

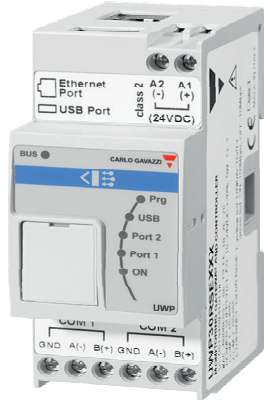


Cybersecurity Guideline

Cybersecurity in Energy Monitoring and Building Automation applications

Cybersecurity

Cybersecurity in Energy Monitoring and Building Automation applications



Abstract

This document will help system integrators, installers and end-users of Energy Monitoring and Building Automation applications to protect their installation by highlighting some core areas in the cybersecurity process and helping them to do the right choices for designing, setting-up or operating a secure and reliable system. It includes an introduction to security topics in data automation and control systems, and points out the responsibility of involved parties, focusing on the most critical parts inside the target installation.

Introduction

Nowadays, cybersecurity in industrial, commercial and residential installations is a source of concern: cyber-threats and attacks increase day by day, and a drastic rise of IT security incidents is reported by the Governmental institutions like ICS-Cert (*Industrial Control Systems Cyber Emergency Response Team*, www.us-cert.gov/ics) or BSI (*Bundesamt für Sicherheit in der Informationstechnik*, www.bsi.bund.de/DE/Home/home_node.html).

Why cybersecurity is so important? Because a lack in cybersecurity could lead to a loss in one or more of the following assets:

- the availability of system functionalities
- the confidentiality of data, and protection of intellectual property
- the integrity of the application function and components in use
- the authenticity of controllers and their data.

Cybersecurity is a process, not a product: security improvements need to be continuously maintained and updated. For these reasons, it is not possible to achieve 100% security. Even when designed with state-of-the-art security measures, a system may still be vulnerable to connections to the networks of suppliers, contractors, and partners.

Different Installations, common needs

There are a multitude of use cases in the building automation and energy monitoring realms; nonetheless, many of them share the same architectures and the same actors. 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.

The actors

The common actors are:

Actor	Description	Potential issues in the cybersecurity process
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 a hardware and/or software component of the system	Insufficient cybersecurity awareness leads to an unsecure component

Basically, it is clear that cybersecurity awareness is the main target of any actor at different levels to avoid missing the target. For the manufacturer it means developing products according to opportune guidelines and for the end-user to operate the system according to the right best practices (i.e. avoiding to use unsecure passwords). On the other side, this is the proof that 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 architecture

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

Level	Description
Field	The operational technology level, close 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 so to provide a better scalability.
Cloud	The Internet level, where the immense resources of distributed servers allow full interoperability and maximum data elaboration.

Each layer interacts with the other ones, so a cybersecurity threat impacting onto one layer could possibly scale and impacting the other ones. Never forget that any system is as secure as its weakest part, when cybersecurity is concerned.

Protection levels

Even if cybersecurity is a global concern, there is not a universally recognized 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 organize threats according to the connected risk; the division proposed by the IEC-62443 standard is based on security levels:

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

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 setting the right budget for assuring a security level in line with the needs of the target system and organization. The system integrator could 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 system can be damaged or interrupted in different ways. Security measures focus on intentional threats such as sabotage, vandalism or spying nonetheless unintentional issues caused by wrong hardware, software, commissioning or service could harm the assets, and must be taken into consideration while designing the system.

A pragmatic approach

Some of the best practices are listed here, 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 nonetheless it is mandatory to know if there are known weaknesses, so to possibly solve them at the next budget review.

Task	Description
Involve external competent resources when it is necessary	Cybersecurity is an evolving matter, where intentional harming is possible. Updated expertise is mandatory to face risks
Choose the best components, according to your goals and budget	For designing the system, use the components that can demonstrate the requested security level thanks to an accredited third party certification or rating.
Define the necessary procedures	A system is made of products and procedures: if an ultra-secure controller is used and the user doesn't tell the password to anybody, there is no way to protect the system. Cybersecurity is responsibility of any of 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

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.

EDGE cybersecurity: the system integrator

The system integrator has the task to build up the system providing the necessary functional requirements according to the expected level of cybersecurity. He needs to choose the right components and set the necessary procedures to get the goal.

There are three 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 authorized 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 assuring their cybersecurity level by means of official ratings provided by accredited third parties
Test the system	A testing procedure to warranty the achieved cybersecurity level is a necessary part of the commissioning

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 to document the achieved level.

There are three 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

EDGE cybersecurity: the end-user

The end-user is in charge of using the system delivered by the system integrator. He/she 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 updated the system: a secure software installed onto an unsecure PC, generates an unsecure system
Marking	Submit the product for an official third party marking from an accredited laboratory


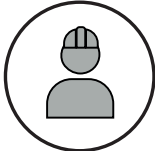


Implementing a secure architecture with UWP 3.0, the Carlo Gavazzi EDGE solution

In this section we will find out how to develop a secure architecture as far as the EDGE layer in an Energy Management / Building Automation installation. The EDGE unit is UWP 3.0. The following architecture is based on the 3-tier model described above, with fieldbus, edge and fog/cloud layers.

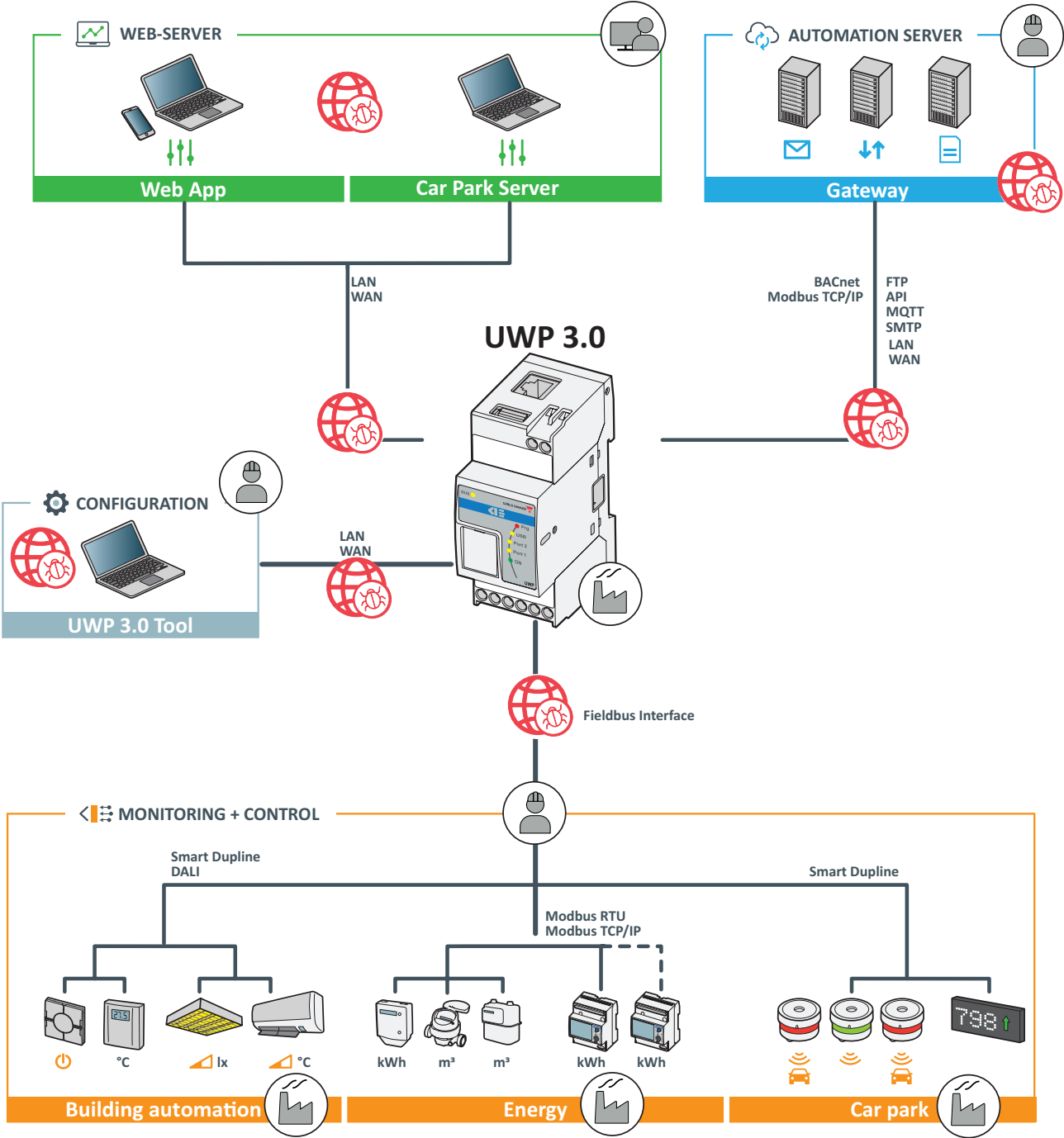
Vulnerability topologies

Both single assets and systems can be compromised by cybersecurity issues at different levels. For further information, refer to the “**Architecture (threats by zone)**”.

Legend

Icon	Meaning
  <p><i>End user/operator</i> <i>System integrator</i></p>	See “Responsibility by role”
	Software and device supplier. See “Responsibility by role”
	Area of potential cybersecurity risks

Architecture (threats by zone)



Pillars of the cybersecurity deployment

Best practice	Description
Training to all the involved people	Training necessary to users about adopting the necessary security procedures (Project owner)
Defining a protected environment	Setting the target system borders according to the functional needs and the expected security level (Project owner, system integrator)
Selecting the right components	Selecting components fulfilling the expected cybersecurity level (System integrator)
Defining responsibilities	Allocating cybersecurity responsibilities according to the stakeholder's scope (Project owner)
Technical documentation	Providing the system's documentation for both the system and the single components (System integrator, manufacturer)
Testing	Periodically assessing the system in terms of its cybersecurity strength (Project owner, system integrator)

System integrator's best practices

- **ASSESSMENT:** always do a risk analysis at the beginning of the project to check the cybersecurity risks, their impact, and the necessary level of security
- **NETWORK SEGMENTATION:** whenever possible, always divide the target networks in physical or logical segments for which it is possible to set the necessary rules for filter the access to the target services
- **ACCESS CONTROL:** define and implement the access authorization according to the target customer policies; define password change policies
- **FIREWALL:** protect the inbound access to any service with a firewall, whose rules must be set according to company policies
- **VPN:** use a Virtual Private Network with encrypted tunnel to provide access to remote users
- **UPDATE:** always update the system's software/firmware components to the patch level which warranties the fulfilment of the company cybersecurity policies
- **REMOVABLE STORAGE:** avoid using removable storage (USB sticks) as they are often cyberthreats carriers
- **ENDPOINT HARDENING:** the whole system is only as secure as its weakest part; having VPN, Firewall and robust protocols is useless if the user's PC is not protected/updated

Defining a protected environment with UWP 3.0

Placing the gateway/controller in a protected environment is mandatory to avoid undesired access to the controller or its application.

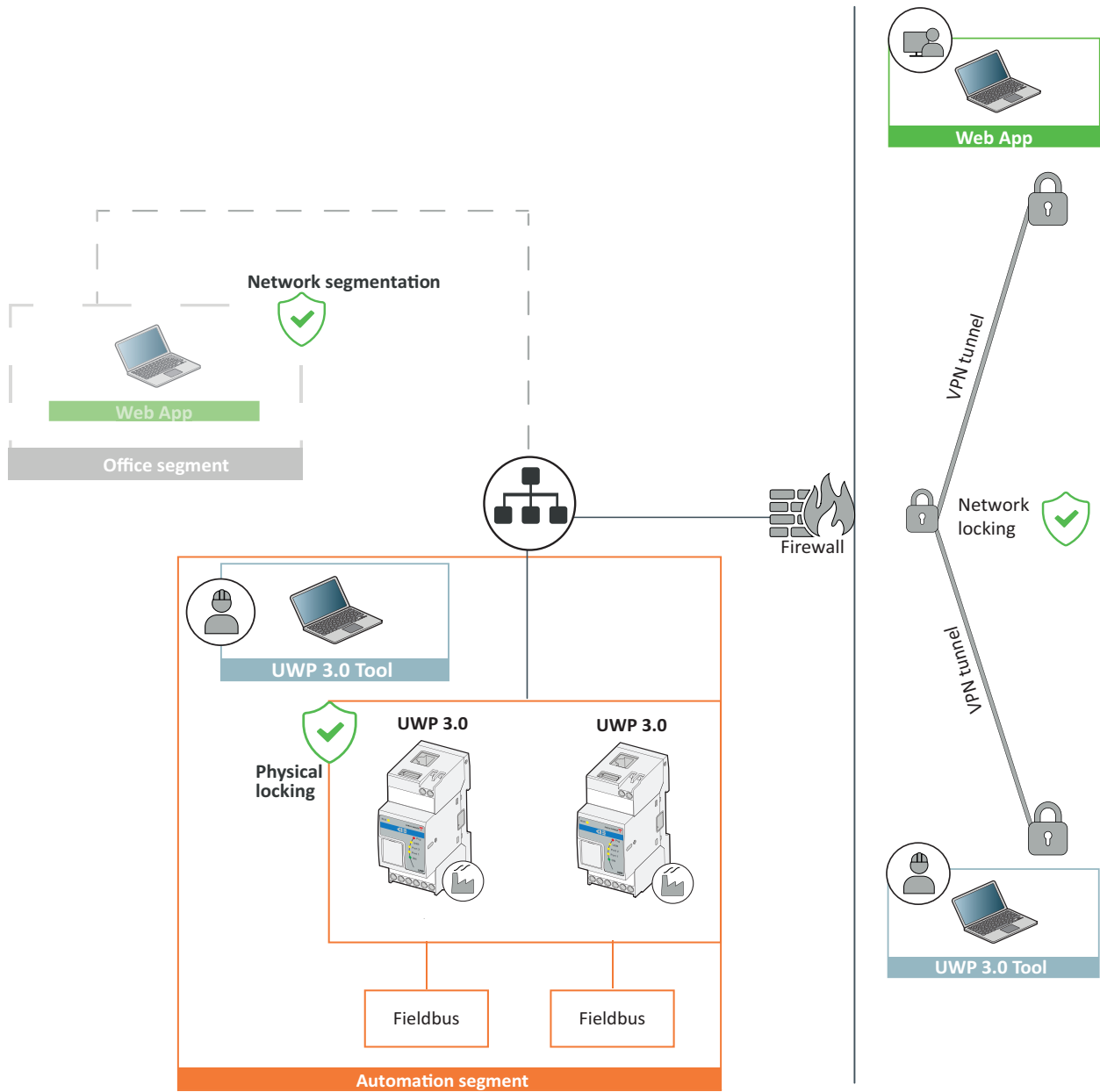
A protected environment is achievable thanks to the following measures:

- Physical locking. Locked cabinets with no chances of directly accessing the protected units.
- Managed LAN. The intranet network has well-defined user rights and no direct access from outside.
- VPN access. Internet access protected by a firewall and VPN tunnelling.

Moreover, the following additional practices are needed:

- **INDEPENDENCY.** Keep the trusted network as small as possible and independent from other networks.
- **FIELDBUS PROTECTION.** Protect the cross-communication of controllers and the communication among controllers and field devices via standard communication protocols (fieldbus systems) by appropriate measures. Very often, they are not protected by additional measures, such as encryption. An open physical or data access to fieldbus systems and their components is a serious security risk.
- **LOCKING.** Lock such networks and strictly separate them from commonly used access.

Architecture



Available security measures with UWP 3.0

As far as the cybersecurity of the UWP 3.0 ecosystem, our target as Carlo Gavazzi is to provide countermeasures to assist users and system integrators for protecting their system availability, integrity, and confidentiality. The UWP 3.0 architecture includes two main parts:

- the UWP 3.0 Tool software, aimed at setting-up and maintaining an UWP 3.0 based system
- the UWP 3.0 device, which includes the gateway/controller's hardware itself and its runtime.

Both parts operate together when setting up a system.

The following sections describe measures and features that are or will be available in the latest generation of UWP 3.0. In order to protect the application and the controller, the use of the latest version of the UWP 3.0 Software and Firmware is required. It can be downloaded for free at the Carlo Gavazzi Website. The tables below provide an overview on the measures, their zones within UWP 3.0, and for whom they are intended. Each measure is explained.

UWP 3.0 Tool (Software IDE)

Measure	Relevant for System Integrators	Relevant for End-Users	Valid against
Protected access to UWP 3.0 via UWP 3.0 Tool IDE	Yes		Occasional/unintentional threats and attacks
"Encryption and signature of the configuration code"	Yes		Intentional attacks
"Alerting for firmware/software update availability"	Yes		Occasional/unintentional threats and attacks
"Online IDE update"	Yes		Occasional/unintentional threats and attacks

Protected access to UWP 3.0 via UWP 3.0 Tool IDE

Measure for System Integrators

Access to the UWP 3.0 system via UWP 3.0 Tool can be restricted to specific user profiles. User rights over specific building automation functions can be profiled according to two separate levels.

Encryption and signature of the configuration code

Measure for System Integrators and End Users

The configuration set-up by using the UWP 3.0 Tool IDE, is signed and encrypted to preserve authenticity and contents.

Both UWP 3.0 Runtime and UWP 3.0 Tool check for available updates onto the Carlo Gavazzi servers. If any update is available, an alert is highlighted:

- Within the UWP 3.0 Tool interface
- Within the UWP 3.0 Web-App interface

By checking the alert's contents, both system integrators and end-user can check which security fixes are available in the updating package.

Note: it is responsibility of system integrator and end-user to decide how and when to deploy the software/firmware upgrade according to the relevant company policies.

Alerting for firmware/software update availability

Measure for System Integrators and End Users

Both UWP 3.0 Runtime and UWP 3.0 Tool check for available updates onto the Carlo Gavazzi servers.

If any update is available, an alert is highlighted:

- Within the UWP 3.0 Tool interface
- Within the UWP 3.0 Web-App interface

By checking the alert's contents, both system integrators and end-user can check which security fixes are available in the updating package.

Online IDE update

Measure for system Integrators

By leveraging the online update system of the UWP 3.0 Tool, the system integrator can easily upgrade both the IDE and the Runtime to the latest release.

Note: it is responsibility of the system integrator to check that the relevant application operation works as expected after the update task.

UWP 3.0 (Runtime)

Measure	Relevant for System Integrators	Relevant for End-Users	Valid against
“User administration”	Yes	Yes	Occasional/unintentional threats and attacks
Embedded API restricted access	Yes		Occasional threats and attacks
“Minimalistic approach (less is more)”	Yes	Yes	Occasional/unintentional threats and attacks
“Encryption and signature of the configuration code”	Yes		Intentional attacks
“Robust implementation of fieldbus communication”	Yes		Occasional/unintentional threats and attacks
“Protected Runtime update”	Yes	Yes	Intentional attacks
Granular user administration	Yes	Yes	Occasional/unintentional threats and attacks
Alerting for firmware/software update availability	Yes	Yes	Occasional/unintentional threats and attacks
VPN Access	Yes	Yes	Intentional attacks
Disaster recovery	Yes		Occasional/unintentional threats and attacks
Signed and encrypted backup file	Yes		Intentional attacks

User administration

Measure for System Integrators and End-Users

User access to the embedded web servers via the Web-App and the Car Park web access is possible only via authentication. Only passwords fulfilling security requirements are accepted. The embedded web-server accepts HTTPS connections for maximum security.

The embedded web-server is pen-tested periodically with updated tools to eventually implement the necessary patches against new vulnerabilities.

Embedded API restricted access

Measure for System Integrators

Access to embedded APIs (Rest-API and SOAP API) is possible only on authentication basis. After authentication a time-limited token is released to allow remote systems to interact with UWP 3.0.

Minimalistic approach (less is more)

Measure for System Integrators and End-Users

The UWP 3.0 firmware is based on Linux O.S. Carlo Gavazzi implemented its own distribution due to 2 reasons:

- Having full control over the whole system, so to implement more secure interfaces
- Having a minimalistic approach and implementing only the sub-systems and services needed by UWP 3.0 applications.

That's a way to avoid vulnerabilities that could leverage unnecessary subsystems/services to attack UWP 3.0.

Encrypted communication

Measure for System Integrators

All the embedded communication functions based on MQTT dialects are encrypted, and the relevant security is based on the updated policies of the target MQTT broker.

Both SFTP and FTPS encrypted protocols are available to implement secure communication based on FTP.

Note: it is responsibility of the system integrator to choose the most secure protocol among the available ones. UWP 3.0 includes also FTP for supporting legacy systems with no encryption available, but its use should be discouraged to prevent man-in-the-middle attacks.

Robust implementation of fieldbus communication

Measure for System Integrators

UWP 3.0 supports many different fieldbuses, including MODBUS/RTU, MODBUS/TCP, Dupline®, BACnet/IP, LoRa®. As Carlo Gavazzi we fully commit to provide cyber-secure systems. Nonetheless, system design choices have a big impact over the application's security. For example, using MODBUS/TCP over internet via an unprotected channel (no VPN) greatly increases cybersecurity risks, due to the open-nature of MODBUS itself.

By leveraging the online update system of the UWP 3.0 Tool, the system integrator can easily upgrade both the IDE and the Runtime to the latest release.

Note: it is responsibility of the system integrator to check that the relevant application operation works as expected after the update task.

Protected Runtime update

Measure for System Integrators and end-users

UWP 3.0 runtime is updated via the UWP 3.0 Tool IDE, so to guarantee better control over intentional/unintentional misconfiguration and firmware upgrades; it can be password-protected.

Granular user administration

Measure for System Integrators and End Users

A set of rules to control the access to different areas of the web-app to specific user profiles will allow strict control over user operation.

▶ Alerting for firmware/software update availability

Measure for System Integrators and End Users

Both UWP 3.0 Runtime and UWP 3.0 Tool check for available updates onto the Carlo Gavazzi servers.

If any update is available, an alert is highlighted:

- Within the UWP 3.0 Tool interface
- Within the UWP 3.0 Web-App interface

By checking the alert's contents, both system integrators and end-user can check which security fixes are available in the updating package.

▶ VPN Access

Measure for System Integrators and End Users

A VPN infrastructure is provided by Carlo Gavazzi to UWP 3.0 users, so to allow easy access to remote applications, via an authenticated, encrypted channel for either operation or set-up purposes.

▶ Disaster recovery

Measure for System Integrators

A disaster recovery procedure to backup and restore completely a working UWP 3.0 system is available within the UWP 3.0 Tool.

Note: it is responsibility of the system integrator to set-up the backup procedure according to the company policies and to restore the system according to the installation needs.

▶ Signed and encrypted backup file

Measure for System Integrators

Backup files are signed and encrypted to prevent any attempt of injecting malicious code by an attacker.

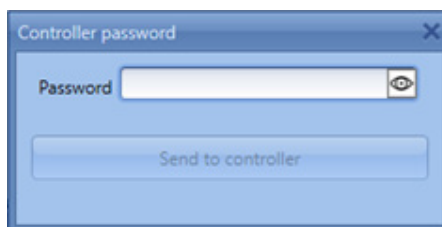
UWP 3.0 Tool and Web App: Password Management

UWP 3.0 TOOL

From the 8.3.5 version onwards, for cybersecurity reasons we added a new management of the communication between the UWP 3.0 Tool and controller so to guarantee the security of the information transmitted by the Tool to the controller and vice versa. In fact, these information are password-protected.
Note: the communication protection is total and mandatory.

First connection to the updated controller

After the controller upgrade to the new version, at your login you see a password input screen. For the first login, use the default password “admin” that you have then to replace with a stronger one.



Strong passwords should be at least 8 characters long and contain at least:

- one lower case character
- one upper case character
- one number
- one symbol (!, ?, @, ...)

Example: “Admin123!”

Once you have sent the new password to the controller, you will lose the connection with the controller and you will need to log in again with the new password.

Note: after every disconnection you will need to enter your password.

Changing your password

From the **Program Setup** panel, click **Password** enter your current password and the new (stronger) password.

Important note: if you lose your password, please contact Carlo Gavazzi.

Connecting to the controller versions earlier than 8.3.5

The connection between the UWP 3.0 Tool version 8.3.5 to the controller versions 8.3.3 - 8.3.5 is always possible. In that case, the Tool will connect to the controller using an unsecure connection and you will be able to update the controller.

Note: the connection has a timeout of 5 seconds that permits Tool to reach the controller in case of slow or congested network.

Compatibility with the old password

In the versions earlier than 8.3.4, the password protection was facultative and custom with the possibility of protecting the controller against some operations.

From the version 8.3.5 onwards, this operation is cancelled and completely replaced with the new password management.

When you update the controller to the 8.3.5 version, for the first connection to that controller you have to use the default password “admin”.

UWP 3.0 WEB APP

The password management in the UWP 3.0 Web App is the same except for the compatibility with the previously set password. In fact, in the Web App, if the old password is strong enough, it will be preserved. Otherwise, for your first login you will have to replace it with a stronger one.

UWP 3.0 SE is officially rated for Cybersecurity



IoT Security Capabilities Verified by the UL laboratories of Frankfurt, to Level Silver for UWP 3.0 SE (SE= Security Enhancement).

The silver rating certifies the enhanced security capabilities of UWP 3.0 SE regarding:

- Access control.
- Industry Privacy Best Practices.
- Product Security Maintenance.
- UWP 3.0 has been awarded with SILVER level IoT marking by the UL laboratories of Frankfurt.

Please find here the relevant notes: <https://ims.ul.com/iot-security-rating-levels>

Please find here the relevant certificate: <https://verify.ul.com/verifications/487>

Our commitment to cybersecurity

Cybersecurity is a process, not a product

Nowadays cyberthreats assume many different shapes: criminal cyberattacks, malware, social engineering. It is not possible to reach 100% cybersecurity, because of the multiple variables entering this game:

Vulnerabilities of products and systems

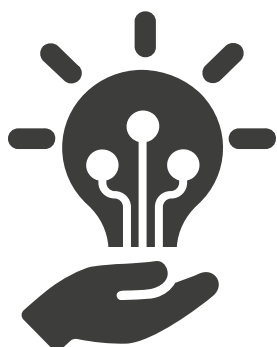
Wrong behaviours of users

Insufficient security policies

Increasing presence of hacking tools and unethical hackers

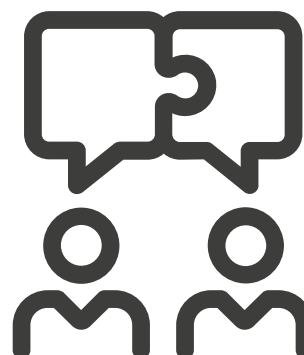
Cybersecurity is not only about devices: it is about people leveraging on social networks and habits. For those reasons while a company defines its approach to cybersecurity, the target is finding the right balance between the acceptable risks and the mandatory countermeasures.

The 4 pillars of cybersecurity in our company



Technology

We always use trusted technologies and best-in-class software and firmware stacks in all of our products



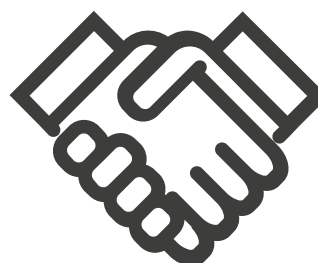
People

We allocated a Cybersecurity Team in our R&D, which undergoes a process of recurrent training to adopt best-practices for designing software and firmware, being updated about the evolution of cyber threats



Presence

Our organization is present in 23 Countries, and our products sold everywhere: we receive and collect tons of feedback that we use to improve and harden our products



Trust

We realize that nobody can fight cyberthreats alone. For this reason best in class cybersecurity labs are helping us in assessing the cybersecurity level in our products

OUR SALES NETWORK IN EUROPE

AUSTRIA

Carlo Gavazzi GmbH
Ketzergasse 374,
A-1230 Wien
Tel: +43 1 888 4112
Fax: +43 1 889 10 53
office@carlo gavazzi.at

BELGIUM

Carlo Gavazzi NV/SA
Mechelsesteenweg 311,
B-1800 Vilvoorde
Tel: +32 2 257 4120
Fax: +32 2 257 41 25
sales@carlo gavazzi.be

DENMARK

Carlo Gavazzi Handel A/S
Over Hadstenvej 40,
DK-8370 Hadsten
Tel: +45 89 60 6100
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@carlo gavazzi.fr

GERMANY

Carlo Gavazzi GmbH
Pfnorstr. 10-14
D-64293 Darmstadt
Tel: +49 6151 81000
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 1 276 854 110
Fax: +44 1 276 682 140
sales@carlo gavazzi.co.uk

ITALY

Carlo Gavazzi SpA
Via Milano 13,
I-20045 Lainate
Tel: +39 02 931 761
Fax: +39 02 931 763 01
info@gavazziacbu.it

NETHERLANDS

Carlo Gavazzi BV
Wijkermeerweg 23,
NL-1948 NT Beverwijk
Tel: +31 251 22 9345
Fax: +31 251 22 60 55
info@carlo gavazzi.nl

NORWAY

Carlo Gavazzi AS
Melkeveien 13,
N-3919 Porsgrunn
Tel: +47 35 93 0800
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 7060
Fax: +351 21 362 13 73
carlo gavazzi@carlo gavazzi.pt

SPAIN

Carlo Gavazzi SA
Avda. Iparraguirre, 80-82,
E-48940 Leioa (Bizkaia)
Tel: +34 94 480 4037
Fax: +34 94 431 6081
gavazzi@gavazzi.es

SWEDEN

Carlo Gavazzi AB
V:a Kyrkogatan 1,
S-652 24 Karlstad
Tel: +46 54 85 1125
Fax: +46 54 85 11 77
info@carlo gavazzi.se

SWITZERLAND

Carlo Gavazzi AG
Verkauf Schweiz/Vente Suisse
Sumpfstrasse 3,
CH-6312 Steinhausen
Tel: +41 41 747 4535
Fax: +41 41 740 45 40
info@carlo gavazzi.ch

OUR SALES NETWORK IN THE AMERICAS

USA

Carlo Gavazzi Inc.
750 Hastings Lane,
Buffalo Grove, IL 60089, USA
Tel: +1 847 465 6100
Fax: +1 847 465 7373
sales@carlo gavazzi.com

CANADA

Carlo Gavazzi Inc.
2660 Meadowvale Boulevard,
Mississauga, ON L5N 6M6, Canada
Tel: +1 905 542 0979
Fax: +1 905 542 22 48
gavazzi@carlo gavazzi.com

MEXICO

Carlo Gavazzi Mexico S.A. de C.V.
Circuito Puericultores 22, Ciudad
Satelite Naucalpan de Juarez, Edo
Mex. CP 53100 Mexico
T +52 55 5373 7042
F +52 55 5373 7042
mexicosales@carlo gavazzi.com

BRAZIL

Carlo Gavazzi Automação Ltda. Av.
Francisco Matarazzo, 1752
Conj 2108 - Barra Funda - São Paulo/
SP
Tel: +55 11 3052 0832
Fax: +55 11 3057 1753
info@carlo gavazzi.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@carlo gavazzi.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
sales@gavazzi-asia.com

CHINA

Carlo Gavazzi Automation
(China) Co. Ltd.
Unit 2308, 23/F.,
News Building, Block 1, 1002
Middle Shennan Zhong Road,
Shenzhen, China
Tel: +86 755 83699500
Fax: +86 755 83699300
sales@carlo gavazzi.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
Fax: +852 26261316

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 02 931 761
info@gavazziautomation.com



CARLO GAVAZZI
Automation Components

Energy to Components!

www.gavazziautomation.com

