GE VERNOVA

POWER CONVERSION'S ICSARMOR

INDUSTRIAL CONTROL SYSTEM SECURITY APPLIANCE

ICSArmor is a dedicated control system security appliance that supports a defense-in-depth approach to improve the security posture of Industrial Control Systems.

Its primary purpose is to host Power Conversion business security tools, and an optional host for third party security applications.

Comprehensive OT cybersecurity platform

- Meets the seven foundational requirements of ISA/ IEC 62443
- Developed following ISA/IEC 62443-4-1 SDLC/SDLA
- Role-based access control to IEC 62351-8
- Built on CIS Benchmark or STIG compliant O/S or VM
- Assists with NIS2 & NERC CIP compliance with recovery planning, incident management and change management
- Includes User management, Syslog, Threat detection & Host intrustion for all GE Vernova HPCi based Control systems
- Resilliant deployment options available

Key Features

- Host for Power Conversions security toolchain
- Hardware-agnostic, able to be deployed on a virtual machine
- Multiple deployment architectures, including RAID 1 for data resilience and backup
- Simple setup process with optional CIS benchmark-compliant OS configuration
- Optional High Windows STIG compliance during installation
- Secure host for third party applications supporting full control system security compliance
- Patching options available
- Optional firewall to provide network segmentation
- Full service and support package available

Standard Package

Includes Power Conversion's:

- ICS Security Management Suite
- ICS SYSLOG
- ICSGuard
- Host hardening

Advanced Package

Includes:

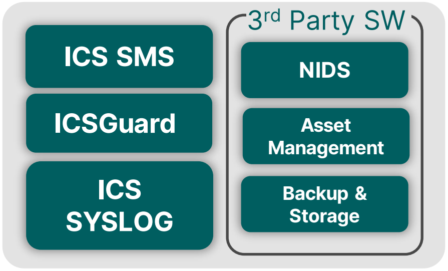
- Power Conversion's Standard Package
- Industry-Leading Third-Party Vendor Packages:
    - Network intrusion
    - Asset management
    - Backup and storage

GE VERNOVA

DEPLOYMENT OPTIONS

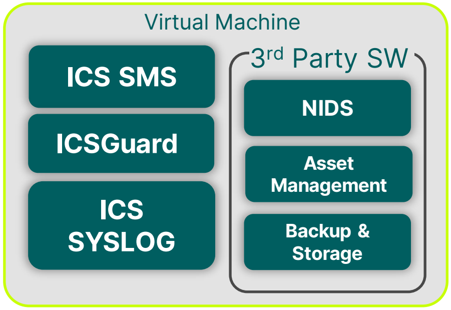
Flexible deployment to integrate seamlessly with the control system to ensure a high level of availability.

Standard Deployment


ICS SMS
ICSGuard
ICS SYSLOG
3rd Party SW
NIDS
Asset Management
Backup & Storage

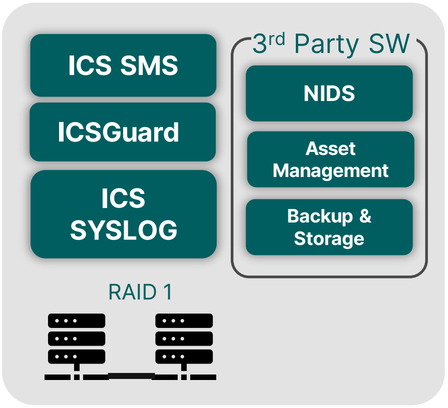
- Cost-effective solution deployed on GE Vernova hardware
- Can be supplied with Windows 10 or 11
- Host hardening out-of-the-box using CIS benchmark or STIG compliant configurations
- Patching options available
- Backup and recovery utility

Virtual Deployment


Virtual Machine
ICS SMS
ICSGuard
ICS SYSLOG
3rd Party SW
NIDS
Asset Management
Backup & Storage

- Virtual deployment on existing server or PC
- Windows server support + Win 10 & 11 ready
- Patching options available
- Backup and recovery utility

Resilient Deployment


ICS SMS
ICSGuard
ICS SYSLOG
3rd Party SW
NIDS
Asset Management
Backup & Storage
RAID 1

- Resilient deployment with RAID 1 disk mirroring providing data redundancy
- Windows 10 or 11 ready
- Host hardening out-of-the-box using CIS benchmark or High STIG compliant configurations
- Patching options available
- Backup and recovery utility

Enhanced Resilient Deployment:

- Spare solid-state disk provided in addition to the RAID 1 configuration to reduce downtime of security-critical infrastructure

GE VERNOVA

ICS SECURITY MANAGEMENT SUITE

Secure Credential Management

Power Conversion's ICS Security Management Suite (SMS) is an application that provides secure credential management for devices to meet IEC 62351-8 RBAC, IEC 62443 4-2/ 3-3 and IEC/ISO 27001.

User Management

SMS provides centralized user credential management using RADIUS and OAuth2.

User Account Management:
SMS provides a centralized method of user credential management and features:
-

- Role-based access control
- Account profile administration
- Password strength definition
- FIPS 140-2 compliant encryption algorithms
- Windows HMI credential management
- Option to integrate other applications and devices
- Two-factor authentication

MS Active Directory LDAP Proxy:

- To mitigate the risk of a comprised AD affecting the availability of the control system, SMS provides a LDAP proxy service.
- The proxy service means OT users can be configured once in the IT active directory and propagated to the OT domain.

Certificate Management

The ICS Security Management Suite provides Certificate management services for registered devices in the control system.

The SMS can utilize a customer's CA as the root, and action CRLs as required.

Authentication & Authorization

Optional M2M Trusted communications :

HPCi controllers can be enabled to utilize SMS certificates to establish secure, unencrypted control channels to ensure MitM/Replay attacks are not successful between critical systems.

M2M Trusted communications should also be enabled if the control system is operating across an untrusted network.

ICS SYSLOG

In accordance with RFC 5424

ICS SYSLOG is a centralized system security database to collect and store:

- User log-in events to control system devices
- Incorrect password or failed login attempts
- User profile creation/ updates
- Device configuration or re-configuration logs
- Device security status
- Windows event log import/ extraction (security events only)
- ICSGuard security events
- Integration with third party SIEM

GE VERNOVA

ICSGUARD

Host Intrusion Detection System

ICSGuard, is an integrated health and security monitor for a system of HPCi controllers and Windows-based workstations, equipped with machine learning capabilities.

ICSGuard will serve as a Host Intrusion Detection System (HIDS).

A component of ICSGuard, 'ICSAgent', is embedded into control system assets that continuously monitor the critical operating environment and report 'indicators of compromise' to the ICSGuard dashboard.

Key Features

Robustness and Scalability:

- Domain-agnostic HIDS for HPCi controllers and workstations
- Scalable from small to large OT networks
- Fills the gap in the detection chain providing protection on the control network

Graphical User Interface:

- Dashboard to monitor the controller and workstation status, alert history, recent alerts, and acknowledgment status
- Features a detailed display that shows alerts in real time
- Provides the ability to visualize and maintain an asset inventory of the HPCI devices and workstations deployed in the OT network

Machine Learning:

- Machine learning capabilities for detecting control system abnormalities and security breaches
- ML performance feedback mimic provides the ability to monitor the performance of the ML models

Reporting:

- Generates an executive event report summarizing all detected events in an easy-to-read format
- Intrusion reports provide details on the leading forms of attack and provides a timeline of how attacks have progressed over time including any patterns detected

Integration:

- Hosted directly on Power Conversion's ICSArmor
- Integrates directly with Power Conversion's ICS Security Management Suite for user account management
- Integrates directly with Power Conversion's ICS SYSLOG
- Integrates with a centralized SIEM solution

Compliance

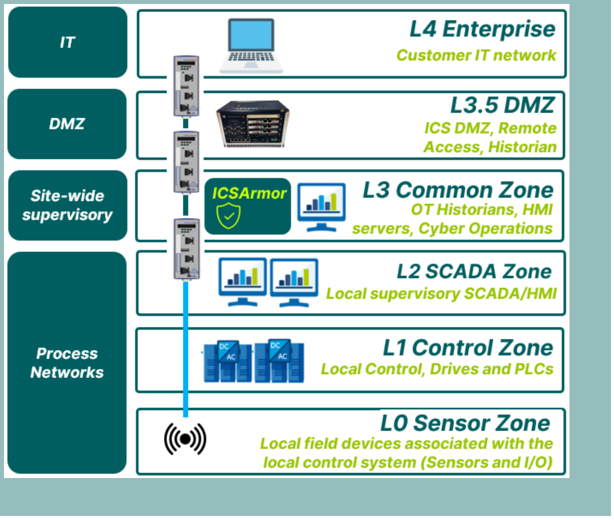
- Meets the requirements of ISA/IEC 62443-4-2
- Complies to alert HIDS requirements of NIST 800-94
- Developed in compliance with ISA/IEC 62443-4-1 SDLC
- Role-based access control is compliant to IEC62351-8
- Continuous threat detection on Windows devices, automatically mapped on MITRE ATT&CK framework

Deployment Architecture

ICSGuard operates in the process control layer, as shown in the Purdue image below. As the HIDS for the controllers and workstations, ICSGuard monitors their behaviour for anomalies.

ICSGuard can be integrated to a centralized security incident and event management solution (SIEM).

Example Network Architecture Model


IT
DMZ
Site-wide supervisory
Process Networks
L4 Enterprise
Customer IT network
L3.5 DMZ
ICS DMZ, Remote Access, Historian
ICSArmor
L3 Common Zone
OT Historians, HMI servers, Cyber Operations
L2 SCADA Zone
Local supervisory SCADA/HMI
L1 Control Zone
Local Control, Drives and PLCs
L0 Sensor Zone
Local field devices associated with the local control system (Sensors and I/O)

Detection Capabilities

ICSGuard detects attacks from both external and internal sources. It provides visibility to threat sources, such as:

Access Control Monitoring:

User login: Any user login needs to be monitored for potential abuse by a plant engineer or third party on site.

Multiple login failure: ICSGuard detects multiple failed controller login attempts. This can indicate a brute force attack, dictionary attack or a rainbow table attack. The algorithm flags this as an alert for further investigation.

Device Monitoring:

SSH session initiated: ICSGuard detects SSH user logins on operational controllers. Since this is not expected on an operating plant, the algorithm will flag an alert.

Unknown command execution: For privilege escalation, the attacker can execute multiple commands. An unknown command to the COTS will be flagged as an alert.

Network Monitoring:

DoS attack detection: ICSGuard can detect a DoS attack or a broadcast storm onto the controller. It utilizes the virtual sensor values to detect the incoming storm. ICSGuard will continue to create alerts until the condition is eliminated

Controller Memory Monitoring:

Memory leak prediction/detection: A memory leak is an unintentional form of memory consumption where an allocated memory block is not released after use. Most memory leaks result in general software reliability problems, but if an attacker can intentionally trigger a memory leak, the attacker might be able to launch a denial-of-service attack (by crashing the program) or take advantage of other unexpected program behaviour resulting from a low memory condition.

ICSGuard identifies memory leaks that may be in progress.

Controller Task Monitoring:

Task overrun detection: Task overruns may occur due to various reasons such as increased network traffic or communication failure.

An attacker may be able to cause a critical task to overrun and then disrupt plant operation. ICSGuard can detect such overruns and alert the plant authority for further investigation.

Task suspension detection: In operations, task suspension is uncommon. But a threat actor can gain access to a controller and can potentially suspend a critical task to disrupt the site operations. ICSGuard can detect such threats using virtual sensor technology.

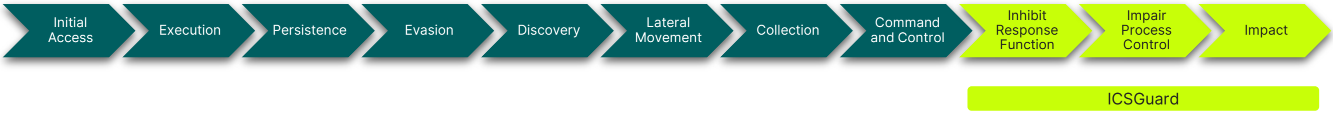
Workstation Monitoring:

The MITRE ATT&CK framework is referred to as a baseline for threat detection. The ICSGuard application has an agent deployed on Windows-based devices that continuously monitors and transfers the diagnostic information of the host machine.

A machine learning algorithm will compare the diagnostic information and local events to the MITRE ATT&CK techniques and tactics for continuous threat detection.

The threats from controllers and Windows-based devices in the network will be centrally collected in ICSGuard alert dashboard for continuous monitoring.

How is ICSGuard different from a NIDS?



- A network-based intrusion detection system (NIDS) detects malicious traffic on a network.
- As per the MITRE ATT&CK framework shown above, several tactics and techniques are used to attack a control system.
- Typically, NIDS are able to detect attacks early in the attack chain. Once the attacker has reached the "inhibit response state" it is almost impossible for a NIDS to detect them.
- ICSGuard is designed to fill this gap in the detection chain. ICSGuard is an important part of a defense-in-depth architecture, protecting the heart of the control system.
- ICSGuard performs prediction and detection of attacks and faults based on behavioural analysis of the controllers and workstations by using patented machine-learning algorithm.