CARLO GAVAZZI
Automation Components

CARLO GAVAZZI

White paper

Cybersecurity

The importance of cybersecurity in Energy Management Systems

Alessio Costantini
International Product Manager

May 2026

Cybersecurity in Energy Management Systems: designing secure architectures in a connected and regulated world

INTRODUCTION

Energy efficiency and digitalization are transforming the way energy is monitored, managed and optimized in industrial facilities and commercial buildings. Energy Management Systems (EMS) play a key role in this transformation by providing real-time visibility of energy consumption, enabling optimization strategies and supporting sustainability objectives.

Modern EMS solutions integrate multiple technologies, including smart meters, automation devices, communication gateways and cloud platforms. These systems collect and process large volumes of data, allowing organizations to improve operational efficiency, reduce energy costs and support environmental targets.

However, the growing connectivity of these systems significantly expands the potential cybersecurity attack surface. EMS infrastructures are no longer isolated networks; they are often connected to corporate IT systems, remote service platforms and cloud-based analytics environments.

As a result, cybersecurity has become a critical design requirement for modern EMS deployments. Protecting energy data, ensuring system availability and preventing unauthorized access to automation infrastructures are essential to maintaining operational reliability and business continuity.

In addition, the regulatory landscape is rapidly evolving. New international standards and regulations require manufacturers and system operators to adopt stronger cybersecurity practices, including secure product development, vulnerability management and lifecycle security updates.

ABSTRACT

This white paper examines the cybersecurity implications of modern EMS architectures and provides practical guidance on how to design, deploy and maintain secure energy management infrastructures

WHY CYBERSECURITY MATTERS IN EMS AND OT SYSTEMS

OT, IT & cloud integration

Energy Management Systems (EMS) and Building Energy Management Systems (BEMS) are increasingly connected infrastructures combining operational technology (OT), information technology (IT) and cloud services.

Smart devices & platforms

Modern EMS installations typically include smart energy meters, controllers and gateways, building automation devices, cloud data platforms and remote maintenance systems.

Expanded attack surface

This convergence creates significant value but also expands the attack surface. Cybersecurity is therefore no longer an optional feature but a core requirement in the design, deployment and operation of Energy Management Systems.

Secure & compliant architecture

A secure EMS architecture must ensure integrity of energy data, availability of automation functions, protection of operational networks and compliance with regulatory frameworks.

CYBERSECURITY REGULATORY LANDSCAPE FOR EMS AND BEMS

In recent years, the regulatory landscape for connected industrial products and energy management systems has evolved significantly. Organizations operating Energy Management Systems (EMS) or Building Energy Management Systems (BEMS) must increasingly comply with new cybersecurity regulations covering product design, vulnerability management and operational security.

These regulatory frameworks affect both product manufacturers and system operators, requiring the adoption of structured cybersecurity practices across the entire lifecycle of connected systems.

The most relevant frameworks affecting EMS and BEMS deployments include:
- the NIS2 Directive and its national implementations
- the EU Cyber Resilience Act
- the Delegated Regulation (EU) 2022/30 under the Radio Equipment Directive
- the UK Product Security and Telecommunications Infrastructure Act

These regulations introduce requirements such as:
- risk management and governance responsibilities
- vulnerability disclosure programs
- security update policies
- supply chain transparency
- incident reporting obligations

For organizations operating EMS infrastructures, understanding these frameworks is essential to ensure both regulatory compliance and operational resilience.

BOX – NIS2 IN ITALY

WHAT NIS2 MEANS FOR EMS AND BEMS OPERATORS

The NIS2 Directive has been transposed into Italian law through Legislative Decree 138/2024, introducing new cybersecurity obligations for organizations operating critical and important infrastructure.

Key obligations include:
- registration of relevant entities with national authorities
- implementation of structured risk management processes
- incident reporting obligations within defined timeframes
- board-level accountability for cybersecurity governance
- mandatory cybersecurity training for executive leadership
- supply chain risk management and vendor oversight

In Italy, the regulatory framework is already in force and introduces operational deadlines between 2025 and 2026 for compliance implementation.

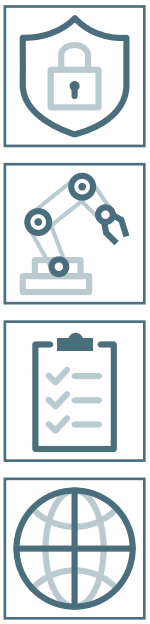
Organizations deploying EMS infrastructures should therefore ensure that cybersecurity controls are integrated not only at the product level but also within operational processes and governance structures.

CYBERSECURITY STANDARDS FOR INDUSTRIAL AUTOMATION

While regulations define legal obligations, technical standards provide implementation guidance.
Important standards are more than 40, including IEC 62443 industrial cybersecurity framework:

- NIST SP 800-82 guidance for industrial control systems
- ETSI EN 303 645 baseline security for connected devices

These frameworks define best practices for risk management, system segmentation, secure development lifecycle and incident response.



THE ARCHITECTURE OF A SECURE EMS

Most modern Energy Management Systems are built on layered architectures inspired by Industrial IoT design principles. This approach separates system functions into different operational layers, allowing improved scalability, maintainability and cybersecurity:

Field Layer:
includes the physical devices responsible for measuring and controlling energy-related parameters. These typically include smart energy meters, sensors, protection devices and actuators installed across electrical distribution systems and building infrastructures. These devices continuously collect operational data such as energy consumption, power quality and system status.

Edge Layer:
it represents the core of many modern EMS architectures. Edge devices such as controllers, gateways and data concentrators aggregate information coming from multiple field devices and perform local processing tasks. This layer often acts as the bridge between operational technology networks and enterprise IT systems. For this reason, it is also one of the most critical points from a cybersecurity perspective. Edge controllers frequently implement security functions such as authentication, encrypted communication, protocol translation and secure data buffering. They may also perform local automation logic and enable communication with cloud platforms for advanced analytics and system management.

Cloud Layer:
Edge controllers frequently implement security functions such as authentication, encrypted communication, protocol translation and secure data buffering. They may also perform local automation logic and enable communication with cloud platforms for advanced analytics and system management.

Each layer must implement strong authentication, encrypted communication and monitoring capabilities.

MODERN COMMUNICATION PROTOCOLS FOR EMS

Communication protocols play a fundamental role in Energy Management Systems, enabling the exchange of information between devices, controllers and cloud platforms. As EMS architecture becomes increasingly connected, the security of these communication channels becomes a critical requirement.
Traditional building automation networks often rely on protocols such as MODBUS for device interoperability. While widely adopted, earlier implementations of these protocols were not originally designed with strong cybersecurity capabilities. To address this limitation, more modern protocols should be taken into consideration while keeping an eye to retrofitting existing installations in compliance with new regulations.

HARDENING MQTT V5 FOR EMS AND IOT INFRASTRUCTURES

The MQTT protocol has become a widely adopted communication standard for Industrial IoT and energy management applications. It enables efficient communication between distributed edge devices and centralized cloud platforms.
However, MQTT implementations must be carefully secured in order to prevent unauthorized access and data manipulation. A secure MQTT deployment should implement several key controls.

MQTT SECURITY CHECKLIST

Recommended implementation practices include:

- mandatory TLS encryption for all MQTT connections
- mutual TLS authentication between clients and brokers
- strict access control policies based on topic permissions
- least privilege configuration for device access
- periodic certificate rotation
- auditing and monitoring of broker activity
- hardened broker configuration with restricted ports and services

When properly implemented, MQTT enables scalable and secure data communication between EMS edge devices and cloud-based analytics platforms.

Selecting the right protocols and implementing them with appropriate security measures is essential to maintaining the integrity and reliability of an EMS infrastructure.

EMS 1.0, UWP 4.0 AND MAIA CLOUD

Modern energy management infrastructures require a coordinated ecosystem of edge devices, controllers and cloud platforms. In this architecture, cybersecurity must be integrated into every layer of the system.
The ecosystem consists of three main components:

EMS 1.0 – EDGE-FIRST ENERGY MANAGEMENT

The EMS 1.0 platform acts as an integrated edge controller combining multiple functions in a single device:

- multi-meter data acquisition
- energy data logging
- embedded web server for visualization
- gateway functions for protocol integration
- local automation and control capabilities

The system supports multiple industrial communication protocols, including BACnet, Modbus, MQTT and REST APIs, enabling integration with building automation systems and cloud platforms.

UWP 4.0 – ADVANCED EDGE CONTROLLER

The UWP 4.0 platform extends the capabilities of the EMS infrastructure for more complex installations requiring additional processing power, connectivity and system integration.

The controller supports secure remote connectivity, industrial protocol integration and future roadmap capabilities such as MQTT integration and secure over-the-air updates.

MAIA CLOUD – SECURE REMOTE MANAGEMENT

The MAIA Cloud platform provides centralized services for:

- secure remote access via VPN
- fleet management of deployed devices
- secure over-the-air software updates
- monitoring and diagnostics

By combining these three components, architecture enables a secure edge-first energy management ecosystem that integrates field devices, controllers and cloud services.

SUPPLY CHAIN SECURITY & SBOM

Cybersecurity is not a one-time activity but a continuous, structured process that spans the entire lifecycle of a product or system. From the initial design phase through deployment and long-term operation, security must be systematically integrated into every stage rather than treated as an add-on.

In this context, the adoption of certified secure development processes—such as IEC 62443-4-1—plays a crucial role. This standard defines rigorous requirements for a secure product development lifecycle (SDL), ensuring that cybersecurity is embedded by design and by default. Compliance with IEC 62443-4-1 provides a formal framework covering key practices such as secure coding, threat modeling, security testing, and controlled management of updates and patches. More importantly, it guarantees that these practices are not applied sporadically, but are enforced through auditable, repeatable, and continuously improved processes.

Manufacturers that follow such certified frameworks can ensure a higher level of consistency and traceability across all development activities. This includes structured vulnerability testing, penetration testing, and continuous monitoring of third-party software components, all governed by defined procedures rather than ad hoc efforts.

Another critical aspect is vulnerability management. Even well-designed systems may contain vulnerabilities that emerge after deployment. A process aligned with IEC 62443-4-1 ensures that vulnerabilities are handled through a formalized workflow: identification, risk assessment, prioritization, remediation, and communication. This reduces response times and improves the overall effectiveness of mitigation actions.

Many organizations complement this approach with a dedicated Product Security Incident Response Team (PSIRT), responsible for coordinating vulnerability handling, issuing security advisories, and delivering timely patches. When supported by certified processes, PSIRT activities become more structured, predictable, and transparent, enabling better coordination with customers and system integrators.

Supply chain security has also become a major concern for connected industrial products. Modern EMS solutions rely on complex software ecosystems composed of open-source and third-party components. Within an IEC 62443-4-1 framework, the management of external components is formalized, requiring systematic evaluation, tracking, and risk assessment throughout the lifecycle.

A key enabler in this area is the Software Bill of Materials (SBOM), which provides a detailed inventory of all software components included in a product. When integrated into a certified development process, SBOMs are not static documents but are continuously maintained and updated. This allows organizations to quickly determine exposure to newly discovered vulnerabilities in third-party libraries and to take prompt corrective actions.

By combining lifecycle security practices, certified development processes such as IEC 62443-4-1, and supply chain transparency through tools like SBOMs, organizations can significantly strengthen the resilience, reliability, and trustworthiness of their EMS infrastructures.

BEST PRACTICES FOR SYSTEM INTEGRATORS AND OPERATORS

While manufacturers play a key role in developing secure products, the overall security of an Energy Management System also depends heavily on how the system is deployed and operated. System integrators and facility operators therefore have an essential responsibility in maintaining a secure infrastructure.

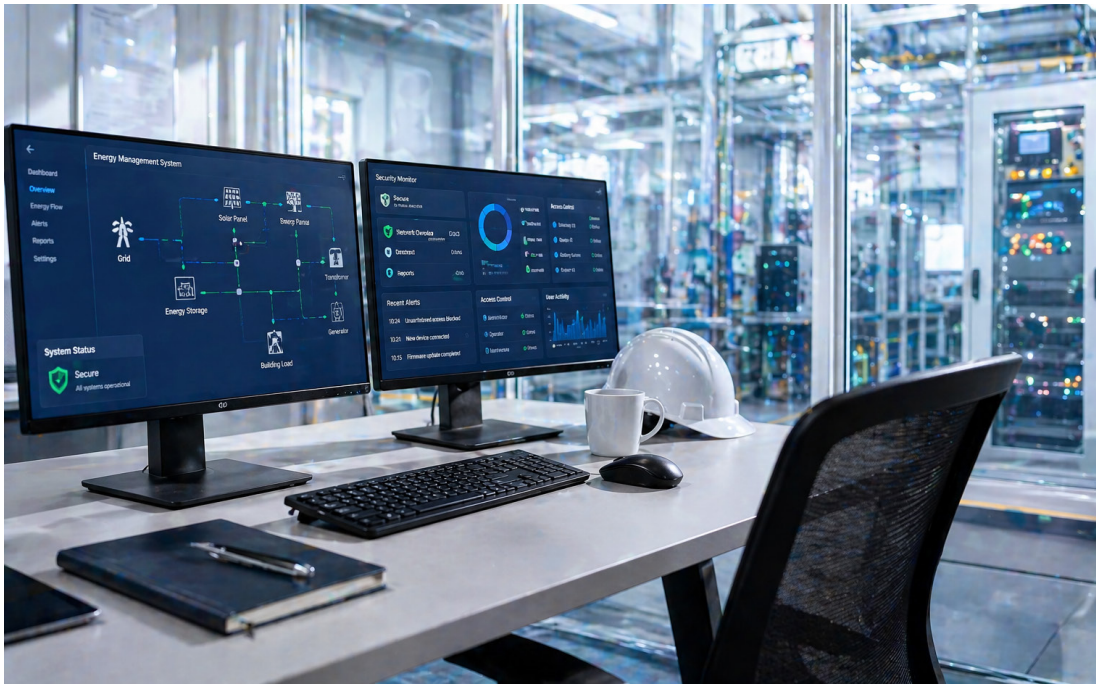
One of the most important practices is the implementation of segmented network architecture. Separating operational technology networks from corporate IT networks reduces the risk that cyber incidents in one environment can propagate to critical automation systems.

Access control mechanisms should also be carefully implemented. Only authorized personnel should be able to access EMS devices and management platforms. Role-based access control policies help ensure that users can perform only the actions required for their responsibilities This is possible by relying on strong authentication policies at user level, and port based access control protocols like IEEE802.1X at network level.

Secure remote access is another critical aspect, especially for installations that require remote monitoring or maintenance. When remote connectivity is necessary, it should be implemented through secure channels such as VPN connections and protected with strong authentication mechanisms.

Regular software updates are equally important. Manufacturers frequently release security patches that address newly discovered vulnerabilities. Ensuring that devices and platforms are kept up to date significantly reduces the risk of exploitation. Finally, organizations should implement monitoring, backup and incident response procedures to maintain operational continuity. Continuous monitoring of system activity helps detect suspicious behavior, while backup strategies ensure that data and configurations can be quickly restored in the event of a cyber incident.

By adopting these best practices, organizations can significantly strengthen the cybersecurity posture of their Energy Management Systems and ensure the reliable operation of critical energy infrastructures.



CONCLUSIONS

The increasing convergence of OT, IT, and cloud technologies has transformed Energy Management Systems into highly connected and potentially exposed infrastructures.

In this context, cybersecurity must be treated as a foundational requirement, embedded from the design phase and maintained throughout the entire system lifecycle. The adoption of secure layered architectures, robust communication protocols, certified development processes, and structured supply chain management practices is essential to ensure operational resilience.

At the same time, evolving regulatory frameworks are driving organizations toward a more systematic and accountable approach to cybersecurity. Solutions such as EMS 1.0, UWP 4.0, and dedicated cloud platforms demonstrate how innovation, energy efficiency, and security can coexist within modern EMS ecosystems.

Ultimately, effective protection depends on strong collaboration between manufacturers, system integrators, and operators, supported by continuous monitoring, regular updates, and a proactive security mindset.

CARLO GAVAZZI

OUR SALES NETWORK IN EUROPE

AUSTRIA
Carlo Gavazzi GmbH
Ketzergasse 374,
A-1230 Wient
Tel. +43 1 888 4112
Fax +43 1 889 1053
office@carlogavazzi.at

FINLAND
Carlo Gavazzi OY AB
Ahventie, 4 B
FI-02170 Espoo
Tel. +358 9 756 2000
myynti@gavazzi.fi

GREAT BRITAIN
Carlo Gavazzi UK Ltd
4.4 Frimley Business Park,
Frimley, Camberley,
Surrey GU16 7SG
Tel. +44 1 276 854110
sales@carlogavazzi.co.uk

NORWAY
Carlo Gavazzi AS
Melkeveien 13,
N-3919 Porsgrunn
Tel. +47 35 93 08 00
post@gavazzi.no

SWEDEN
Carlo Gavazzi AB
V:a Kyrkogatan 1,
S-652 24 Karlstad
Tel. +46 54 85 11 25
Fax +46 54 85 11 77
info@carlogavazzi.se

BELGIUM
Carlo Gavazzi NV/SA
Mechelsesteenweg 311,
B-1800 Vilvoorde
Tel. +32 2 257 41 20
sales@carlogavazzi.be

FRANCE
Carlo Gavazzi Sarl
Zac de Paris Nord II, 69,
rue de la Belle Etoile,
F-95956 Roissy CDG Cedex
Tel. +33 1 49 38 98 60
Fax +33 1 48 63 27 43
french.team@carlogavazzi.fr

ITALY
Carlo Gavazzi SpA
Via Milano 13,
I-20045 Lainate (MI)
Tel. +39 02 931 76 1
info@gavazziacbu.it

PORTUGAL
Carlo Gavazzi Lda
Rua dos Jerónimos 38-B,
P-1400-212 Lisboa
Tel. +351 21 361 70 60
Fax +351 21 362 13 73
carlogavazzi@carlogavazzi.pt

SWITZERLAND
Carlo Gavazzi AG
Verkauf Schweiz/Vente Suisse
Sumpfstrasse 3,
CH-6312 Steinhausen
Tel. +41 41 747 45 35
Fax +41 41 740 45 40
info@carlogavazzi.ch

DENMARK
Carlo Gavazzi Handel A/S
Over Hadstenvej 40,
DK-8370 Hadsten
Tel. +45 89 60 61 00
Fax +45 86 98 15 30
handel@gavazzi.dk

GERMANY
Carlo Gavazzi GmbH
Pfnorstr. 10-14
D-64293 Darmstadt
Tel. +49 6151 81 00 0
info@gavazzi.de

NETHERLANDS
Carlo Gavazzi BV
Wijkermeerweg 23,
NL-1948 NT Beverwijk
Tel. +31 251 22 93 45
info@carlogavazzi.nl

SPAIN
Carlo Gavazzi SA
Avda. Iparraguirre, 80-82,
E-48940 Leioa (Bizkaia)
Tel. +34 94 480 40 37
Fax +34 94 431 60 81
gavazzi@gavazzi.es

OUR SALES NETWORK IN THE AMERICAS

USA
Carlo Gavazzi Inc.
750 Hastings Lane,
Buffalo Grove, IL 60089-6904,
USA
Tel. +1 847 465 61 00
sales@carlogavazzi.com

CANADA
Carlo Gavazzi Inc.
2430 Meadowpine Bvd Unit 104
Mississauga, ON L5N 6S2,
Canada
Tel. +1 905 542 0979
gavazzi@carlogavazzi.com

MEXICO
Carlo Gavazzi Mexico S.A. de C.V.
Circuito Puericultores 22,
Ciudad Satelite
Naucalpan de Juárez,
Edo Mex. CP 53100 - Mexico
Tel. +52 55 5373 7042
Fax +52 55 5373 7042
mexicosales@carlogavazzi.com

BRAZIL
Carlo Gavazzi Automação Ltda.
Av. Francisco Matarazzo,
1752 Conjunto 2108
CEP 05001-200 -
São Paulo - SP - Brazil
Tel. +55 11 3052 0832
Fax +55 11 3057 1753
info@carlogavazzi.com.br

OUR SALES NETWORK IN ASIA AND PACIFIC

SINGAPORE
Carlo Gavazzi Automation
Singapore Pte. Ltd.
61 Tai Seng Avenue #05-06
Print Media Hub @ Paya Lebar
iPark
Singapore 534167
Tel. +65 67 466 990
Fax +65 67 461 980
info@carlogavazzi.com.sg

TAIWAN
Branch of Carlo Gavazzi
Automation Singapore Pte. Ltd.
12F-3, No. 530, Yingcai Rd.,
West Dist., Taichung City 403518,
Taiwan, China
Tel. +886 4 2258 4001
Fax +886 4 2258 4002

MALAYSIA
Carlo Gavazzi Automation (M)
SDN. BHD.
D12-06-G, Block D12,
Pusat Perdagangan Dana 1,
Jalan PJU 1A/46,
47301 - Petaling Jaya,
Selangor, Malaysia
Tel. +60 3 7842 7299
Fax +60 3 7842 7399
info@gavazzi-asia.com

CHINA
Carlo Gavazzi Automation
(China) Co. Ltd.
Unit 2308, 23/F.,
News Building, Block 1,1002
Middle Shennan Zhong Road,
Futian District,
Shenzhen, China
Tel. +86 755 8369 9500
Fax +86 755 8369 9300
info@carlogavazzi.cn

INDIA
Carlo Gavazzi Automation
India PVT LTD.
1105/06, Kamdhenu 23 West,
Thane Belapur Road,
TTC Industrial Area
Kopar Khairane, Navi Mumbai
400709, India
Tel. +91 88282 84033
info@carlogavazzi.in

OUR COMPETENCE CENTRES AND PRODUCTION SITES

DENMARK
Carlo Gavazzi Industri A/S
Hadsten

ITALY
Carlo Gavazzi Controls SpA
Belluno

LITHUANIA
Uab Carlo Gavazzi Industri
Kaunas
Kaunas

MALTA
Carlo Gavazzi Ltd
Zejtun

CHINA
Carlo Gavazzi Automation
(Kunshan) Co., Ltd.
Kunshan

MEXICO
Carlo Gavazzi Americas Inc.
Tijuana

HEADQUARTERS

CARLO GAVAZZI AUTOMATION SPA
Via Milano, 13
I-20045 - Lainate (MI) - ITALY
Tel. +39 02 931 761
info@gavazziautomation.com

Energy to Components!

www.gavazziautomation.com

Printed on 100% recycled paper
produced using
post consumer de-inked waste.

CARLO GAVAZZI
Automation Components

Energy to Components!

www.gavazziautomation.com

CARLO GAVAZZI

WP Cybersecurity in EMS ENG REV.00 05/26