CARLO GAVAZZI
Automation Components

CARLO GAVAZZI

White paper

VPN in operational technology

Secure remote access in building automation and energy monitoring applications

Alessio Costantini
International Product Manager

July 2021

CARLO GAVAZZI

VPN in operational technology. Secure remote access in building automation and energy monitoring applications.

ABSTRACT

This document aims at presenting system integrators, installers and operators of energy monitoring and building automation applications a solution to protect their remote access to the target system. The hereby proposed solution is a secure Virtual Private Network (henceforth VPN) tunnelling, described in the following chapters.

INTRODUCTION

Nowadays, the so called "Internet of things" (IoT) has become part of our society, transforming the way we work and consume. In recent years, the ubiquity of the IoT objects has exponentially grown from 2 billion in 2006 to a expected 200 billion by 2020. Energy monitoring and building automation systems are following this trend, with an increasing number of interconnections to the Internet. The need of remote connection for end-users and system integrators is almost mandatory. Typically, users want to control their devices from their smart phones, and system integrators prefer to connect from their of fice to their customers' plant for solving problems. This way, they avoid trip and consequently save time and money.

As is already well known, a system where end points are connected to network and each other through smart devices, cyberattacks risks - and in general cybersecurity issues - grow exponentially.

67% of the Global State of Information Security Safety 2018 (henceforth GSISS 2018) respondents have an IoT security strategy in place or are currently implementing one.

WHY DO WE NEED SECURE REMOTE CONNECTION SOLUTIONS?

Connection headaches	Very often, reaching a remote system placed behind a firewall or a router is a problem. With a NAT (Network Address Translation), the inbound traffic is blocked and/or the target address cannot be reached. Moreover, network operators use to frequently change the IP address on a specific connected SIM card. Due to security reasons, they are applying stricter rules for incoming traffic.
Avoiding expensive trips to the field	Digitalization plays a vital role especially after the coronavirus pandemic has brought many changes. Companies have been forced to find new ways of working, avoiding business trip and increasing the so called smart-working. This situation has raised awareness about cybersecurity issues and at the same time the needs to set up secure remote access.
A balance is needed	According to this scenario, network administrators have to balance the need to provide the access of remote devices and IoT to internal network, and the desire to lock their organization network. This balance is achiev- able with the VPN tunnelling.

DISCOVERING THE VPN

The VPN ("Virtual Private Network"), is the best choice to provide end-users and system integrators of end points with a secure remote access to smart phones, PC and IoT without threatening the network cybersecurity.

As mentioned before, the goal is to guarantee the interconnection among devices, from device to external and the access to devices from outside, without mining the IT security and the sensitive data protection. The wellknown Internet services are conceived to be accessed by everyone; the so-called "public network" servers and the sensitive data are subject of fraudulent users' intrusions.

The creation of a private network (VPN) permits isolating a company network by using an IP address unreachable via Internet, with restrictions permitting the access only from external authorized devices. Moreover, the private network can be extended beyond the public network with an encrypted virtual connection.

VPN ADVANTAGES

When accessing a remote location via Internet, the security of the connection includes:
a. Hardening the two endpoints (the target remote system and the user's PC).
b. Hardening the channel connecting the endpoints.
c. Setting up an adequate authentication procedure.

Notes:
- Point b and a are our target, because a VPN tunnel is a secure way to interconnect via Internet two endpoints with an encrypted channel and access control.
- Point c is out of the scope of this document.

These are the main strong points of a VPN:

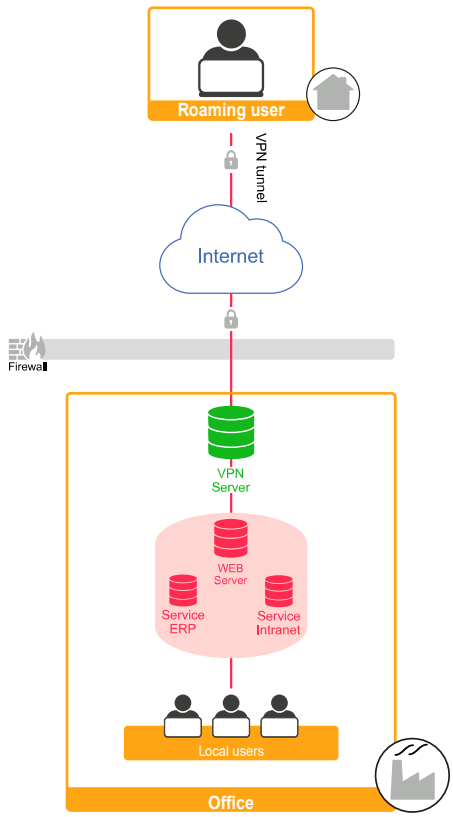
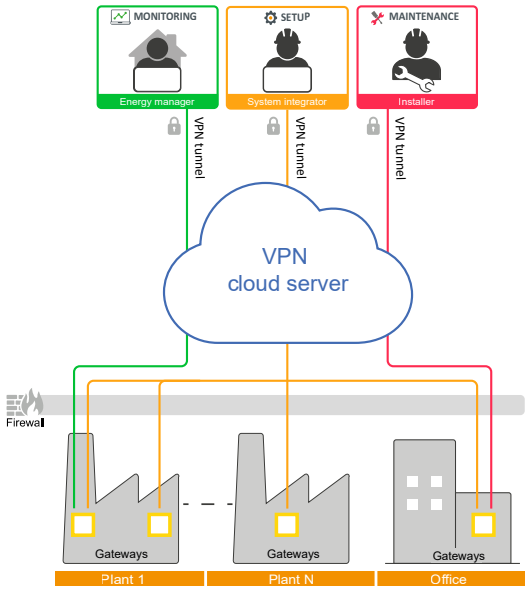
Easy to use	A VPN allows a seamless connection of different end points (field devices), to a centralized server (the Cloud*) through gateways (the EDGE).
System integrators and operators cost reduction	Thanks to a secure remote connection (VPN tunnelling), some problems can be solved without missions to the field. No trips, no costs!
Target system easily reachable	No NAT and firewall hassles. Thanks to the tunnelling techniqueand a trusted server in the middle, the channel to the target system is started by the target device itself
Less strict firewall rules and blocking polices	Since the connecting traffic is perceived like going to the Inter- net, it is easier to manage the relevant firewall rules. This way, it is also possible to avoid mobile/wired router connection hassles.
Protection against insecure Wi-Fi	Data encryption provided by the VPN allows to lock the communication channel

VPN IN COMPARISON

A VPN service can be used in different use cases:

- IT Case. Office is the most common example. VPN allows workers to access remotely to office network and use the relevant services and servers.
- OT (operation Technology) case like in energy monitoring and building automation: In this use case VPN allows users to access the endpoints (EDGE or FIELD devices) located in different plants, according to user's role. VPN Cloud Server allows users with specific permission to send commands to endpoints or monitoring and manage data remotely.

As shown in the architecture below, OT structure is more complex than IT.

IT CASE: OFFICE ROAMING USERS	OT CASE: BUILDING AUTOMATION
	

Different user's roles mean a system which manage the relevant permissions with authentication and safe connection channels. Multisite endpoints increase the system management complexity.

In this relatively simple OT case, 3 users are represented:

- **The Installer:** it is in charge of physically installing, commissioning and maintaining the system; he/she needs to remotely access the system for eventually check the system status in the case of failure
- **The System integrator:** he/she is in charge of configuring the whole system; he needs remote access to update configuration parameters or evolving the installation setup
- **The Energy Manager:** he/she needs to access the system to set-up the KPIs to be monitored and periodically check the energy consumption.

The OT case is typically affected by a higher level of complexity: it is quite common that the aforementioned users should access a set of different installations located in different places; the complexity of the system rises exponentially, and so the relevant costs: only remote access could help to control all the installation from a central location and avoid trip costs and organisational issues (i.e. matching agendas to be in the same place at the same time for updating the system).

CYBERSECURITY RESPONSIBILITIES IN ENERGY MONITORING AND BUILDING AUTOMATION INSTALLATION

RESPONSIBILITY BY ROLE

Several active parties and suppliers are involved in setting-up and operating an energy monitoring or building automation system:
- the suppliers of software and hardware components
- the system integrator or builder of the industrial control applications
- the operators.

All of the aforementioned parties have to make a certain effort in order to protect the application against attacks.

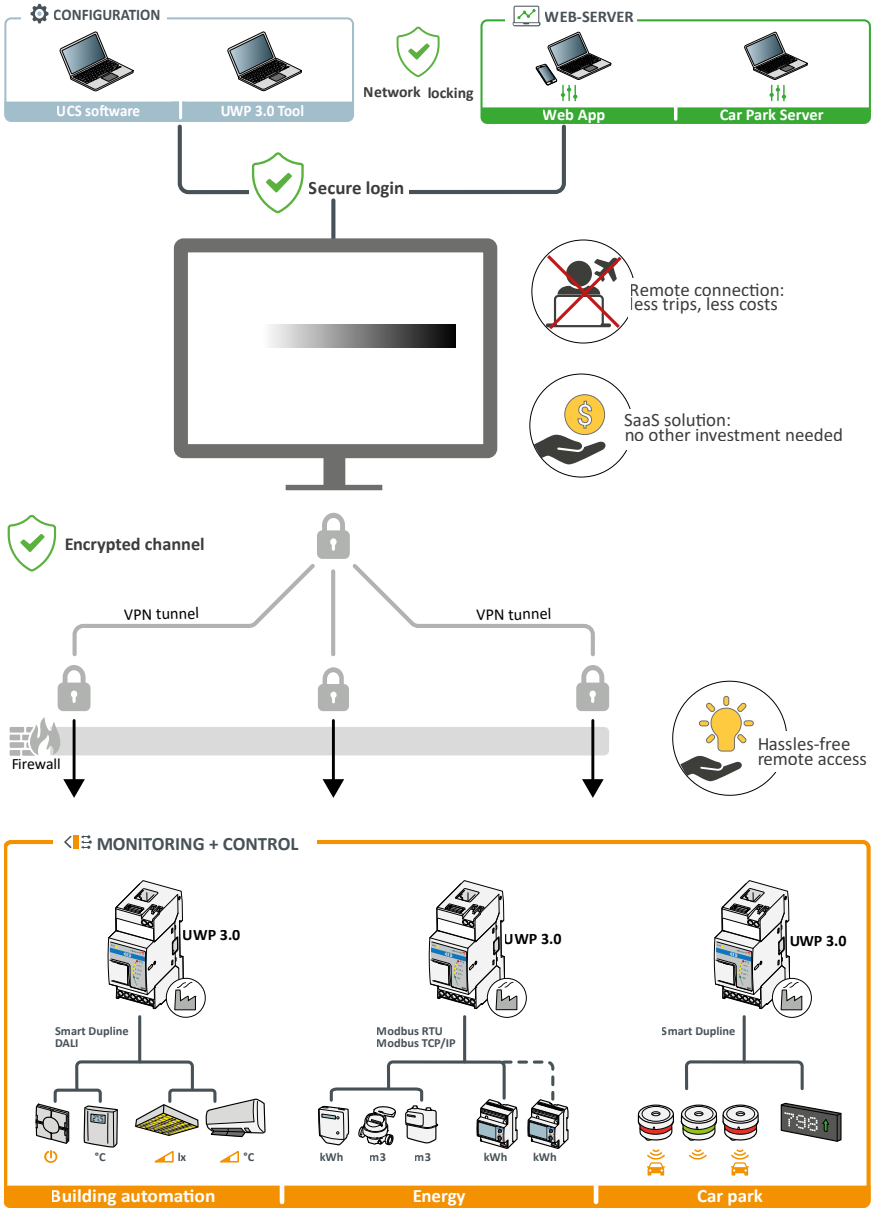
ROLE	RESPONSIBILITIES
Software Supplier	• Identify assets and analyse threats • Provide recognized security measures • Provide technical documentation
Device Supplier	• Identify assets and analyse threats • Develop software and hardware security measures • Provide technical documentation
System Integrator	• Identify assets and analyse threats • Implement provided software and hardware security measures • Implement system security measures • Provide technical documentation
End-user/operator	• Identify assets and analyse threats • Use available software and hardware security measures • Use available system security measures • Test/audit/certify the system • Provide updated trainings to involved people

A system is as secure as the weakest part: a lacking training to end-user could compromise the most secure installation.

Using a VPN tool can facilitate a lot of procedures, nonetheless it does not change roles and responsibilities: cybersecurity is the result of collective efforts of coordinated users. Nonetheless, by simplifying common actions, remote access tools allow users to focus their efforts in maintaining the system more often, so improving the overall cybersecusrity.

THE CARLO GAVAZZI SOLUTION

MAIA Cloud is a PaaS (Platform as a Service) solution that allows a seamless connection of different remote devices, through UWP 3.0 gateways, so to develop the necessary energy management and building automation solutions by connecting and setting the relevant items. Users who have access to the MAIA Cloud can easily reach the gateways and the endpoints, provided they have the necessary access rights, using a PC application called MAIA Cloud Connector.



- Secure remote login
- No other investments needed
- Cost reduction avoiding business trips
- Only a standard browser needed to register and login into Maia Cloud
- With Maia Cloud Connector it is possible to set up a remote access with UCS Desktop or UWP 3.0 Tool

Hassles-free remote access thanks to encrypted VPN channel

Ease of connection to gateway (UWP 3.0) or endpoints (CG energy meters or field devices)

By connecting to a centralized web portal, with a secure login, users can reach their fleet of UWP 3.0 items. Permissions for specific users or groups of users can be set by the organization administrator so to prevent any misuse. The VPN tunneling technology permits to set a secure encrypted channel between users and IoT devices; the authentication procedure secures the access to the portal endpoint.

THE 2 FURTHER USER ADVANTAGES OF MAIA VS. A COMMON VPN

BEST-IN-CLASS AUTHENTICATION

Maia's VPN tunnels are provided with best in class authentication:
users always need to authenticate themselves to a trusted portal for being able to access the system. The overall security of the authentication portal is maintained according to the last updates in cybersecurity best practices.

NO INVESTMENT AND EASE OF CONNECTION

While some VPN solutions need to buy, install, set-up and operate dedicate HW and SW, MAIA is based on a SaaS paradigm: you need only a web browser to connect and operate safely.

CONCLUSIONS

The security of systems in energy monitoring and building automation applications becomes increasingly critical as different networks are connected and systems are integrated. Accordingly, system integrators and users need to pay increased attention to these issues. Cyber-security is not a product, but a process, similar to functional safety. Reaching 100% cybersecurity is an impossible mission, nonetheless the analysis of risks,
be a mandatory part of any project. By allowing remote access, VPN tools help users to manage their process
easily, so to focus on the overall security and reliability of the system.

Notes

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@carlogavazzi.at

BELGIUM
Carlo Gavazzi NV/SA
Mechelsesteenweg 311,
B-1800 Vilvoorde
Tel: +32 2 257 4120
Fax: +32 2 257 41 25
sales@carlogavazzi.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@carlogavazzi.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@carlogavazzi.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@carlogavazzi.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
carlogavazzi@carlogavazzi.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@carlogavazzi.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@carlogavazzi.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@carlogavazzi.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@carlogavazzi.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@carlogavazzi.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@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,
Shenzhen, China
Tel: +86 755 83699500
Fax: +86 755 83699300
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

OUR COMPETENCE CENTRES AND PRODUCTION SITES

DENMARK
Carlo Gavazzi Industri A/S
Hadsten

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

MALTA
Carlo Gavazzi Ltd
Zejtun

ITALY
Carlo Gavazzi Controls SpA
Belluno

LITHUANIA
Uab Carlo Gavazzi Industri Kaunas
Kaunas

HEADQUARTERS

Carlo Gavazzi Automation SpA
Via Milano, 13
I-20045 - Lainate (MI) - ITALY
Tel: +39 02 931 761
info@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 VPN in operational technology ENG REV.00 07/21