

White paper



Cybersecurity

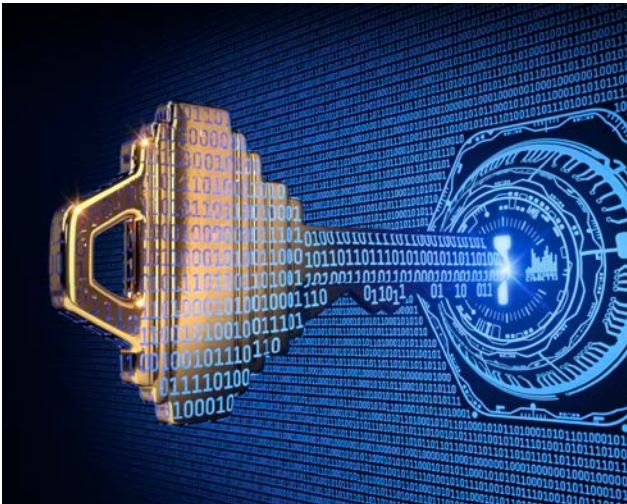
The importance of cybersecurity in Energy Management Systems

Alessio Costantini
International Product Manager

October 2021

Cybersecurity.

The importance of cybersecurity in Energy Management Systems



INTRODUCTION

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. Sometimes it may seem a kind of wizardry or rocket science; nevertheless,, it is part of our everyday lives.

News about people stealing money from bank accounts or personal information from Internet accounts are very common. Sometimes it is not clear that it is not only a matter of PCs and smartphones: there are billions of connected devices in our homes, workplaces and buildings that could be attacked. In the dark web there are databases of compromised connected devices, with information which can be used to attack them. When it comes to Energy Management Systems and their IT+OT=IoT infrastructure, it is necessary to ask ourselves "Why" their cybersecurity should be a concern to us.

ABSTRACT

This document will help decision makers, system integrators, installers and end-users of Energy Management Systems (EMS), including both the Energy Monitoring and Building Automation parts, to decide if cybersecurity should be considered while designing/deploying/proposing a new EMS.

MANY INSTALLATIONS, COMMON NEEDS

There is a multitude of cases in the building automation and energy monitoring realms. However, many of them have the same architectures and the same factors. For these reasons, it is possible to address a common strategy to get rid of the most critical cybersecurity issues and start the process in the right way. Cybersecurity problems are the same as the ones experienced in the IT world: attackers can decide to mount an attack from both inside and outside the perimeter of any organisation, exploiting known vulnerabilities, potentially causing huge amounts of damage. The consequences are unwanted and vary from privacy issues to tampering of the automation system.

A drastic rise in IT security incidents is reported by Governmental institutions like ICS-Cert (<https://www.us-cert.gov/ics>) or BSI (Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Home/home_node.html), and specific standards, like ETSI EN 303 645 and IEC-62443, have been developed to create a common playground for both consumer and industry. Unfortunately, there are no worldwide standards, but responsible authorities are working towards harmonisation.

Finally, cybersecurity is the result of the combined efforts of all the involved factors: only strong products combined with strong user habits (i.e., strong passwords) generate secure systems.

WHY SHOULD I CYBER-PROTECT ALL THE COMPONENTS OF MY EMS SYSTEM?

1. BECAUSE INFORMATION MEANS VALUE

The target of any EMS system is to use the available information about energy consumption to drive decisions aimed at saving energy and money: information means energy and money saving. Corrupted information could have a strong impact on decisions and results. Protecting data communication, storing and analysing is as important as measuring variables and calculating KPIs, because nobody likes to take decisions on the basis of wrong or corrupted information.

2. AN INSTALLATION IS AS SECURE AS ITS WEAKEST LINK

We should not forget that in the case of cyber-attacks, the attacked system may be a backdoor used by malicious hackers to reach their target, which can be another system. For this very reason, it is important to remember that any installation is as secure as its weakest link: maybe a weak gateway is an easy way for cyber-attackers to get control of the BMS and EMS systems. This is the reason why it is important to secure all the sub-systems.

3. IT IS A MATTER OF BEST PRACTICES

Very often users do not apply the same best practices to all of their networked connections: maybe they are very strict in their working environment and have an easy approach to their personal smartphone or PC. It has been reported that, in many cases, in the same building the automation infrastructures are weaker than the IT systems for the offices. Ultimately, it is a matter of habits: why not transform best-practices in habits, so to have a common level of security in all the daily tasks?

4. RISK ANALYSIS

Very often a risk analysis is underrated while deploying projects. It should be part of the main project pillars, instead. What is the value of our data? What if someone takes control of my building automation system? How much will it cost to repair a compromised system? Am I liable in the case of a compromised installation? All these questions should arise at the early stages of any EMS project implementation.

5. IT IS NOT ABOUT "IF" BUT "WHEN"

Automated scanners work day and night to find weak systems to attack via the Internet. Criminal organisations work daily to pursue their intents against unaware owners of networked systems. Being behind a firewall is not a warranty against cybercrime: very often the attacks come from inside the organisation. Cybercrimes are increasing: maybe it is time to seriously consider the chance of being attacked and ask yourselves "when", not "if".



▶ THE FACTORS IN AN EMS INSTALLATION

The common factors are reported below: each of them has a role in the complete implementation of a secure system.

Building use	Advantages of tunable white control	How?
System integrator, system designer	Who is in charge of designing the system according to the project specification	Insufficient cybersecurity awareness leads to wrong design choices
Installer	Who is in charge of commissioning the system according to the designer's instructions	Insufficient cybersecurity awareness leads to wrong deployment
End-User	Who is in charge of operating the system in the daily usage	Insufficient cybersecurity awareness leads to wrong operation
Owner	Who is in charge of setting the budget limits, cybersecurity targets and functional specification for the project	Insufficient cybersecurity awareness leads to overestimate/underestimate the necessary countermeasures
Manufacturer	Who is the manufacturer of the hardware and/or software components of the system	Insufficient cybersecurity awareness leads to unsecure components/hardware

It is clear that cybersecurity awareness is the main target of any factor at different levels. For the manufacturer, the target is developing products according to opportune guidelines; for the end-user, operating the system according to the right best practices (i.e., avoiding unsecure passwords). On the other side, an ad-hoc mix of cybersecurity training and guidelines is the first point to be addressed, at any level, to implement a secure system.

▶ THE LAYERED ARCHITECTURE OF AN EMS SYSTEM

As stated before, most of the systems in the building automation and energy monitoring applications can be layered according to a common set of parts, which corresponds to the IIoT paradigm.

Level	Description
Field	The level of operational technology, near to the application level. It includes meters, sensors, actuators and the relevant fieldbuses.
Edge	The borderline between field and cloud. It is where gateways and controllers are located.
Fog	An intermediate level which could mix part of the Edge and Cloud functions to provide improved scalability.
Cloud	The Internet level, where immense resources of distributed servers allow full interoperability and maximum data interchange.

Each layer interacts with the others, so a cybersecurity threat impacting onto one layer could possibly penetrate into other layers. Always remember that any system is as secure as its weakest link.

▶ PROTECTION LEVELS

Despite cybersecurity being a global concern, there is not a universally recognised standard. However, threat recognition and countermeasures are usually shared by different standards. The worldwide accepted IEC 62443 standard defines five different levels of security. It is important to follow an established guideline to establish threats according to the connected risk; the division proposed by the IEC-62443 standard is based on the following security levels:

Security level	Description
0 (SLO)	No protection required.
1 (SL1)	Prevent the unauthorised disclosure of information via eavesdropping or casual exposure. Example: wrong set-up.
2 (SL2)	Prevent the unauthorised disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation. Example: no security measures, hacker.
3 (SL3)	Prevent the unauthorised disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, application specific skills and moderate motivation. Example: moderate security measures, high level hacker.
4 (SL4)	Prevent the unauthorised disclosure of information to an entity actively searching for it using sophisticated means with extended resources, application specific skills and high motivation Examples: Specific development, knowledge of the application, or corruption of insiders.

Eliminating 100% of cybersecurity risks involves a potentially unlimited budget, due to the impact of the needed countermeasures onto all assets and people. The purpose of any decision maker should be to set the right budget for assuring a security level according to the needs of the target system and organisation; the system integrator can then design the system according to the functional needs and the acceptable risk, by choosing the right components and using the right guidelines. The operational functions of a system can be damaged or interrupted in different ways. The security measures focus on intentional threats such as sabotage, vandalism or spying; however, unintentional issues caused by wrong hardware, software, commissioning or service could harm the assets, and must be taken into consideration while designing the system.



▶ OUR LINE OF DEFENCE

1. EXPERTISE

Cybersecurity is like rocket science: to advance you need to be at the edge. Luckily, it is not necessary to be a cybersecurity guru to protect your system: you just need good products (i.e., the result of expertise applied to product engineering) and best practices (i.e., the result of expertise applied to procedures). If you do not have the expertise, you can buy it!

2. SECURE PRODUCTS

A secure system is made up of secure components: how can you claim that your component is secure? Very often it seems that by adding some extra security software or hardware is the only way to go. The right advice is based on minimalism: limit the number of components in use to the bare minimum and make sure that all of them are secure enough for the application; the point is how to evaluate cybersecurity of a component. Not one of us has the necessary expertise, right? The best way is to rely on trusted certification or ratings: a product which has undergone a cybersecurity rating or certification by a cyber lab with a good reputation gives you peace of mind that your defences will protect against the vast majority of common cyber attacks.

3. TRAINING

Setting the necessary best practices requires at least basic training; at each level of all the involved parties (designers, installers, users) an adequate training is necessary to avoid compromising the security with bad practices. At the end, Cybersecurity is a process, not a product.

4. A PRAGMATIC APPROACH

Some best practices are listed below, with the purpose of setting up a line of defence for the target system.

Task	Description
Define the system constraints and the critical assets	Define the acceptable and unacceptable risks when it comes to the cybersecurity of the system.
Train the people	Assure that all the people involved in the project receive the training level corresponding to their tasks, and to the relevant risks.
Define a target and a budget	Define a clear cybersecurity target and allocate the budget accordingly. Each project is the result of a compromise between expected goals and budget constraints. However, it is mandatory to know every possible weaknesses, so to try to solve them at the next budget review.
Involve external competent resources when it is necessary	Cybersecurity is an evolving matter, where intentional harm is possible: updated expertise is mandatory to being able to face risks.
Choose the best components, according to your goals and budget	When designing the system, use those components which can demonstrate the requested security level. Choose those components which can demonstrate their security level thanks to an accredited third-party certification or rating.
Define the necessary procedures	A system is made of products and procedures. If a ultra-secure controller is used and the user tells the password to everybody, there is no way to protect the system: cybersecurity is responsibility of all the parties involved in the system lifetime.

The above guideline is valid for any party involved in the project, from the system integrator who designs the system, to the manufacturer who develops the software and hardware components.

▶ A REAL-WORLD EXAMPLE: SECURING THE EDGE LEVEL

The EDGE level is possibly the most critical: being at the same time in contact with the operational technology (OT) part in the field and the information technology part (IT) in the cloud, it is the most sensitive brick in the IoT paradigm. A strong EDGE level is for sure a robust foundation on which to base the whole architecture.

1. EDGE CYBERSECURITY: THE SYSTEM INTEGRATOR

The system integrator has to:

- build up the system providing the necessary functional requirements according to the expected level of cybersecurity.
- choose the right components.
- set the necessary procedures to get the goal.

There are 3 important best practices:

Best practice	Description
Training	Continuous training with competent trainers is the key to keep the pace with evolving cybersecurity threats.
Define a protected environment	Place the EDGE part in a protected environment, in which both physical and logical access is regulated. This means: <ul style="list-style-type: none"> • installing EDGE controllers into locked cabinets. • defining a trusted network, so to restrict communication to authorised systems/users. • use encrypted communication whenever possible.
Choose best in class components	Choose software and hardware components from solid companies with an established reputation, and assure their cybersecurity level by means of official ratings provided by accredited third parties.
Test the system	A testing procedure to guarantee the achieved cybersecurity level is a necessary part of the commissioning.

2. EDGE CYBERSECURITY: THE MANUFACTURER

The manufacturer has the task of developing software and hardware components with the necessary level of cybersecurity according to the demand of the target applications, and of documenting the achieved level.

There are 3 important best practices:

Best practice	Description
Training	Continuous training with competent trainers is the key to keep the pace with evolving cybersecurity threats.
Development techniques	Adopting development practices which put cybersecurity at the top rank of the expected goals is the key point to warranty future proof products.
Testing	Testing products with respect to cybersecurity.
Assessment	Checking the cybersecurity level with the help of an experienced and trustable third party.
Marking	Submit the product for an official third-party marking from an accredit laboratory.

3. EDGE CYBERSECURITY: THE END USER

The end user is in charge of using the system delivered by the system integrator and has some responsibilities, too.


Here are the most important best practices:

Best practice	Description
Training	Continuous training with competent trainers is the key to keep the pace with evolving cybersecurity threats.
Rules	Always follow the rules defined in the company policies as far as cybersecurity is concerned.
Confidentiality	Preserve confidential data like user profiles and passwords, as they are the key access points to the system; follow GDPR rules.
Update	Always keep the system updated: a secure software installed onto an unsecure PC, generates a unsecure system.

▶ UWP 3.0 SE, A SECURE SOLUTION FOR THE EDGE LEVEL

UWP 3.0 is the IoT gateway and controller by Carlo Gavazzi for EMS systems. It is the core of an ecosystem of more than 200 meters, sensors, actuators by Carlo Gavazzi. Besides, it can be connected both at field level and at cloud level to other systems so to play as the EDGE tier in an EMS architecture.

Carlo Gavazzi is committed to provide the best security level to customers and users; for this reason, UWP 3.0 SE (Security Enhanced) is now available. UWP 3.0 SE' security capabilities have been verified by UL, one of the top worldwide laboratories for cybersecurity assessment and advisory. An official rating represents a solid and secure reference for the product selection. By having solid networking foundations and encouraging customers to protect their system via VPN and passwords, UWP 3.0 SE is one of the first EDGE products in the market with an official cybersecurity rating.

UWP 3.0 SE Cybersecurity rating	https://verify.ul.com/verifications/487
UWP 3.0 SE Cybersecurity marking	

Disclaimer: Carlo Gavazzi assumes no liability whatsoever for indirect, collateral, accidental or consequential damages or losses that occur by (or in connection with) the distribution and/or use of this document. All information published in this document is provided "asis" by Carlo Gavazzi. None of this information shall establish any guarantee, commitment or liability of Carlo Gavazzi. The technical specifications of products, and the contents relevant to the topics reported in this document are subject to change. Errors and omissions excepted. No reproduction or distribution, in whole or in part, of this document without prior permission, is allowed.

OUR SALES NETWORK IN EUROPE

AUSTRIA

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

BELGIUM

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

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

FINLAND

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

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

GERMANY

Carlo Gavazzi GmbH
Pfnorstr. 10-14
D-64293 Darmstadt
Tel: +49 6151 81 00 0
Fax: +49 6151 81 00 40
info@gavazzi.de

GREAT BRITAIN

Carlo Gavazzi UK Ltd
4.4 Frimley Business Park,
Frimley, Camberley, Surrey GU16 7SG
Tel: +44 1 276 854110
Fax: +44 1 276 682140
sales@carlogavazzi.co.uk

ITALY

Carlo Gavazzi SpA
Via Milano 13,
I-20045 Lainate
Tel: +39 02 931 76 1
Fax: +39 02 931 76 301
info@gavazziacbu.it

NETHERLANDS

Carlo Gavazzi BV
Wijkermeerweg 23,
NL-1948 NT Beverwijk
Tel: +31 251 22 93 45
Fax: +31 251 22 60 55
info@carlogavazzi.nl

NORWAY

Carlo Gavazzi AS
Melkeveien 13,
N-3919 Porsgrunn
Tel: +47 35 93 08 00
Fax: +47 35 93 08 01
post@gavazzi.no

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

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

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

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

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
Fax: +1 847 465 73 73
sales@carlogavazzi.com

CANADA

Carlo Gavazzi Inc.
2660 Meadowvale Boulevard,
Mississauga, ON L5N 6M6, Canada
Tel: +1 905 542 0979
Fax: +1 905 542 2248
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
T +52 55 5373 7042
F +52 55 5373 7042
mexicosales@carlogavazzi.com

BRAZIL

Carlo Gavazzi Automação Ltda.
Av. Francisco Matarazzo, 1752
Conj 2108 05001-200 - São Paulo - SP
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

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
sales@carlogavazzi.cn

HONG KONG

Carlo Gavazzi Automation
Hong Kong Ltd.
Unit No. 16 on 25th Floor, One Midtown,
No. 11 Hoi Shing Road, Tsuen Wan,
New Territories, Hong Kong
Tel: +852 26261332 / 26261333
Fax: +852 26261316

TAIWAN

Branch of Carlo Gavazzi Automation
Singapore Pte. Ltd.
22F-1, No.500 Shizheng Rd, Xitun Dist,
Taichung City 407,
Taiwan, China
Tel. +886 4 2258 4001
Fax +886 4 2258 4002

OUR COMPETENCE CENTRES AND PRODUCTION SITES

DENMARK

Carlo Gavazzi Industri A/S
Hadsten

MALTA

Carlo Gavazzi Ltd
Zejtun

ITALY

Carlo Gavazzi Controls SpA
Belluno

LITHUANIA

Uab Carlo Gavazzi Industri Kaunas
Kaunas

CHINA

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

HEADQUARTERS

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



CARLO GAVAZZI
Automation Components

Energy to Components!

www.gavazziautomation.com

