



# Cybersecure Brownfield Plant Automation Architecture Solution

## Technical Solution Overview



## Important information

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content.

Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

© 2021 Schneider Electric. All rights reserved.

# Table of contents

<b>1.</b>	<b>Introduction</b>	<b>5</b>
1.1.	<i>Manufacturing and process as plant operations under Attack</i>	5
1.2.	<i>Schneider Electric is proposing a comprehensive approach</i>	5
<b>2.</b>	<b>Customer Challenges</b>	<b>7</b>
2.1.	<i>What are the challenges?</i>	7
2.2.	<i>What are the values of the solution?</i>	9
2.3.	<i>Glossary</i>	10
<b>3.</b>	<b>Solutions Overview</b>	<b>11</b>
3.1.	<i>Solutions presentation</i>	11
3.2.	<i>Security functions</i>	11
<b>4.</b>	<b>Solution Architecture Description</b>	<b>15</b>
4.1.	<i>Recommended EcoStruxure Plant Architecture</i>	15
4.2.	<i>How we adapt the recommended architecture in brownfield plants</i>	16
4.3.	<i>Helping Secure the Architecture Dataflow</i>	17
4.4.	<i>Architecture Components Description</i>	21
<b>5.</b>	<b>Solution Use Case Examples</b>	<b>25</b>
5.1.	<i>Helping to Secure a Water Plant</i>	25
5.2.	<i>Wastewater Treatment Plant Enhanced Protection</i>	28
5.3.	<i>Large pumping Station Protection</i>	32
5.4.	<i>Summary of generic uses and segments</i>	35
<b>6.</b>	<b>Appendix</b>	<b>37</b>
6.1.	<i>Glossary</i>	37
6.2.	<i>Reference Documents</i>	39

## 1. Introduction

### 1.1. Manufacturing and process as plant operations under Attack

Media reports regularly highlight cyber-attacks on industrial players across all verticals, wreaking expensive havoc on operations. The growing number of cases shows that industrial networks have become a target and enhancing their security is now the key to help ensure production integrity, continuity, and safety.

Cyber-attacks on Industrial Control Systems are becoming more prevalent. These systems are generally easy targets for attackers due to their extended life expectancy and their dependence on legacy technologies. Many systems did not consider cybersecurity during their conceptual definition and render themselves vulnerable to even the most basic attacks.

This solution focuses on brownfield plants, where the migration of installed base PLCs or network infrastructure is not possible in the short term. We are proposing a solution with a minimum impact at the level of existing network infrastructure and zero configuration of existing automation assets.

### 1.2. Schneider Electric is proposing a comprehensive approach

Cybersecurity consists of three basic pillars: people, processes, and technology. This paper focuses on the technology pillar. It is strongly recommended to understand the people (social engineering) and process pillars as they are fundamental to security enhanced integration, deployment, and maintenance.



**Figure 1: Cybersecurity lifecycle**

Moving outward from the center of the circle, we find the four key requirements for helping to secure industrial networks that serve as guides to the development of a security lifecycle process.

---

These key requirements are:

- **Permit:** Manage access to operations systems and information through network and physical controls.
- **Protect:** Specific controls that are part of the operations systems help provide ongoing protection.
- **Detect:** Active processes monitor the operating environment to detect and communicate threats.
- **Respond:** Capabilities and systems support rapid response to cyber incidents to contain and mitigate attacks.

Depending on the security framework we use to define the security plan, we can also add asset identification requirement as part of the asset management function.

Schneider Electric has selected IEC 62443 as its core cybersecurity standard and provides water and wastewater operators with end-to-end cybersecurity surrounding its digital solutions as part of its cybersecurity strategy. Briefly these are the key points:

- We commit to help protect our assets, persons and portfolio using the recommended practices and standards, like NIST framework, IEC 62443, and IEC 27001.
- We develop security enhanced products in a controlled environment and provide evidence of this by displaying site and product certifications consistent with local and international cybersecurity standards.
- We deploy this security enhanced offer with a global cybersecurity team, using standard and certified secure recommended practices, and providing services like consulting, training, and so forth.

Finally, we offer defined solutions based in our security enhanced products and our specialized partners for meeting the needs of our customers operating in the main industrial segments.

## 2. Customer Challenges

### 2.1. What are the challenges?

Technology evolution has exposed control systems to vulnerabilities that previously affected only office and business computers. Industrial Control Systems (ICS), employing the same technology as home, office or business computers, have become exposed to the same malware that targets those computers, through lax internal security practices, external contractors with access to industrial systems, and inadvertent publicly accessible network interfaces.

Associated with the digitalization benefits for the plant, there also exist the challenges to secure the industrial Internet of Things (IIoT) through secure cloud or Internet connectivity. This solution provides a security enhanced connection between specific areas of the plant where the IIoT are located and the cloud where the data is sent, for example, to Schneider Digital advisors.

It is highly recommended to select and follow an industrial cybersecurity standard when defining the security plan to help protect the assets and persons of the plant. This is a challenge and Schneider Electric recommend following IEC 62443 recommended practices. This solution is designed according to the principle of helping the customer become aligned with this standard.

As a first step in every mitigation plan to help protect the assets, it is necessary to solve the challenge of having an updated and accurate picture of the devices connected to the network. This solution provides a network inventory feature assisting the customer in identifying its install base of assets in a passive way with no interference in production operations.



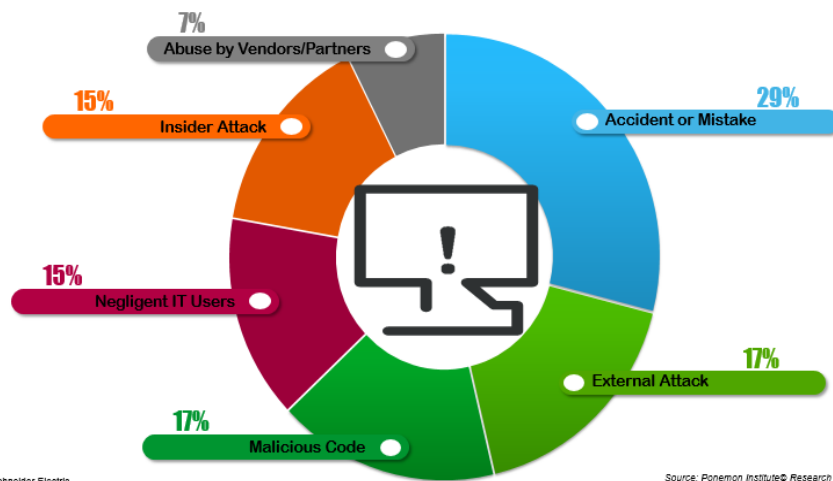
**Figure 2: Mitigation plan for help securing a network**

Ethernet and TCP/IP technologies have provided many new and attractive capabilities:

- Integrated applications through network intelligent devices.
- Embedded web servers for remote access.
- Wireless connectivity.
- Remote access for maintenance.
- Automated software management.
- Distributed control.
- Instant access to up-to-date information through the business systems (e.g. inventory, production, shipping and receiving, purchasing, and so forth).

With the use of standard technologies such as Ethernet, control systems are now vulnerable to cyber-attacks from inside and outside of the control system network.

### Data Breach Root Cause Distribution



**Figure 3: Security Categories**

The security challenges for the control system environment are:

- Physical and logical boundaries vary.
- System can span over large geographical regions with multiple sites.
- System security implementation can adversely impact process availability.

With the political terrorism threats increasing during recent years, plus the threat of cyber-attacks and other new forms of internal security threats, end users must be more diligent than ever with how their systems are protected. The motivations of attackers can be hard to understand, but their consequences can include devastating production loss, damaged company image, environmental disaster, or such other losses.

Companies need to be more concerned about security than ever. No longer will barbed wire and security guards satisfactorily protect assets. Lessons learned from the IT world must be employed to help protect facilities and infrastructure from disruptions, damage, or worse.



## 2.2. What are the values of the solution?

Having discussed customer challenges, we next turn to the benefits and value of the proposed solution. Simply stated, this solution helps customers to enhance the security protection of their plants with a minimum impact on production and the existing configuration of network and automation assets.

Because of its simplicity, the proposed solution can be deployed by OT people who possess minimum IT skills and also can be managed and maintained by existing IT personnel in charge of monitoring the state of plant security.

The inherent benefits of this solution include:

- The skills needed to deploy the solution are defined for OT profiles and the configuration interfaces are defined and simplified according to the OT profiles.
- Commissioning the solution caused minimum impact, without the need to modify the configuration of the automation assets. Optionally, we can modify the configuration of a single switch to mirror the traffic of the network.
- Maintenance and configuration are centralized. Upgrading firmware of the cipher - Mercury software running on Harmony Edge Box - can be performed without impacting production operations.

No single solution can provide adequate protection against every cyber-attack on the Control Network. Schneider Electric cybersecurity strategy recommends employing a “defense-in-depth” approach by the application of multiple layers of security controls to help mitigate risk. Defense-in-depth is a common international approach to help protect the control network by applying enhanced cybersecurity methods.

The “defense-in-depth” approach recommends six layers of defense:

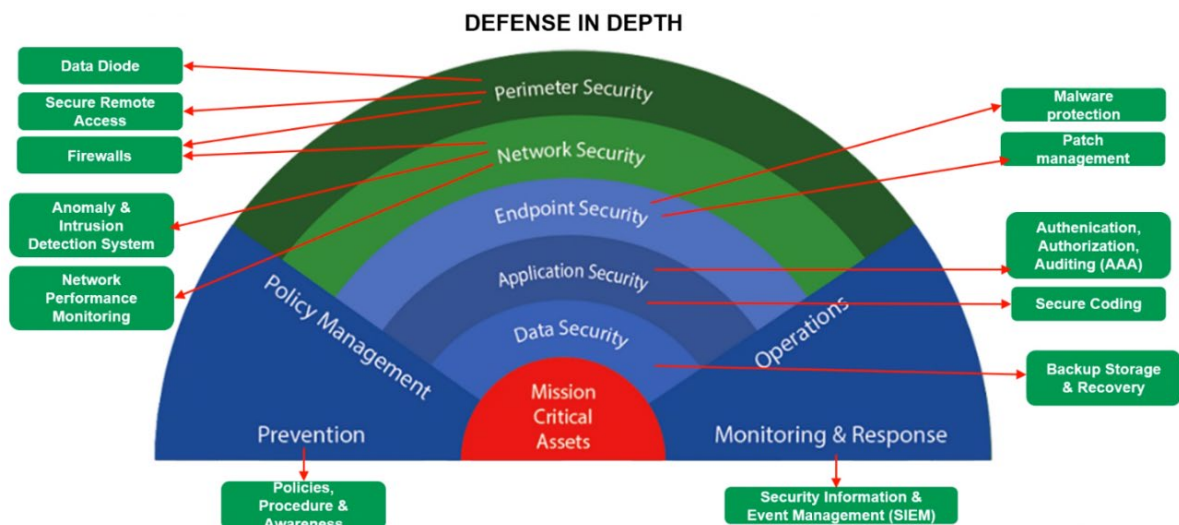


Figure 4: Defense in depth layers

The main values of this solution are aligned with the recommended practices of the defense-in-depth strategy from Schneider Electric and are summarized in **Table 1**. This approach is consistent with the recommended practices defined by IEC 62443 standard series:

Function	Description
Network Separation	Physically separating the control system network from other networks, including the enterprise, by creating demilitarized zones (DMZs).
Perimeter Protection	Helping to prevent unauthorized access to the control system using firewalls, authentication and authorization and VPN (IPsec). This includes remote access.
Network Segmentation	Sub-divide the network providing containment in the event of a security breach within a subnet. It can be further enhanced using the concept of communication zones. Each zone would be buffered from other zones using a security firewall to limit access, monitor communications and report incidents.
End-to-End Security	This is the process of helping to protect the end-to-end communications to help protect their communication-based threats. It involves use of security enhanced protocols encrypted, signed and authenticated. In this solution using an external protection to the device without impacting the device itself and transparently to the existing network infrastructure

**Table 1: Main Benefits and Values of Proposed Solution**

## 2.3. Glossary

A glossary is available in the appendix chapter of this document. Please refer to it whenever necessary.

## 3. Solutions Overview

### 3.1. Solutions presentation

This solution is designed to enhance the degree of protection of OT networks, data, and industrial communications with a minimum impact on the existing industrial network architecture and industrial assets, including controllers such as the PLC. The solution is scalable with respect to the required number of assets or areas to be secured and supports a very flexible deployment by the end customer, system integrator or our cybersecurity global service team.

The solution proposed supports the recommended practices for helping to secure the network infrastructure defined in IEC-62443-3-3. The most critical cybersecurity solution elements are defined in four categories: Permit, Protect, Detect, Respond. In the section **Security functions**, we delve deeper into the specific security functions that are associated with the categories referenced in and provided by this solution.

Schneider Electric has developed an ecosystem of technological partners, including Enigmedia, who are a part of the Exchange platform. This solution has been developed using the Enigmedia Mercury Cybersecurity Products Suite embedded in a Harmony Edge Box from Schneider Electric.



[More Info.](#)

### 3.2. Security functions

The solution comprises 3 key elements: as software, the security enhanced appliance acts as cipher and the orchestrator acts as the centralized management console of the Mercury Ciphers; as hardware, the cipher runs in the Harmony Edge Box; then Mercury Ciphers gather and send L2 traffic to remote locations or cloud services securely, providing integrity, privacy and enhanced security.

The security functions described below are executed by the Mercury Ciphers running in the Harmony Edge Box, and the configuration of the security functions is done in the Orchestrator.

In this chapter we go deeper into the list of specific security functions related to these categories.

- **Inventory**

Enigma Mercury Products Suite includes inventory functionality to map the devices and connections in an industrial OT network. Mercury Inventory analyzes network traffic and maps devices and connections showing:

- Device manufacturer
- IP address
- Packets size
- Communication Ports

Mercury Inventory is an easy to use, fast, and cost-effective tool for discovering network assets that helps system integrators and end-users sketch the network diagram, identify devices, communication protocols and how they are related.

- **Perimeter protection and segregation**

Users can easily define network segments and **secure zones** from the Mercury Orchestrator control panel.

Also, they can specify which devices will be part of a specific zone, which ones are authorized to communicate with others, and what protocols will be authorized.

- **Firewall and definition of conduits**

Firewall is essential, as it helps prevent attacks from spreading between zones and devices. With Mercury Orchestrator, it is very easy to manage the configuration of authorized ports and traffic.

Ports can be configured as "permanent ports" or "temporary ports". This functionality is very powerful, as having the ports exposed permanently can pose a risk to the integrity of the network and devices.

- **Threat detection and security monitoring**

Mercury helps prevent attacks to the network, whether they are connection attempts through unauthorized protocols, network scanning, or denial of service attacks. This prevention capability can be combined with the monitoring of suspicious behavior, through centralized management of logs.

The Mercury Orchestrator server centralizes the logs of each Mercury Cipher which can be integrated with Security Incident Event Management (SIEM) monitoring tools, to detect and manage alerts as well as suspicious behavior.

The solution is compatible with 3rd party products such as IDS/IPS and SIEMs.

Mercury approach helps prevent incidents, reduces complexity and standardize events to simplify correlation processes and help to avoid false-positive alarms.

- **Helping to prevent vulnerabilities by armoring the network**

Mercury encrypts the traffic that goes through its appliances and distributes the information to validated endpoints.

Mercury is designed for ICS/OT environment. Mercury ciphers the industrial protocols adding less than 1 ms latency. Mercury provides extensive vulnerability masking, limiting the available attack surface. The end-point devices simply ignore other unknown or unapproved access attempts.

Most of the advanced attacks in OT need to gather information from the targeted infrastructure as a first step. By cloaking the network, a malicious adversary is not able to perform such actions since the asset cannot be seen.

Mercury architecture encrypts and obfuscates the network while providing visibility to authorized users. This architecture is compatible with DPI/IDS/IPS solutions.

- **Secure remote access and connections**

Mercury is a robust and easy to deploy solution that provides enhanced security by enabling remote connection via WIFI/GSM/2G/3G/LTE. It is compatible with interfaces, devices, and protocols and is directly applicable to any infrastructure without replacing devices or changing configurations.

Mercury is configured, managed, and monitored from Mercury Orchestrator. Thanks to its centralized console, authorized users can remotely configure temporary ports, firmware settings, and send copies of the traffic to SIEM/SOC or check operational status. Updates can be performed remotely in a security enhanced environment.

Mercury Ciphers provide a trusted platform module (TPM), firewall features, and enforces authentication and encryption in the channel. It also provides several features for helping to prevent Denial of Service (DoS) attacks and sends alerts to the SIEM if it detects suspicious network behavior. Different roles are supported in order to avoid privilege escalation.

Thanks to the temporal firewall rules and different role assignments, plant operators can grant access to maintenance providers in a controlled and auditable manner in an enhanced security environment. Tunneled devices cannot access to the configuration interface.



## 4. Solution Architecture Description

There is a clear difference between the ideal or recommend security enhanced architecture and the feasible measures we can adopt in any existing industrial plant. For this reason, the following sections show both the recommended architecture and a practical real-world example of how we are enhancing the security of real use case in brownfield water plants.

### 4.1. Recommended EcoStruxure Plant Architecture

First, we present the recommended EcoStruxure Architecture, and then how this solution adapts the legacy architecture to fit the recommended architecture. The recommended architecture is the preferred choice for greenfield projects where we have the freedom to define the architecture from the very beginning.

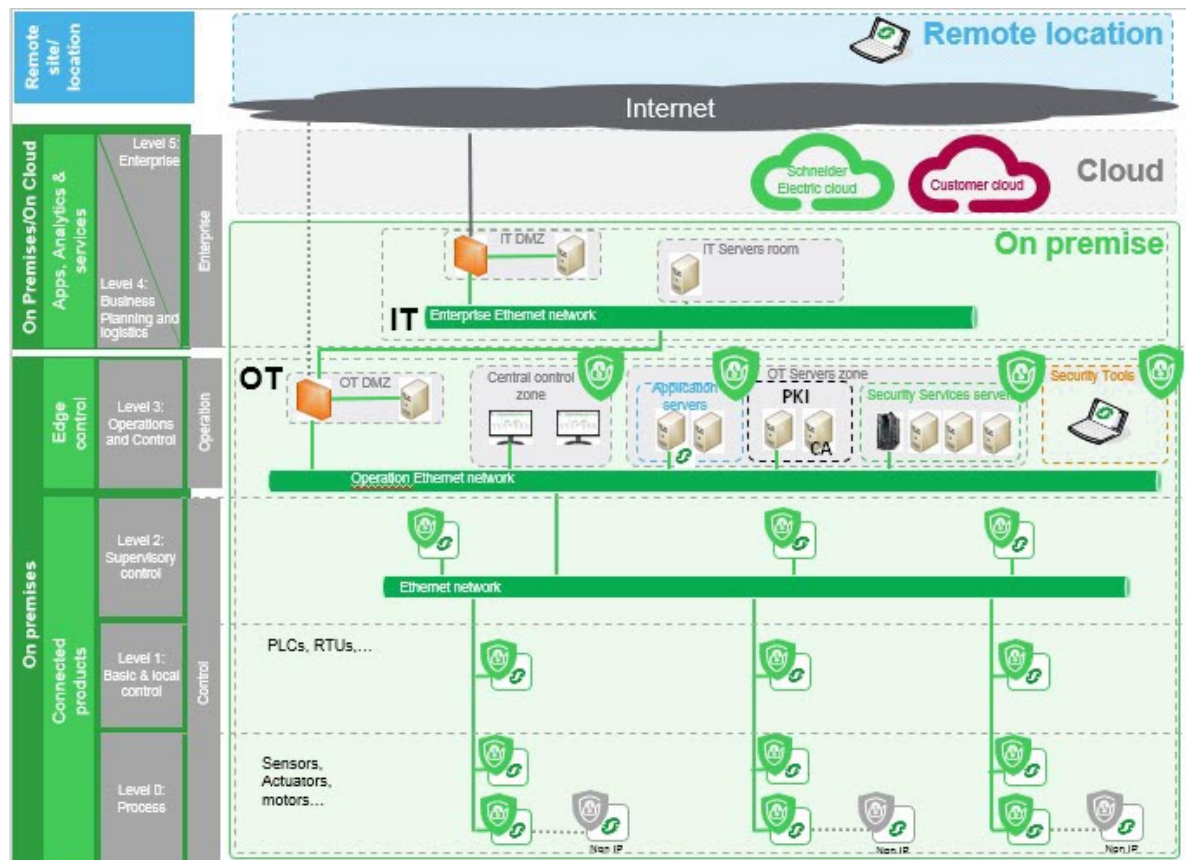


Figure 5: Recommended EcoStruxure plant Security Enhanced Architecture

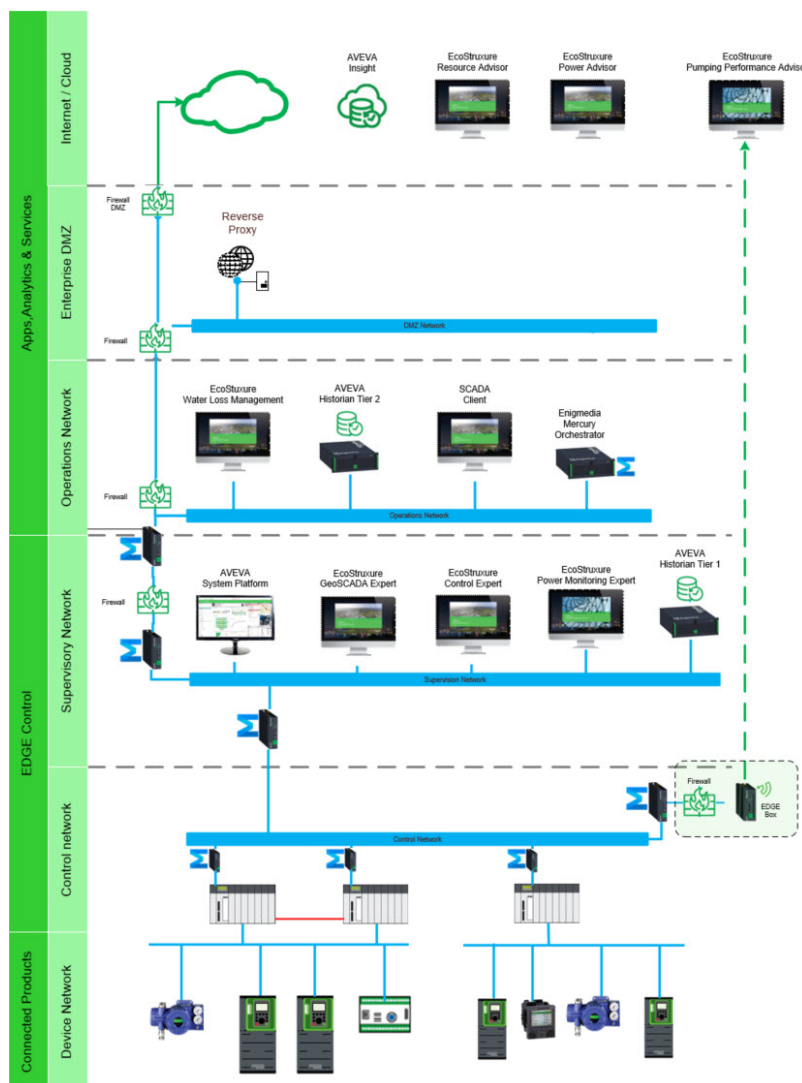
In the recommended architecture, you will find the recommended practices defined by IEC 62443, for example the use of an IDMZ, the definition of separate and distinct conduits, and segregation by secure zones. In the next section, we describe how our solution implements several of these recommended practices with minimal impact on the existing network infrastructure and legacy asset base.



## 4.2. How we adapt the recommended architecture in brownfield plants

When dealing with brownfield plants, we need to adapt the security recommendations to the existing network infrastructure and the legacy install asset base. This means that in most of the cases we need to implement enhanced security but with a minimum impact in the current OT assets.

The proposal defined here with EnigmaMedia and Schneider Electric Harmony Edge Box is the most suitable solution in this context. Figure 6 presents a high-level view of security enhanced network connectivity in the edge control layer between the Supervisory Network and Control Network, between SCADA and PLCs. This architecture adds a Harmony Edge Box with Mercury Cipher between both networks, helping to secure traffic between them. Additionally, this architecture shows a Harmony Edge Box connected to another Harmony Edge Box with Mercury Cipher to connect to advisors, for instance EcoStruxure Pumping Advisor. To further enhance security at the device level, a Harmony Edge Box with Mercury Cipher is necessary for each device.

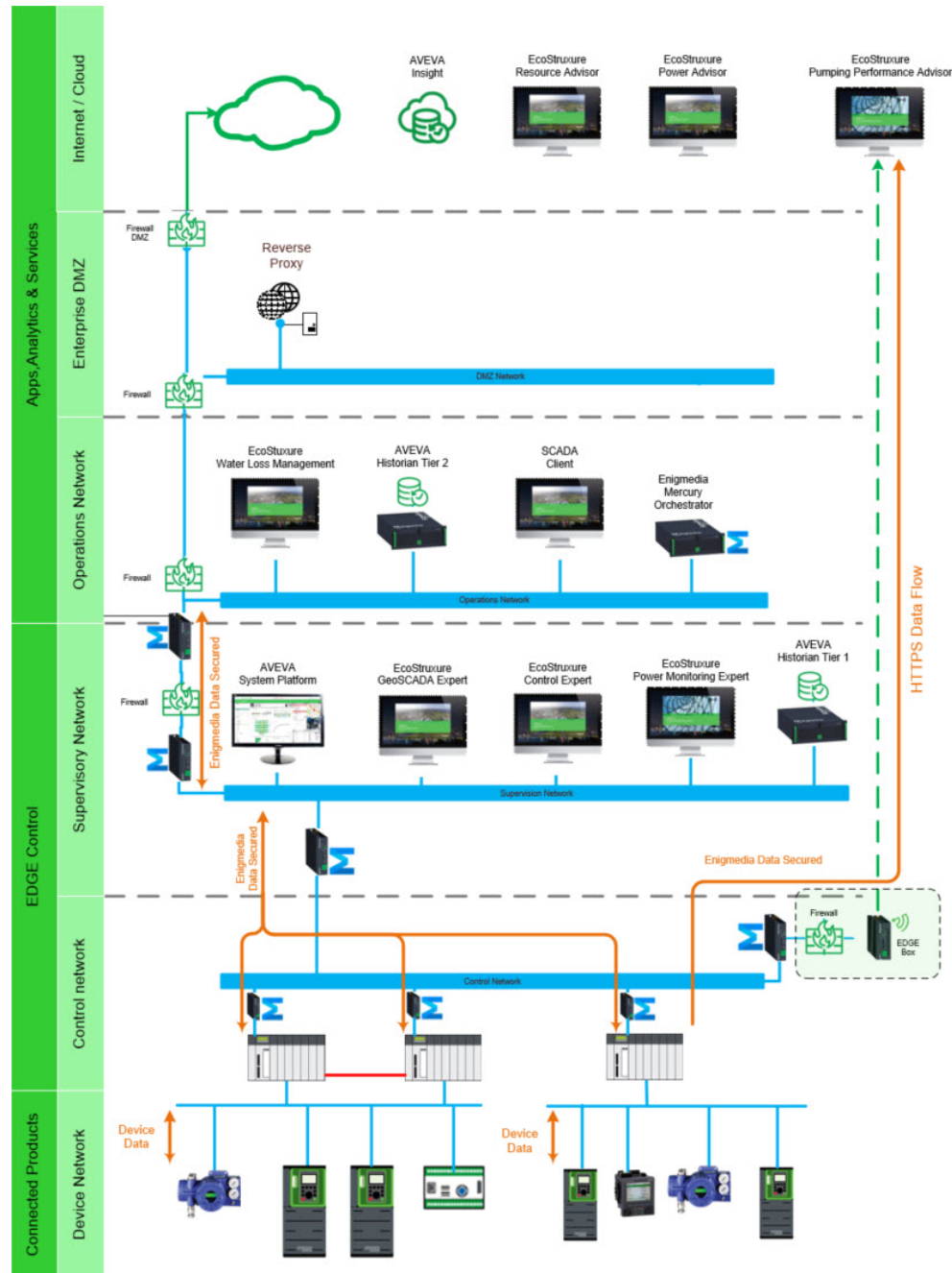


**Figure 6 - Securing between Supervisory Network and Control Network at Device Level**



### 4.3. Helping Secure the Architecture Dataflow

The following drawing shows the main dataflows used in the solution.



**Figure 7: Example of data flow drawing**

Data mainly flows between the control network and Supervisory Network, except for devices connected directly to advisors like EcoStruxure Pumping Advisor as shown.

### 4.3.1. Encryption

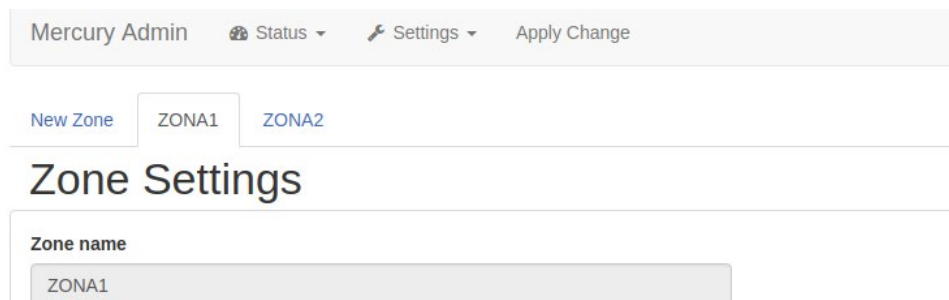
Ciphers are deployed in each location to increase the cybersecurity level of the infrastructure. These ciphers encrypt communications by means of RSA-4096 bit certificates, key sessions established via Ephemeral Diffie-Hellman, low latency symmetric encryption and SHA-3 hash-function with timestamping in order to enhance data-integrity.

These enhanced security mechanisms are transparent to the end-user and the system integrator. No specific configuration is required.

Thanks to the encryption, malicious attackers are not allowed to gather information about the plant or malformed data packages to stop the production. This design mitigates risks and helps prevent and mitigate external and advanced threats.

### 4.3.2. Segmentation and Zone Definition

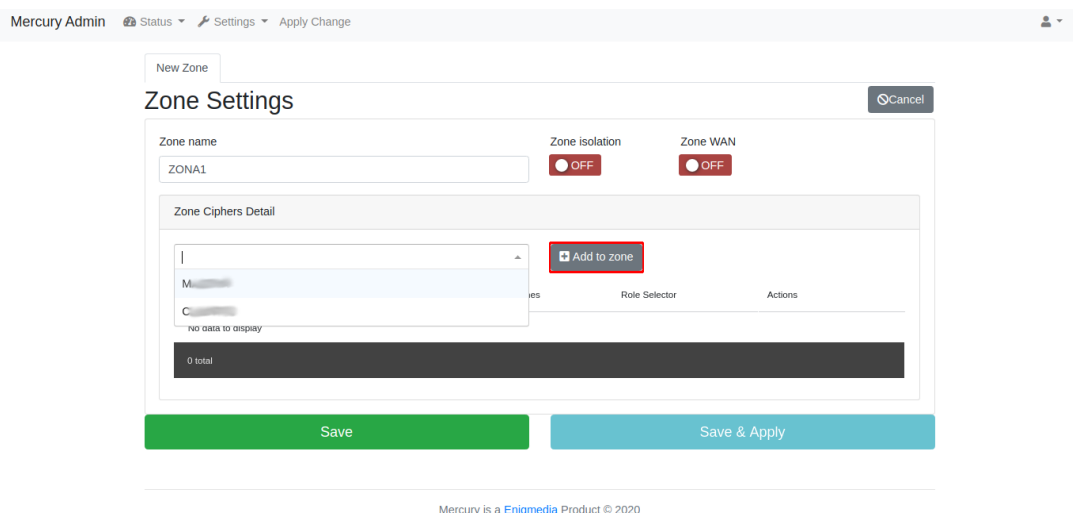
In the Orchestrator's Mercury Admin menu, you can create a new zone by clicking in the New Zone tab.



The screenshot shows the Mercury Admin interface. At the top, there's a navigation bar with 'Mercury Admin', 'Status', 'Settings', and 'Apply Change'. Below this, there are tabs for 'New Zone', 'ZONA1', and 'ZONA2'. The 'New Zone' tab is active, and the page title is 'Zone Settings'. A form for 'Zone name' is visible, with 'ZONA1' entered in the input field.

**Figure 8: Creating new zones**

Owing to the dashboard it is simple to assign each cipher pair to a zone, as shown in Figure 9. Assign ciphers to each zone. Mercury also supports WAN zones and zone isolation, depending on customer requirements.



This screenshot shows the 'Zone Settings' page with the 'New Zone' tab selected. The 'Zone name' is 'ZONA1'. There are toggle switches for 'Zone isolation' and 'Zone WAN', both currently set to 'OFF'. The 'Zone Ciphers Detail' section features a search bar, a list of ciphers (currently empty), and an 'Add to zone' button. At the bottom, there are 'Save' and 'Save & Apply' buttons. A footer note states 'Mercury is a Enigmmedia Product © 2020'.

**Figure 9: Assigning new ciphers to a zone**

After defining zones, we can set the firewall rules by assigning network services per zone and cipher. These steps are performed in the Firewall Settings menu, as shown in Figure 10

## Firewall Settings

Select zone

ZONA1

Ciphers Firewall Configurations

Specify Services

Cipher	Open ports	Test mode	Firewall status
M	<ul style="list-style-type: none"><li>Modbus Modbus_tcp 502 TCP</li><li>NTP NTP_udp 123 UDP</li><li>HTTPS HTTPS_tcp 443 TCP</li></ul>	<input type="radio"/> OFF	<input type="radio"/> OFF
C	<ul style="list-style-type: none"><li>HTTPS HTTPS_tcp 443 TCP</li><li>Modbus Modbus_tcp 502 TCP</li></ul>	<input type="radio"/> OFF	<input type="radio"/> OFF

**Figure 10: Firewall Settings status window**

Mercury Firewall is a stateful firewall, and as a result we can create new network services if required through the **Settings > NetService Settings** tab and configure the network services features as shown in Figure 11.

Name

TELNET

Net Services Rules List

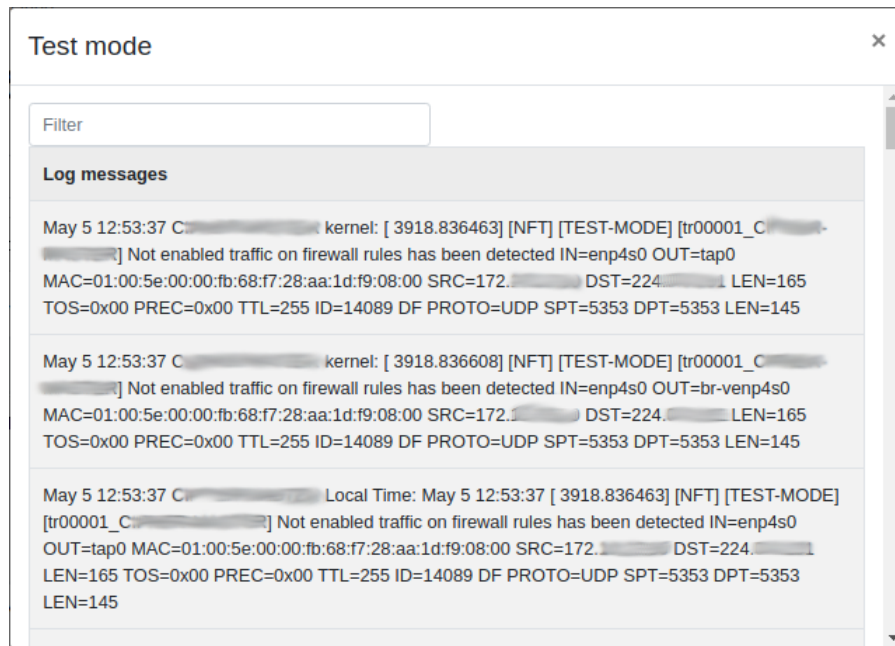
TELNET

Rule Name  Temporal Rule ☐ OFF

Init port  End port  Transport type

**Figure 11: Net Services definition Example**

Mercury Firewall also has a TEST MODE. In this mode, the firewall status is OFF, but Mercury automatically generates a log of those events not supported by the firewall rules. As a result, system integrators and end-users can verify that the firewall setting are properly set. An example is shown in Figure 12:



**Figure 12: Example of Test Mode log result**

Segmentation and Firewalling help prevent the spread of malware through the zones and reduce the likelihood that unauthorized users can access devices in the infrastructure, thereby reducing risks and helping to prevent cyberattacks.

### 4.3.3. Monitorization

Mercury implements IDS features and detects attacks such as port-scanning, DoS or failed login attempts, unauthorized communication trials, and so forth. Logs are centralized in the Mercury Orchestrator. It is possible to configure the Orchestrator to send logs to a remote server by properly filling the Remote Log form in the panel as shown in Figure 13.

Monitorization is a building-block for cybersecurity maintenance and forensics, solving potential conflicts when operations are interrupted.

Remote Log Settings + Add Remote Log

Address\*

Port\*

Protocol\*

Security\*

Authentication\*

**Save & Apply**

Mercury is a Enigmedia Product © 2020

**Figure 13: Configuration form to send logs to third parties via Orchestrator**

## 4.4. Architecture Components Description

The cybersecurity requirements include segmentation, firewalling, encryption and network monitorization. Configuration is done remotely thanks to a centralized dashboard management tool, accessible from IT or out-of-band port.

The objective of this section is to provide more information on the key components of this security enhanced solution and to highlight their role in helping to protect the plant.

### 4.4.1. Connected Products

#### *Sensors, Harmony Hub, Energy Meters*

These products include:

- Any connected product acting as end point equipment providing data to the cloud for app and analytics.
- Any connected product acting as intermediate equipment to collect data to the cloud for app and analytics.

[More info.](#)

#### 4.4.2. Edge control

##### *Harmony Edge Box from Schneider Electric*

The Harmony Edge Box is employed by this solution as the preferred security enhanced hardware container for embedding the Mercury Cipher from Enigmedia. Thanks to its embedded trusted platform module (TPM), the Harmony Edge Box supports the encryption features needed to manage the secret keys. This is mandatory to provide enhanced security for authentication and encryption, and to help secure communications in the OT plant. The Harmony Edge Box is plugged in at the top of your current application, so there is no need to stop or modify your control application.



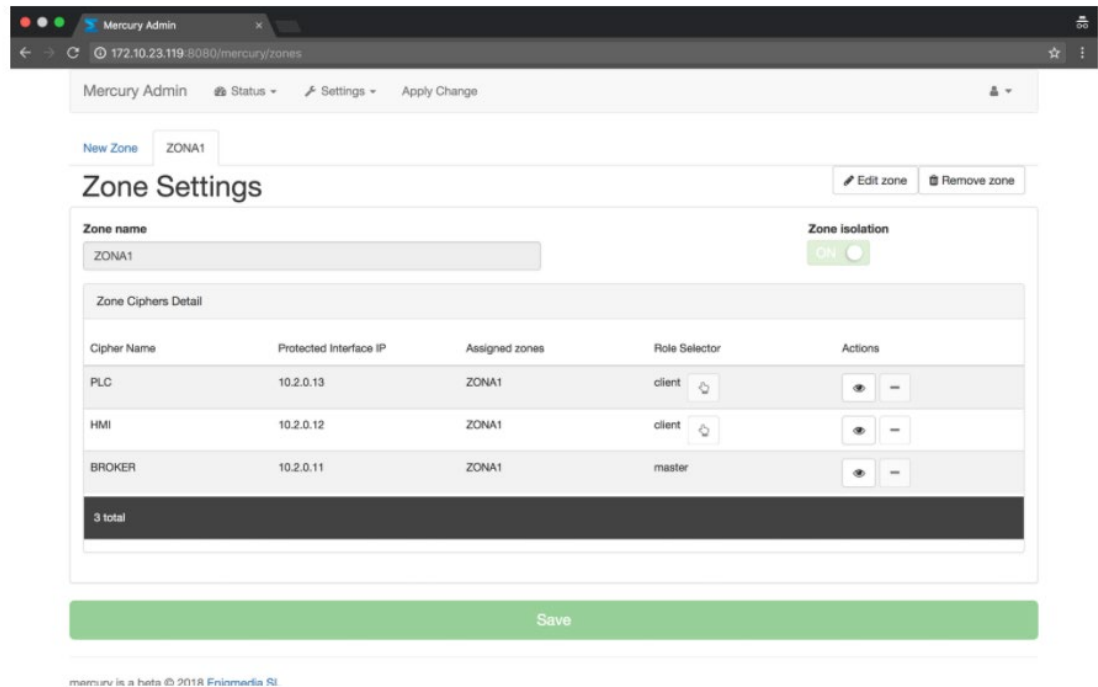
**Figure 14: Harmony Edge Box**

The versatile industrial design capitalizes on multiple hardware and software combinations to address both industrial PC and IIoT wiring needs.

[More info.](#)

##### *Mercury Cipher from Enigmedia*

Mercury is a software-based suite of native ICS cybersecurity products, which is truly hardware-agnostic. Mercury products can be deployed using customer preferred appliances. For full functionality and interoperability, we recommend modern Intel or ARM architectures with Linux-based platforms. If you have a different use case, our engineers can customize our products and adapt them to your specific needs. Deployment of Mercury cybersecurity products is easy and fast. You don't need to change any existing configuration or IP address. Mercury products are transparent to the existing ICS network. Our ICS Encryption is unique and can encrypt and help protect your data and traffic at Layer 2, adding negligible latency to the existing industrial process and with no impact to the communications from PLCs to SCADA.



**Figure 15: Mercury software suite**

Depending on the use case and the cybersecurity challenge, Mercury is deployed in the OT network in different strategic locations: connected to a mirroring port for enhanced security data collection; deployed to connect remote sites through authenticated and encrypted channels; or deployed inline to create enhanced security zones and define firewalls in conformity with IEC-62443.

[More info.](#)

### 4.4.3. Apps and Analytics

This solution is compatible with Schneider Digital advisors with security enhanced connection from the cloud to the IOT gateway and with AVEVA Insight.

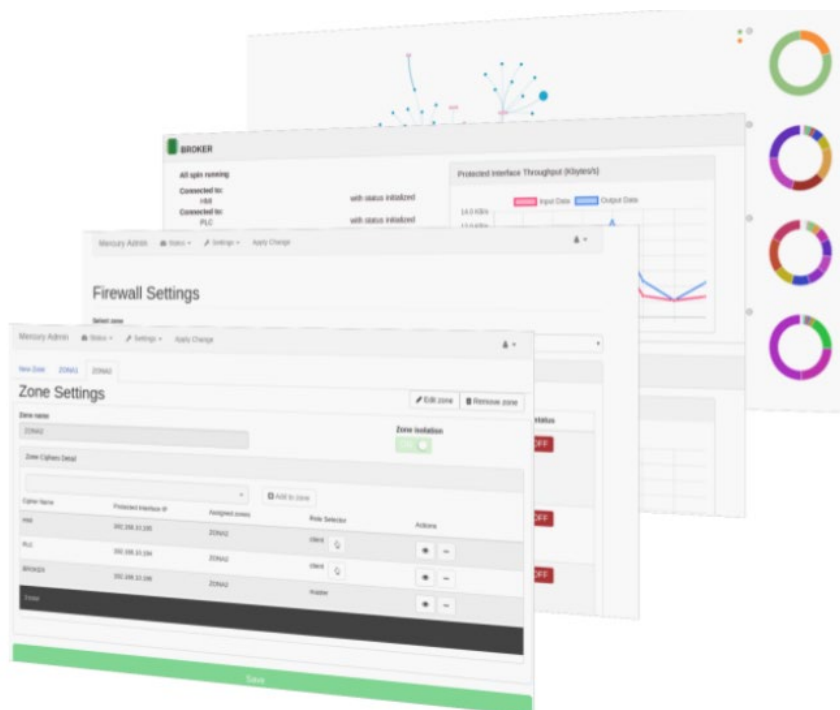
#### *Mercury Orchestrator software*

Mercury Orchestrator offers a simple and intuitive panel to configure and manage the Mercury features. It can be deployed on-premise, or cloud.

Mercury is configured, managed, and monitored, from Mercury Orchestrator. Thanks to its centralized console, authorized users can remotely configure temporary ports and firmware settings, send copies of the traffic to SIEM/SOC, or check operational status. Updates can be performed remotely with enhanced security. The preferred location is in the edge layer on-premises, but

optionally can be located in the cloud. It can be hosted in any Harmony Edge Box having an embedded TPM.

[More info.](#)



**Figure 16: Dashboard example Mercury Orchestrator**



## 5. Solution Use Case Examples

New threats and regulations require advanced security features not supported in legacy architectures. Additionally, implementing cybersecurity may require changes that impact production and lead to unplanned downtimes. Usually, system integrators only have a limited time window for deploying new solutions and this can be challenging given the general complexity of cybersecurity products. Potential challenges can arise when deploying and configuring a solution, thereby affecting functioning of the network.

In the following use cases, the customer desires to increase the cybersecurity level of the architecture and demands that it be done without modifying any existing infrastructure configuration. Adding to the challenge, deployment time is limited to only a few hours.

The cybersecurity requirements include segmentation, firewalling, encryption and network monitorization. Configuration is performed remotely thanks to a centralized dashboard management tool, accessible from IT or out-of-band port.

As a result, the customer has increased its cybersecurity level and mitigated potential cyber risks with minimum impact to its architecture. including charts, dashboards, newsfeeds, and alerts. The cloud-based approach saves you the cost of investing in additional hardware servers and software.

The next two sections describe how to approach, and possible solutions for, applying cybersecurity to both an existing water plant and an existing wastewater treatment plant.

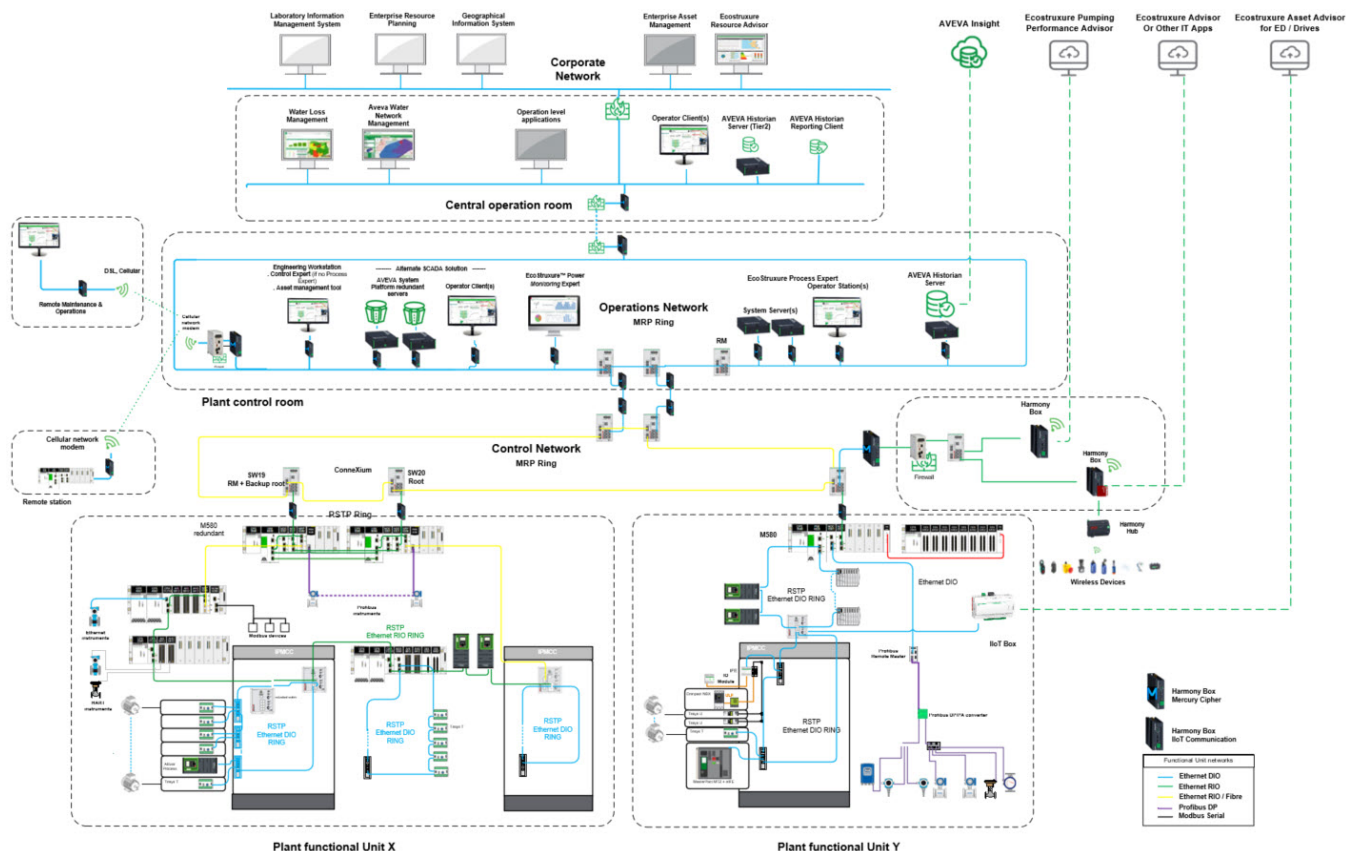
### 5.1. Helping to Secure a Water Plant

The existing architecture consists of a flat network with unencrypted communications between the control room, the field network, and the cloud for secondary sensing solutions. Potential threats could result in a facility shut-down with a negative impact in the business operation.

The customer needs to encrypt the communication among sites, providing integrity, privacy and confidentiality by means of advanced cryptography mechanisms.

Furthermore, insiders or third parties can access the network infrastructure from any of the sites of the facility. Segmentation and firewalling can be introduced to minimize potential mistakes or misuses.

Finally, the customer requires that the solution provide detection and monitorization capabilities.



**Figure 17 – Security Enhanced Water Plant Example**

#### Use case architecture description:

This architecture presents a two-ring network setup: one ring for supervision, and the other for Control Network. In the supervision network, we find examples of AVEVA System Platform and AVEVA Plant SCADA, with AVEVA Historian and operator workstation.

Adding two Harmony Edge Box with Mercury Cipher installations in front of each functional unit allows the creation of one security enhanced zone per functional unit. In addition, we can segregate these units and define whether they can communicate with each other. In addition, a security enhanced channel is transparently created for communication between the functional units and the automation assets. This channel carries encrypted and signed communications between the ciphers. The latency added for this communication is less than 2 ms.

By adding another couple of ciphers for the control room, we thereby create another secure enhanced zone for the control room and help secure the communication between the control room and the functional units.

This solution applies the following security functions:

1. **Remote Connectivity:** It shows how to connect securely for a remote Operator Maintenance Workstation or a remote plant PLC.
2. **EcoStruxure Pumping performance Advisor Connectivity:** Between the Harmony Edge Box with Mercury Cipher connected to EcoStruxure Pumping Advisor and the Control Network there is a Firewall and Harmony Box with Mercury Cipher that provides enhanced security for and encrypts the connection to PLCs.
3. **Network Monitoring and Segmentation:** The four Harmony Edge Boxes with Mercury Cipher situated between the two rings are used for traceability and monitoring the traffic between the two networks. Harmony Edge Boxes with Mercury Cipher already provide network segmentation by firewalling between the two ring networks.
4. **Encryption point to point:** The Harmony Edge Boxes with Mercury Cipher connected beside SCADAs and PLCs are used to encrypt and help protect access between the different systems: SCADA to PLC, PLC to PLC. Connectivity between SCADAs and PLC is through a ring network.

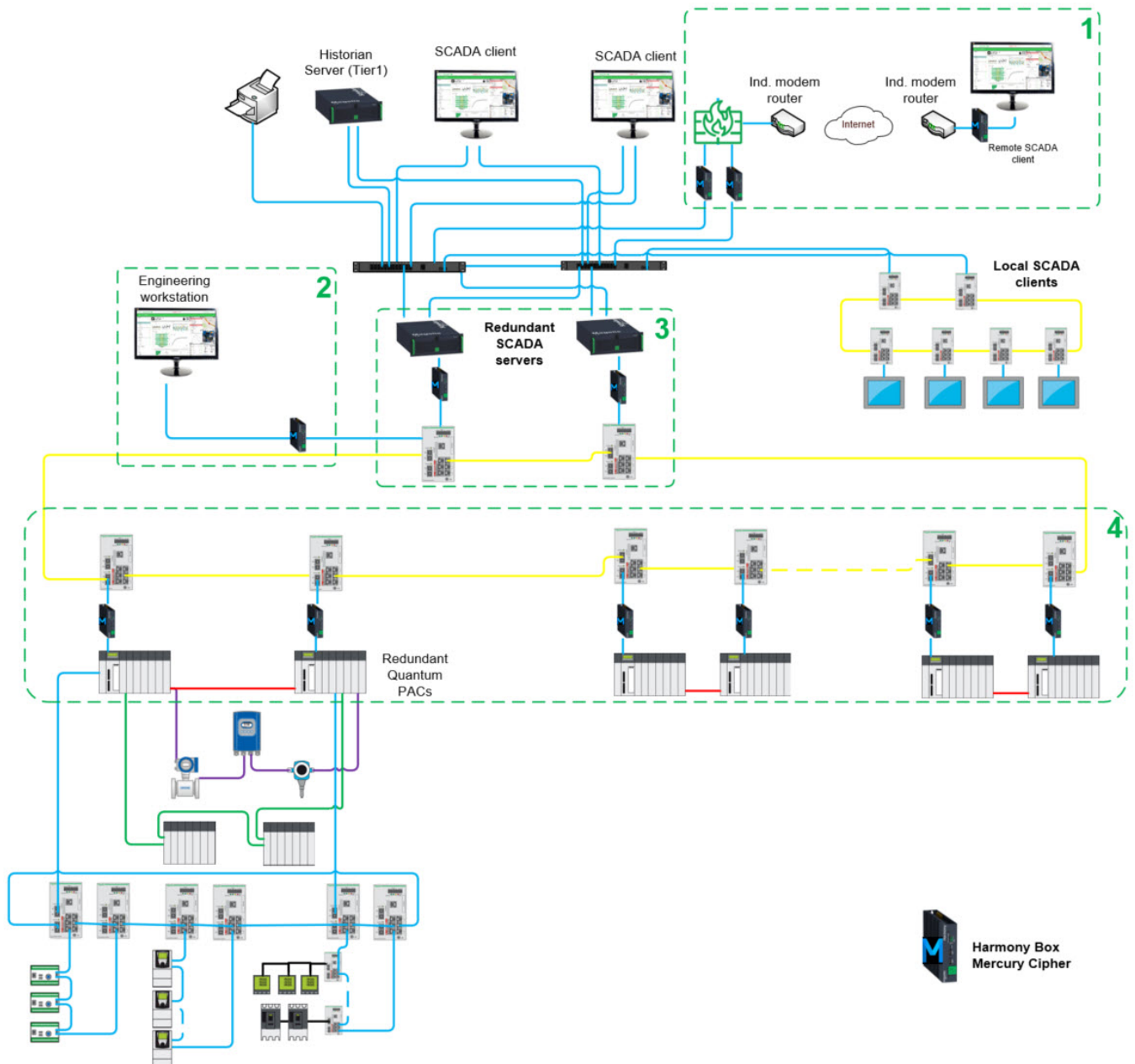
In this architecture example the following products are used:

- **SCADA:** Redundant SCADA servers (AVEVA Plant SCADA) / AVEVA System Platform
- **Historian:** AVEVA Historian
- **Control:** Modicon PLCs (Modbus TCP Protocol)
- **Supervisory Network:** Ring Network
- **Control Network:** Ring Network
- **Security:** Harmony Edge Box with Mercury Cipher.

## 5.2. Wastewater Treatment Plant Enhanced Protection

This example is based in a WWTP with Redundant SCADAs and PLCs in a ring. This example shows how to help protect the network between the SCADAs and remote access to the PLCs. Enhanced protection is provided at PLC level.

The selected use case architecture is described below.



**Figure 18 – Redundant SCADA and one ring architecture**

Use case architecture description:

This architecture includes a couple redundant SCADA servers (AVEVA Plant SCADA), Redundant PLCs and Ethernet Remote IO. At device level, Profibus DP and Modbus TCP are used. There is also an engineering workstation to program PLCs.

Connectivity between SCADAs and PLC is through a ring network. To help secure connectivity between SCADAs, the engineering workstation, and PLCs, Harmony Edge Boxes with Mercury Cipher are placed before the fiber optic switches that manage the ring network.

The following uses cases are considered:

1. **Remote Connectivity:** The design shows how to create a security enhanced connection to a remote SCADA client through Internet connection. A Harmony Edge Box with Mercury Cipher is installed at the SCADA client remote site along with two Harmony Edge Boxes, due to the redundant network, placed behind the firewalls at the plant.
2. **Helping to secure engineering workstation to PLC:** This is accomplished placing a Harmony Edge Box with Mercury Cipher between the Engineering workstation and PLCs.
3. **End-to-End security enhanced communications:** The Harmony Edge Box with Mercury Ciphers help protect communications between redundant SCADAs and redundant PLCs. They are used to encrypt and help protect access between the different peers.
4. **Helping to Protect PLCs:** A Harmony Edge Box with Mercury Cipher is used to help protect each PLC.

In this architecture example the following products are used:

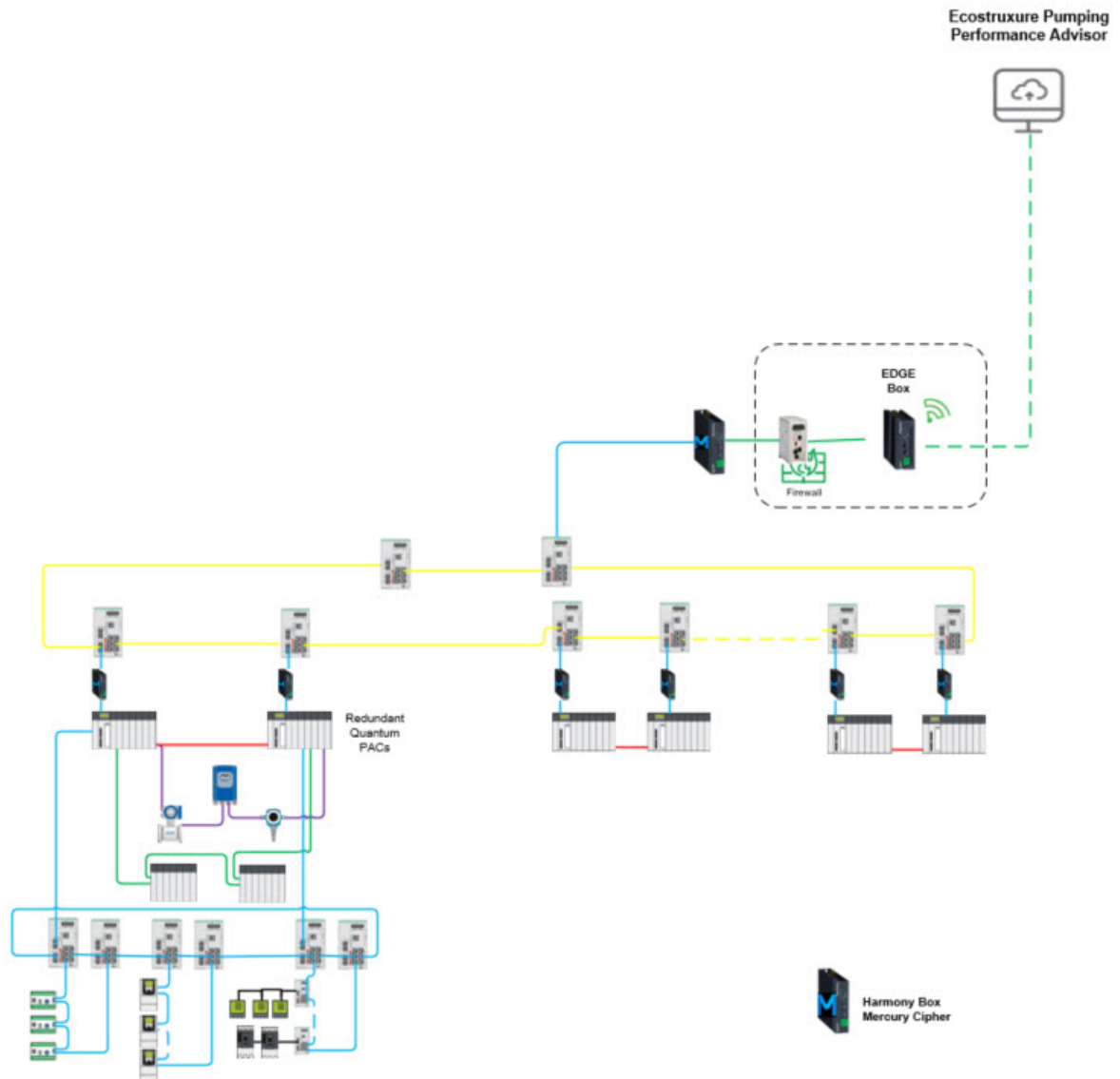
- **SCADA:** Redundant SCADA servers (AVEVA Plant SCADA).
- **Control:** Quantum HSBY + ERIOs + Profibus DP + Devices on Modbus TCP.
- **Supervisory Network:** Each server and client are connected to both managed switches.
- **Local SCADA HMI** are linked to the Supervisory Network with ring topology.
- **Control Network:** Ethernet ring network between SCADA servers and controllers.
- **Device networks:** Ethernet ring network for iPMCCs (power and motor control), and Profibus network for smart instrumentation (dual Profibus master).
- **Security:** Harmony Edge Box with Enigmedia.

### 5.2.1. Connecting an Advisor - EcoStruxure Pumping Performance Advisor example

In this architecture it's shown how to connect EcoStruxure Pumping Performance Advisor to a Control Network with enhanced security that has Harmony Edge Boxes with Mercury Cipher. Control Network is in a ring configuration.

A Harmony Edge Box with Mercury Cipher helps protect each PLC.

The selected use case architecture is described below.



**Figure 19 - EPPA use case architecture**

Use case architecture description:

This architecture is useful for connecting the EcoStruxure Pumping Performance Advisor with the Control Network for which enhanced protection has already been provided. If the advisor is connected directly in the ring network, it would not be able to connect with the PLCs because a Harmony Edge Box with Mercury Cipher is already used to help protect them.

In this architecture example the following products are used:

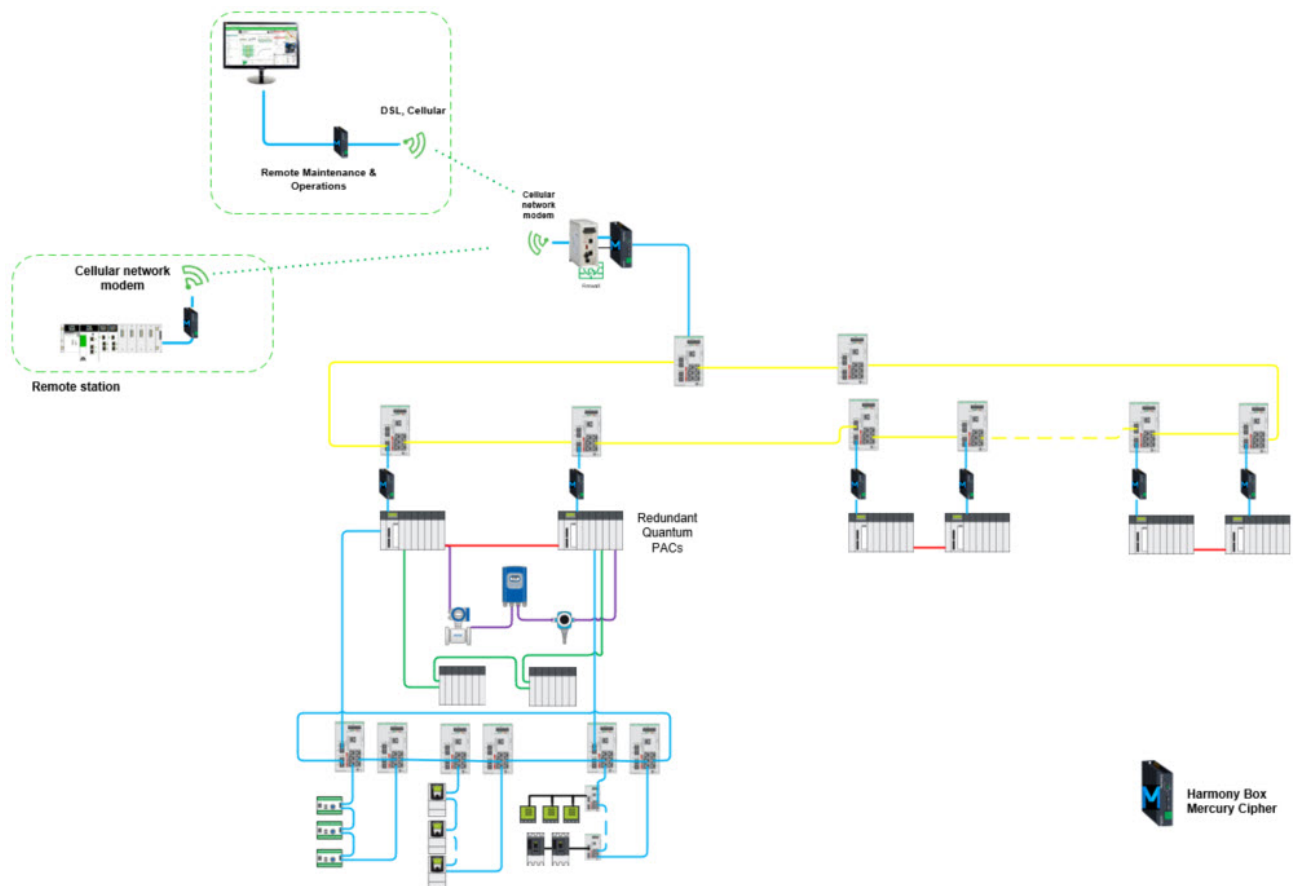
- **Control:** Redundant Quantum PLCs and non-redundant Quantum PLC.
- **Control Network:** Fiber Optics two rings network between controllers.
- **Security:** Harmony Edge Box with Mercury Cipher.

### 5.2.2. How to connect for Remote Operation & Maintenance

This architecture shows how to connect EcoStruxure Pumping Performance Advisor to the Control Network with enhanced security that has Harmony Edge Boxes with Mercury Cipher. Control Network is in a ring configuration.

A Harmony Edge Box with Mercury Cipher helps protect each PLC.

The selected use case architecture is described below.



**Figure 20 – Remote Maintenance & Operation**

Use case architecture description:

This architecture is used to provide a security enhanced connection to the EcoStruxure Control Expert through Harmony Edge Boxes. This would allow to connect remotely to PLCs for the



purpose of remotely monitoring and maintaining PLC programs in a security enhanced environment.

In this architecture example the following products are used:

- **Remote Maintenance:** EcoStruxure Control Expert to maintain automation layer.
- **Control:** Automation layer based in redundant Quantum PLCs and not redundant Quantum PLC.
- **Control Network:** Fiber Optics two rings network between controllers.
- **Security:** Harmony Edge Box with Mercury Cipher.

### 5.3. Large pumping Station Protection

This example is based on a large pumping station configuration.

This architecture shows how to help secure a redundant network ring setup. There are two network rings and redundant SCADAs.

This design offers enhanced protection between the SCADAs and PLCs while PLCs can continue communicating between them.

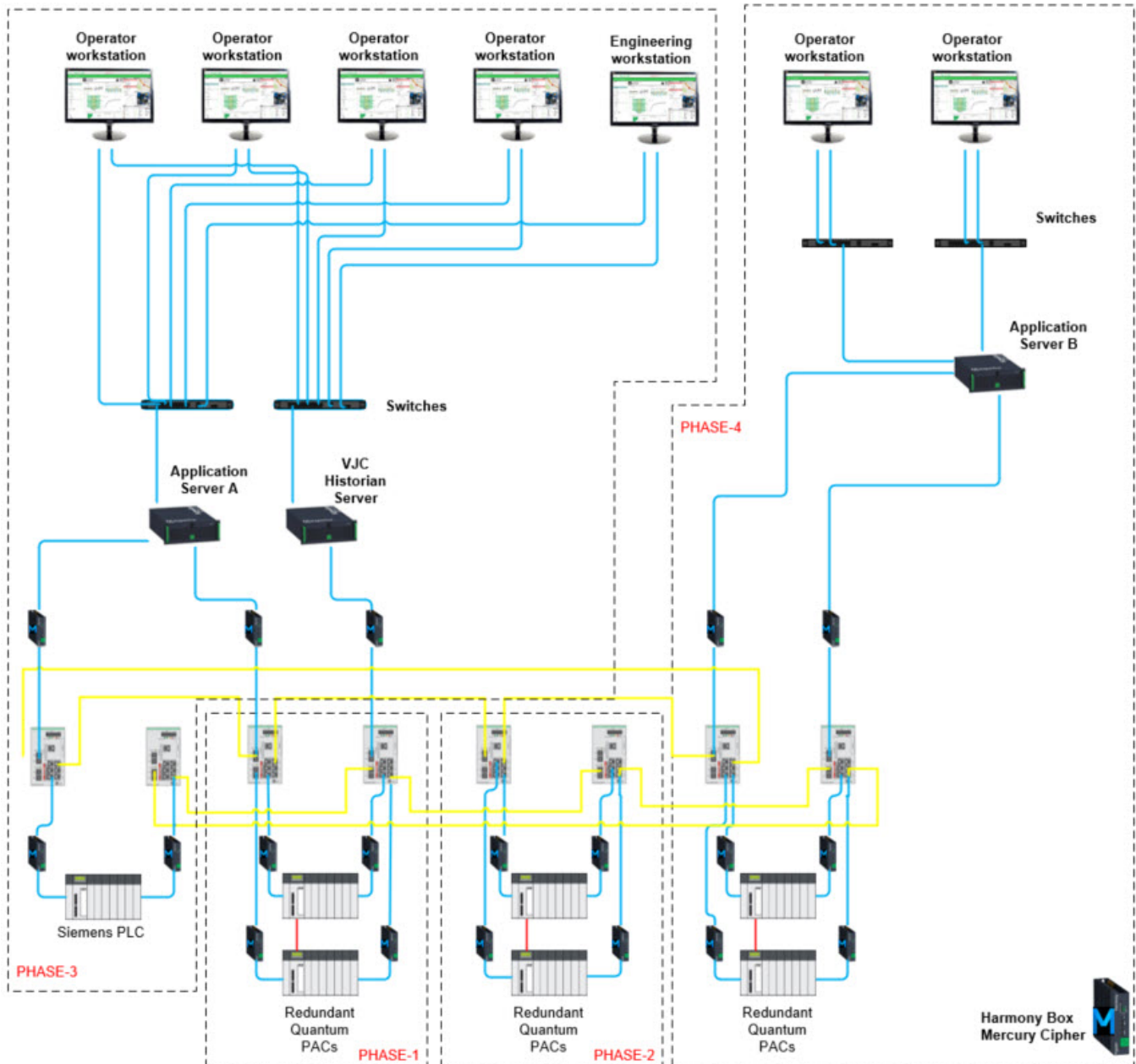
This use case presents a security enhanced, robust and easy to deploy solution that enables remote connection via WiFi/GSM/2G/3G/LTE, compatible with interfaces, devices, and protocols and is directly applicable to any infrastructure without replacing devices or changing configurations.

Mercury software embedded in the Harmony Edge Box provides a TPM, firewall features and enforces authentication and encryption in the channel. It also includes several features for helping to prevent DoS attacks and send alerts to the SIEM if it detects any suspicious behavior in the network. Different roles are supported in order to avoid privilege escalation.

The system is deployed in minutes in the field and configured, managed, and monitored by a centrally located Mercury Orchestrator dashboard.



The selected use case architecture is described below.



**Figure 21: Pumping Station use case architecture**

**Use case architecture description:**

This architecture is useful to help protect connectivity between Supervisory Network and PLCs.

If anyone plugs directly in the ring network, it will not be possible to connect the PLCs.

This architecture is based in a couple of SCADA servers (AVEVA Plant SCADA), and Redundant Quantum PLCs. There is also a 3rd party PLC (Siemens).

Connectivity between SCADAs and PLCs is provided by a ring network. To help secure connectivity between SCADAs and Engineering Workstation and PLCs a Harmony Edge Box with Mercury Cipher with Enigmedia are installed before the fiber optic switches that manage

the ring network and another Harmony Edge Box with Mercury Cipher for each network interface in PLC.

Mercury implements advanced cryptographical mechanisms to provide privacy, confidentiality and integrity of the data in-motion. These capabilities are deployed in a transparent way for the end-user and system integrator.

Managing certificates is a friction point between IT and OT. IT managers require the use of certificates and password policies. However, this design involves the adoption of tedious cybersecurity procedures as this design requires several communications between IT/OT personnel and configuration for each field device.

Mercury solves this challenge by making the key management totally transparent to the integrator and enforcing cybersecurity standards.

Mercury helps prevent vulnerabilities by armoring the network. This product is designed for ICS/OT environment and ciphers the industrial protocols even those in Layer 2, adding less than 1 ms. latency.

Mercury encrypts the traffic that passes through its appliances and distributes the information to validated endpoints. Because of this, the solution provides extensive vulnerability masking, limiting the available attack surface. The end-point devices simply ignore other unknown or unapproved access attempts.

**In this architecture example the following products are used:**

- **SCADA:** Two AVEVA Plant SCADA servers.
- **Historian:** AVEVA Historian Servers.
- **Control:** Redundant Quantum PLCs and a 3rd party PLC (Siemens).
- **Supervisory Network:** Each server and client are connected to both managed switches.
- **Control Network:** Fiber Optics two rings network between controllers.
- **Security:** Harmony Edge Boxes with Mercury Cipher.

## 5.4. Summary of generic uses and segments

This solution delivers the primary user expectations for brownfield plants. The key use cases per segment and the customer challenge they resolve are set forth below:

Segment	Function	Use case	Challenge Resolved
WWW	Inventory	Pre-configured HW that enables plug play inventory	Out-date architecture documentation
Automotive	Segmentation	Segregate IT/OT with no-downtime	Avoid cybercrime and causal or coincidental violations
WWW	Remote Connection	Connecting remote sites/plants with control room	Malware can be spread among different plants and the control center
Automotive	Remote Connection	Connecting machinery with data analytics server	Conflicts on security and network security policies when gathering data
WWW	Full	Helping to protect IoT sensors in an unsecure network	Use third-party sensor in an unsecure plant with security requirements
Utility Grid	Full	Segregating and hardening functional units	Avoid cybercrime and causal or coincidental violations. Auditability



## 6. Appendix

### 6.1. Glossary

The following table describes the acronyms and defines the specific terms used in this document.

Acronyms & items	Substation Automation Solutions main components and definitions
APT	Advanced Persistent Threat
Brownfield	A location that needs the development and deployment of new software systems in the immediate presence of existing legacy software systems.
CA	(certification authority) An entity that issues digital certificates.
CA Certificate	A certificate that is issued by a CA (Certificate Authority) to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy
CERT	Computer Emergency Response Team
Certificate	An electronic document that uses a digital signature to bind a public key with an identity — information such as the name of a person or an organization, their address, etc. The certificate can be used to verify that a public key belongs to an individual
Control Network	The portion of the control system network where process data is transferred. It includes SCADA-to-PAC traffic and PAC-to-PAC traffic
DMS	Distribution Management System
DMZ	De-Militarized Zone
Cosi	System User Interface (HMI/ SCADA)
DoS	Denial of service
DPI (Deep packet inspection)	A firewall method of examining the contents of each packet in addition to header information, providing the capability to filter traffic based on packet contents
ESP	Electronic Security Perimeter
ETHERNET	Wide Area Network, Computers network, Upper network
EWS	Engineering Workstation
Field network	The portion of the control system network in which field device monitoring and control traffic are primarily transferred. It includes PAC to-I/O, PAC-to-drive, and primary-to-Hot-Standby-PAC traffic
FRTU	Feeder Remote Terminal Unit

Acronyms & items	Substation Automation Solutions main components and definitions
GATEWAY, GATEWAY COMPUTER	Gateway Computer, Terminal Equipment, Gateway to the remote-control point
HIPS	Host Intrusion Prevention System
HMI	Human Machine Interface
HVAC	Heating, Ventilation and Air-Conditioning
ICS	Industrial Control System
IDS	Intrusion Detection System
IDMZ	Industrial De-Militarized Zone
IEC 61850, IEC-60870-5-104, OPC UA,	Industrial Network protocols
IPMCC	Intelligent Power and Motor Control Center
IPS	Intrusion Prevention System
NERC	North American Electric Reliability Council
NIDS	Network Intrusion Detection System
PAC	Programmable automation controller
PKI	Public key infrastructure
PMT	Patch Management Team
RALxxxx	Cubicle Color Code
RBAC	Role Based Access Control
RTU	Remote Terminal Unit
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SSL	Secured Socket Layer
Syslog	A standard method of data collection on computers and other devices such as firewalls and switches
TLS	Transport Layer Security: network protocol, successor of SSL
TPM	Trusted Platform Module

**Table 2: glossary**

## 6.2. Reference Documents

The following table is a list of documents you might want to refer to when more details are needed.

Document Title	Reference
Schneider Electric	<i>How Can I Reduce Vulnerability to Cyber Attacks?</i>
Schneider Electric	<i>How can I Reduce Vulnerability to Cyber Attacks in Control Room V2?</i>
US Department of Commerce	<i>National Institute of Standards and Technology Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security</i>

**Table 3: Reference documents**

Life Is On



## About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

[www.schneider-electric.com](http://www.schneider-electric.com)

Schneider Electric Industries SAS  
Head Office  
35, rue Joseph Monier  
92506 Rueil-Malmaison Cedex  
FRANCE

Due to evolution of standards and equipment, characteristics indicated in texts and images in this document are binding only after confirmation by our departments.

Version 1.0 – 01 2021

©2021 Schneider Electric. All Rights Reserved. Life Is On Schneider Electric is a trademark and the property of Schneider Electric SE, its subsidiaries and affiliated companies. All other trademarks are the property of their respective owners.