Fr. SAUTER AG

Cybersecurity Guideline

SAUTER modulo 6

Im Surinam 55
4016 Basel
Schweiz
Tel.: +41 61 – 695 55 55
Fax: +41 61 – 695 55 10
www.sauter-controls.com
info@sauter-controls.com

Document number: D100529003
Revision: 03
Version: 01
Released: 01.09.2026

Change History

Date	Rev.Ver	Changes
13.11.2024	1.1	Initial revision
10.04.2025	2.1	Release
31.08.2026	3.1	Update Portfolio, Firmware enhancements motivated by CSPN, CRA

Products

At the time of release of this document revision and version (Rev. 03, Ver. 01 Release Date 01.09.2026), modulo 6 included the following products and references:

Product	Reference	Description
modu680-AS	EY6AS80F021, EY6AS80F022	BACnet Building Controller
modu660-AS	EY6AS60F011, EY6AS60F012	BACnet Building Controller
modu630-RT	EY6RT30F001	BACnet Router, BACnet/IP BBMD and BACnet/SC Hub
modu612-LC	EY6LC12F011, EY6LC12F012	IP-Coupler
modu6**-IO	EY6IO**F001	I/O-modules for AS, LC products
modu6**-CM	EY6CM**F001	COM-modules for AS, LC products
modu600-LO	EY6LO00F001	Local Operation and Indication device for I/O-modules

Tab. 1: Table of products included in modulo 6 portfolio

Product	Content	Version
modu6**-AS, modu612-LC	Firmware	4.0.0
modu6**-AS, modu612-LC	moduWeb Unity	4.0.0
modu6**-AS, modu612-LC	Mobile App (iOS, Android)	3.3 .0.70
modu630-RT	Firmware	1.2.0

Tab. 2: Product content versions

1 Table of contents

2 Foreword

In today's fast-paced digital landscape, building automation has become a cornerstone of modern living—driving comfort, efficiency, and sustainability in our offices, buildings and cities. As this technology becomes ever more intertwined with our daily routines, its security is no longer optional—it's essential.

We are witnessing a growing convergence between building automation and traditional IT. Modern automation systems rely heavily on established IT technologies and infrastructures to enable seamless communication between system automation, room control, and building management and ultimately the Internet and its services. These technologies are the backbone of intelligent, energy-efficient, and interoperable buildings.

But with this progress comes responsibility. Because building automation now leverages the same technologies as conventional IT systems, it must also meet the same high standards of cybersecurity. To protect what we build, we must secure it like we secure our networks—proactively, thoroughly, and continuously.

This Cybersecurity Guideline is a concise and practical resource aimed at providing clear directives to enhance the cybersecurity posture of building automation stations.

As technology continues to advance, so do the potential risks associated with interconnected systems. This guideline summarises key principles and best practices, offering a straightforward approach to improving the security of building automation. It is intended to be a user-friendly tool for system administrators and stakeholders, providing actionable steps to mitigate cybersecurity threats.

SAUTER understands the need for simplicity when navigating the complexities of cybersecurity. This document should not be seen as a static rulebook but a dynamic guide that adapts to emerging threats. Just like in conventional IT, cybersecurity in building automation is not a one-time effort—it must adapt continuously. Threats and technologies change rapidly, and to remain resilient, security measures must be regularly updated, kept state-of-the-art, and adapted to new risks, system architectures, and operational requirements. By adhering to the guidelines outlined here, we can contribute to a more secure and resilient environment for building automation.

SAUTER appreciates the collaborative efforts of the professionals who contributed to the development of this guideline. May it serve as a practical companion in the ongoing mission to safeguard our interconnected spaces.

2.1 To whom this document is intended (Target audience)

This document is intended for a large yet professional audience of building automation stakeholders. The recommendations shall be considered already in the planning phase, as they may impact the architecture. The recommendations remain valid all along the deployment of the solution as well as during the use of it until the installation is dismantled at the end of its life cycle. Hence, the intended audience reaches out to:

Audience Group	Expectations
Sales technicians	To identify the requirements for the targeted security level (SL-T) and make the appropriate offering, the sales team must know what the products are capable of (SL-C), what are additional requirements to be provided by the environment and what possible mitigation measures can be suggested.
Planners	In close cooperation with the sales team, the planners must know what the products can offer by themselves and what must be solved with additional products, different concepts or organisational measures.
Installation and commissioning technicians	Technicians need to know what must effectively be done to attain the expected security level given the capabilities of the products. They are concerned with the initial and final phases of the product life cycle.
Owners and users	The most important actors during the operational phase shall know the capabilities of the products as well as their appropriate behaviour. This must be enforced with appropriate policies.
Maintenance technicians	Also, during the operation phase maintenance operations must be executed accurately to avoid the generation of new opportunities for cyber-attacks.

Tab. 3: Audience Group and their expectations

2.2 Related SAUTER documents

Document title	Reference	Language	Rev./Ver.
Product Data Sheet modu680-AS	D100380476	EN	13/1
Product Data Sheet modu660-AS	D100380662	EN	8/1
Product Data Sheet modu612-LC	D100380644	EN	5/1
Product Data Sheet modu630-RT	D100445236	EN	5/1
modulo 6 System description	D100402674	EN	7/1

Tab. 4: Related documents

3 Disclaimer

The following **Cybersecurity Guideline for SAUTER modulo 6** has been written to assist users in enhancing the security of building automation when using this product line. It is important to note that while this guide provides recommendations and best practices, it does not guarantee absolute immunity from cyber threats or attacks. Users are advised to use their judgment or seek professional assessment and implement additional security measures as deemed necessary based on their specific environment and requirements.

The cybersecurity guidance provided herein is intended as a general resource and may not cover all potential vulnerabilities or risks. Users are encouraged to stay abreast of emerging threats and regularly update their cybersecurity measures accordingly.

Building automation applications can vary widely in their configurations, integrations, and deployment scenarios. Users are responsible for customising and adapting cybersecurity policies to the unique aspects of their systems. Therefore, an individual risk assessment for the building automation is recommended.

Cybersecurity threats evolve and new vulnerabilities may emerge. It is essential that users establish a continuous monitoring programme and regularly update their security measures to address emerging threats.

Building automation applications often rely on third-party components and integrations. Users should be aware that the cybersecurity of their systems may be affected by the security practices of these third parties. It is recommended that users check and select trustworthy partners and regularly assess the security situation of integrated components.

In addition to the cybersecurity efforts of used and configured building automation hardware and software, and although the Cybersecurity Guideline aims to mitigate risk and enhance security, it is impossible to guarantee absolute security. Users must understand the dynamic nature of cyber threats and recognise that no system can be completely immune to attack.

Users are ultimately responsible for the security of their building automation applications. This includes implementing recommended cybersecurity measures, staying informed about security best practices, and promptly addressing identified vulnerabilities.

Users who lack expertise in cybersecurity are strongly encouraged to seek assistance from qualified security professionals. Consultation with experts can help ensure the effective implementation of security measures and the development of a robust cybersecurity strategy.

This Cybersecurity Guideline is subject to updates and revisions. Users are encouraged to regularly check for the latest version and incorporate any new recommendations or best practices into their security protocols.

By implementing the cybersecurity guidelines provided, users can improve the security posture of their building automation applications. However, users should remain vigilant, continually assess their security measures and be prepared to adapt to the evolving threat landscape.

4 Security context

4.1 Cybersecurity for Building Automation: Context

Building automation consists of automated solutions to control and monitor the systems used within a building to provide different types of services such as heating, ventilation, air conditioning, water management and more. These primary services have now been extended to include many others such as lighting control, occupancy detection, fire and life safety systems, access control, etc. The primary goal of automation is to improve efficiency and comfort for users while controlling energy and resource consumption to optimise costs for the owners.

Building automation is primarily found in commercial buildings, ranging from office buildings, hotels, shopping centres, residential and healthcare buildings, etc., but also all types of public buildings from museums, schools, universities, and in general any type of large building where centralised operation and management of large primary systems make sense. As part of a primary service, building automation systems are part of the underlying infrastructure of the building and are not intended to be directly accessible by the average user of the concerned building and its reach is not intended to go beyond the building.

Building automation can therefore be considered part of operational technology (OT). Its components are expected to be:

- in areas of restricted access, i.e. technical rooms with closed doors
- in electrical cabinets or closed enclosures

connected to an exclusive internetwork, not accessible to the public.

With the advent of cloud technologies, the Internet of Things (IoT) and the general vision of smart buildings and cities, self-contained solutions become unrealistic and the interconnectivity of building automation with other networks is self-evident. Hence, appropriate measures must be taken to properly isolate and protect the building automation network from unauthorised access by setting up technical solutions (Firewalls, DMZ, IDS, IPS, PNAC, …) and policies.

Depending on the reach of the building automation solution, the impact of a security incident can range from simple discomfort to operational disruption with worse consequences. The deeper the integration, the larger the damage potential. For example, if the parking is equipped with car presence detectors and a place can be assigned to a particular person, then the presence or absence of the person can be inferred. The same applies to the presence detection in a particular bureau. This kind of information can be misused.

4.2 BACnet

BACnet stands for Building Automation and Control Network, an ASHRAE/ISO standard that has become the standard as the backbone protocol for building automation (BSRIA, 2023).

BACnet focuses on interoperability, i.e. the easy exchange of data between BACnet devices, servers- and/or clients. BACnet also supports different physical layers (OSI model) and the corresponding data links, e.g. BACnet/SC, BACnet/IP, BACnet MS/TP, etc.

As the primary protocol, BACnet supports the internetworking of different BACnet subnetworks, either using BACnet-specific routers or BACnet functions such as BBMD (BACnet Broadcast Management Device) or FD (Foreign Device). The networks to be interconnected must both be protected zones and use a secure infrastructure (to be provided).

While BACnet/IP (which is based on UDP) is in fact the most widely used data link used in non-residential buildings, the latest developments in this ISO standard include BACnet Secure Connect (BACnet/SC) which aligns with common IT technologies like TCP, WebSockets and TLS v1.3 for data encryption and mutual authentication. This major step forward is clearly aimed at cybersecurity.

4.3 Product security context

4.3.1 Intended location in network(s)

The image below is a synthetic representation of the location in the networks of modulo 6 automation devices.

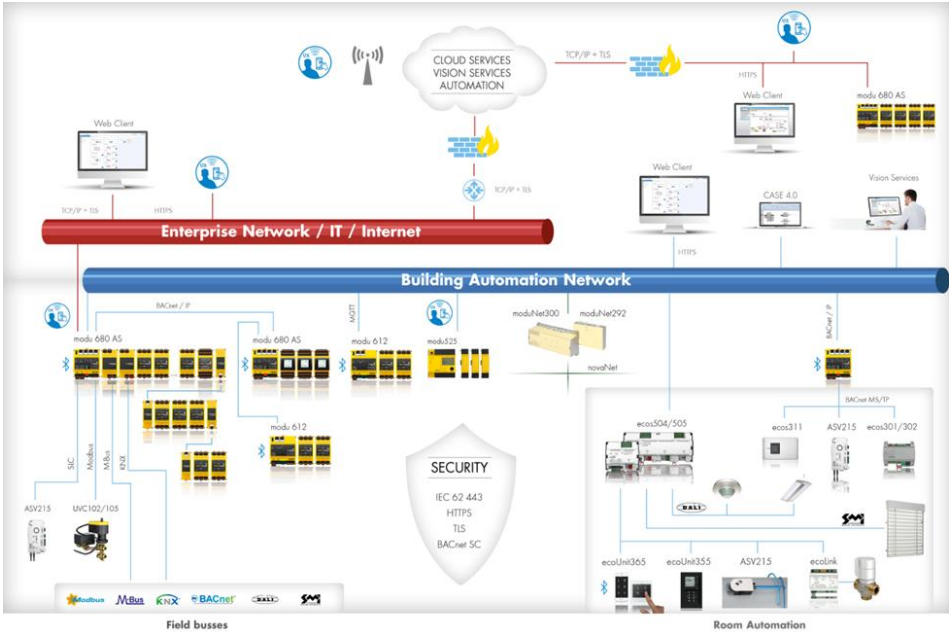

Figure 1:Building Automation Network

Building Automation Networks are located in individual Buildings (on premises) and rarely across neighbouring Buildings. Only dedicated services (e.g. BMS, ERP) may be cloud-based. Some external services may require outbound connections (e.g. time-server, weather forecast, e-mail provider).

Building Automation Networks are very often dedicated exclusively to this purpose, although it can be shared among different providers (multi-vendor installations).

Regarding the connectivity modulo 6 devices are equipped as follows:

modu680-AS and modu630-RT are equipped with 4 Ethernet connections.

- (1) WAN connection for uplink communication with standard, secured protocols, e.g. HTTPS
- (3) LAN connection (switch) for the building automation network. This shall prefer-ably be a dedicated network for this purpose only.

modu660-AS and modu612-LC are equipped with two Ethernet connections

- (2) LAN connection (switch) for the building automation network. This shall preferably be a dedicated network for this purpose only.

4.3.2 Security provided by the environment

Physical

modulo 6 Building Automation devices are designed for installation in electrical cabinets with physically locked doors. Some general-purpose switches or buttons may be mounted on the door, as well as a control panel.

modulo 6 Building Automation devices and their enclosures are mainly on the primary (production) side of the installation and are therefore assumed to be located in dedicated, locked spaces, e.g. enclosed plant rooms with locked doors and restricted access to qualified personnel only.

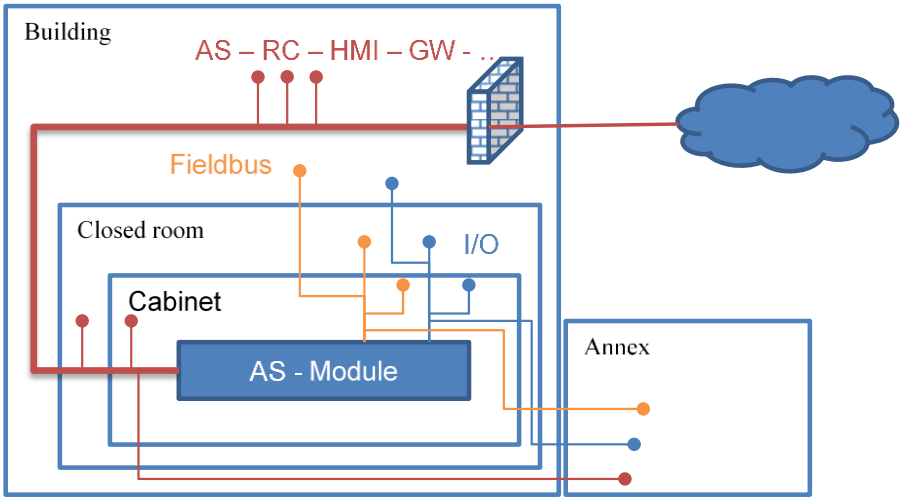

Figure 2:Schematic representation of Network, fieldbus, and IO connections.

The modulo 6 devices (Automation Stations, IO-Modules, CM-Modules, …) are installed in an electrical cabinet, which should be locked with a key. The cabinet itself is in the building's technical room, also locked with a key or equivalent means.

Individual signals (analogue or digital, depicted in blue) are wired either within the cabinet, outside the cabinet and outside the room, within the building. Some signals may come from an annex building or from a system directly attached to the outer shell of the building. The same applies to the field-busses (depicted in orange). Finally, the IP connections (depicted in red) follow the same scheme but may be connected to the internet to access some form of cloud service or be accessed.

Depending on the exposure, mitigation measures shall be implemented. For example, the internet connection requires a firewall and other measures, but also the connection to the annex building is clearly exposed. Also, if the BA Network shares the infrastructure with the IT, then the network shall be properly managed, with VLANs and similar solutions etc.

Technical Network

Network infrastructure is not part of the modulo 6 portfolio but remains an integral component of its operational environment. In most cases, HVAC will get a dedicated Network (physical and/or logically separated), like an OT-Network. In some cases, Internet access for particular use cases (e.g. accessing external cloud services, providing access from the outside to particular services or information, …) may be required.

Beyond the cybersecurity measures specific to this infrastructure—such as firewalls, IDPS, and SIEM—modulo 6 can enhance security through seamless integration. For instance, modulo 6 devices support IEEE 802.1X

port-based network access control using RADIUS. modulo 6 devices can be configured as supplicants for each Ethernet interface individually, offering support for multiple EAP variants.

modulo 6 devices have their own firewall, meaning that only the required ports are open.

Network infrastructure can close ports other than:

WAN Interface (modu680-AS)

Protocol/Service	Port	Type	Direction
HTTPS (moduWeb Unity, API)	443	TCP	Inbound
HTTPS (Meteomodule)	443	TCP	Outbound
SMTP (moduWeb Unity)	25	TCP	Outbound
SMPP (moduWeb Unity)	2775	TCP	Outbound
SFTP (moduWeb Unity)	22	TCP	Outbound
MQTT/TCP	Configurable	TCP	Both
MQTT/WSS	Configurable	TCP	Both
RADIUS	1812/1813	TCP	Outbound
NTP (if configured)	123	UDP	Outbound

Tab. 5: Supported protocols over the WAN interface

LAN Interface

Protocol/Service	Port	Type	Direction
HTTPS (moduWeb Unity, API)	443	TCP	Inbound
HTTPS (Meteomodule)	443	TCP	Outbound
* HTTPS (MQTT CT)	9879	TCP	Inbound
SMTP (moduWeb Unity)	465/587/25	TCP	Outbound
SMPP (moduWeb Unity)	2775	TCP	Outbound
SFTP (moduWeb Unity)	22	TCP	Outbound
MQTT/TCP	Configurable	TCP	Both
MQTT/WSS	Configurable	TCP	Both
* mDNS	5353	UDP	Outbound (local-link multicast)
* CASE Sun (WSC)	5627	TCP	Both
* License Manager	44444	TCP	Outbound

Protocol/Service	Port	Type	Direction
BACnet/SC	Configurable	TCP	Node: Outbound Hub: Inbound
BACnet/IP	47808…23	UDP	Both
* VPorts	21002…7	TCP	Outbound
modu612-LC ←→modu6*-AS	16443	TCP	Both
RADIUS	1812/1813	TCP	Outbound
NTP (if configured)	123	UDP	Outbound

*Tab. 6: Supported protocols over the LAN interface. Entries starting with * are used only temporarily during configuration (Service-mode).*

Furthermore, SAUTER stations are equipped with a reverse proxy, exposing only a secured inbound interface.

Bluetooth

The Bluetooth connection is intended for commissioning and maintenance operations for use with the dedicated SAUTER modulo 6 mobile app. It is protected with username and password as defined over moduWeb Unity.

Network protocols

modulo 6 automation station's primary function as BACnet Building Controller relies on the use of the BACnet Protocol (ISO 16484-5).

- BACnet/IP (UDP)
  As a technical data link, it is unencrypted and therefore shall never be accessible from external networks. To communicate across sub-networks, a device supporting BBMD is required or BACnet/IP specific routers.
- BACnet/SC (TCP + TLS 1.3)
  BACnet/SC is a newer data link supporting encryption natively. It prescribes a hub-and-spoke topology with mutual authentication. Standard nodes start connections (outbound) with the hub (inbound).

  Other protocols are used and supported, either in the installation phase (mDNS, SOAP, HTTPS) or in the operational phase (HTTPS, SFTP, SMTP, SMPP, …).

Isolation from networks

BACnet communication is only supported over the LAN interface. This interface should never be connected to open networks (IT, Internet). When nevertheless required, the adequate mitigation measures shall be taken:

- Firewall

- VLAN
- IDS/IPS
- DMZ
- PNAC
- …

Network segmentation

Network segmentation is recommended.

- Have a dedicated (sub-)network for building automation
- In large projects, have sub-networks (VLAN) and use the appropriate means when intercommunication is needed (BBMD, router)
- Use WAN if moduWeb Unity access is required from the IT side
- Use WAN if external services are required (email ,Meteomodul, SAUTER Cloud, Vision Services, …).

Potential impact of a security incident

modulo 6 devices, in particular the automation stations, are Linux-based programmable controllers intended for HVAC and building automation applications. Therefore, the impact described here is reduced to this scope. Nevertheless, it cannot be excluded that in the hypothetical case of an attack, the consequences go beyond the HVAC application, particularly if networks are not properly segmented and protected.

The impact of security incidents described here is directly related to the specific implementation done with modulo 6 (scope).

Potential impact of a security incident in a HVAC installation:

- Interruption of service. A security incident that affects the equipment to the point that it is no longer operational could have the following effects:
  - Controlled systems not operating or operating in a degraded mode. This primarily affects the production of heat, ventilation and air conditioning.
  - Systems relying on HVAC may have to work in a degraded mode or stop working completely.
  - Damage to property or persons due to malfunction caused by the incident.
  - Access to embedded BMS data. Interruption of alarm and reporting functions.
  - Discomfort for the users.
- Access. A security incident that prevents access to the device, although it still fulfils its primary function, could be:
  - Access to the BMS. Access to the control HMI. Access to historical data.
  - Access to the system, preventing the rollout of firmware updates.

- Cost. A security incident can result in additional costs:
  - To counter the incident. Professional support and/or ransom.
  - To compensate for the damage
  - Caused by incorrect operation
  - Loss of data (PII or operational)
  - Penalties
- Reputation. A security incident becomes public and damages reputation

To minimize the impact of threats, it is recommended to follow the security operation guidelines in chapter 6, the security hardening guidelines in chapter 7 and secure disposal guidelines in chapter 9. Instructions how to submit security issue are described in chapter 8.

4.4 Regulatory Constraints

The regulatory framework can have an impact on the cybersecurity requirements of a particular installation. For example, the European Union has updated the NIS-2 Directive [1], extended the RED directive and released a new CRA (Cyber Resilience Act [2]). While the RED Delegated Act (RED DA [3]) introduces cybersecurity requirements for specified classes of radio equipment, it is the CRA which has a major impact on products like modulo 6 controllers. These regulatory constraints have an impact on conformity assessment and CE marking for products placed on the EU market.

Other regulation can have an impact on the use of the products. For example, the NIS 2 distinguishes between essential and important entities; covered sectors are listed in Annexes I and II. In addition, Article 21 of the Directive lists a number of recommendations, ranging from technical to organisational.

Other countries are likely to have similar requirements (PSTI in the UK, FISMA in the USA, ...) which must be considered accordingly.

By complying with IEC 62443-4-1 and other standards, SAUTER develops products including security measures by design.

4.5 Defence in depth approach

Defence in depth is an approach to defend the system against any particular attack using several independent methods. It implies layers of security and detection, even on single systems, and provides the following features:

- is based on the idea that any one layer of protection, may and probably will be defeated
- attackers are faced with breaking through or bypassing each layer without being detected
- a flaw in one layer can be mitigated by capabilities in other layers

- system security becomes a set of layers within the overall network security - and -
- each layer should be autonomous and not rely on the same functionality nor have the same failure modes as the other layers.

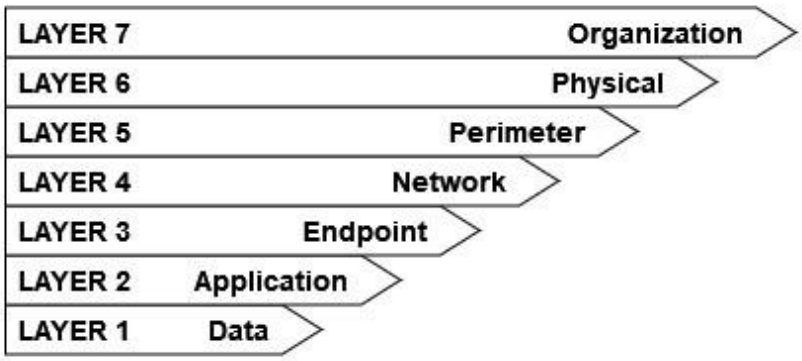

Figure. 3: Layers of defence in depth

Organisation layer focuses, among others, on establishing policies, procedures, and governance frameworks to support and enforce security measures across all layers of an organisation's infrastructure, systems, and operations.

Physical security layer primarily focuses on protecting physical assets, such as control systems, industrial equipment, and facilities from unauthorised access, tampering, or damage.

Perimeter security layer focuses on protecting the boundaries of the industrial control system network from external threats. This layer acts as the first line of defence against unauthorised access, malicious attacks, and other security risks.

Network layer focuses on protecting the communication infrastructure and data flows from various cyber threats and vulnerabilities.

Endpoint layer focuses on protecting individual devices, such as computers, servers, industrial controllers, and other endpoints from various cyber threats and vulnerabilities.

Application layer focuses on securing the software applications and services that are used within devices. This layer aims to protect against vulnerabilities and threats that target the functionality and behaviour of these applications.

Data layer focuses on safeguarding the integrity, confidentiality, and availability of data within devices. This layer aims to protect sensitive information from unauthorised access, tampering, or disclosure.

This approach cannot be realised at product level alone but requires both technical and organisational measures at different levels.

5 Secure installation guidelines

This section provides guidelines for installation of product in secure intended environment.

5.1 Recommendations for intended location

modulo 6 Building Automation devices are designed for installation in electrical cabinets with physically locked doors. Some general-purpose switches or buttons may be mounted on the door, as well as a control panel.

modulo 6 Building Automation devices and their enclosures are mainly on the primary side of the installation and are therefore assumed to be installed in dedicated, locked spaces, e.g. enclosed plant rooms with locked doors and restricted access to qualified personnel only.

Depending on the risk evaluation made for a particular installation, the following recommendations may be relevant.

Access Control

- Implement strict access control measures to limit physical access to the area where the security device is located
- Use physical barriers such as fences, gates, and locks to control entry points
- Consider implementing biometric access control systems or key card access systems for authorised personnel
- Reduce the authorised personnel that can access the concerned area
- Besides the physical access, take care of the handling of credentials providing physical (e.g. keys) or logical (e.g. passwords) access. Apply “least functionality” and “need-to-know” criteria to assign rights, and apply hardening policies (2FA, password strength & complexity, auto logout, limited validity, …)

Surveillance

- Install surveillance cameras to monitor the area around the security device
- Ensure adequate lighting to enhance visibility, especially during non-business hours
- Regularly review surveillance footage to detect any suspicious activities or security breaches

Environmental Controls

- Ensure the physical environment is suitable for the security device's operation, free from hazards such as excessive heat, humidity, dust, or vibration
- Use environmental monitoring systems to detect and alert personnel to any environmental anomalies that could affect the device's performance

Tamper Detection

- Implement tamper-evident seals or enclosures to detect unauthorised access or tampering attempts
- Use intrusion detection sensors to detect any physical tampering or unauthorised entry into the area
- Enforce a clear visitor management policy, requiring all visitors to sign in and be escorted while in the area

Additional checks

- Frequent inspections or security checks by maintenance
- Physical tests if access to device is limited only to authorised persons

5.2 Recommendations for connection to external devices (e.g. power supply, other logic modules, sensors, etc.)

Redundancy and Resilience

- Implement redundant power supplies and backup systems (UPS) to ensure continuous operation of the security device in the event of power outages or equipment failures
- Regularly test backup systems and emergency procedures to ensure they are functioning correctly

Remote[1] Monitoring and Management:

- Implement remote monitoring and management capabilities to allow security personnel to monitor status of device and respond to any alerts or incidents remotely
- Use remote access technologies to perform maintenance tasks and software updates without the need for physical access to the device

Recommendations for network connection

Stand-alone (see Figure 4, p. 23):

[1] Remote access, in particular over the Internet, has further implications regarding the organisational and technical cybersecurity requirements.

- The preferred topology is an Ethernet network for building automation purposes only, isolated from another network both logically and physically. Likely, field buses are only for building automation purposes. With regards to BACnet, a combination of internetworks is supported, but requires dedicated solutions, for example, BBMD or FD in BACnet/IP-based solutions.

Interconnected Networks (LAN, VLAN) (see Figure 5, p. 23):

- Segment the LAN into smaller VLANs based on premise, function, or security requirements
- use BACnet BBMD or BACnet routers
- configure routing table where appropriate
- be aware of communication restrictions across sub-networks, that may be restricted by firewalls, DMZ, etc.

Connection to or through trusted networks (see Figure 6, p. 24):

- Deploy IDPS solutions to monitor network traffic for signs of suspicious activity or potential security breaches
- Configure IDPS to alert administrators or automatically block malicious traffic
- Use VPNs when the underlying network is untrusted.
- Implement port-based authentication, e.g. using IEEE 802.1X to ensure that only authorised devices can access the network. This can be integrated with a RADIUS server for centralised authentication

Connection to or through untrusted networks (see Figure. 7, p. 25):

- Enable the firewall on your device to block unauthorised incoming connections and control outgoing traffic
- Configure the firewall to restrict access to specific applications and services, allowing only necessary communication
- Use BACnet Secure Connect (a.k.a BACnet/SC) encrypted communication instead of BACnet/IP when possible. Use a failover BACnet Secure Connect Hub for redundancy of the hub functionality
- Use secure communication protocols such as HTTPS for web browsing, SFTP for file transfers
- Avoid using insecure protocols like HTTP or FTP, which can expose your data to interception and manipulation
- Install and regularly update reputable antivirus and anti-malware software on your devices (where applicable) to detect and remove malicious software that may be encountered on untrusted networks

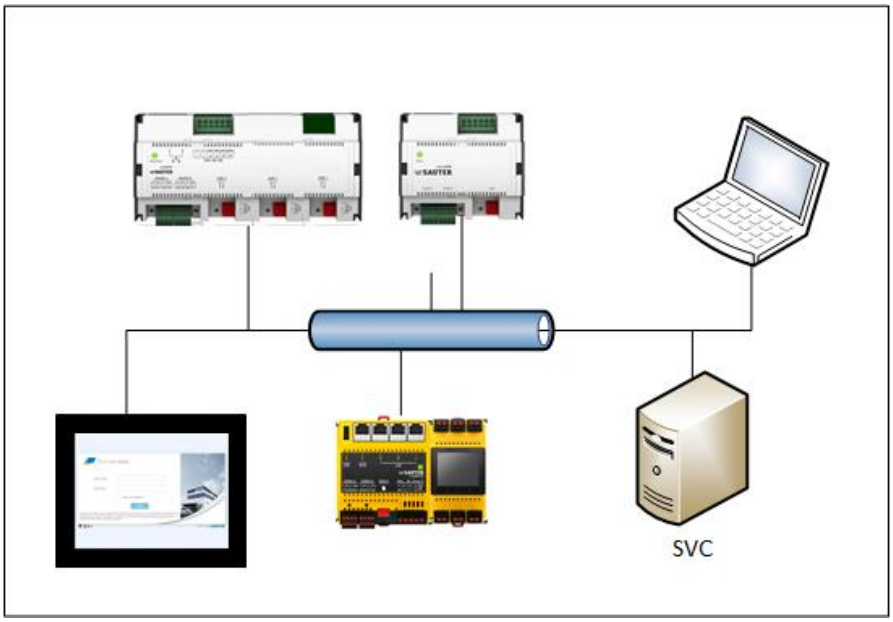

Figure 4:Simplest topology: Stand-alone, On-premises w/o internet connection.

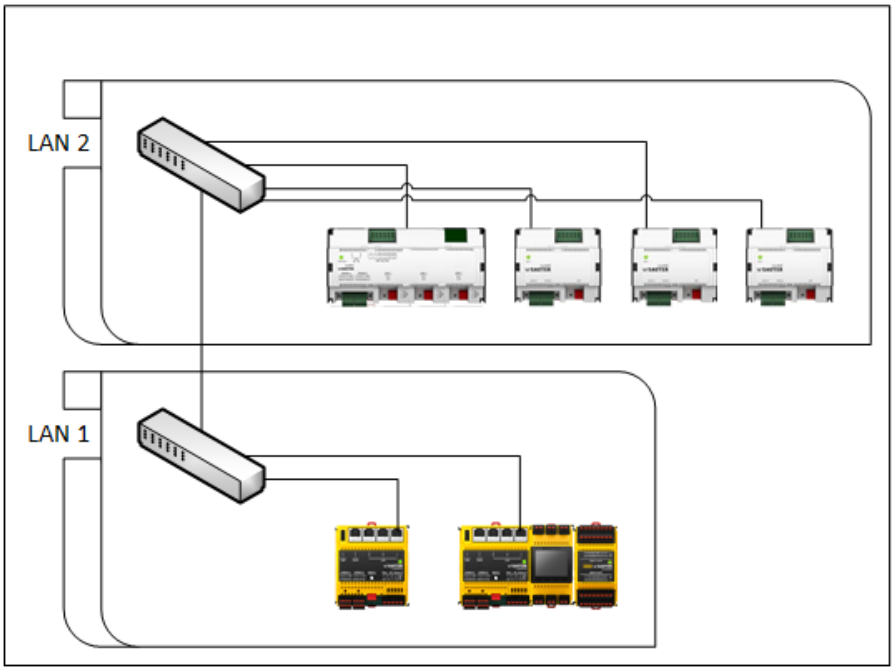

Figure 5:Interconnected local networks.

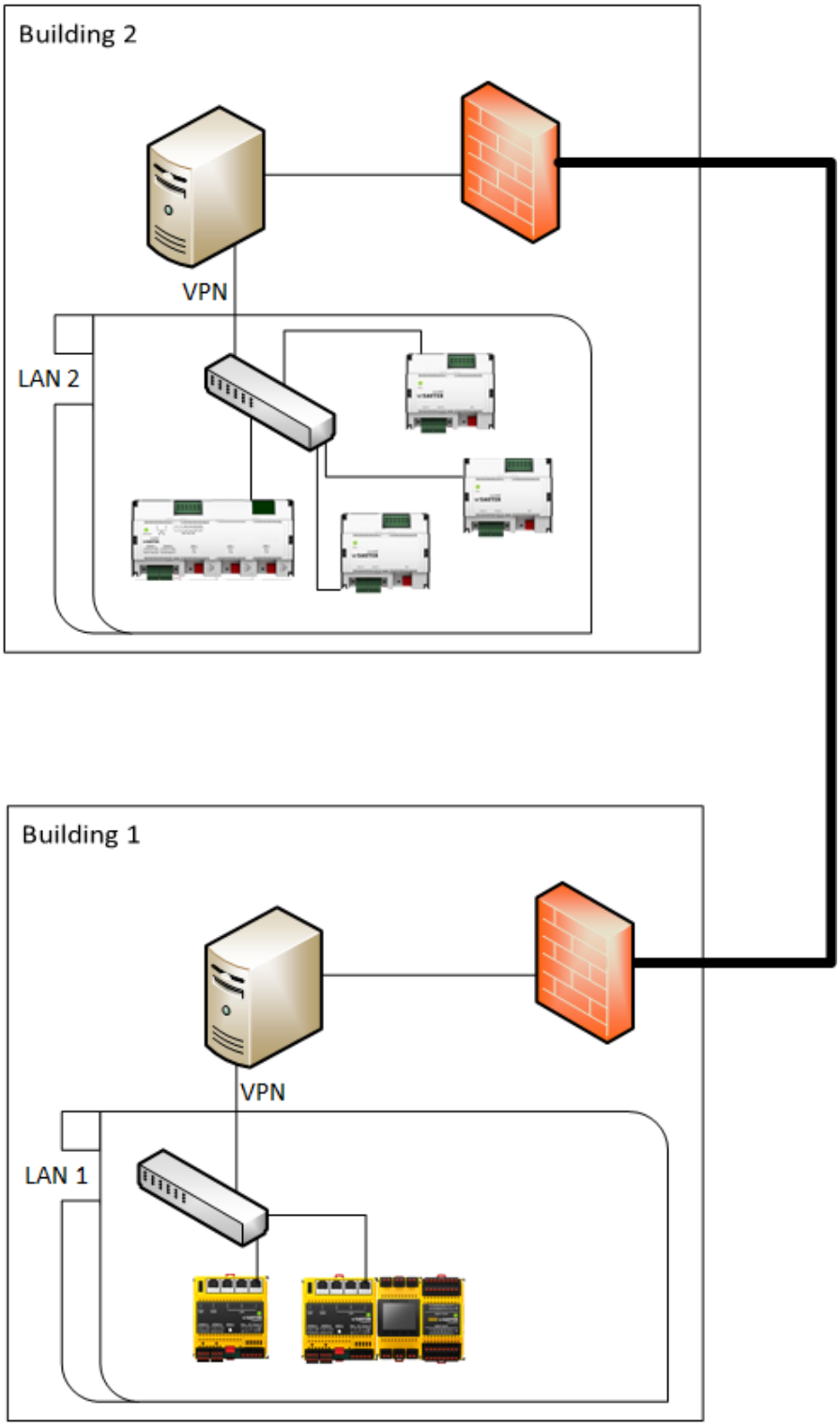

Figure 6:Interconnected networks through trustworthy link.

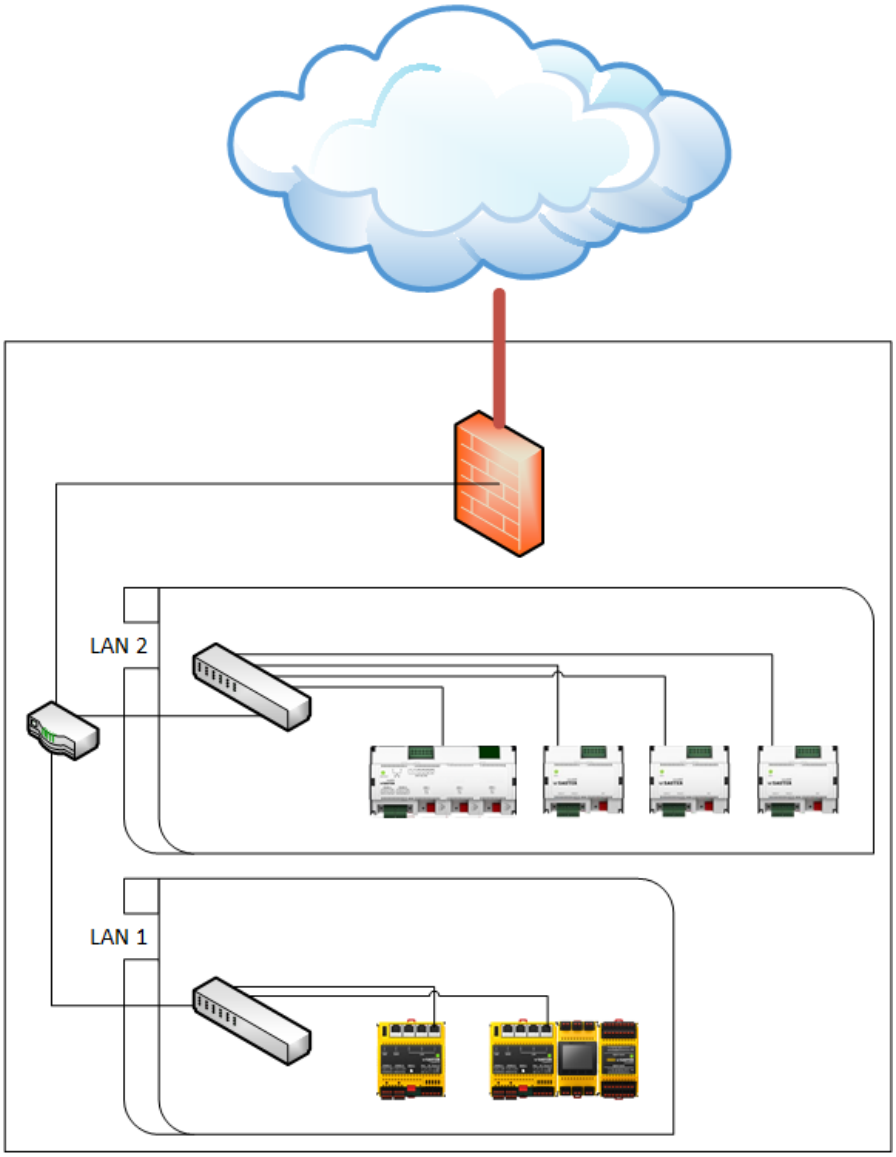

Figure. 7: Interconnected networks through untrustworthy links.

Disable everything that is not required for the end user, e.g.:

- ports
- logical interfaces
- services

5.3 Operating system and external devices hardening

- Firmware Update. SAUTER publishes regularly new firmware versions for modulo 6 devices. The updates include kernel updates, regulation program update and also update packages for attached modules. It is recommended to update the firmware regularly to include the latest fixes to known CVEs.

- Block Firmware downgrade. Set this flag with CASE Sun in order to block the possibility of downgrading the firmware version to take advantage of a vulnerability in an older firmware version.
- modulo 6 IP-capable devices have an on-board firewall, i.e. all the ports are closed excepting those required for the intended purpose, e. g. the port used for BACnet communication. With CASE Sun, it is possible to switch between two modes, service and standard. The service mode opens additional ports for set-up, maintenance and commissioning purposes. For normal operation, the standard mode must be set.
- modulo 6 devices are not intended for customisation. Installation of foreign firmware or software is not supported. Only Firmware signed by SAUTER can be installed.
- The Linux Kernel is tailored to the intended purpose and does not include unnecessary packages, e. g. a Web browser. Accordingly, the devices do not include either antivirus or anti-malware packages nor is it possible to install them. In case of a security incident, report it immediately to SAUTER for quickest remediation.
- SAUTER firmware is regularly scanned to find vulnerabilities. Finding relevant vulnerabilities will trigger immediate reaction from the development team.

Cybersecurity requires a global approach and therefore all components are concerned. The same recommendations for modulo 6 apply in general for any other device or component:

- Follow the recommendations of the product manufacturer, i.e. their security guideline.
- Keep the components up-to-date by updating software or firmware.
- Replace components that are no longer state-of-the-art, especially if they are exposed to external threats.

5.4 Recommendation on commissioning

The configuration channel used by the SAUTER toolchain (CASE Suite), in particular CASE Sun, is encrypted. To enhance security, it is strongly recommended to replace the default certificates with customer- or site-specific certificates.
This measure ensures that access to the core configuration of modulo 6 devices is restricted to authorised personnel and approved tooling only, thereby reducing the risk of unauthorised configuration changes.

Considerations for maintenance

Replacing the certificates used for the commissioning channel introduces stricter access control. Only users in possession of the corresponding certificates will be able to modify the device configuration.

To maintain secure and reliable operations:

- Manage site-specific certificates with appropriate care and security controls
- Clearly define ownership and responsibilities for certificate management
- Ensure secure storage and controlled distribution of certificates
- Establish procedures to guarantee certificate availability for authorised maintenance activities

5.5 modu630-RT as BACnet Router and BACnet/SC Hub

The modu630-RT supports operation as a BACnet Router and, in BACnet/SC environments, as a BACnet/SC Hub. These roles enable secure communication between BACnet networks and can be used to establish connectivity across IP-based infrastructures, including the internet.

Within BACnet/SC architectures, the modu630-RT provides built-in security mechanisms (e.g. TLS-based communication and certificate-based authentication), which can reduce the need for additional tunnelling technologies such as traditional VPN solutions in certain use cases.

It is important to note that the terms “router” and “hub” refer to BACnet-specific communication roles and are not equivalent to full-featured network infrastructure devices.

5.5.1 Security Considerations for Deployment

When using the modu630-RT for communication over public or untrusted networks, the overall system design shall still follow established cybersecurity principles:

- The modu630-RT should be integrated into a secure network architecture appropriate to the risk level of the installation
- Infrastructure-level protections (e.g. firewalls, network segmentation) should be applied where required by the system context
- Access to the device and BACnet/SC services shall be restricted to authorised entities
- Certificate management and trust relationships shall be properly maintained

The suitability of using BACnet/SC functionality as an alternative to VPN-based approaches depends on the specific security requirements and risk assessment of the deployment.

5.5.2 Additional Considerations for Routing and BACnet/SC Hub Operation

When operated as a BACnet Router, the modu630-RT primarily performs protocol routing functions and does not introduce additional security controls beyond those inherent to the configured communication mechanisms.

When routing between BACnet/IP and BACnet/SC, especially where BACnet/SC communication traverses untrusted networks (e.g. the

internet), it is recommended to leverage network separation between trusted (LAN) and untrusted (WAN) segments. This supports the implementation of zone-based architectures and reduces the exposure of internal building automation networks.

When the modu630-RT is configured as a BACnet/SC Hub, it shall be ensured that incoming connection requests from authorised BACnet/SC nodes can reliably reach the hub. This includes proper configuration of network infrastructure (e.g. routing, firewall rules, and, where applicable, NAT traversal) while maintaining appropriate access restrictions.

5.6 Other recommendations

Although Fr. SAUTER AG is IEC 62443-4-1 certified and follows a secure development lifecycle, its products are not intended to be directly connected to the Internet or open networks. They shall be considered part of an OT-network and therefore appropriately protected from external threats. The IEC 62443-3-3 standard and others provide expert guidance for this purpose. If nevertheless an Internet connection is needed to access certain services for example a weather forecast service, SAUTER Cloud or SAUTER Vision Services, e-mail provider, a BACnet Secure Connect Hub, or to provide access to a local service from the outside for example to SAUTER Vision Center or moduWeb Unity, make sure that this access is strictly limited to the concerned service, device and functionality. This may have important implications in the infrastructure and organisation. Therefore, it is imperative that an appropriate risk assessment is conducted before proceeding.

Also, be aware of your local regulatory framework e.g. in Europe, the EU regulations and directives, including the national transposition of directives.

6 Secure operation guidelines

This section provides guidelines for secure operation of product.

6.1 Access to the tools

SAUTER provides different means to configure modulo 6 devices. The CASE Suite toolchain and particularly CASE Sun provides means to commission out of the box modulo 6 devices. CASE Sun is also available as an open tool (resp. the CASE Tool package) with restricted functionality when not licensed. Access to licenses is restricted. They are available for SAUTER subsidiaries and selected partners or customers and are limited in time. They are not freely available to buy. Use the lock functionality of the licensed CASE Sun to prevent the modification of the configuration with the unlicensed CASE Sun tool. For further details on the CASE Suite see the corresponding documentation. As already mentioned in § 5.4, p. 26, it is recommended to set new certificate for the commissioning channel between CASE Sun and the devices that are site or customer-specific.

modulo 6 IP-capable devices (modu680-AS, modu660-AS, modu612-LC) include an embedded web server, moduWeb Unity. It includes access control and role-based user management. Properly manage the authorisations to prevent misuse (see following paragraphs). It is also possible to disable the web server completely, thus avoiding its misuse. Be aware that disabling the web server also disables the WebAPI and the TouchAPI.

6.2 Authorising access

There is no general-purpose access to the modulo 6 devices and their underlying operating systems. The only access possibilities are:

- the SAUTER Toolchain CASE Suite
- the embedded web server moduWeb Unity and API
- the modulo 6 App
- the standard communication protocols, e.g. BACnet (see Tab. 13, p. 38)

6.2.1 CASE Suite

When unboxing or commissioning a modulo 6 device for the first-time, it is in a so-called Service-mode. This allows the CASE Suite tools to connect to the device for configuration purposes with CASE Sun. Once the configuration is complete, the device must be set in the Standard-mode for operation. Furthermore, the device can be sealed to avoid modification of the base configuration with unauthorised (unlicensed) tools.

6.2.2 moduWeb Unity

The moduWeb Unity provides Access Management capabilities including:

- User management
  - Creating individual user accounts
  - Role-based access and rights
  - Individual restriction of access to content
- Policies
  - Password length and complexity
  - Password duration/renewal
  - Password reuse
  - Auto-logout and token expiry
  - Two-factor authentication, TOTP

By providing user management capabilities, access to the controller can be restricted to users. Not only the access to the functionality is therefore restricted, but it is also possible to identify in the Audit Trail which user has made a change. The reach of moduWeb Unity as a user interface may go beyond technical staff and its accessibility may be available from outside the technical room. Therefore, a restrictive access authorisation is of high importance.

Role name	Rights	Scale
Administrator	Full access to device configuration, including factory reset. Use: Installation, Commissioning, Decommissioning	Highest
Specialist	Limited access to device configuration. Access to plant and project-specific content (Nodes, BACnet Objects) for reading and writing can be individually restricted by higher roles. Use: Operation, Maintenance	High
User	No access to device configuration. Access to plant and project-specific content (Nodes, BACnet Objects) for reading and writing can be individually restricted by higher roles. Use: Operation	Medium
Guest	Access to plant and project-specific content (Nodes, BACnet Objects) for read-only can be individually restricted by higher roles. Use: Operation	Lowest

Tab. 7: moduWeb Unity Roles and Rights

Administrators and specialists can manage the user list too.

- Create new users

- Delete old users
- Harden password policies
- Force users to change their password
- Enforce general auto logout rules per role type
- Set general token validity duration by role type
- Enable Two-factor authentication

By default, an admin account exists. The change of the default password is enforced upon the first login.

Password strength is to be enforced following the latest recommendations. Set the minimum password length in accordance with current guidance and the identified risks. Administrators can set a general minimum password length and complexity for all the user accounts of the device.

Value	Default	Range
Minimum number of characters	8	[8; 256]
Lowercase characters	1	-
Uppercase character	1	-
Special characters (non-alphanumeric characters)	1	-
Number of old passwords that cannot be reused	3	-

Tab. 8: Password strength settings

Password expiry can be configured where required by policy. For better implementation of this policy, it is recommended that all accounts include an operational e-mail address and that the service is operational to inform users of the due date for password change.

When enabled, every user can set its own two-factor authentication. moduWeb Unity supports TOTP based two-factor authentication. Many Apps for mobile phone are available for this purpose. TOTP stands for Time-based One-Time Password and is a well-established solution requiring a mobile phone with the appropriate App and a reliable time base. The two-factor authentication hardens security by adding a second authentication factor, in this case the password (something the user knows) and his mobile phone (something only the user has). Because of the time-based nature of TOTP, it is strongly recommended to set-up a reliable time reference with an NTP service.

The permanent authentication of a user terminal into the web server shall be time-limited to avoid opportunistic misuse of the authentication by unauthorised users. Automatic logout shall be set according to the intended use and risk evaluation. Two main strategies can be set up:

- Authentication duration based on token validity

- Automatic logout if the user is inactive for a given time

Automatic logout with a relatively short inactivity time shall be preferred for Administrator and Specialist roles. If the access to terminals is intended to be restricted, this policy shall be extended to User roles too. If the access to terminals is intended to be free, then the token validity policy can be used for User roles. Nevertheless, the operations available shall be strictly limited. If the purpose of the terminal is informational only, then the Guest role with unlimited validity can be used.

The use of tokens implies that there is no connection "session" and that a request to moduWeb Unity can be made by anybody with a valid token. Token validity is configured per role and depends on the selected authentication strategy. Be aware that modifying the token policies invalidates all tokens that were valid upon the instant of the modification. moduWeb Unity also provides the administrators with a button to invalidate immediately all currently valid tokens at once.

Role	Duration of inactivity (default)	Token validity (default)
Administrator	30 minutes	480 minutes (8 hours, 1/3 day)
Specialist	30 minutes	480 minutes (8 hours, 1/3 day)
User	void	43200 minutes (30 days)
Guest	void	5256000 minutes (10 years)

Tab. 9: Default Settings for authentication duration set as: ***Automatic logout if user is inactive***

Duration inconsistency

Inconsistent configuration, e.g. shorter token validity than inactivity duration will lead to unresponsive interface.

- Set a Token validity which is consistently longer than the duration of inactivity.

Role	Token validity (default)
Administrator	7 days
Specialist	7 days
User	30 days
Guest	unlimited

Tab. 10: Default Settings for authentication duration set as: ***Duration based on token validity***

The Web API is an extension of moduWeb Unity. Therefore, the same identification and authentication methods and policies apply. The use of a dedicated user account for this purpose is recommended to properly identify its activity in the audit trail.

6.2.3 modulo 6 App

modulo 6 IP-capable devices (modu680-AS, modu660-AS, modu612-LC) can be operated with the modulo 6 App for iOS and Android. The app access requires identification and authentication. The same accounts and role restrictions of moduWeb Unity are supported.

6.3 Authentication to external services

moduWeb Unity allows clients to use different services requiring authentication. Only one connection can be established with the corresponding credentials. Administrators can set this up. The management of these credentials is on the provider side. Policies may apply regarding complexity, validity etc. Although these outbound connections represent a lower threat to the hosting devices, the information shall nevertheless be handled with the same utmost care.

The e-mail SMTP client included in moduWeb Unity for alarm notification and report notification purposes authenticates itself with a single account to an external provider. This service will require access to an e-mail server, most likely over the Internet. Providers have strengthened their policies to access their services by forbidding old TLS versions or opportunistic TLS. A provider shall be chosen that requires authentication and TLS for encryption of SMTP communication. TLS or "implicit TLS" is recommended. Use SMTP with TLS and authentication. Enforce implicit TLS or STARTTLS; do not allow clear-text fallback. Unencrypted communication shall be avoided in any case. Any piece of information can be used to identify issues or behavioural patterns.

SMS notification can be set up with external devices providing SMTP-to-SMS translation. The same recommendation applies to the regular SMTP communication. Alternatively, the SMPP service requires authentication too.

The FTP (File Transfer Protocol) client can be configured to store generated reports in a remote FTP server location. Use SFTP (SSH File Transfer Protocol) for report transfers; avoid FTP.

The Instant Messaging (IM) client can be configured to push/publish alarm and audit trail notifications to a so-called bot. The transport itself is encrypted but moduWeb Unity has no further control over the actions within the IM platform. Access to the IM user or membership to groups sharing the content must be held under tight control. Otherwise, disable the service. It is recommended to use a dedicated moduWeb Unity user account to identify all the interactions in the Audit Trail log.

6.4 Data storage and encryption

Project data at rest in the device is neither encrypted nor signed. Loading of any data must be from secure sources and through secure channels by authorised personnel only. Appropriate measures must be taken to restrict access. This applies to the unit, the engineering tools and the data involved, i.e. data in the unit, engineering data on engineering tools (e.g. laptops) and backups.

Firmware updates are signed with RSA2048 keys using SHA512 hash. The signature is checked before the update is installed. moduWeb Unity user passwords are hashed.

6.5 Responsibility

modulo 6 devices are professional equipment for building automation purposes and for use by qualified personnel only. As described in chapter 5, the physical access to the system must be restricted. The interfaces which are intended for use by authorised personnel are nevertheless protected by several means and technologies. These measures are intended to support deployments targeting SL 2.

7 Security hardening guidelines

The following paragraph lists security-related features of modulo 6 devices. Following the principle of least functionality, all unused features shall be disabled.

- Disable unused communication interfaces
- Do not configure unused protocols
- Do not disable encryption
- Handle PKI Credentials with appropriate care

Every accessible interface, hardware or software, represents a potential access point to perform a cyberattack or to deploy harmful content.

7.1 Default configuration

As part of the security by default policy, modulo 6 devices are delivered with minimum functionality and accessibility. Most features must be explicitly enabled after unboxing or factory-resetting the product. Examples of this secure-by-default setting are:

- Firewall = Standard. The technician must switch to „Service“ before trying to change the settings. Note that the Commissioning Tools (e.g. for MQTT) only work in Service-Mode.
- moduWeb Unity = Disabled. The technician must enable moduWeb Unity. Then, the default password must be changed.

Below, the default settings of physical and logical interfaces as delivered or following a factory reset.

Default settings for Physical Interfaces

Interface	Default
RS485 (A)	OFF
RS485 (B)	OFF
MEM (C)	OFF
USB (E)	OFF
WAN(F)	ON
LAN(G)	ON
LAN(H)	ON
LAN(J)	ON
Bluetooth	OFF

Tab. 11: Default setting of physical interfaces

Services exposed over the interfaces

Service	Default	Comment
Firewall	Standard	Modes: Standard / Service
ICMP “Ping”	Disabled	
moduWeb Unity	Disabled	
REST API	Disabled	Requires license and enabled moduWeb Unity.
TPC	Disabled	Touch-Panel Client API requires license
MQTT COT UI	Disabled	Must be licensed AND Firewall in Service mode
MQTT Broker/Client	Disabled	Must be licensed and configured
MQTT for modu612-LC binding	Disabled	Requires configuration of the binding
BACnet/IP	Enabled	Needed for configuration purposes
WSC	Enabled	Needed for configuration purposes
Bluetooth	Disabled	

Tab. 12: Default setting of software interfaces (services, protocols)

7.2 Enabling / Disabling interfaces

modulo 6 devices with IP capabilities (modu680-AS, modu660-AS, modu612-LC, modu630-RT) include several interfaces which can be disabled either with CASE Suite toolchain or moduWeb Unity. Disabling unnecessary interfaces and providing only the required functionality reduces the exposure to cyber-attacks. It is strongly recommended to disable any interface that is not essential, as this action contributes to fortifying the overall security of the device.

●: Supported, available - : not supported, not available

Interface	How to enable / disable?	modu680-AS	modu660-AS	modu612-LC	modu630-RT
Ethernet – LAN G	CASE Sun, moduWeb Unity	●	-	-	●
Ethernet – LAN H	CASE Sun, moduWeb Unity	●	●	●	●
Ethernet – LAN J	Always Active	●	●	●	●

Interface	How to enable / disable?	moduo680-AS	moduo660-AS	moduo612-LC	moduo630-RT
Ethernet – WAN F	CASE Sun, moduWeb Unity	●	-	-	●
USB	CASE Sun, moduWeb Unity	●	●	●	-
microSD Card	CASE Sun, moduWeb Unity	●	●	-	-
Bluetooth	CASE Sun, moduWeb Unity	●	●	●	-

7.3 Function related to communication protocols

The modulo 6 devices offer support for various protocols designed for specific purposes. Adhering to the least functionality principle, it is imperative to configure only the interfaces that are essential for the intended operation. The following list outlines the distinct features of modulo 6 devices associated with communication protocols that should remain unconfigured unless their use is deemed necessary. While certain communication protocols involve outbound connections and may pose a lower risk to the device itself, their mere presence could potentially constitute a threat to the entire installation.

Function	How	moduo680-AS	moduo660-AS	moduo612-LC	moduo630-RT
moduWeb Unity Web Server	Disable over CASE Sun (Default: Disabled)	●	●	●	-
Firewall	Switch between Service and Standard over CASE Sun	●	●	●	-
SMTP	Configure only if used for moduWeb Unity notifications	●	●	-	-
SMPP	Configure only if used for moduWeb Unity notifications	●	●	-	-
(S)FTP	Configure only if used for moduWeb Unity reporting. Requires enabling Y6WS**F007 with the License Manager tool.	●	●	-	-
Web API	Requires enabling Y6WS**F008 with the License Manager tool. Can be disabled over moduWeb Unity.	●	●	-	-

Function	How	moduo680-AS	moduo660-AS	moduo612-LC	moduo630-RT
Touch API	Requires enabling Y6WS**F100 with the License Manager tool. Can be disabled over moduWeb Unity.	●	●	-	-
BACnet/IP	Backbone protocol	●	●	-	●
BACnet/SC	Requires enabling Y6FX04F001 with the License Manager tool.	●	●	-	●
RADIUS	Requires enabling Y6FX03F001 with the License Manager tool.	●	●	●	-
MQTT Client and Broker	Requires enabling Y6FX02F001 with the License Manager tool.	●	●	●	-
MQTT Client	Requires enabling Y6FX02F001 with the License Manager tool.	●	●	●	-
MQTT COT Web server	Requires enabling Y6FX02F001 with the License Manager tool and Firewall in Service mode				

Tab. 13: Protocols and functionality by device

Further communication or integration features are based on interfaces other than a RJ45 for Ethernet. The so-called field busses use physical layers like RS-485, RS-232 or proprietary solutions. These are not directly exploitable over an Ethernet network. For example, on a modu680-AS:

- Modbus RTU over the RS-485-A interface or modu620-CM
- SLC (proprietary) over the RS-485-B interface
- MBus over modu630-CM
- The proprietary IO-Bus for the IO- and CM- modules

7.4 Handling of Certificates

Always encrypt communication when possible. With the exception of BACnet/IP, the protocols supported by moduWeb Unity are/can be encrypted. By default, the access to the moduWeb Unity server is encrypted (HTTPS).

X.509 certificates are widely used for authentication and to establish encrypted connections. There are no means foreseen to retrieve the private keys. Only CSR (Certificate Signing Request) can be generated and retrieved for external signing.

Protocol	Service / Function	Self-Signed	CSR	Import
HTTPS	moduWeb Unity Web Server and APIs	Yes	No	Yes, PKCS12
MQTT CT	MQTT configuration tool	Yes	Opt	Yes, PKCS10, PKCS12
MQTT	Client, Broker	No	No	Yes
BACnet/SC	BACnet communication	No	Yes	PEM, CRT
RADIUS	EAP-TTLS / PAP	No	No	PEM
RADIUS	EAP-PEAP / MSCHAPv2	No	No	PEM
RADIUS	EAP-TLS	No	No	PEM(x2)
SOAP	WSC / CASE Sun	Yes	No	PKCS12

Tab. 14: Protocols requiring certificates

Actions related to certificate handling for each phase of the life cycle:

Phase	Actions
Installation, commissioning	Require from the service provider the appropriate Certificates. Take note of the due date for replacement.
Operation, Maintenance	During operation, certificates can become outdated. Require from the service provider appropriate replacement certificates before the due date.
Decommissioning	Delete all certificates, keys, etc. Use CASE Sun or moduWeb Unity to trigger a factory reset that will erase the concerned files.

Tab. 15: Use of certificates in modulo 6 lifecycle

Call to action

TLS version 1.3 shall be used wherever possible. TLS version 1.2 may only be used with cipher suites that are currently considered secure, and with cryptographic key sizes of at least 2048 bits for RSA and 256 bits for elliptic curve algorithms. Earlier protocol versions (TLS < 1.2) and all SSL versions are deprecated and must not be used.

Information

moduWeb Unity's User Interface allows Administrators to locally generate a key-pair and certificate that is then used by nginx for the different web servers (e.g. moduWeb Unity, MQTT COT). The cipher suites supported by the server are:

TLS1.3

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

TLS1.2

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

7.5 Backup

modulo 6 and SAUTER provide different means for making backups and to restore them.

- CASE Sun
- BACnet Backup/Restore

Backups may contain sensitive data, including operational data and personally identifiable information (PII). The Backups shall therefore be stored and handled safely and securely.

7.5.1 CASE Sun

Once CASE Sun has listed the concerned device, the contextual menu allows the user to select "Save device configuration". This triggers the generation of a backup using the device's BACnet functionality. The backup is then completed with the specific device settings and finally wrapped into a zip file, which is locally stored in the technician's computer.

7.5.2 BACnet Backup

The BACnet backup is a service provided by the device. BACnet clients can trigger a backup, but the backup content is limited to BACnet files. The successful execution requires the BACnet password of the device.

7.6 Firmware downgrade protection.

Set this flag with CASE Sun to avoid firmware downgrade. A firmware downgrade can be a security risk if it contains a vulnerability that can be exploited. The flag cannot be removed unless the whole station is reset to factory settings. This will erase all data and configurations, including cryptographic keys and certificates.

8 Reporting guidelines

SAUTER is willing to fortify our products by reporting any issues that users encounter. Together, we will ensure a safe and secure environment for all. Sauter welcomes reports of potential security issues to improve product security.

Security issues can be reported to the PSIRT (Product Security Incident Response Team) over the dedicated web page form (https://www.sauter-controls.com/en/cybersecurity/) or by writing an email to: psirt@sautergroup.com. Provide as much detailed information as possible to reproduce the issue, for example (as of EN ISO/IEC 29147:2020):

a. Product or service name, URL, or affected version information
b. Operating system of involved components
c. Version information
d. Technical description of what actions were being performed and the result in as much detail as possible
e. Sample code that was used to test or demonstrate the vulnerability
f. Reporter's contact information
g. Other parties involved
h. Disclosure plans
i. Threat/Risk assessment details of the identified threats and/or risks including a risk level (high, medium, low) for assessment result
j. Software configuration of the computer or device configuration at time of discovering the vulnerability
k. Relevant information about connected components and devices if vulnerability arises during interaction. When a secondary component or device triggers the vulnerability, these details should be provided
l. Time and date of discovery
m. Browser information including type and version information.

With the entry in force of EU regulations like CRA [2] among others, reporting of product vulnerabilities and incidents becomes mandatory within the EU. By enforcing measures such as security by default and mandatory reporting obligations, the objective is to minimise both the risk and the potential consequences of a cyberattack.

Looking precisely to the CRA, Importers and Distributors are precisely cited and obligations are described (CRA [2] Art. 19 & Art. 20). For example, CRA Art. 19 (5) indicates that the importer shall inform the manufacturer without undue delay upon becoming aware of a vulnerability in the product. The same applies for distributors (CRA Art. 20 (4)).

For this purpose, contact SAUTER PSIRT immediately.

9 Secure disposal guidelines

Documentation**:** Before disposing of the product, ensure that the product configuration, connections, and any customised settings are thoroughly documented. This information may be required later for reinstallation, replacement, or troubleshooting purposes

9.1 Removal from intended environment

Backup configuration**:** Before removing the device, create a backup of its configuration, including settings, firmware, and any stored data. This backup will help in restoring the device or transferring its configuration to a new location if necessary.

Disconnect from network**:** Safely disconnect the device from the network to prevent any unauthorised access or data breaches. This may involve disabling network interfaces or physically unplugging network cables.

Power down: Power down the device following the manufacturer's instructions. Ensure all power sources, including backup batteries or secondary power supplies, are disconnected.

Physically remove: Carefully remove the device from its mounting location or enclosure. Take precautions to prevent any damage to the device or surrounding equipment.

Secure storage: If the device will be stored temporarily before disposal or relocation, ensure it is stored securely in a controlled environment to prevent unauthorised access or tampering.

9.2 Removal of references and configuration data stored within the environment

Identify relevant configuration data: Determine all references and configuration data associated with the device or system being removed. This includes any configuration files, log data, databases, or documentation stored within the environment.

Backup configuration data: Before removal, create a backup of all relevant configuration data. This ensures that you have a copy in case it's needed for future reference or system restoration. Ensure that the backup process is secure and that the backup files are encrypted to protect sensitive information. Ensure that restoration is also fully functional.

Review configuration data for sensitivity: Assess the sensitivity of the configuration data being stored. Identify any personally identifiable information (PII), proprietary information, or other sensitive data that requires special handling. For example, moduWeb Unity user accounts may include personal data such as name, phone number, e-mail.

9.3 Secure removal of data stored in the product

Data Inventory: Identify all data stored within the product, including configuration settings, logs, user data, and any other sensitive information.

Backup: Before removal, create a backup of the data to ensure that you have a copy in case it's needed for future reference or system restoration. Encrypt the backup to protect sensitive information.

Data encryption: If the data is not already encrypted, encrypt it using strong encryption algorithms. This ensures that even if the data is accessed, it remains unreadable without the appropriate decryption keys.

Data deletion: Use secure deletion methods to permanently remove all sensitive data from the product. This may involve overwriting data multiple times to prevent recovery, or using specialised data erasure tools. Physical destruction may be considered when secure deletion is not feasible or when it is more cost-effective than data overwriting.

Removable media: modulo 6 supports the use of removable media, such as microSD cards and USB storage devices, for storing information. These media must be handled appropriately, for example by storing them securely, securely deleting all or selected data such as PII, or physically destroying the media when necessary.

Factory reset: Perform a factory reset of the product to revert it to its original state, removing all user-configured settings and data. Follow the manufacturer's instructions for performing a secure factory reset.

9.4 Secure disposal of the product

Physical Destruction: If the product contains storage media or components that may retain data (e.g., hard drives, memory chips), physically destroy them to prevent data recovery. Use methods like shredding, degaussing, or incineration to render them irrecoverable. If needed, contact a specialised service for this purpose.

Component Disassembly: Disassemble the product to separate its components for recycling or disposal. Ensure hazardous components (e.g., batteries, electronic components containing heavy metals) are handled and disposed of properly according to environmental regulations.

Recycling: Send non-hazardous components and materials for recycling to authorised recycling facilities. Separate recyclable materials like metals, plastics, and glass for proper recycling. Follow your local legislation.

Certified Recycling Services: Use certified recycling services that adhere to environmental standards and regulations. Ensure the recycling facility has processes in place to handle electronic waste (e-waste) responsibly.

Data Destruction Certificate: Obtain a data destruction certificate from the recycling facility or service provider as proof that sensitive data has been securely disposed of according to industry standards.

10 Global references

10.1 Standards

Standard	Purpose
ISO 16484-5	ASHRAE/ANSI Standard 135: A Data Communication Protocol for Building Automation and Control Networks (aka BACnet)
IEC 62443	Security for Industrial automation and control systems (IACS) throughout their lifecycle.
ISO 27000	Information technology – Security techniques.
EN 18031	Security requirements for radio equipment. EU Harmonised standard for the Radio Equipment Directive (RED)
EN 17640	Fixed-time cybersecurity evaluation methodology for ICT products (FiT CEM) Standard for French ANSSI's Certification Sécurité Premier Niveau (CSPN) or German BSI's Beschleunigte Sicherheitszertifizierung (BSZ)
FIPS-140-*	US Federal Information Processing Standards
EN ISO/IEC 29147	Information technology - Security techniques - Vulnerability disclosure
EN ISO/IEC 30111	Information technology - Security techniques - Vulnerability handling processes
EN 40000-1-x	CRA horizontal standards (in public review as of April 2026)
ETSI EN 304 6xx	CRA vertical standards

Tab. 16: Some Standards related to cybersecurity

10.2 National and international public organisations

Organisation	Purpose	Link
CSIRT Network	European Computer Security Incident Response Team Network	https://csirtsnetwork.eu/
ENISA	The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.	https://www.enisa.europa.eu/
CEN	European Committee for Standardization	https://cencenelec.eu
CENELEC	European Committee for Electrotechnical Standardization	https://cencenelec.eu

Organisation	Purpose	Link
ECCC	The European Cybersecurity Competence Centre: The ECCC aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community	https://cybersecurity-centre.europa.eu/index_en
VINCE	Vulnerability Information and Coordination Environment (VINCE).	https://kb.cert.org/vince/
CISA	CISA is committed to working with the industrial control systems (ICS) community to address urgent operational cyber events as well as long-term ICS risks.	https://www.cisa.gov/topics/industrial-control-systems/
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germany)	https://www.bsi.bund.de/
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)	https://www.ssi.gouv.fr/
NCSC	National Cyber Security Centre	https://www.ncsc.gov.uk/
BACS OFCS UFCS NCSC	Bundesamt für Cybersicherheit Office federal de la cybersécurité Ufficio fedeerale della cibersicurezza National Cyber Security Centre	https://www.ncsc.admin.ch/
NIST	National Institute of Standards and Technology	https://nist.gov/
MITRE	Knowledge-base for product cybersecurity	https://attack.mitre.org
CWE	Common Weakness Enumeration	https://cwe.mitre.org
CVSS	Common Vulnerability Scoring System	https://www.first.org/cvss
CVE	Common Vulnerabilities and Exposures	https://www.cve.org https://www.cvedetails.com

Tab. 17: Some national and international public organisations

10.3 Private organisations, initiatives

Organisation	Purpose	Link
OWASP	The Open Worldwide Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software.	https://owasp.org/
CIS	At CIS®, we're harnessing the power of global IT community to safeguard public and private organisations against cyber threats. Join us.	https://www.cisecurity.org/
SANS	it is SANS' ongoing mission to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place.	https://www.sans.org/
Heise.de	heise.de is a leading German-language online news portal run by Heise Group, focusing on independent reporting about IT, technology, digital policy, and related topics for professionals and enthusiasts.	https://www.heise.de/security/
ICS Advisory Project	ICS Advisory Dashboards provide ICS asset owners, analysts, CISOs, and researchers with a way to quickly identify new and previously reported ICS Advisories affecting control system assets in OT environments across multiple critical infrastructure sectors.	https://www.icsadvisoryproject.com/ics-advisory-dashboards
CERTVDE	CERT@VDE is Germany's first IT security platform and Computer Emergency Response Team focused on coordinating and handling cybersecurity issues for industrial companies, especially SMEs in industrial automation.	https://certvde.com/

Tab. 18: Private organisations or initiatives related to cybersecurity

10.4 CERTS / National Coordination Centres

CERT stands for Computer Emergency Response Team. Initially created by DARPA and the SEI of the Carnegie-Mellon University.

Country	Office (Link)
Austria	Federal Chancellery of Austria in cooperation with the Austrian Research Promotion Agency
Belgium	Centre for Cybersecurity Belgium (CCB)
Bulgaria	Ministry of Electronic Governance
Cyprus	Digital Security Authority (DSA)
Czech Republic	National Cyber and Information Security Agency
Germany	National Coordination Centre for Cybersecurity - Federal Office for Information Security (BSI)
Denmark	The Danish Business Authority
Estonia	Estonian Information System Authority
Greece	National Cybersecurity Authority of Greece
Ireland	National Cyber Security Centre of Ireland
Finland	NCSC-FI
France	Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
Italy	Agenzia per la Cybersicurezza Nazionale (ACN)
Lithuania	National Coordination Centre, Ministry of National Defence
Luxembourg	National Cybersecurity Competence Center Luxembourg
Latvia	Ministry of Defence
Malta	Malta Information Technology Agency
Netherlands	The Netherlands Enterprise Agency (RVO)
Poland	National Cybersecurity Coordination Centre Unit in the Chancellery of the Prime Minister
Portugal	Portuguese National Coordination Centre
Romania	Centrul Național de Coordonare
Sweden	Swedish Civil Contingencies Agency
Slovenia	Office of the Government of the Republic of Slovenia for Information Security
Slovakia	Cyber Security Competence and Certification Centre (KCCKB)
Spain	National Cybersecurity Institute (INCIBE)
Switzerland	GovCERT
USA	Cybersecurity & Infrastructure Security Agency

Tab. 19: National Cyber Emergency Response Teams

10.5 Legal references

ID	Description	Ref.
RED	Radio Equipment Directive.	EU 2014/53
RED DA	Radio Equipment Directive Delegated Act.	EU 2022/30
GDPR	General Data Protection Regulation.	EU 2016/679
NIS-2	Network and Information Systems (directive)	EU 2022/2555
CER	Critical Entities Resilience	EU 2022/2557
CRA	Cyber Resilience Act	EU 2024/2847
PSTI	Product Security and Telecommunications Infrastructure Act	2022 (UK)
Zero Trust	Executive Order 14028	(USA)
FISMA	Federal Information Security Management Act	2002 (USA)

Tab. 20: Some legal references for information purposes

10.6 Bibliography

[1] *NIS-2 Directive (EU 2022/2555),* 2022, p. 60.

[2] *Cyber Resilience Act (EU 2024/2847),* 2024, p. 81.

[3] *Radio Equipment directive Delegated Act (EU 2022/30),* 2021, p. 5.

[4] IEC technical committee 65, *Part 4-1: Secure product development lifecycle requirements,* 1.0 ed., Vols. 4-1, I. E. Commission, Ed., Geneva: International Electrotechnical Commission, 2018.

[5] BSRIA, “Market Penetration of Communications Protocols,” BSRIA, 2023.

[6] *FAQ on the Cyber Resilience Act,* 2026, p. 66.

[7] ANSSI, *Recommandations de sécurité relatives à TLS,* ANSSI, 2020, p. 72.

[8] CNIL, *Recommandations relatives à l'authentification multifacteur et aux mots de passe,* ANSSI, 2021, p. 52.