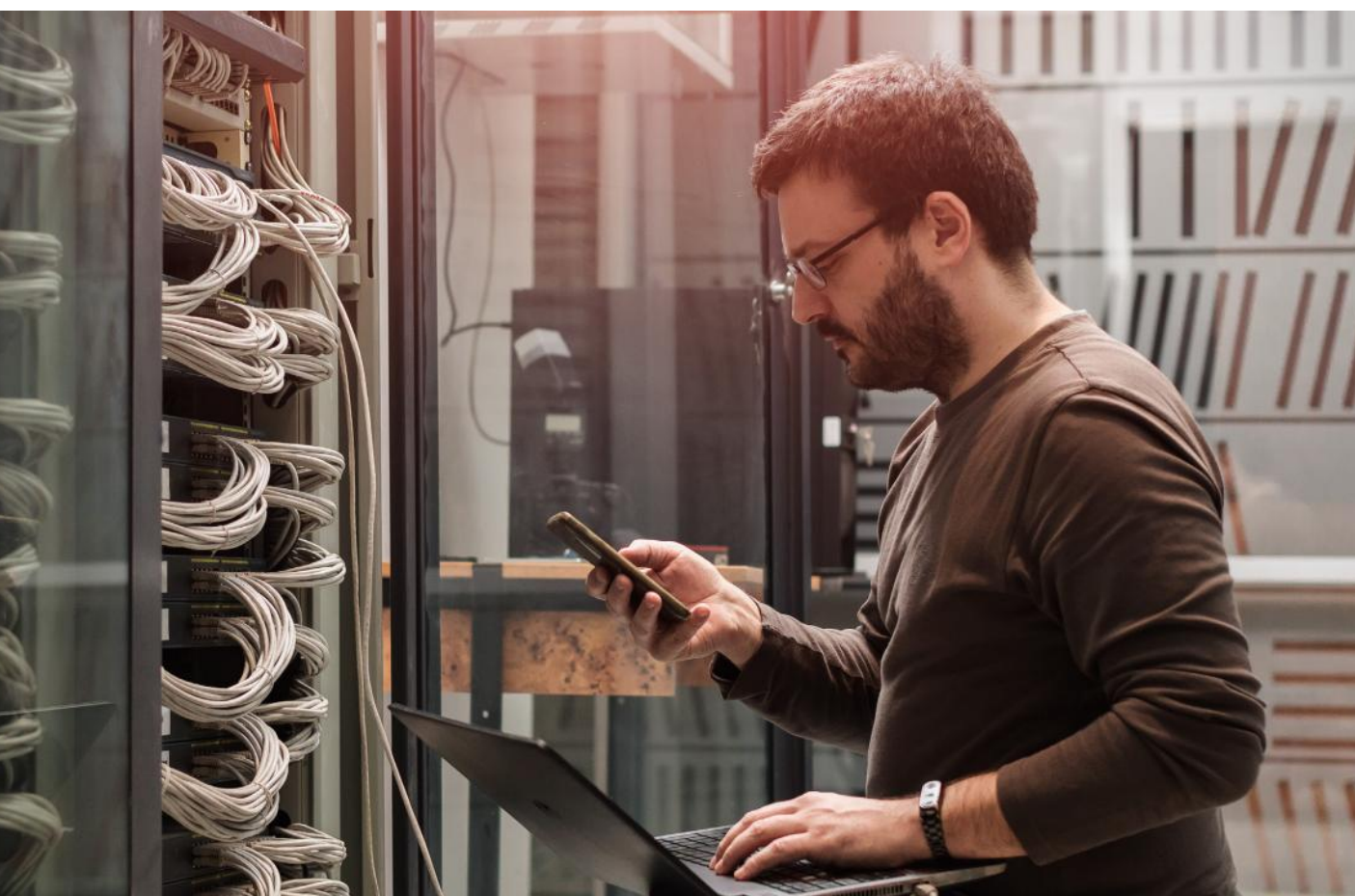

ABB BUILDINGPRO

Cybersecurity



The industry is experiencing continuously intensifying cybersecurity threats.

To improve the stability, safety, and robustness of its solutions, ABB has established cybersecurity robustness testing as a mandatory component of the product development process. The following measures are required for safe system operation.

ABB accepts no liability for non-compliance with these requirements.

Table of contents

1.	General disclaimer.....	3
2.	Cybersecurity disclaimer.....	3
2.1.	Regulations and standards in automation.....	3
2.1.1.	NIS2 Directives at ABB	4
2.2.	Physical network security.....	5
2.3.	Don't forget about "People"	5
2.3.1.	Risky practices.....	5
2.3.2.	Roles and responsibilities	6
3.	A secure framework of operation.....	7
3.1.	Cybersecurity program & governance	7
3.2.	Cybersecure by design	7
3.3.	Test methodology	9
4.	BuildingPro Solution	10
4.1.	General prerequisites	11
4.2.	Access control and limitations	11
4.2.1.	Rules for strong passwords.....	12
4.3.	Networking & cabling	13
4.3.1.	Fieldbus	13
4.3.2.	IP Network	13
4.3.3.	Connection to internet	14
4.4.	ABB BuildingPro Cloud Portal.....	15
4.4.1.	Communication flows	15
4.4.2.	DPS and X.509 Certificates.....	15
4.4.3.	AMQP runtime phase	15
4.4.4.	Cloud-based endpoints	16
4.4.5.	Internet facing ports and services.....	17
4.5.	ABB Building Edge.....	18
4.5.1.	Linux distribution.....	18
4.5.2.	Security rules on hardware	18
4.5.3.	Performance limits	19
4.5.4.	Local ports and services.....	20
4.6.	Network topologies	22
4.7.	Software bill of materials	27
5.	Additional notes	28

1. General disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by ABB.

ABB assumes no responsibility for any errors that may appear in this document.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.

2. Cybersecurity disclaimer

This product is designed to be connected to and to communicate information and data via a network interface. It is your sole responsibility to provide and continuously ensure a secure connection between the product and your network or any other network (as the case may be). You shall establish and maintain any appropriate measures (such as but not limited to the installation of firewalls, secure VPNs, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system and the interface against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

ABB Ltd and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

2.1. Regulations and standards in automation

ABB recognizes the importance of cyber security standards, and ABB is an active member of several industry initiatives, including IEEE and IEC. This involvement ensures that the needs of our customers are considered in the development of new standards and that ABB remains abreast of new developments.

It also enables ABB as a company to incorporate new standards into ABB's products and systems, helping ABB's customers to comply with regulations as they come into force.

The cyber security regulations in automation affecting ABB are:

- The NIS 2 Directive: The Network and Information Security Directive applies to public and private entities of a type referred to as essential entities and as important entities. The Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation of European Union.
- The European Cyber Resilience Act: The proposal for a regulation on cyber security requirements for products with digital elements reinforces cyber security requirements to ensure more secure hardware and software products.

In general, the most important cyber security standards in automation are:

- IEC 62443 series: Industrial communication networks – Network and system security
- IEC TR 63074: Safety of machinery – Security aspects related to functional safety of safety-related control systems
- NIST 800-53: Security and Privacy Controls for Information Systems and Organizations
- NIST Cyber security Framework: Framework for Improving Critical Infrastructure Cyber security
- NERC CIP: Critical Infrastructure protection standards
- ISO 27000-series: The ISO 27000 series of standards for all information security matters.

2.1.1. NIS2 Directives at ABB

At ABB, cybersecurity compliance is a core aspect of our commitment to protecting digital operations. We take a proactive approach to assessing and addressing the impact of the NIS 2 Directive across our organization, ensuring that our processes and systems align with their requirements.

We maintain robust policies and procedures to continuously evaluate the effectiveness of our information security measures. Our efforts also extend to fostering a strong cybersecurity culture - promoting sound cyber-hygiene practices, delivering regular cybersecurity training to enhance preparedness, and ensuring the secure management of users and accounts.

Our key compliance measures in alignment with NIS 2 include:

- Policies for risk analysis and information system security
- Incident handling procedures
- Business continuity planning
- Supply chain security management
- Network and information systems protection
- Evaluation of cybersecurity risk management effectiveness
- Organization-wide cybersecurity awareness

2.2. Physical network security

Cybersecurity guidance emphasizes that physical network security is the foundation of a secure building management system (BMS) environment. Physical access to network components often allows attackers to bypass many logical controls, so organizations must treat rooms, ports, and cabling as critical assets.

A core principle is to ensure that BMS devices are never directly connected to untrusted networks, and that BMS networks remain logically and physically isolated from external or less-trusted segments, including the public internet and partner networks that could be compromised. Where integration with other systems is necessary, it should be mediated through secured gateways, firewalls, and demilitarized zones (DMZs) to limit exposure.

Physical security controls should include placing all critical servers, switches, firewalls, and controllers in locked, access-controlled rooms or cabinets, with access granted only to authorized, trained personnel. Visitor access should be logged, and maintenance work should follow defined access procedures to reduce the risk of tampering or accidental misconfiguration.

Endpoint and workstation security is equally important: each engineering station, operator workstation, and maintenance laptop should be protected against unauthorized use through both physical (locks, badges) and logical (unique credentials, MFA, automatic screen locking) controls. Shared accounts and unattended logged-in sessions in technical rooms should be strictly prohibited, as they provide easy entry points for misuse.

2.3. Don't forget about "People"

In the 2024 [Cost of Data Breach] report (conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM), human error accounted for 26% of all breaches, while IT failures represented 23%, totaling 49% of breaches caused by non-malicious factors. The remaining 51% were attributed to malicious or criminal attacks.

Often this is due to the lack of expertise required to implement security controls, enforce policies or conduct incident response processes.

Training employees on risk-mitigation techniques including how to recognize common cyberthreats such as a spear phishing attack, best practices around Internet and e-mail usage, and password management. Failure to enforce training and create a security-conscious work culture increases the chances of security breach.

2.3.1. Risky practices

The following are 10 risky practices employees routinely engage in, according to the findings of the study:

1. Connecting computers to the Internet through an insecure wireless network.
2. Not deleting information on their computer when no longer necessary.
3. Sharing passwords with others.
4. Reusing the same password and username on different websites.
5. Using generic USB drives not encrypted or safeguarded by other means.
6. Leaving computers unattended when outside the workplace.
7. Losing a USB drive possibly containing confidential data and not immediately notifying their organization.
8. Working on a laptop when traveling and not using a privacy screen.
9. Carrying unnecessary sensitive information on a laptop when traveling.
10. Using personally owned mobile devices that connect to their organization's network.

2.3.2. Roles and responsibilities

Usually, the owner of the business has the main responsibility for selecting, deploying, and maintaining the cyber security of applied technical solutions.

However, it is practically impossible for one player to control all aspects of cyber security, production continuity and defense in depth layers. Co-operation is needed with many partners to design, construct, and maintain a feasible level of cyber security for continuous operation.

The following list presents examples of actors and their roles ensuring valuable cyber security co-operation. The division of roles is based on IEC 62443 standard series. It should be noted that the same actor can act in several roles. For example, ABB can also have system integration or maintenance responsibilities in addition to product supplier responsibilities.

- **Building / business owner**
 - Own and operates a commercial building that has an automation and control system and provides operational as well as maintenance policies and procedures regarding cyber security.
- **System integrator**
 - Competence in and experience of valuable cyber security co-operation: platform weaknesses and cyber security bottlenecks in system integration
 - Validation and approval of all cyber security solutions before their actual commissioning in the field. Adviser on secure usage of devices and applications, upgrades, patches, maintenance, and monitoring services, etc.
- **Maintenance service providers**
 - **Network services:** Maintaining a secure network architecture together with managed switches (VLANs), routers (networks), firewalls (access control), and monitoring services (identification of malicious behavior or software).
 - **Telecommunication network operator.** Establishing and cyber security monitoring of private access points and possibly VPNs for customers.
 - **Office security services.** Physical access control and monitoring of facilities, rooms, cabinets, etc.
- **Product suppliers**
 - **Embedded device providers.** ABB works primarily in this role providing Building Edge devices, BuildingPro solutions and other field products.
 - **Software providers.** Maintenance of operation system software, antivirus software, management software, etc.
 - **Network equipment vendor.** Establishing a secure network architecture together with managed switches (VLANs), routers (networks), firewalls (access control).

3. A secure framework of operation

Cybersecurity is a fundamental component of our company's operations and digital trust. As our activities increasingly rely on interconnected systems, cloud platforms, and intelligent devices, protecting data, assets, and infrastructure from cyber threats has become a shared responsibility across all teams.

This document outlines the cybersecurity policies, standards, and procedures adopted within our organization. Its purpose is to ensure that every employee, partner, and contractor understands the principles guiding our security posture, including data protection, system integrity, network defense, and compliance with relevant regulations and industry standards.

By following these rules, we aim to maintain a resilient digital environment that upholds confidentiality, integrity, and availability of information — the three core pillars of cybersecurity. Adherence to these policies is mandatory and contributes directly to safeguarding our clients, our reputation, and the continuity of our operations.

3.1. Cybersecurity program & governance

ABB operates a global cybersecurity program that defines policies, processes and technical standards for product development, cloud operations and field deployments.

ABB Ability™ BuildingPro and ABB Building Edge are developed within this framework, including secure development practices, security robustness testing and controlled release management, with Yocto-based images tailored for security and maintainability. (see detailed documentation below).

If you want to learn more about cybersecurity:

<https://new.abb.com/low-voltage/products/building-automation/product-range/abb-i-bus-knx/cyber-security-protection-for-smart-buildings>

3.2. Cybersecure by design

Device Security Assurance Center (DSAC) is a dedicated ABB internal security assurance center which is independent from the product development organization.

DSAC assures consistent approach in carrying out cyber security testing, penetration testing on ABB products such as wired embedded devices, software applications (thick-client and desktop based), web applications/ API (hosted in cloud/device/system), mobile applications (Android and iOS), and wireless embedded devices (802.11 and BLE). DSAC collaborates closely with ABB developers providing in-depth analysis and recommendations.


If you want to learn more about DSAC:

<https://search.abb.com/library/Download.aspx?DocumentID=9AKK107680A9866&LanguageCode=en&DocumentPartId=&Action=Launch>


DSAC covers all aspects of security testing mandated by ABB Security Development Life Cycle (SDLC) standard, but development teams may perform additional testing part of IEC 62443-4-1 if needed. For example:

- Verification of security requirements
- Software composition analysis (SCA)
- Threat mitigation testing of threats identified in Threat Model

The DSAC Cyber Security Test Process has been certified by Exida for IEC62443 Part 4-1: 2018 Secure Product development lifecycle requirements.



The manufacturer may use the mark:




Revision 2.1 August 1, 2024
Surveillance Audit Due August 1, 2027

Assessment Report:
ABB DSAC 2101029 R001
V2R2 Assessment Report

Validity:
This certificate is for the referenced security development lifecycle at the time of evaluation. This lifecycle is used for the development and maintenance of products meeting the criteria defined in the scope section in the assessment report.

exida
80 North Main St.
Sellersville, PA 18960



T-177-V1B3

Certificate / Certificat Zertifikat / 合格証

ABB DSAC 2101029 C001

exida hereby confirms that the

Cybersecurity Test Process Assessment of the Device Security Assurance Center (DSAC)

Practiced by

ABB
Bangalore, India

Has been assessed per the relevant requirements of:

IEC 62443 Part 4-1: 2018 Secure product development lifecycle requirements

And meets the requirements for:

MATURITY LEVEL 3

For the following requirements:

SM-1A, SM-1D, SM-1E, SM-2, SM-3, SM-4,
SM-5, SM-7, SM-11, SM-12, SM-13,
SVV-1, SVV-2, SVV-3A1, SVV-3A3, SVV-3A5,
SVV-3B, SVV-3C1, SVV-3C2, SVV-4, SVV-5, DM-1A



Shashana I Wood

Evaluating Assessor

Bill Thonson

Certifying Assessor

The ABB Ability™ BuildingPro solution is fully tested by the ABB DSAC.

3.3. Test methodology

The objective of security testing is to employ a multitude of test methods to gain a comprehensive Cyber-security assessment of a product.

DSAC uses the concept of attack surfaces to categorize types of testing that are applied to the products. An attack surface is defined as a collection of points/vectors where a threat agent tries to perform a malicious action that causes the product to operate not according to its specification.

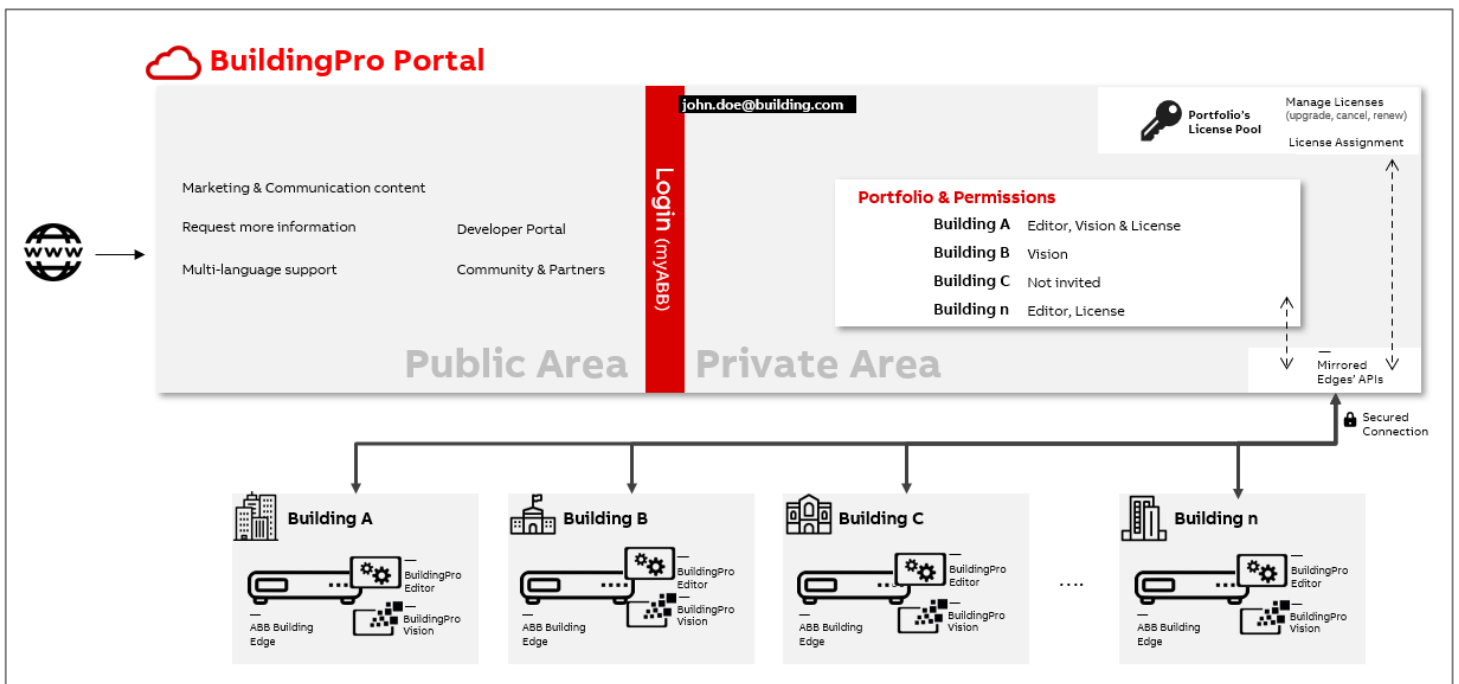
DSAC supports the following attack surfaces as seen in the following table:

Nature of Product	Applicability	Applicable Attack Surface
Wired and Wireless embedded device (ABB Building Edge device)	Applicable for a product that does Ethernet based communication	<ul style="list-style-type: none">• Web vulnerability• Network vulnerability• Device vulnerability• Pre-Robustness• Robustness• API Security
Web application – as well any SaaS offering (BuildingPro Editor) (BuildingPro Vision)	Applicable for a product that has a web server, web application	<ul style="list-style-type: none">• Web vulnerability• API security

4. BuildingPro Solution

The ABB Ability™ BuildingPro is structured around 2 main infrastructure elements:

- On-premises, composed of:
 - Field devices for sensing and acting,
 - The ABB Building Edge:
 - Connected to the internet,
 - Embedding a webserver from which the solution can be integrated and configured via “BuildingPro Editor” by the system integrator.
- ABB BuildingPro Portal
 - Accessible from: <https://buildings.ability.abb>
 - Composed of:
 - A public area, available to any internet user to get presentation of the solution,
 - A private area, available to registered users (free).



4.1. General prerequisites

The following prerequisites must be met for commissioning the ABB Building Edge device:

- The ABB Building Edge is connected to the local network via an RJ45 LAN cable connected to its 1st IP Port (LAN1)
 - Communication with the field equipment in BACnet, KNX, Modbus, MQTT. Always use the secure version of the protocols when feasible.
 - Connected to a standard IP switch or router of the building
- A computer is connected to the same local network, where LAN1 of the Building Edge is connected, via RJ45 LAN cable
 - A computer is required for the initial startup. This comp
 - Subsequent changes can also be made using a tablet.
 - Commissioning via smartphone is not possible.
- No other user is connected to the BuildingPro Editor Configuration Tool.
- The ABB Building Edge is connected to the internet via a LAN cable connected to its 2nd IP Port (LAN2)
 - State-of-the-art secured internet connection
 - Enabling communication with ABB Ability™ cloud-platform
 - Connected to a standard IP switch or router of the building



LAN1 and LAN2 can be used indifferently to serve one or the other purposes listed above. Not recommended but feasible: have only 1 IP port used to connect to internet and to the field devices simultaneously.

For a first commissioning of the ABB Building Edge, like setting up its network properties to ensure its proper connection to both the local network and the ABB Ability™ cloud portal, the user connects to the ABB Building Edge via the local IP network.

A third-party computer should be used to configure the ABB Building Edge.

The user's computer must be connected to the same IP network as the ABB Building and must belong to the same IP Subnet or (V)LAN.

The IP addresses configuration and their respective subnet masks must be correctly set to ensure proper communication.

Care must be taken towards the opening of the correct communication ports inherent to the proper operation of the ABB Building Edge. These communication ports are listed in this document.

The user shall proactively ensure the used computer is running the latest updates and security patches for the operating system used. An up-to-date anti-virus and anti-malware solution needs to be installed and run on the user's computer.

The ABB Building Edge embeds a webserver from which the configuration can be done.

Once connected to the ABB Ability™ BuildingPro cloud portal, the whole configuration can be made indistinguishably from the local interface and from the cloud portal.

4.2. Access control and limitations

The careful isolation of the system against unauthorized access is the basis for every protective concept. Only authorized people (fitter, caretaker, tenant) are allowed physical access to the IP network or bus system and its components. This also includes the ABB Building Edge device described in the instruction manual.

The best possible protection of the IP or network media (LAN/WLAN) and the transfer node must be guaranteed already during planning. Sub-distributions with fieldbus devices must be lockable or be in rooms to which only authorized personnel have access.

Secured connections must be enforced as often as possible, making use of HTTPS connections. Self-certification is available in the ABB Building Edge configuration tool. 3rd party authority's certification will be available in later stage of the product development.

4.2.1. Rules for strong passwords

- A password should contain at least 10 characters.
- A password should consist of upper- and lower-case letters, numbers and special characters (e.g., § & ? ! ?) and should not be found in a dictionary or be related to you and your family. Therefore, do not use names, dates of birth, telephone numbers or the like.
- It should not represent a mere sequence of numbers (12345...), an alphabetical sequence (abcdef...) or a series of adjacent keys on the keyboard (qwerty).
- The more sensitive the access (e.g., access to online banking), the more care you should take when selecting a strong password. If the provider does not set a character limit for the password, the longer the better!
- Do not choose the same password for all portals. Instead, create separate passwords at least for the most important and most used services.
- Change a password on your first login if it was sent to you by a provider. Other reasons to change the code would concern your online provider asking you to do so, major data leaks being known, or your device being infected with malware.
- Keep passwords secret and use a password manager with two-factor login as memory aid.

4.3. Networking & cabling

4.3.1. Fieldbus

Physical protection of fieldbus networks is as important as protecting IP networks, because direct access to the bus can allow manipulation, eavesdropping, or disruption of building control functions. Physical layout, routing, and termination of fieldbus cabling should therefore be planned and implemented with security in mind.

Cabling and network interfaces must be physically protected so that unauthorized individuals cannot connect rogue devices or interception equipment. This includes routing cables through secure conduits, avoiding exposed patch panels in public or shared spaces, disabling unused network ports, and labeling or documenting connections so that suspicious, undocumented links can be quickly identified and removed.

- For security reasons, the ends of fieldbus cables must never be exposed or left visible.
- They must not protrude from walls, conduits, or cable ducts, whether inside or outside the building, and should always terminate in secured junction boxes, distribution boards, or locked cabinets.
- Any unused bus segments or stubs should be properly terminated and kept inaccessible to prevent unauthorized devices from being connected.
- Fieldbus cables installed in outdoor areas, technical yards, or zones with limited physical protection present an elevated security risk. In such locations, physical access to the cabling and connection points should be made exceptionally difficult, for example by routing cables through buried, armored, or tamper-resistant conduits and by enclosing all junctions and interfaces in locked, vandal-resistant enclosures.
- Where field devices must be accessible (e.g., sensors or actuators on facades or in parking areas), mounting and cabling should be designed to minimize the ability of an attacker to unplug devices, insert a rogue node, or tap the bus without being noticed.

4.3.2. IP Network

The local network represents a sensitive component for secure communication. That is why unauthorized access to the local network should be prevented.

A decentralized network infrastructure strategy shall be in place with a strong focus on network segmentation and segregation, e.g., for manufacturing, logistics, facilities, and other areas of the company. The aim is to restrict the level of access to sensitive information, hosts and services while ensuring an organization can continue to operate effectively.

Implementing the principle of least privileges across a network will significantly increase the overall security posture of the environment.

The usual security mechanisms for IP networks are to be used, for example, but not limited to:

- Secure encryption of wireless networks
- Use of complex passwords and their protection against unauthorized people
- Physical access to network interfaces (Ethernet interfaces) and network components (router, switches) should only be possible in protected areas
- MAC filter (table with certified device addresses)
- Physical or logical (VLANs) network segmentation on the data link layer
- Restrict communication on the network layer (routing)

- Restrict communication on the network and transport layer (firewall),
- Use of encrypted and secured connection to the ABB Building Edge (HTTPS).

4.3.3. Connection to internet

The stable and reliable function of the device also depends on the reliability of the local IP network to which the Building Edge is connected. It is also dependent on the reliability of the internet connection, used to connect to the cloud-based ABB BuildingPro Portal.

For this reason, additional network components are to be used to repel DoS attacks (Denial of Service) from the Internet.

Such attacks can overload the local IP network or the individual components and make them inaccessible.

4.4. ABB BuildingPro Cloud Portal

ABB ensures a cybersecure connection between Building Edge and BuildingPro Cloud Portal.

- The Building Edge device uses an X.509 certificate for authentication.
- Communication protocols include AMQP over WSS with TLS 1.2 and MQTT over WSS with TLS 1.2.
- Azure Relay facilitates broadband communication to the device using WSS over TLS 1.2
- SignalR over WSS is used when a customer accesses the device via the user interface

This setup ensures secure, authenticated, and encrypted connections between the Building Edge device and the ABB cloud services, maintaining robust protection of data in transit.

The ABB Building Edge uses the TLS v1.2 with reinforced ciphers to establish the communication between the device and the ABB Ability™ BuildingPro Cloud Portal.

TLS is a cryptographic protocol designed to provide security for communications, including privacy (confidentiality), integrity, and authenticity through the use of certificates.

4.4.1. Communication flows

Step	From	To	Purpose
1	ABB Building Edge	Azure DPS	The device contacts Azure Device Provisioning Service (DPS) to be assigned to the correct IoT Hub. DPS is the bootstrap step used before the device knows its final hub.
2	Azure DPS	ABB Building Edge	DPS returns the assigned IoT Hub and enrollment outcome so the device can continue with hub-specific onboarding.
3	ABB Building Edge	Certificate authority / trust chain	The device validates the server identity and, depending on the chosen authentication model, uses an X.509 certificate or certificate chain for authentication.
4	ABB Building Edge	Azure IoT Hub	The device opens the runtime connection to IoT Hub using AMQP over WebSockets .
5	Azure IoT Hub	ABB Building Edge	IoT Hub can push cloud-to-device messages and management commands back to the device over the established protocol channel.

4.4.2. DPS and X.509 Certificates

DPS is used to register or enroll the device before it connects to the target hub. Due to X.509-based certificates, the Building Edge must present its certificate during authentication, and the trust chain must be in place so the TLS connection can be validated correctly.

Certificate handling covers device identity, server validation and the certificate authority trust chain.

4.4.3. AMQP runtime phase

Once provisioned, the ABB Building Edge device communicates with Azure IoT Hub over AMQP over WebSockets on 443/TCP.

This phase carries telemetry, reported properties, cloud-to-device messages, and command/control exchanges. AMQP allows server push for cloud-to-device messages, used for managed edge connectivity.

4.4.4. Cloud-based endpoints

Some internet-based addresses need to be whitelisted on the local IT network (in the building) to ensure the proper functioning of the ABB BuildingPro solution.

It is recommended to rely on DNS entries rather than IP addresses.

Indeed, the underlying IP addresses of public endpoints can change dynamically over time. It is recommended to whitelist the following IoT Hub FDQN (fully qualified domain name):

- [buildings.ability.abb](#) (ABB Cloud Portal)
- [iotebospeu1ns01.servicebus.windows.net](#) (Azure Relay)
- [iotehubpeu1ih01.azure-devices.net](#) (IoT Hub)
- [iotesigpeu1sr01.service.signalr.net](#) (Service for SignalR)
- [iotehubpeu1dps01.azure-devices-provisioning.net](#) (Device Provisioning Services)
- [azure-devices-provisioning.net](#) (Device Provisioning Services)
- [azure-devices.net](#) (Main Device-facing domain for connection, messaging, telemetry, etc.)
- [api.buildings.ability.abb](#) (Main API interface of the ABB Cloud Portal)
- [api.buildings.ability.abb/buildings/openbos/firmwareupdate](#) (Firmware Update)
- [login.microsoftonline.com](#) (Login)
- [clientauth.one.digicert.com](#) (Certificate Authority)
- [pki-scep.symauth.com](#) (Certificate Authority)
- [apim.eu.mybuildings.abb.com/ssht-api/v1](#) (SSH)

4.4.5. Internet facing ports and services

Port	Protocol	Direction from Edge	Internet facing	Comment
2222/TCP	SSH	Outgoing	Yes	Outgoing SSH channel used upon manual activation of the remote tunneling service to receive remote assistance from ABB. This is the port reached on the remote target, but it is not open on the Building Edge
2223/TCP	SSH	Incoming	Yes	Incoming SSH channel used upon manual activation of the remote tunneling service to receive assistance from ABB
68/UDP	DHCP	Outgoing	Yes	Needed once DHCP protocol will be supported by the device
80/TCP	HTTP	Incoming	Yes	Web server port listing for incoming HTTP requests (non-secure)
443/TCP	HTTPS	Incoming	Yes	Web server port listing for incoming HTTPS requests (secure) if enabled by the customer.
443/TCP	HTTPS	Outgoing	Yes	Azure Cloud Connectivity: IoT Hub messaging, Device Provisioning Service, SCEP Protocol, Firmware download, Backup and Restore Functionality. AMQP over WebSockets and MQTT over WebSockets might need to be explicitly authorized depending on the security level, in case HTTPS does not embed it natively.

Whitelisting might be necessary to be done across the different elements of the local infrastructure, such as:

- Firewalls
- mTLS proxy (mutual TLS)
 - Mutual authentication in which the two parties in a connection authenticate each other using the TLS protocol.
 - TLS inspection could get into the traffic between the Building Edge and the cloud portal, intercept the certificate and replace it with its own. Request is then sent to IoT Hub, but certificate is not recognized. Communication is dropped. Disable proxy TLS inspection might be helpful in case individual whitelisting is not performed.
- Proxy
- VPNs
- IP routers
- Security gateways
- UTM (Unified Threat Management)
 - Single security appliance that combines several protections in one device, such as firewall, intrusion prevention, antivirus, anti-spam, web/content filtering, and sometimes data loss prevention), etc.

4.5. ABB Building Edge

The ABB Building Edge is a set of hardware devices that serve as a key component of ABB's BuildingPro offering.

The Building Edge integrates multiple types of building data from various sources into a single device, enabling seamless connectivity and secure data transmission to the cloud for digital services. The device embeds openBOS®, ABB's operating system for smart buildings, and can be remotely managed and maintained through ABB's secure cloud-based BuildingPro Portal.

4.5.1. Linux distribution

The Building Edge Device runs on Linux as its low-level operating system. ABB has developed a customized Yocto Linux build environment to enhance cybersecurity and optimize performance. The four key advantages of ABB's customized Yocto-based Linux distribution are:

1. Unparalleled Security and Transparency

Yocto is an industry-standard toolchain recognized for its transparent development process recognized for its strong security practices and transparent development processes. With Yocto, ABB can provide an accurate and transparent Software Bill of Materials (SBOM), giving you full visibility into the components used in your system. This transparency helps you verify software integrity and confirm that all components are securely patched.

2. Optimized Firmware for Enhanced Performance

Yocto enables the creation of streamlined firmware images purpose-built for ABB's embedded devices. Yocto-based firmware is custom designed to minimize footprint and maximize performance, delivering a safer and more reliable solution.

3. Flexibility Amid Supply Chain Challenges

Yocto is supported by a broad community, including major silicon manufacturers such as Intel, ARM, and NXP, who are key contributors to the project. This strong industry backing gives ABB the flexibility to adapt to potential supply chain disruptions, such as chip shortages, by integrating software support for alternative hardware platforms.

4. Easier Maintenance and Focus on Innovation

By leveraging a common Yocto-based code base, ABB reduces the complexity of maintaining multiple software configurations. This allows more resources to be dedicated to developing impactful features tailored to your needs, accelerating innovation and increasing the overall value of ABB's solutions.

4.5.2. Security rules on hardware

The BuildingPro Edge adheres to the cybersecurity rules outlined below:

- Building Edge integrates a microchip designed to securely store and manage cryptographic keys and sensitive information, such as passwords and certificates, directly in hardware rather than in software - like TPM (Trusted Platform Module) or HSM (Hardware Security Module).
- Building Edge supports Secure Boot to verify system integrity before startup and to prevent unauthorized applications from running.
- All applications on Building Edge devices are digitally signed and are started by the Yocto Linux operating system only when their signatures are successfully validated.
- Building Pro Edge series devices support dual boot with a dedicated safe recovery partition to restore the system in case of a failure. two identical root partitions (A and B), each capable of booting the full system, and updates are always written to the inactive slot before switching over. When the device runs from slot A, a new firmware bundle is installed into slot B; when running

from B, the update is installed into A. If the new slot fails to boot correctly or health checks fail, the bootloader falls back to the previous slot, effectively rolling back to the last known good version without manual intervention.

- The internal storage of Building Edge devices is fully encrypted and cannot be read without proper authorization. Passwords are stored in database hashed and salted inherited from storage best practices.
- At this stage, a secure cloud connection is required to update the system; offline update capabilities will be introduced in a future release.

4.5.3. Performance limits

The web-based interface of ABB BuildingPro Editor can be used simultaneously by several participants (computers and/or tablet devices).

Depending on the scope of the changes made, performance losses may occur (changes take longer to be implemented).

It is therefore recommended to operate the user interface with a maximum of 5 participants at the same time. However, as many user accounts as desired can be registered.

4.5.4. Local ports and services

To support the main functionalities of the device, communication via specific ports and services must be possible in your local network. Contact your network administrator to set up, if necessary, the appropriate port sharing.



Attention!

Enabling communication ports increases the risk of cyber-attacks.

- Enable only necessary ports.
- Regularly check which ports are enabled for which purpose.

Port	Protocol	Direction from Edge	Internet facing	Comment
502 (TCP or UDP)	Modbus	Outgoing	No	Outgoing requests to communicate with Modbus devices
502 (TCP or UDP)	Modbus	Incoming	No	Incoming communication from Modbus devices
1628/TCP	LonWorks	Outgoing	No	LonWorks E1852 protocol
1629/TCP	LonWorks	Incoming	No	LonWorks E1852 protocol
1883/TCP	MQTT	Incoming	No	MQTT Broker listening for incoming MQTT connections from MQTT Devices
2223/TCP	SSH	Incoming	No	Incoming SSH channel in case the customer has activated the local SSH access / SSH Server
8883/TCP	MQTT/TLS	Incoming	No	MQTT Broker listening for incoming MQTT connections using TLS from MQTT Devices
47808/UDP	BACnet	Outgoing	No	Outgoing requests to field BACnet devices
47808/UDP	BACnet	Incoming	No	Incoming requests from field BACnet devices

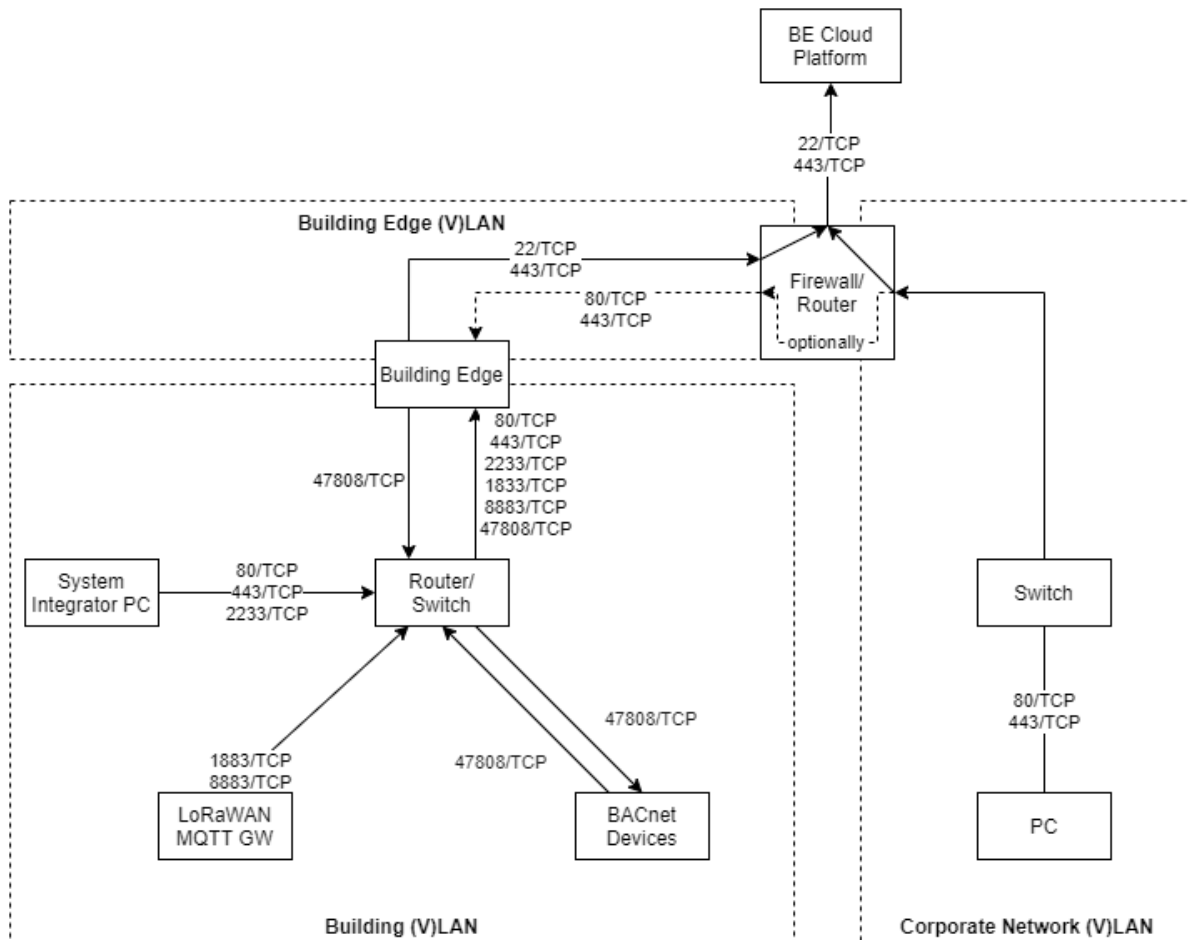
Whitelisting might be necessary to be done across the different elements of the local infrastructure, such as:

- o Firewalls
- o VPNs
- o IP routers
- o VLANs

4.6. Network topologies

4.6.1. Network topology with 3 (V)LANs & 2 IP ports

This topology features 3 VLANs and 2 IP ports, it supports segmented network traffic across multiple VLANs with dual IP connectivity for enhanced redundancy or separation.



Strengths

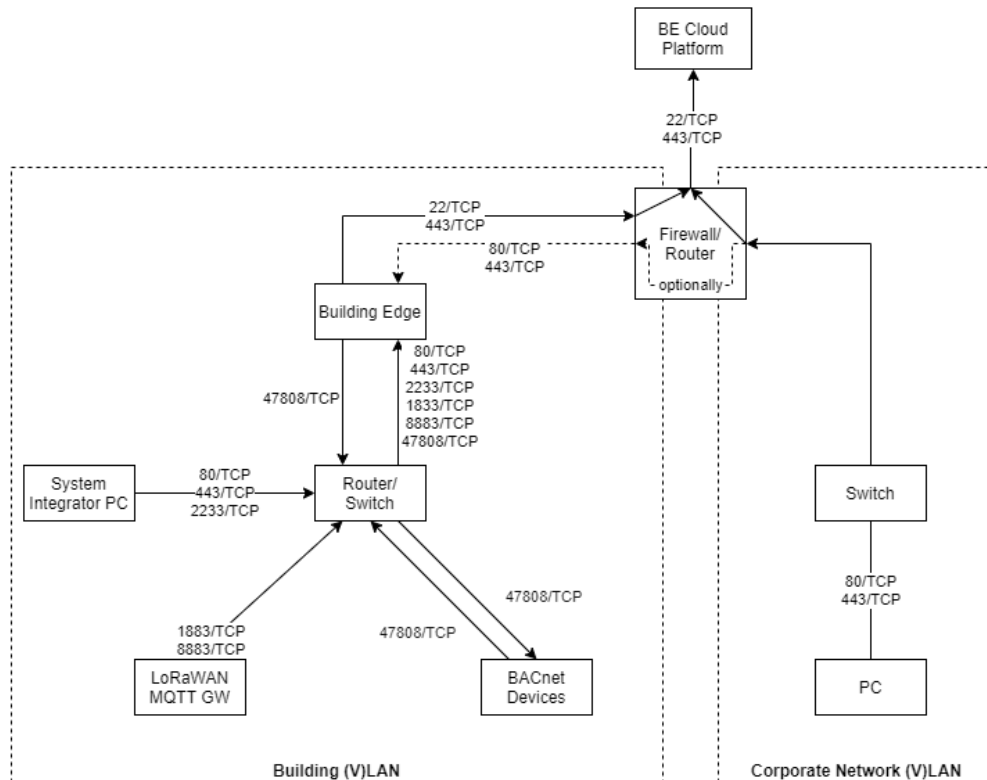
- Clear segregation of three traffic domains (e.g. IT / BACS / guest or DMZ), improving security and fault isolation.
- Allows fine-grained policy (firewall rules, QoS, ACLs) per VLAN, which is useful for complex sites or multi-tenant buildings.
- Two IP ports let you implement redundant upstream paths (dual routers, dual firewalls, or IT vs OT uplink separation).
- Facilitates compliance with stricter segmentation requirements (e.g. separating management, field, and external access networks).
- Easier to scale by adding more devices within each VLAN without changing the physical wiring.

Weaknesses

- Higher configuration complexity: more VLANs, more routing, and more firewall rules to maintain.
- Troubleshooting can be slower because issues might span multiple VLANs, trunks, and routing points.
- Risk of misconfiguration (wrong VLAN tagging, wrong interface membership) causing crosstalk or outages.
- Requires more capable switches/routers that support multiple VLANs and inter-VLAN routing with sufficient performance.
- Potentially higher operational overhead (documentation, change management, coordination with IT).

4.6.2. Network topology with 2 V(L)ANs & 2 IP ports

This topology features dual ports to enable failover and load balancing between the VLANs.



Strengths

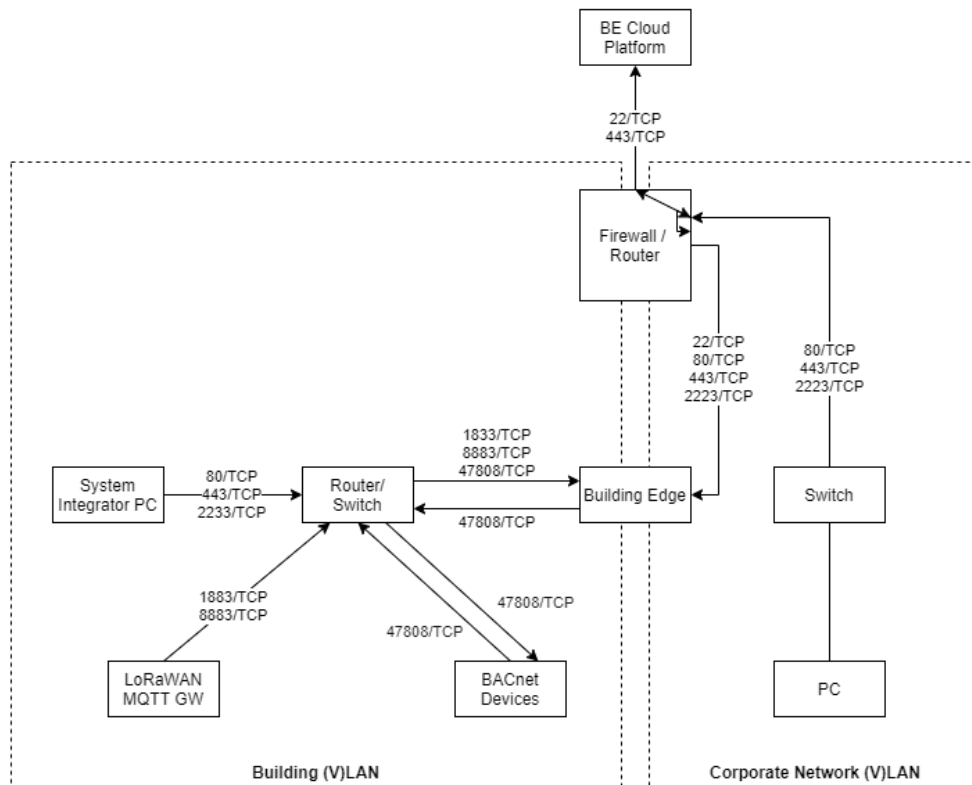
- Two separate VLANs provide basic segmentation (e.g. IT vs OT, or management vs field devices) without the complexity of three domains.
- Two IP ports still allow dual-homing (e.g. one port to IT core, one to a dedicated BMS/OT router or firewall).
- Simpler security policy model than the 3-VLAN design while still enabling clear trust-zone separation.
- Easier to explain and document to stakeholders and installers; topology is more intuitive.
- Good compromise between security and manageability for medium-complexity sites.

Weaknesses

- Less granular segregation than the 3-VLAN option; some traffic types may have to share the same VLAN.
- If one VLAN carries multiple functions, lateral movement risk within that VLAN is higher.
- Still requires VLAN-aware hardware and correct trunk/access port configuration.
- Policy changes on one VLAN might impact multiple services sharing it, increasing change-impact risk.
- If both IP ports are used toward the same upstream device without proper design, redundancy may be illusory rather than real.

4.6.3. Network topology with 2 (V)LANs & 2 IP ports

This setup includes 2 VLANs and 2 IP ports. It mirrors Topology 2 in configuration highlighting variations in device connections and routing.



Strengths

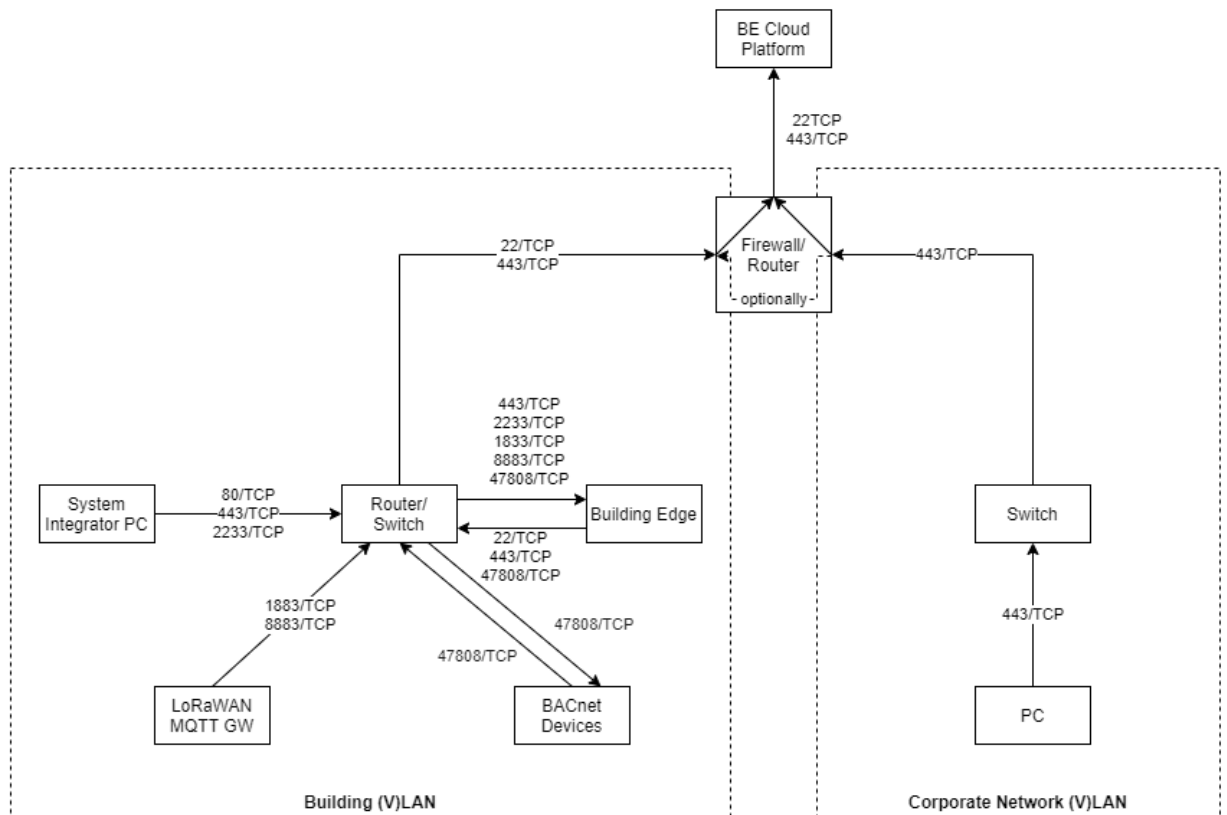
- Two VLANs still give logical separation, but the alternative wiring may optimize for specific use cases (e.g. direct uplink per VLAN, or split external/internal access).
- The changed arrangement can improve resilience if each IP port terminates in a different network segment or security zone.
- May reduce the number of hops or devices in the path for some traffic flows, improving latency or simplifying paths.
- Can be tailored so that critical control traffic uses a shorter, more deterministic path while non-critical traffic uses the other.
- Helpful when aligning with existing site constraints (e.g. legacy IT core on one side, dedicated OT firewall on the other).

Weaknesses

- Different layout from the previous 2-VLAN option may make operations less consistent across sites if both designs are used in your portfolio.
- The split paths can complicate end-to-end visibility, as monitoring tools must cover multiple segments.
- Asymmetrical routing or firewalling is easier to introduce unintentionally, complicating troubleshooting.
- Documentation must be very clear, or technicians may confuse which IP port/VLAN serves which function.
- If not carefully designed, one of the ports/VLANs may be underused, wasting available bandwidth/resources.

4.6.4. Network topology with 2 (V)LANs & 1 IP port

This simpler port arrangement prioritizes cost-efficiency or single-interface management over redundancy



Strengths

- Simple physical design: a single IP uplink reduces cabling and port requirements.
- Still supports two VLANs, allowing basic separation (e.g. management vs field devices) over one trunk.
- Easier to deploy and troubleshoot than multi-uplink designs; only one upstream path to analyze.
- Lower hardware cost, as you need fewer IP ports on firewalls/routers and possibly simpler switch infrastructure.
- Good fit for small sites or demo/lab environments where redundancy is not critical.

Weaknesses

- Single uplink is a single point of failure; no link-level redundancy for the IP path.
- Bandwidth for all VLANs is shared on one link, which can become a bottleneck in busy systems.
- Any upstream outage (switch, router, firewall) directly impacts all VLANs.
- Fewer options to implement separate security zones using physically distinct paths.
- Harder to meet high-availability or regulatory requirements that expect dual-path connectivity.

4.7. Software bill of materials

For better understanding which versions of software components are used in Building Pro environment, Building Pro Edge Editor provides access to the following sBOM License components:

- Licenses of components used in User Interface,
- Licenses of components used in openBOS (Ontology & Publication),
- Licenses of components used in openBOS (Middleware),
- Licenses of components used in firmware (Linux Distribution).

ABB can export and deliver the sBOM to you upon request.

Open-Source licenses are available to all users from the “Manage my account” menu, “Licenses” tab accessible in both BuildingPro Editor and BuildingPro Vision.

5. Additional notes

This software uses library spdx-exceptions developed by Kyle E. Mitchell and C. Scott Ananian. Library is licensed by Creative Commons Attribution 3.0.

Details are available at this page: <https://github.com/jslicense/spdx-exceptions.json#readme>



Postal address

ABB Switzerland Ltd
Bruggerstrasse 66,
CH-5400 Baden,
Switzerland

new.abb.com/buildings