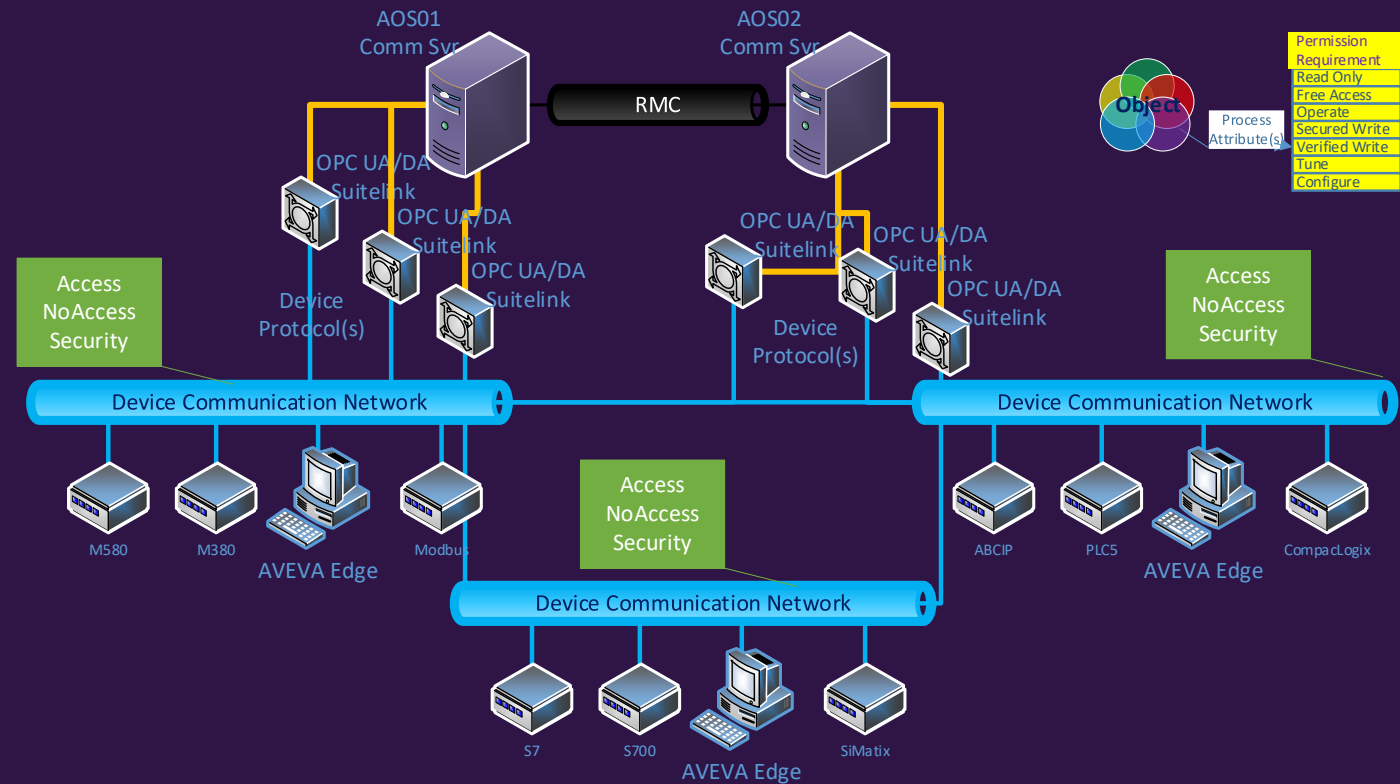
- Switch Controlled Routing Paths
- Isolated Network Connections
- All Interactive Logins are Disabled
- Connection only by Service Accounts
- Device Level Security Varies Widely
 - Certificates
 - Access/No Access Restrictions (Logins)
 - Nothing (Proper Message Format)
- Communication Servers Isolated to a Single Client from the Process Network



Device Level Network (Blue Network)

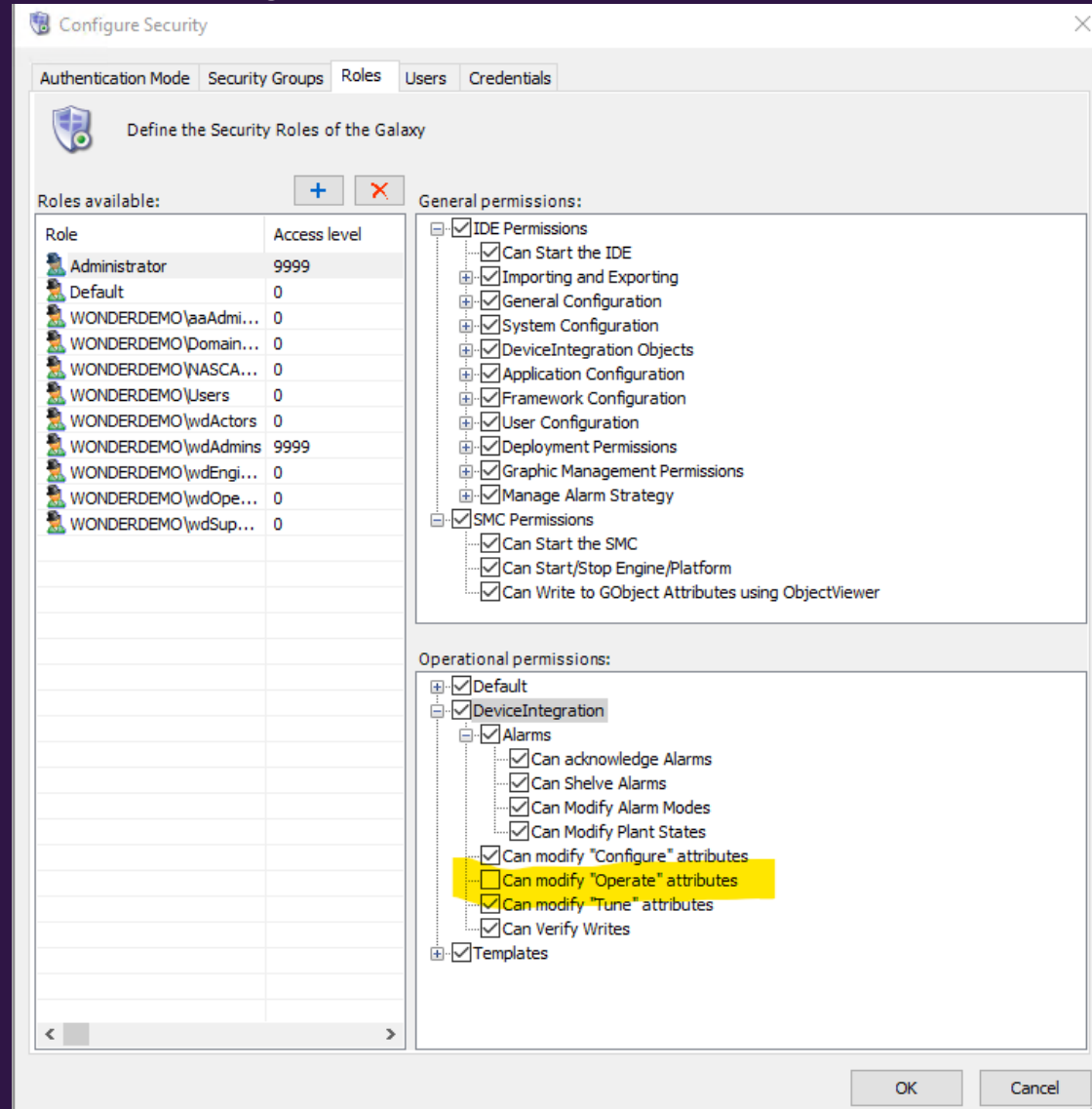
Least Secure and Most Vulnerable Network

- Implement a Managed Device Network
- Example: Cisco FluidMesh now called Cisco Ultra-Reliable Wireless Backhaul
 - Modeled Connections
 - Deep Packet Inspection
 - Mesh Redundancy (Mobile Connections)
 - Physical Connectivity Options
 - Wired
 - Fiber
 - Wireless
 - Cellular
 - Radio



Dedicated Device Integration Objects

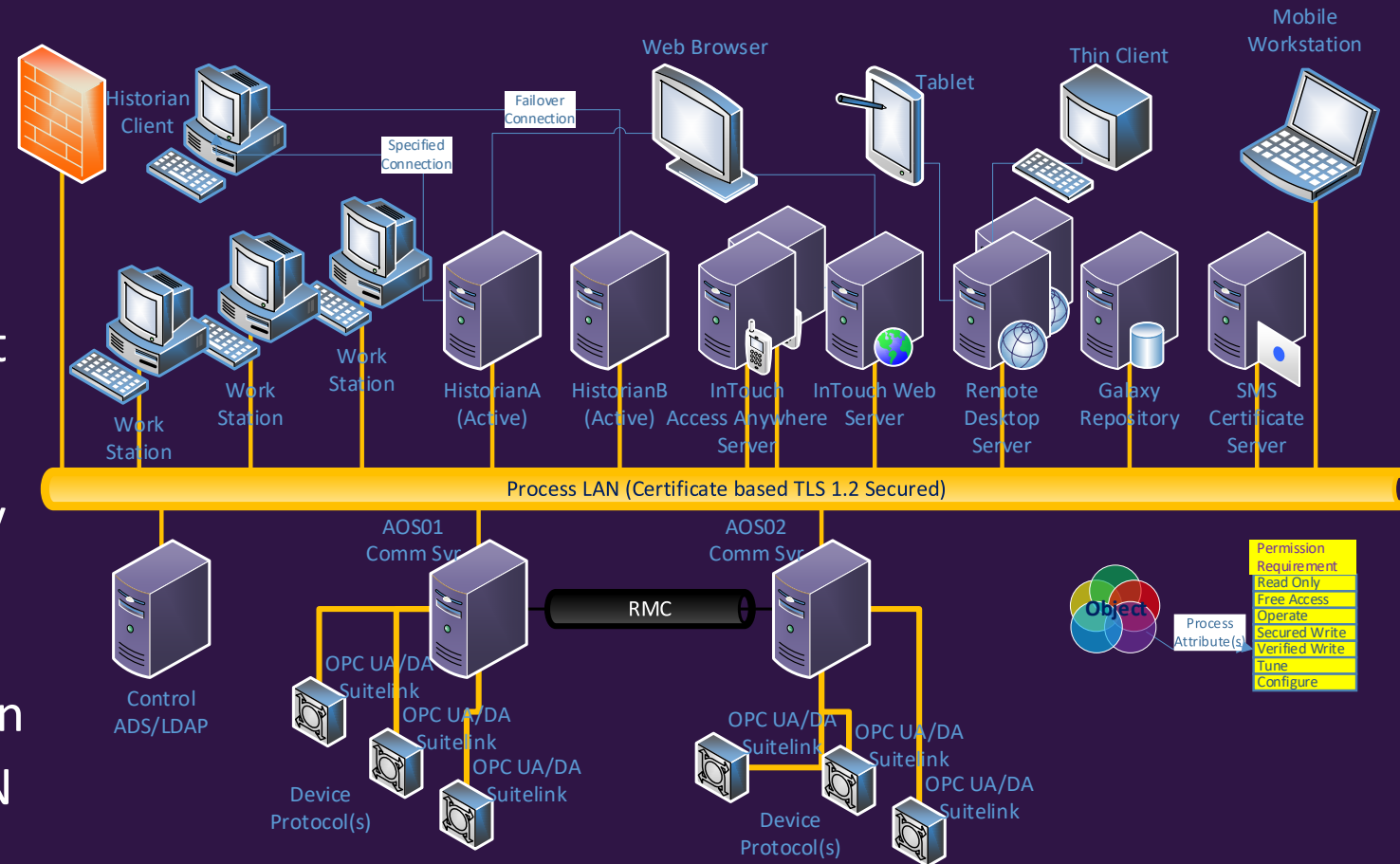
- Device Server Clients
 - DDESuitelink Client
 - OPCClient
 - PCS Service Connectivity
- Isolated in a Security Group
 - Deny all Access to Operate Attributes by Default
 - All Device Items are in the Operate Category
 - Use Tune for Object Settings
 - Allow Operate Access only in Justified Business Cases



Process Control Network (Orange Network)

Secured with Certificate Based TLS 1.2

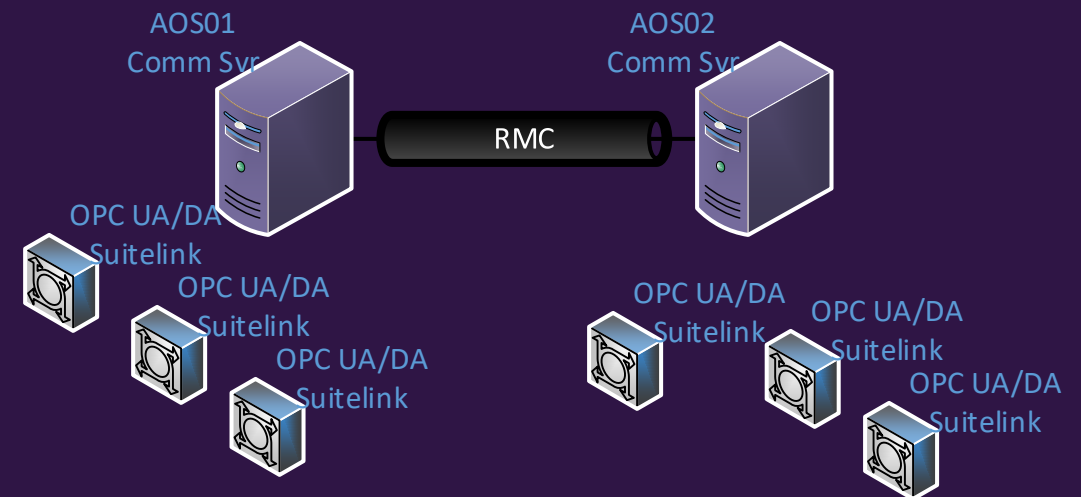
- Firewall Isolated from DMZ
- Domain Isolated from Business IT
- Internode Comms Encrypted at Rest and In Motion
- All Access via Object Model Security
- AOS's denied Interactive Login
- Outbound Only Communications can only be originated from Process LAN



Redundancy Message Channel (Black Network)

Service Level Redundancy Between Application Engines

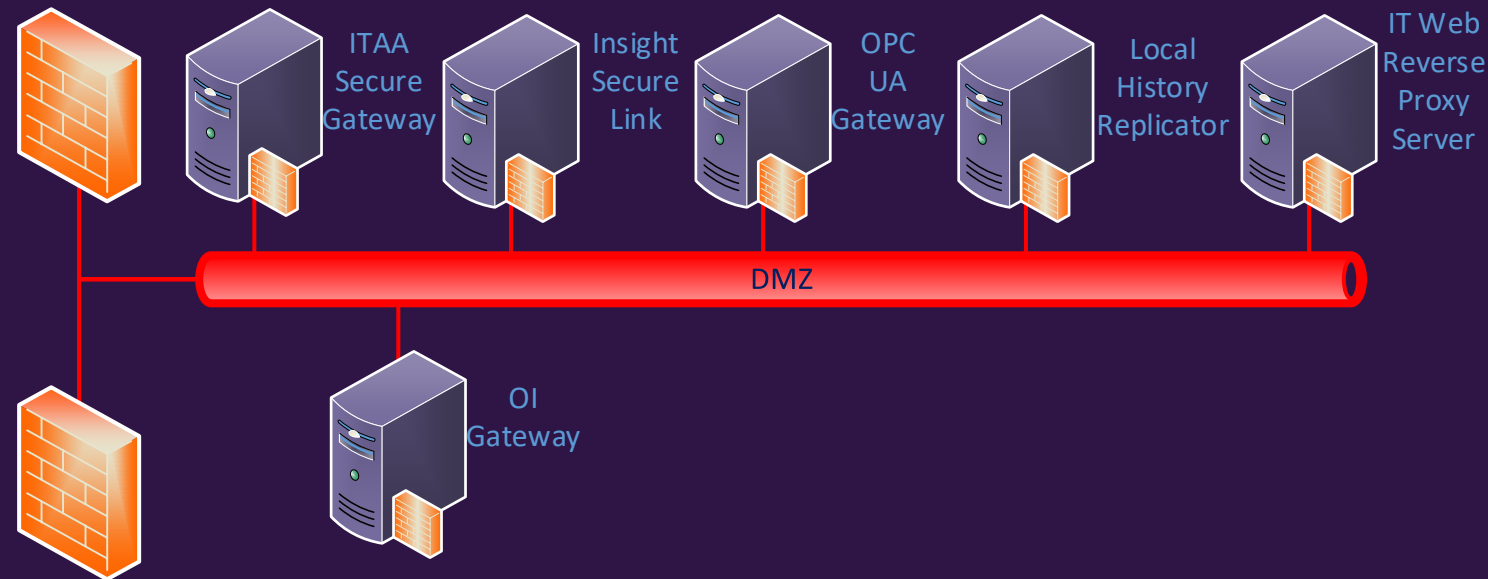
- Application Engines are Partnered (Services)
- Primary and Backup in Configuration (Only Primary Changeable)
- Active and Standby in Runtime
- Everything Application Synchronized by Active AppEngine to Standby
 - Software Installs (Even when GR Unavailable)
 - Configuration Changes (Even when GR Unavailable)
 - Calculations, Real-time Values, Memory Values
 - Alarms
 - Detection Time Preserved
 - Alarm States (Active, Ack, RTN, Silenced, Disabled, Enabled)
 - History Store Forward (Both Active and Standby)
- Redundancy Supports Administration and Failure Induced Downtime
 - OS Patches, AVEVA Software Version Updates, OS Failure, Hardware Failure



DMZ Network (Red Network)

Isolation between Control and Business

- Firewall Isolated from Control and Business Networks
- Access Routed through Proxies
 - Insight Secure Link
 - Local History Replicator
 - (Currently Enterprise Historian)
 - ITAA Secure Gateway
 - IT Web Reverse Proxy
 - OPC UA Gateway
 - OI Gateway (OPC DA, MQTT, Suitelink, DDE)



Ensuring a Defensible Control System

AVEVA System Platform based Application Server Provides the Only Solution in the Industry

- **AVEVA InTouch** can easily have all device communications routed through Application Server
 - Access Name Galaxy secures the data communications
 - Secure and Verified Writes Supported
- **AVEVA Edge** is a Certificate Based TLS 1.2 End Point Device for System Platform
 - Device Drivers are internal to AVEVA Edge
- **AVEVA Batch Management** and **AVEVA MES Operations** can route all communication through System Platform
- **AVEVA Recipe Management Plus** can direct all communication through System Platform
- **AVEVA Workflow** conforms to the Object Security Model when linked through System Platform

Requirements of Defensible Control System Security

- Certificate based access only
- Four **A**ces's of Control System Security
 - **Authenticated**
 - **Authorized**
 - **Approved**
 - **Archived**
- Enforced at the Destination of Every Command
- Completely Independent of Client Configuration and Protocol
- Securely Engineered Network Segmentation and Intrusion Protection



AVEVA System Platform Security Enables the Defense Required


Message Exchange and Platform Common Services (PCS)

- Certificate based TLS 1.2 Encryption
- User Identification Transmitted with Every Write
- Read Path Independent to Write Path, Guaranteed Delivery of Commands
- Graphic Animated to Reflect Write/Read Status independent of Graphic Design
- Security Modeled and Enforced at Object.Attribute Destination
- Changes Logged by the Destination Write Target in Historian (Write Once)
- Object.Attribute Security Model cannot be Bypassed
- Safe and Secure Cloud Integration through Existing Intrusion Protection Layers



This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

 linkedin.com/company/aveva

 [@avevagroup](https://twitter.com/avevagroup)

ABOUT AVEVA

AVEVA is a global leader in engineering and industrial software driving digital transformation across the entire asset and operational life cycle of capital-intensive industries.

The company's engineering, planning and operations, asset performance, and monitoring and control solutions deliver proven results to over 16,000 customers across the globe. Its customers are supported by the largest industrial software ecosystem, including 4,200 partners and 5,700 certified developers. AVEVA is headquartered in Cambridge, UK, with over 4,400 employees at 80 locations in over 40 countries.

aveva.com