How to Protect ICS legacy devices with Mercury

enigmedia

Mercury: "All-in-One" cybersecurity solution

Mercury is an "all-in-one" cybersecurity solution designed for industrial systems (ICS/OT/IoT) that provides multiple features in just one appliance:

- ❖ Assets Discovery
- ❖ Devices Protection
- ❖ Network Segmentation
- ❖ Firewall
- ❖ Conduits definition
- ❖ Encryption

Save up to 70% deploying Mercury to secure your network in conformity with IEC-62443

Protect your legacy PLC

Mercury can be used to protect legacy PLCs and data and communications from PLCs to Control Center. Legacy PLCs present software vulnerabilities that can be exploited by malicious code, either provoked by human errors or intentional attack.

The main challenges to secure legacy devices in the industrial network are:

- ❖ Impossibility to update or patch PLC firmware
- ❖ Multiplicity of devices
- ❖ Variety of protocols
- ❖ Inability to change existing IPs
- ❖ Low Latency requirements

Mercury: the perfect solution to protect your legacy PLC

Mercury Features

Mercury Box, best-in-class "Plug&Protect" appliance, overcomes these challenges in an easy, fast, and affordable way.

Mercury has been designed with industrial CIOs and CISOs, and provides unique features:

- ❖ Compatible with all legacy devices and protocols
- ❖ "Zero-touch" provisioning: do not require changing any existing configuration nor any IP
- ❖ Protects from attacks and vulnerabilities adding an advanced encrypted layer
- ❖ World's fastest and most efficient Encryption (less than 2ms. latency)

Easy and fast deployment

Deploying Mercury is as easy as plug Mercury Box directly to the interface or network switch. The next image shows a flat network where Level 0 sensors and actuators are connected to Level 1 PLC presented in Safety and Field Control zone and these devices are connected to Level 3 Supervisory workstations.
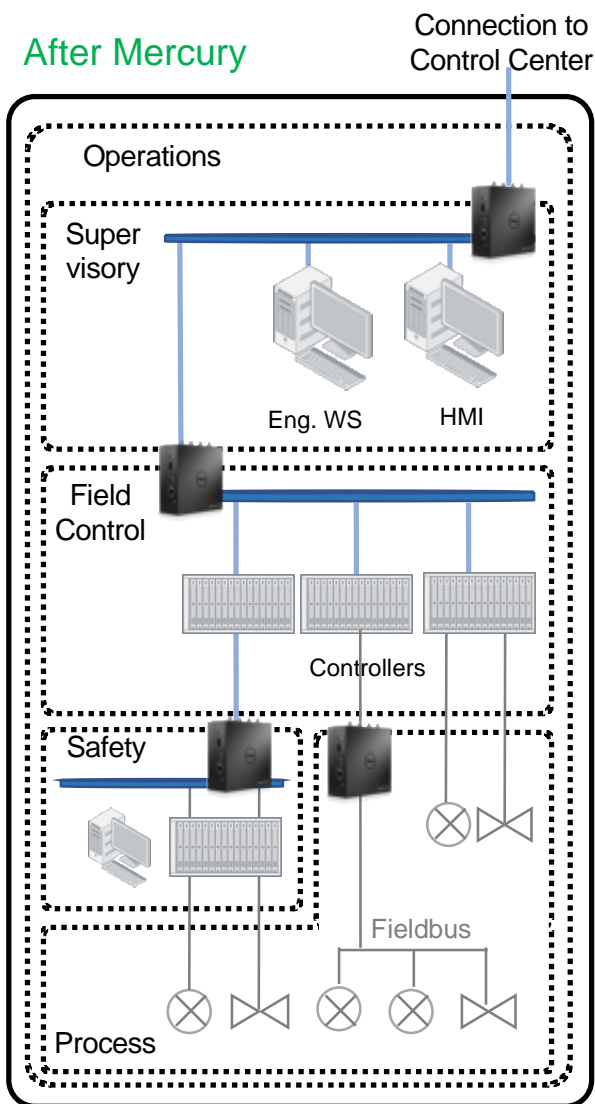
enigmedia
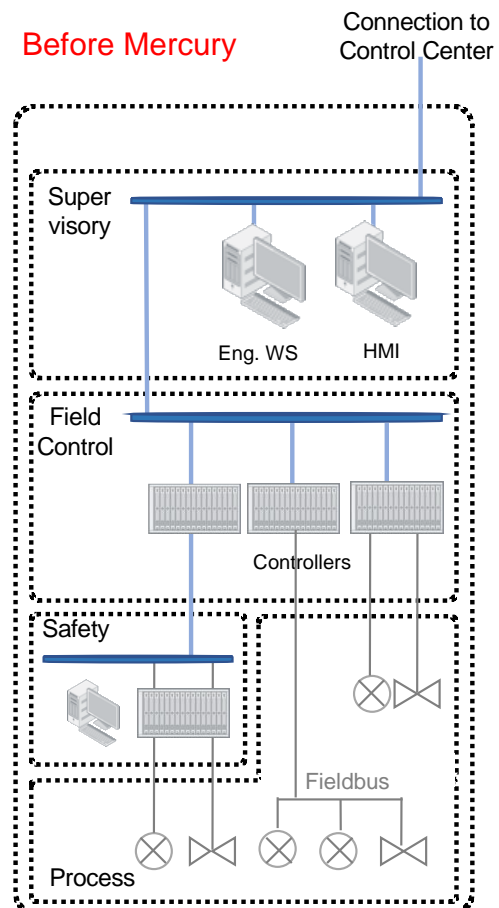
Once deployed, Mercury protects PLCs encrypting all network traffic, offering:

- ❖ Protection to legacy PLC against cyber-risks avoiding vulnerabilities exploitation
- ❖ Transparent communication without interruption from Level 0 upwards
- ❖ Prevents attacks to PLC's Ports that are not in use
- ❖ Define permissions to access to Ports in use
- ❖ Latency below 2ms. (unique compatible with industrial protocols)

After Mercury

Connection to Control Center

Operations

Supervisory

Eng. WS   HMI

Field Control

Controllers

Safety

Fieldbus

Process

Mercury Native Industrial Encryption

- ❖ World's fastest and most efficient encryption
- ❖ 20 times faster and 10 times more efficient than standards
- ❖ Less than 2ms. latency encrypting industrial protocols
- ❖ Specially designed for Industry

Mercury encryption has been reviewed by the European and American authorities and has passed the tests of laboratories such as Epoche & Espri, NIST, CSIC and ISO.

Enigmedia is registered in the directory of the DGAM as an authorized supplier of the Spanish Ministry of Defense, as well as a qualified provider of the UN.

Enigmedia is also a founding member of the ECSO (European Cybersecurity Organization) and participates as an accredited expert in the ISO International Committee.

The foundations of Chaos have been published in several specialized journals and in international conferences. Mr. Whitfield Diffie, considered the father of asymmetric cryptography, is one of the founders of this technology and is a member of the Scientific Advisory Board of Enigmedia.

Mercury, Native Cybersecurity for Industrial Systems

Enigmedia builds native cybersecurity solutions to enable digitisation towards Industry 4.0. Enigmedia delivers essential building-blocks for secure digital transformation. Enigmedia follows IEC-62443 in our product strategy. For further information and to explore all our ICS Cybersecurity portfolio, please contact us at:

contact@enigmediasecurity.com

DELL IoT Solutions Partner

ECS EUROPEAN CYBER SECURITY ORGANISATION

EDGE X FOUNDRY MEMBER

ISO