BACS SECURITY IN BUILDINGS

Cybersecurity Planning Guide for KNX Systems

Contents

1. Cybersecurity for Building Automation and Control Systems (BACS) 3

2. Weaknesses in BACS as Risk Factors 3

3. Cybersecurity in the Planning and Tendering Process 4

3.1. Trade Siloes 4

Sufficient Documentation 4

3.2. Monitoring of the Building Automation and Control Systems (BACS) 4

3.3. Role and Authorization Management 5

4. IT and OT Networks 5

4.1. Cybersecurity Requirements for Building Automation and Control Systems (BACS) 6

4.2. Assessment of the Current Condition 6

4.3. Responsibilities and Accountability for Cybersecurity 7

4.4. Network Segmentation and Management 8

5. Building Automation and Control Systems Cybersecurity Requirements 8

5.1. Basic Cybersecurity Requirements (MUST Requirements) 9

5.1.1. INF.14.A1 Planning the Building Automation and Control Systems (BACS) 9

5.1.2. INF.14.A2 Commissioning and Integration Schedule 11

5.1.3. INF.14.A3 Secure Integration of Control Silos 12

5.1.4. INF.14.A4 Integration of Critical Systems 13

5.1.5. INF.14.A5 Documentation of Building Automation and Control Systems (BACS) 13

5.1.6. INF.14.A6 OT and IT- Network Segregation 14

5.2. Standard Cybersecurity Requirements (Should Requirements) 16

5.2.1. INF.14.A7 Definition of Cybersecurity Policy 16

5.2.2. INF.14.A8 Cybersecurity Specification for Building Automation and Control Systems 17

5.2.3. INF.14.A9 Building Automation and Control Systems Concept 18

5.2.4. INF.14.A10 Building Automation and Control System Segmentation 18

5.2.5. INF.14.A11 Control and Restrict Access 19

5.2.6. INF.14.A12 Secure IP Communication 19

5.2.7. INF.14.A13 BACS Network Segmentation 20

5.2.8. INF.14.A14 Access Control for Central BACS Devices and Software. 21

5.2.9. INF.14.A15 Security Mechanisms for BACS Networks 21

5.2.10. INF.14.A16 Wireless Communication 21

5.2.11. INF.14.A17 Use of Mobile Networks for BACS 22

5.2.12. INF.14.A18 Communication Interfaces to External Systems 22
5.2.13. INF.14.A19 Use of Dedicated IP Address Range for BACS 23
5.2.14. INF.14.A20 Broadcast Communication 23
5.2.15. INF.14.A21 Ensuring Displayed and Control Values are Up to Date 23
5.2.16. INF.14.A22 Self-sufficiency as a Security Principle 24
5.2.17. INF.14.A23 Robust Components 24
5.2.18. INF.14.A24 Time Synchronization 24
5.2.19. INF.14.A25 Status Logs 24
5.2.20. INF.14.A26 Change Logs 24
5.2.21. INF.14.A27 Emergency Planning 25
5.3. Requirements for Critical Systems with Enhanced Cybersecurity Needs 25
5.3.1. INF.14.A28 Dedicated Physical Network for BACS 25
5.3.2. INF.14.A29 OT-Network Segmentation 25
5.3.3. INF.14.A30 Dedicated Time Server for Critical Systems 25

6. Conclusion: A fault-resilient BACS system also has good resilience against cybersecurity risks 26

Purpose of the Document

This guide emphasizes the importance of cybersecurity in planning, implementing, and operating Building Automation and Control Systems (BACS) and outlines related security requirements.

This document focuses on aspects relevant to system integrators and installers.

1. Cybersecurity for Building Automation and Control Systems (BACS)

Building Automation and Control Systems (BACS) improve building efficiency by automating technical functions, including heating, ventilation, lighting, and security. These systems serve as the core of Technical Building Management. IT security for building management has become increasingly critical due to changing laws, evolving risks, and heightened customer awareness.

Internal threats can affect the availability, integrity, authenticity, and confidentiality of systems, which are vital for the safe operation of building infrastructure. External threats usually involve sabotage, espionage, or unauthorized access. Most cyberattacks target the automation and management layers of building systems.

The field level (such as KNX sensors and actuators) is less frequently targeted. Therefore, cybersecurity resilience is critical at both the automation and management levels (such as SCADA, visualizations, DDC, or PLC controllers).

It is important to acknowledge that building control systems themselves may not always be the direct focus of cybersecurity threats; rather, adversaries may seek to exploit vulnerabilities within Building Automation and Control Systems (BACS) or leverage weaknesses introduced into the IT network during BACS implementation. BACS can be utilized by one or multiple occupants within a facility, including various tenants, and distinct sections of a property may operate under different BACS configurations. Consequently, cybersecurity represents not only a technical issue but also a significant organizational concern.

The need for clearly defined contractual responsibilities is expected to increase. Emerging legislation is aiming to ensure that systems are inherently cybersecure. This progression may reverse the burden of proof: whereas customers currently bear responsibility for specifying and verifying security requirements, the presumption in the future will be that systems are secure by default unless customers are expressly notified of, and consent to, particular security exceptions.

2. Weaknesses in BACS as Risk Factors

Several issues in Building Automation and Control Systems (BACS) pose significant risks to the cybersecurity of building control systems and potentially any connected IT or 3rd System.

- Often, security is not considered in the planning stage, especially when the future building operator is unknown.
- Poor documentation, with incomplete or missing records, makes it harder to assess the current cybersecurity status of building systems.
- Vulnerable interfaces between building control systems and other systems can be intentionally or unintentionally exposed.
- Inadequate monitoring allows critical system failures to go unnoticed, thereby increasing the risk of major disruptions.

- Weak role and access management occur when multiple people share the same user account, making it challenging to track actions or ensure accountability.

The long lifecycles of building systems, often lasting decades, require long-term planning and strategic approaches to maintain security over time.

Building control system integrators and suppliers now have additional responsibilities, including delivering software updates to address vulnerabilities.

In the EU, the reverse burden of proof means that if a vulnerability is exploited, customers may claim they believed the system was secure and compliant. It is then the responsibility of manufacturers, suppliers, installers, and integrators to demonstrate that products were secure, installed properly, and that any accepted security exceptions were clearly communicated to and approved by the customer.

3. Cybersecurity in the Planning and Tendering Process

During building construction, tenants and end users are often unknown. The objectives and requirements for the Building Control System are finalized later to suit the user's needs. The system may require adjustments to meet cybersecurity standards.

System planners and suppliers should expect adjustments after occupancy. Inadequate planning can lead to incomplete documentation, making future updates costly and complicated. System integrators depend on precise as-built records to implement changes correctly. Clear specifications and well-kept records help determine if modifications are due to defects or chargeable variations.

3.1. Trade Siloes

Building Control System and Technical building management often operate in isolated trade silos, leading to delays during system failures due to unclear responsibilities and missing contact details or service level agreements. This can increase fault correction costs. Cybersecurity risks are frequently overlooked at gateways and handover points between siloed systems because they lack clear contractual assignments.

Working with other trade silos introduces both technical and contractual challenges. As future customers will assume systems are cybersecure by default, special attention is required when interfacing with third-party systems or trades, especially when connecting to legacy systems that lack or have compromised cybersecurity defenses. Standard practice involves using some form of firewall, edge, or proxy to mitigate security threats. If this interface was not specified properly and security considerations were overlooked, the cost of addressing the security risk becomes contractually undefined.

Sufficient Documentation

System modifications are often needed or requested late in projects. Good documentation helps implement changes and prevents unnecessary costs.

Clear documentation makes it easier to distinguish between changes for fixing faults and those needed to meet contract requirements or approved variations.

3.2. Monitoring of the Building Automation and Control Systems (BACS)

Building Automation and Control Systems (BACS) include sensors, actuators, controllers, and often a supervisory or visualization system. Without proper monitoring, faults and security breaches can go

unnoticed. It is essential to establish a monitoring strategy that guarantees efficient operation, manages system access, and records changes.

This requirement often involves several parties. Devices or data may be part of sub-systems like a KNX line, while services such as trend logs or notifications are handled by the supervision or visualization system. Clearly divide tasks and assign deliverables to specific contracts.

3.3. Role and Authorization Management

For central Building Automation and Control Systems, such as Supervisory Control and Data Acquisition (SCADA), a dedicated system for managing user identities and access rights must be put in place. Poor design or implementation can cause issues like shared logins or former employees still having access, potentially leading to unauthorized entry. It's crucial to address access management and monitor user access rights early in the process.

Commissioning tools like ETS should be treated in the same way. However, these tools often lack role-based access and typically protect only a local database with a password. As a result, anyone with a copy of the ETS project can access it, even if the customer changes the password after handover.

System suppliers and integrators must keep a record of everyone who has accessed the project engineering databases and coordinate security policies with the customer.

4. IT and OT Networks

Cybersecurity for Building Automation and Control Systems (BACS) involves stakeholders from IT and building control trades, each with different safety and operational priorities. Understanding these differences is essential to prevent misunderstandings.

IT (Information Technology) and OT (Operational Technology, including Building Control) networks differ in purpose, environment, and priorities. Here's a comparison:

IT (Information Technology) Networks

- Purpose: Manage data, communication, and business processes.
- Environment: Offices, data centers, cloud infrastructure.
- Examples include Email systems, ERP software, databases, and websites.
- Priorities:
    - Confidentiality (protecting data from unauthorized access)
    - Integrity (ensuring data is accurate and unaltered)
    - Availability (systems are up and running)

OT (Operational Technology) Networks

- Purpose: Monitor and control physical devices and processes.
- Environment: Industrial settings like factories, power plants, and building automation.
- Examples include Programmable Logic Controllers (PLCs), SCADA systems, sensors, and actuators.
- Priorities:
    - Availability (systems must run continuously)
    - Safety (preventing harm to people and equipment)
    - Integrity (accurate control of physical processes)

The stakeholders from the IT and building control most likely have different priorities, and aligning on requirements, cybersecurity deliverables, and priorities is crucial. Each requirement must have a designated primary stakeholder. Additional stakeholders or suppliers can participate, but the main responsible stakeholder should be clearly identified.

Good communication between the IT departments and BACS system integrator is essential to maintain the security of the system. In most cases the OT and IT network need to be managed and administrated by the IT department, as the OT-Network will likely be a Virtual LAN (VLAN) and not a physically separate LAN.

KNX-system integrators should note that KNX relies on multicast IP communication (KNXnet/IP Routing), which IT engineers often try to avoid. Early coordination with the IT department is recommended to address potential issues and clarify requirements.

It is important to ensure not only that the BACS remains secure from attacks, but also that IT settings which permit BACS IP devices to communicate do not introduce vulnerabilities that could allow unauthorized network access.

4.1. Cybersecurity Requirements for Building Automation and Control Systems (BACS)

Establish core security principles while creating BACS requirement specifications. Utilize resources such as AMEV, VDMA 24774, and the BSI Cybersecurity Compendium for guidance.

Although these guides and regulations are designed for the German construction market, they are based on common IT standards and practices, making them a helpful reference for other markets as well. The guides include relevant security topics:

- Building automation networks (interfaces, remote maintenance, etc.)
- Hardening of building automation components (services, accounts, encryption)
- Password policies (complexity, expiration, failed attempts, auto-logout, history)
- Updates, upgrades, and maintenance (hardware, internal/external laptops, interfaces)
- Logging (user actions, data changes, switching, and configuration actions, while respecting data protection laws)

To mitigate cybersecurity risks, the following principles should always be considered when planning a building automation system:

- IT security from the outset.
- Ensure thorough documentation and system transparency.
- Design secure interfaces and consider access controls for central and critical BACS components.
- Plan for ongoing system maintenance and updates to ensure optimal performance.

Many cybersecurity requirements apply to the full BACS system, which is often provided by several suppliers through different contracts. It is essential to assign requirements to the correct stakeholders and confirm they match the commercial agreements.

4.2. Assessment of the Current Condition

Begin by evaluating the cybersecurity of existing equipment, installations, or specified technologies. Do not assume devices are secure without verification. Network segmentation is necessary for proper security. Has this been considered?

- What cybersecurity properties does the existing or specified equipment provide?
- Does the equipment support secure communication protocols, such as KNX Secure, BACnet/SC, or OPC UA?
- Has the existing equipment been configured to utilize encrypted communication?
- Does the specification explicitly require secure equipment to be commissioned to communicate using secure protocols whenever possible?
- If proprietary communication protocols are employed, is the communication encrypted, or is the vendor relying on security by obscurity?
- If non-encrypted communication is used, can a sufficient level of security be achieved through network segmentation and IT security?
- Is enough information available to ensure that the system meets the customer's security needs and policies?
- Who will provide and maintain the OT-Network IT infrastructure and its components?
- What is the handover process for passwords, security keys, or certificates?
- What is the process to monitor who has access to the password, project data, or even the system itself?

System suppliers and integrators are expected to provide accurate information when possible. If certain details are unavailable or if devices lack cybersecurity protection due to limited options, this should be disclosed. The assessment does not determine the final selection; all relevant facts should be presented, and any missing information noted, to support an informed decision-making process.

4.3. Responsibilities and Accountability for Cybersecurity

For each managed system or group, clearly define and document who holds responsibility and accountability. Specific tasks may require additional clarification. Responsibility and accountability can differ; the responsible person, such as the system integrator, should regularly report to the accountable individual, typically the contractor. This communication is crucial for informed decision-making and effective risk management, particularly when multiple parties, such as building owners, tenants, or organizations, are involved in the process.

The terms **"responsibility"** and **"accountability"** are often used in conjunction, but they have distinct meanings, particularly in management and organizational contexts. Here's a simple breakdown:

Responsibility

Definition: Overseeing the performance of a task or duty.

Focus: Action — what someone is supposed to do.

Example: A technician is responsible for maintaining the air conditioning system.

Responsibility refers to the "doing" part. The Building Control System Integrator typically fulfils this role.

Accountability

Definition: Being answerable for the outcome of a task or decision.

Focus: Ownership — The party that is ultimately responsible if something goes wrong.

Example: The Contractor is accountable for ensuring that the building systems function correctly, even if others perform the actual work.

Accountability means "owning the result" and usually refers to the party responsible by contract, often the mechanical or electrical contractor in building controls.

The designation of e.g., the KNX system integrator as a responsible party depends on the specific contractual arrangement. If an electrical contractor supplies the KNX system to the customer and engages the system integrator to handle commissioning, the contractor assumes primary accountability and liability. In this scenario, the system integrator bears a responsibility to the contractor.

4.4. Network Segmentation and Management

A security strategy for Building Automation and Control Systems (BACS) planning must specify protective measures such as data backups, firewalls, and uninterruptible power supplies. Usability requirements should be applied based on the operational concept. The goal is to provide strong protection for the entire building system, including connected systems.

The objectives should be defined during the planning phase as part of a comprehensive Operational Technology (OT) security strategy, which details measures for integrating all OT components. Responsibilities must be assigned to suppliers, system integrators, and ultimately, the building operator. The following elements need to be incorporated into the security strategy for building automation systems.

- **OT Architecture:** Define the structure and components of the operational technology environment.
- **Network Design and Segmentation**: Plan the network structure and divide it into secure zones to limit access and reduce risks.
- **Patch Management**: Ensure regular updates and security patches are applied to all systems and devices.
- **Asset Management:** Maintain an up-to-date inventory of all hardware and software assets in the system.
- **Emergency Management:** Implement backup solutions and redundancy strategies to maintain operations in the event of IT network failures or incidents.
- **Risk Assessment and Protection Needs:** Identify potential risks and determine the necessary level of protection for each system or component to ensure optimal security.
- **Staffing Recommendations:** Provide guidance on the number and qualifications of personnel required to operate and maintain the system securely. It is essential to have staff who understand the specific IT requirements of building control systems.

BACS protocols such as KNX and BACnet are appropriate for network segmentation and asset management. A BACS system designed with fault tolerance, which contains faults within specific areas, can improve robustness and cybersecurity resilience. To enhance BACS resilience and robustness, control functions should be kept as local as possible—ideally on the KNX "green cable".

Apply security patches and updates systematically, verifying system functionality afterward, which may require commissioning tools. It's important to check whether these tools are publicly available, free, paid, or require a commercial agreement with the provider. Anyone can purchase the KNX commissioning tool ETS from the KNX Association.

5. Building Automation and Control Systems Cybersecurity Requirements

The following requirements are based on the German Bundesamt für die Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Baustein INF.14 Gebäudeautomation. This guide offers recommendations and guidance for authorities, companies, and institutions seeking to safeguard their data, systems, and information.

The BSI emphasizes a comprehensive approach to information security, addressing not only technical aspects but also infrastructural, organizational, and personnel issues. This provides a systematic method for identifying and implementing necessary security measures. This guideline is officially only applicable in Germany. However, it is based on best practice IT network security methods and can be used outside of Germany, even though it is not formally binding.

5.1. Basic Cybersecurity Requirements (MUST Requirements)

These baseline requirements should always be applied.

5.1.1. INF.14.A1 Planning the Building Automation and Control Systems (BACS)

Building Automation and Control Systems (BACS) must integrate cybersecurity requirements into their design and development processes. The design should incorporate all BACS controls, including HVAC, lighting, shading, and energy management, utilizing best-practice security concepts, standardized systems, and protocols. Regular updates to specifications and drawings are crucial.

Technology Definition and Selection
Determine the number of siloed automation systems based on:

- Equipment and appliances to be connected.
- Wiring, product availability, and customer needs.
- Required connection and communication technologies.
- Ensure alignment with regulatory and security requirements.

Minimize Use of BACS Technologies
Follow security policies by using standardized communication protocols and avoiding proprietary ones that lack modern security standards.

Reduce Unwanted Interactions and Dependencies in Building Automation
Design each system to prevent errors or failures from affecting other parts of the system; for example, KNX segments isolate systems both logically and galvanically.

Assess whether the device and BACS services rely on continuous cloud service availability. Service providers should have enough flexibility to handle changes in ISP or cloud providers and offer an opt-out option with limited functionality, while maintaining clearly defined offline capabilities.

Key Aspects of Detailed Planning
Secure cross-building networking includes:

- Internet, WAN, LAN, WLAN, wireless networks, and fieldbuses
- Secure communication protocols
- Access protection for central control components
- Securing public ports
- Secure integration of external systems, like facility management
- Protecting and logging remote maintenance access
- Secure IP communication in BACS VLAN networks
- BACS network segmentation

Use of Internet Protocol (IP)
Many BACS protocols, such as KNXnet/IP, BACnet/IP, or Modbus TCP, are based on IP (IPv4 and IPv6). To use IP securely:

- Address ranges must be scalable and well-structured.
- Plan IP mechanisms, such as broadcast and multicast, carefully to avoid network issues.

Protecting Interfaces
Defining protective measures at the interfaces (gateways & routers) with subsystems, controlled equipment, other Building Automation and Control Systems (BACS), and remote or cloud services is essential in building automation planning. This is especially important when:

- BACS must operate independently, unaffected by other subsystems or segments (see INF.14.A22).
- Required subsystems cannot or can only be partially securely integrated into BACS due to technical limitations (see INF.14.A3).

Planning must detail the cybersecurity components and mechanisms, such as:

- Native Security methods provided by the BACS system
- Firewalls protecting subsystems or segments

The detailed planning phase must define all parameters essential for a secure building automation system. It should also provide specific configuration guidelines.

Implementation Planning for BACS
Implementation planning outlines how the detailed planning will be executed. It includes:

- Specifying required steps.
- Defining the sequence, responsibilities, and timeline.

During the final acceptance phase, it must be verified that the implementation exactly follows the detailed plan and that specified requirements are met. Any deviations should be reported to the planning team for analysis and potential correction.

Additionally, the implementation plan must identify all interactions and dependencies between:

- Equipment, appliances, siloed systems, and BACS
- Different Building Automation and Control Systems (BACS).

Based on this, the commissioning (startup) of the BACS must be carefully planned (see INF.14.M2 on commissioning and interface management). The implementation plan should also specify the tests that need to be conducted during the commissioning of the BACS.

Operational Security Planning for Building Automation and Control Systems (BACS)
After completing the detailed and implementation planning, the next step is to plan for the secure operation of the building automation system. This includes specifying at least the following:

- Security measures for BACS management systems (Supervisor,
  (see INF.14.M12 – secure communication protocols, INF.14.M13 – network segmentation, INF.14.M14 – access protection)
- A role and permission model to control who can access what
- Distribution of configuration files to BACS components
- Integration of BACS components into monitoring, alerting, and logging systems
  (see INF.14.M25 – dedicated monitoring, INF.14.M26 – logging in BACS)
- A dedicated backup system for BACS or connection to a central backup solution

Staffing and Availability Considerations
Since Building Automation and Control Systems (BACS) often require 24/7 availability, it's essential to plan for situations where trained personnel may not be on-site. This means:

- Either adapting processes to match the skills of available staff

- Or training staff so they can handle urgent tasks when needed
  (see INF.14.M27 – accounting for interactions between BACS components in emergency planning)

Ongoing Reviews and Compliance Checks
To maintain or improve information security:

- Regularly review all planning documents and concepts
- Compare the planned vs. actual system state
- Check whether systems are configured according to specifications
- Document all findings clearly
- Justify or immediately fix any deviations

It is necessary that requirements are broken down into individual components that can be linked to specific commercial contracts. In addition to specifying deliverables and required security features, it is also important to document any known limitations and agreed deviations from established security policies. For instance, certain field devices may need to communicate without encryption, and a risk assessment might determine that this poses minimal risk. According to EU cybersecurity regulations, such as the Cybersecurity Resilience Act, this is permissible provided the supplier can demonstrate that the customer was explicitly informed and both parties agreed.

5.1.2. INF.14.A2 Commissioning and Integration Schedule

Effective coordination of technical and Building Automation and Control Systems (BACS) is vital for smooth building operations. Clearly defined interfaces between teams must be established and documented, with regular reviews and updates to maintain ongoing effectiveness and efficiency. Any modifications should be reflected in updated definitions. This documentation must detail all security measures for building control systems and technical facility management. It should be well-organized and easy to understand, explicitly outlining requirements and specifications for secure operations. Specific security policies for each trade domain should align with the overall security framework.

Commissioning Management
Commissioning management guarantees that a building functions as intended and fulfills operational requirements. Its main role is to coordinate various trades and stakeholders throughout all project stages and during the building's initial use. Since numerous trades and components are involved, commissioning needs to be planned across disciplines and should be incorporated early in the building design. Commissioning must also take into account the different roles that interact with building automation, such as:

- Building users or tenants
- Internal or external operators (e.g., facility management) managing BACS and related control siloes, e.g., lighting control, HVAC control, or energy monitoring and management.
- External service providers needing access for maintenance
- Facility managers for administrative tasks and optimizing costs
- System administrators are responsible for backups, system settings, and support
- Installers who update software or firmware

One person might assume several roles, or one role can be occupied by multiple groups (like different tenants in a building).

Commissioning management must also consider the dependencies and interactions between BASC components and other building systems. For example, the sequence in which systems are made operational should be determined and coordinated. Key points to define include:

- The order of commissioning building systems

- The sequence for connecting control silos and applications to BACS
- The process for connecting BACS to other systems (like technical management)

Checkpoints should be established to ensure that each step is completed before the next one begins. After construction and initial commissioning, procedures should be reviewed for the operational phase. Temporary access accounts, which are used only during commissioning, should be deleted.

Commissioning management remains crucial during operation. For example, restarting a system can disrupt automation, so it should be clear which systems need to be restarted together and in what sequence. Updating systems must also be handled carefully. These commissioning plans are essential for effective emergency planning and system safety operations.

During the commissioning phase of a building control system, multiple engineers—including some freelance contractors—may access engineering databases. Security features like firewalls are sometimes disabled to speed up commissioning and troubleshooting. To reduce liability, it's important to document these actions and implement appropriate risk mitigation measures.

5.1.3. INF.14.A3 Secure Integration of Control Silos

To ensure effective interaction between control silos and the overall Building Automation and Control Systems (BACS), it is essential to clarify whether individual control silos or their components can initiate actions. The automated actions triggered by BACS should be clearly defined and carefully managed.

In cases where a control silo—such as access control or emergency systems—cannot or should not be fully integrated into BACS but still requires limited data exchange, the specific nature and extent of the information shared with the building automation system must be clearly defined.

Both full integration of a control silo with BACS and the non-intrusive connection of siloed systems to an overarching BACS require robust security measures. This involves careful planning of process and function chains, whether within a single automation system or across multiple systems. All transitions between control silos and technologies must be thoughtfully considered and planned. Extensive testing of these processes and functions is essential, with iterative adjustments made based on identified issues. All definitions must be accurately documented, with regular reviews to keep the documentation current. Any discrepancies should be promptly resolved.

As part of the planning process, all control silos and components relevant to building automation, including their interfaces, functionalities, and critical parameters, must be systematically documented. Where practical, systems should be sequentially connected to BACS, facilitating the rapid detection and resolution of errors.

Key steps for integration or connection include:

- Independently test each control silo (for example, the KNX system) and its components before integrating them with the overarching BACS.
- Address any issues encountered during these independent tests before connecting to the BACS.
- Ensure that segment or silo control systems retain autonomous operational capability, particularly in emergencies.
- Sequentially test the integration of siloed subsystems (e.g., the KNX field control system) with BACS before full deployment.
- Guarantee that only explicitly defined data and actions are exchanged between BACS and the connected siloed control systems.
- Restrict communication between BACS and connected siloed subsystems to authorized channels and methods.
- Resolve any problems before linking subsequent systems or commencing full-scale operations.

Integration of Building Systems

Siloed control systems, such as a KNX room's control system integrated into a BACS, can be influenced by messages or data from a central BACS component or other siloed system, like a BACnet system managing the central HVAC plant. Therefore, integration must be carefully planned and thoroughly tested.

Minimum requirements:

- During setup, define acceptable ranges for all key parameters, such as the maximum and minimum values or heating setpoints.
- Specify which automated actions can be triggered via an interface to a control silo, either by BACS or other control siloes

A system is often supplied by an individual control silo. The interfaces between two silos may need to be defined. Further we need to consider that siloes system may be handed over in different project stages. Delays and variations encountered in one control silo may affect other siloes.

In cybersecurity, the shift to encrypted communication in BACS systems has introduced new challenges. Security information is often only accessible after commissioning, delaying interface development, and last-minute system changes can require updates to security data. For example, replacing a central KNX DATA Secure device such as a secure touch panel affects group keys, which are essential for supervisory or visualization systems communicating with KNX. Additional work may be required in other control siloes.

While KNX and BACnet set security and communication standards for their own gateways, they don't govern the security or functionality of third-party clients receiving data through these gateways. These security properties should be indicated in the project specification.

5.1.4. INF.14.A4 Integration of Critical Systems

Health, safety, and security systems should connect with building automation systems in a way that prevents feedback or interference, remaining separate from full BACS integration. For network connectivity, it is recommended to use physically separated network components and segments.

Utilize certified and standardized protocols to ensure the reliable integration of components from different manufacturers. The following requirements relate to integrating alarm systems into networks:

- Critical system segments must maintain both functional and technical independence, ensuring continued operation even in the event of connectivity issues or data loss from the broader network.
- Physical separation, such as dedicated cables and hardware, should be implemented to ensure optimal performance. Critical system components must operate independently of external network services, maintaining full functionality even during service interruptions in another segment or systems.
- Network connections with other systems should be controlled to prevent any adverse impact on alarm system performance due to incorrect or extraneous external data or signals.
- Security tools, including firewalls, must be employed to manage and regulate all data and signal connections systematically. Alternatively, unidirectional transmission may be adopted, permitting solely outbound data flow.

All unauthorized or unnecessary communication with critical system segments must be blocked. When choosing wireless technologies and frequency bands, measures must be taken to prevent interference between alarm systems and other devices, as well as among multiple alarm systems (refer to INF.14.M15 and INF.14.M16).

KNX systems are generally not used for critical applications, largely due to historical and commercial factors rather than technical limitations. When using KNX, consider whether device monitoring, runtime communication monitoring, or devices with control algorithms for defined fault states are needed.

5.1.5. INF.14.A5 Documentation of Building Automation and Control Systems (BACS)

All enabled and disabled physical communication interfaces, protocols, and access points related to BACS should be documented. Additionally, interactions and dependencies between BACS-related

components and any connected or integrated technical systems must be recorded. The security features of the protocols in use should be included in the records. Keeping comprehensive and current documentation enables effective system management. Regular review and updates help maintain accuracy regarding the system's status. Accurate documentation facilitates issue resolution, dependency identification, and the evaluation of proposed modifications.

Operational changes should be documented, and systematic reviews should be conducted to identify and address any alterations or exceptions that may arise. The format of documentation must align with the requirements of each BACS installation. Documentation may be maintained separately for individual Building Automation and Control Systems or consolidated, depending on specific needs. To maintain compatibility, the data structure and required content for each system, including connected control silos, should be specified. Centralizing system documentation in a shared repository, such as an online platform, supports convenient access and sharing.

Documentation must remain accessible at all times, including during outages or emergencies. This can include maintaining backup copies on emergency systems or providing printed versions at designated locations. It is also important to implement measures to protect documentation from unauthorized access.

Creating as-built project documentation is often challenging, as many system integrators lack the tools or time for it. Frequently acting as subcontractors, they may rely on the electrical contractor—who supplies the KNX system and holds responsibility for documentation. This setup can result in thorough records of physical installation but insufficient documentation of security and commissioning details.

5.1.6. INF.14.A6 OT and IT- Network Segregation

Operational Technology (OT) networks must be logically isolated from general IT networks and all other institutional networks. Communication between Building Automation and Control Systems (BACS) and other IT systems must be monitored and controlled. To accomplish this, security devices, such as firewalls, should be placed at all points of transition between these networks.

Historically, BACS (Building Automation and Control System) networks were isolated from the larger organizational network through physical separation, particularly for critical systems such as alarm setups. Today, however, BACS increasingly needs to integrate with building management and office IT systems and often manages multiple facilities. Setting up separate physical networks for each BACS has become generally impractical.

For multi-site deployments, BACS networks can connect via campus or wide-area networks but must remain logically separate using technologies like VLANs. External or third-party access should be carefully controlled. Firewalls should protect connections from other networks to BACS and, ideally, be segmented by application. Physical separation isn't always required. Remote third-party maintenance must follow strict remote access protocols.

Separation of Network Services

BACS has distinct security requirements, particularly regarding availability, and network services must meet these standards.

Internet Access

When BACS devices share the organization’s main internet connection, the connection must meet BACS security standards while ensuring logical separation. If BACS operates on a separate network with independent internet access, it must follow established cybersecurity rules and only permit essential outbound connections.

Separation of End Devices

Ways to separate BACS end devices include:

- Assigning dedicated, marked VLAN ports for BACS on shared switches.

- Using network access control (NAC) to zone devices by port.
- Deploying entirely separate physical switches for BACS, if needed.

Typically, IT and OT networks are virtualized over a single physical network, creating several challenges:

- OT networks need to be operational early in a project, while IT networks are not required until after building handover and occupancy.
- IT systems are provided by tenants, not as part of the permanent infrastructure, and roles for OT network provision and maintenance are undefined.
- IT departments often request security features common in IT but unsupported in BCS.
- Communication between BACS system integrators and IT departments is difficult due to differences in networking expertise.

Effective communication between the IT department and the BACS system integrator is essential.

5.2. Standard Cybersecurity Requirements (Should Requirements)

In addition to the basic requirements, the following criteria reflect current technology standards and should generally be met.

5.2.1. INF.14.A7 Definition of Cybersecurity Policy

In accordance with standard security policies and IT security guidelines, a Building Automation and Control Systems security policy should clearly outline cybersecurity requirements. A security policy serves as the fundamental framework for establishing requirements and strategies related to BACS. While it is not a technical specification or requirements document, it outlines general rules that apply to all Building Automation and Control Systems (BACS) and their components. This policy is essential and must be communicated to all stakeholders involved with BACS, including any updates that may be made. Regular communication helps ensure stakeholders stay informed about security directives.

Regular compliance checks, such as benchmarking against standards, are recommended. For example, KNX systems require clear guidelines for ETS password and Device Certificate management. For other BACS components and subsystems, user roles and permissions should be correctly assigned.

The policy should be regularly reviewed to ensure it stays aligned with technological advancements.

Key areas to be addressed by the security policy include:

- Guidelines for identifying which control silo systems are managed or interfaced through BACS.
- Criteria for identifying systems that need independent operation and the protocols managing their interface with BACS.
- Requirements for choosing and utilizing tools, such as commissioning tools like ETS.
- Policies and procedures for securely connecting less-trusted BACS components, including processes for managing legacy systems that do not meet current security standards. New components should comply with existing security requirements where feasible.
- Guidelines for remote maintenance tools or services accessing BACS networks or components.
- Policies concerning physical security, system access, and user permissions ensure that critical BACS components are in secure zones and that access rights adhere to the principle of least privilege. Access should be granted based on authentication, and these requirements must be documented, with personal accounts used for system interactions.
- Requirements for secure communications, including approved protocols for use in BACS and criteria for exceptions to these protocols.
- Monitoring requirements specifying monitoring frameworks and identifying the types of components being monitored.

Depending on institutional arrangements, a consolidated security policy may encompass both Technical Facility Management and BACS; however, BACS-specific security requirements must always be considered.

If technical facility management is handled by an external party while BACS remains institutionally managed, the technical facility management security policy should be aligned with the BACS security policy.

5.2.2. INF.14.A8 Cybersecurity Specification for Building Automation and Control Systems

The specifications must cover all key aspects related to the architecture, design, and connections of each system. These documents must be consistently updated to incorporate technological advancements and undergo periodic review during the implementation process.

The requirements specification establishes the BACS security policy through a two-step process: first, a detailed requirements analysis is performed to assess and organize the collected requirements, and then, clear requirements are defined for all relevant BACS components.

Per the Cybersecurity Policy, the specification should provide:

- A complete requirement specification for the Building Automation and Control Systems (BACS).
- Separate requirement specifications for each BACS subsystem.
- Evidence of compliance with relevant legal and regulatory standards.

Detailed Requirements Analysis

During the analysis phase, organizational and technical requirements for secure BACS operation are identified. This includes planning requirements, integration specifications, and gathering customer feedback. Both functional and non-functional needs, especially information security and BACS access points, are assessed.

In new facilities where user groups have not yet been identified, general BACS requirements should be established during the planning stage to accommodate future adjustments.

Operational considerations should also be included in the analysis. Secure BACS operation generally requires trained personnel. As a result, specific needs might arise due to limited support outside regular business hours; for example, issues with key HVAC plant components may need to be addressed overnight using pre-configured replacements. Operational security requirements, including incident management, must be evaluated.

Requirement Specification

The resulting specification document consolidates both organizational and technical information security requirements derived from the analysis, covering all relevant BACS components and operational parameters. It also includes clear requirements related to the network architecture and infrastructure.

Provisions for system scalability ensure that both current and future operational needs are considered. When all requirements are systematically prioritized and documented, referencing these specifications during procurement helps reduce the risk of unsuitable last-minute purchases.

At a minimum, specifications should include

- Specifications for IT systems and 3rd party interfaces, i.e., web browsers accessing BACS-relevant components.
- Definitions of permissible access methods (e.g., remote access solely via jump server)
- Determination of roles and permissions
- Specification of permitted protocols for access
- Identification of requisite security features (encryption, authentication, authorization, integrity verification)
- Access restrictions, including emergency protocols
- Definition of advanced security mechanisms, such as the four-eye principle for administrative activities

Ultimately, the BACS requirement specification acts as the basis for both concept development and subsequent detailed work planning.

5.2.3. INF.14.A9 Building Automation and Control Systems Concept

A comprehensive Building Automation and Control System (BACS) plan should be created in accordance with relevant cybersecurity guidelines and standards. Each BACS system requires a detailed strategy that addresses integrated or connected siloed systems, all BACS-related components, and their communication links.

The plan must specify technical and organizational requirements, with regular reviews and updates as necessary. BACS should reduce dependencies between segments and subsystems to ensure that failures remain contained. Each building segment must be independently controllable, and configured segments should be visible in management interfaces.

The BACS concept establishes a foundation for dependable and cost-efficient operation by outlining the architecture, tasks, and rules for both routine use and system modifications. It serves as a high-level framework that is further developed during planning and should address both organizational and technical concerns.

At minimum, include:

- System layout and segmentation
- Function descriptions and automation diagrams
- Interfaces to other systems
- System dependencies
- Communication protocols
- Network segmentation
- Availability measures (e.g., redundancy)
- Role-based permissions
- Access control

Regularly review and update the BACS concept to reflect current technology and practices, ensuring it aligns with the actual system and detects any unauthorized changes.

From a commercial perspective, it is important to consider both the contractual and technical boundaries of individual control silos. It is necessary to ensure that work items or hardware are clearly assigned to a specific contract.

When switching to encrypted communication, certificates or passwords in a control silo may need changes, potentially affecting integration with other silos. Identify interfaces where such impacts could occur. The control concept should account for cases where security adjustments in a subsystem can't be immediately reflected in the main building control system. Essential control functions must remain operational even if security details aren't yet updated.

5.2.4. INF.14.A10 Building Automation and Control System Segmentation

It is crucial to design the Building Automation and Control System segments with minimal interdependencies, ensuring that each segment can be managed independently. A malfunction in one area should have little to no impact on the others.

Standardizing BACS Areas for Efficiency and Stability
BACS siloes that serve similar purposes, i.e., room control, should adopt the same technology to facilitate easier planning, enhance day-to-day operations, and maintain system stability. Example: If you have a floor with offices or meeting rooms and each space has its own lighting, shading, and climate

control, it's best to manage these BACS features locally. Whenever possible, a BACS zone or segment covering several areas should stay operational even if the main system fails.

Network Architecture and Segmentation

To avoid disruptions, BACS areas should be separated into sub-networks:

- **Subnet Isolation**: BACS segments or areas should be assigned to their own subnet, such as a KNX line. This helps prevent one area from impacting another, for example, if a faulty device floods the network with messages or if there is a wiring problem.
- **Management Visibility**: Each BACS sub-network should be easily identifiable, controllable, and manageable by a BACS management system or BACS commissioning tools, such as ETS.

Security and Addressing

- **Dedicated Network Components**: Each BACS area should utilize its own network hardware, such as a KNX Router or Coupler, to meet security requirements.
- **IP Address Planning**: IP communication with and between BACS areas should be controlled and restricted using firewall functions, depending on the overall security requirements of the BACS or individual BACS areas. Firewalls must be adequately documented. If they are not, it can be challenging and time-consuming to detect faults during troubleshooting.

Planning and Dependencies

Before defining and designing BACS areas, all dependencies between them and other BACS-related components should be identified.

Firewall and Access Control

- **Controlled Communication**: Depending on security needs, communication with BACS areas should be regulated using filter functions.
- **Transparent Firewalls**: These can be used to separate BACS areas without changing their subnet structure. They allow control within a single subnet.
- **Documentation**: Firewalls must be documented. If not, they can be challenging to work with during troubleshooting and cause delays.

A well-designed KNX system easily meets these requirements. KNX infrastructure components logically and galvanically isolate lines, areas, or segments. Following KNX guidelines distributes functionality within each segment.

5.2.5. INF.14.A11 Control and Restrict Access

Control and restrict unauthorized or unknown devices from connecting to the Building Automation and Control Systems Networks. Log connected devices and block unauthorized communication on the OT network. Use network access control to isolate unauthorized devices. Activate temporary maintenance interfaces (VPN ports) only when necessary.

Access to IP networks is managed by OT network settings and administrators, while access to BACS devices, services, and data is determined by BACS settings.

5.2.6. INF.14.A12 Secure IP Communication

Use secure protocols to communicate over Ethernet and IP, especially on untrusted networks. Encrypt BACS-IP traffic using current standards, such as KNXnet/IP Secure, OPC-UA or BACnet/SC.

Sensitive information not transmitted through native and standardized BACS IP protocols should be securely sent using current secure communication protocols, such as HTTPS (for web traffic) and FTPS (for file transfers), both of which are protected with valid TLS encryption. If proprietary IP protocols

are used by building automation components, assess their security and ensure they utilize encryption and are not relying on obscurity for security.

If IT network access control is not feasible, protect ports using one or more of the following:

- Restrict communication at the access switch (Port Security).
- Configure access switch ports connected to public BACS components to allow only specific IPs and ports.
- Secure ports physically, such as with locked cabinets or port locks, so connections require approval.

5.2.7. INF.14.A13 BACS Network Segmentation

Segmenting the network to isolate individual systems and control zones is essential. Establish rules for transitions between segments and enforce them with security components, such as routers or gateways. The first step is to create a communication matrix that shows which BACS-related components communicate with each other within the system and which ones connect with systems outside of BACS. This matrix should also specify the protocols being used and the organizations involved as the user or operator.

Communication within individual network segments is generally unrestricted, but any communication between segments should be controlled and limited to what's necessary for operation. Connections should typically be made from the segment with higher security requirements to the one with lower needs. Firewalls are recommended to manage communication between segments.

At a minimum, consider these areas for a review of the segmentation:

- Entire Building Automation and Control Systems (BACS)
- Groups of control silo installations within a BACS system, e.g., a group of KNXnet/IP or BACnet/IP networks
- Individual control of silo installations within a BACS system, e.g., the primary plant control systems
- BACS components belonging to different user organizations, e.g., a BACS Supervisor that is interfacing with multiple control silos and protocols
- Network areas managed by different organizations

The segmentation of networks within control silo installations should adhere to the rules of relevant industrial standards, such as KNX or BACnet.

When planning and implementing segmentation, all business requirements and dependencies must be considered. Segmentation should not compromise the necessary system stability.

Both the existing network segments and the communication matrix should be regularly reviewed, especially after updates such as upgrades to control silo installations. These reviews must be thoroughly documented, including all security components, such as firewalls, particularly transparent firewalls used for micro-segmentation.

Micro Segmentation of Insecure BACS Components

To secure BACS, isolate less secure parts by separating devices with unencrypted communication and applying micro segmentation based on risk. Use secure proxies or encrypt data for transmission between segments. Both KNX and BACnet protocols offer suitable methods for this. Micro segments must be connected according to defined security policies.

5.2.8. INF.14.A14 Access Control for Central BACS Devices and Software.

Implement an identity and access management system for central building automation devices, tailored explicitly to BACS requirements. This may involve deploying a dedicated BACS authentication solution or integrating with the institution's central IT authentication system.

Roles and permissions must be precisely defined, including BACS system operators, technical equipment operators, and other relevant users, especially in complex, multi-silo control environments.

It is crucial to assign clear roles (like tenants and operators), limiting permissions to only necessary functions; for instance, tenants should only access their assigned areas. Roles must be updated quickly after organizational changes, such as tenant changes or construction work.

Standard permission levels typically include read-only and read/write. Full admin rights should be reserved solely for qualified personnel during initial setup or significant modifications.

Commissioning tools and project data should be protected with strong passwords, and all access to engineering tools and databases needs to be logged and monitored.

Whenever feasible, replace insecure devices that lack port security or password protection. Maintenance devices should be isolated from the main network through segmentation and strict access controls. Additionally, avoid components with manufacturer-defined credentials that cannot be changed.

Check if software and commissioning tools are readily available, and whether access depends on maintenance contracts or subscriptions. According to the EU Cyber Security Resilience Act, hardware suppliers must provide free security updates for the product's average lifetime (at least 5 years), although this only applies to security updates.

5.2.9. INF.14.A15 Security Mechanisms for BACS Networks

Whenever possible, secure BACS IP protocols—such as KNXnet/IP Secure, OPC UA, and BACnet/SC—should be used. Both authentication and encryption are advised. Communications with BACS-specific networks should generally be monitored and, when appropriate, restricted using security-enabled gateway components. For BACS-specific networks, security measures consistent with those used for primary network segments should be implemented.

Communication encryption should utilize current industry-standard methods. For example, BACnet/SC uses the latest TLS 1.3 protocol for both IPv4 and IPv6, whereas KNX IP Secure employs AES-128 encryption.

If a BACS component cannot support adequate security, its deployment must undergo risk analysis. Legacy systems may not meet modern security standards due to technical limitations. If they continue to be used after a risk evaluation, a phased plan for their replacement should be created. In the meantime, such devices should be isolated within dedicated subnets, and their traffic closely monitored and controlled at network connection points. This can be achieved using gateways with BACS-specific security implementations, such as security proxies.

Gateways to BACS-specific networks must be configured only to allow authorized communication. For Ethernet-based BACS networks, such as BACnet/IP and KNXnet/IP, it is recommended to deploy switches that support Access Control Lists.

Finally, the network architecture must guarantee that there are no unintended connections or shortcuts between network segments via BACS networks or gateway devices.

5.2.10. INF.14.A16 Wireless Communication

Many building automation and control systems (BACS) utilize wireless communication methods like Wi-Fi, Bluetooth, Zigbee, LoRaWAN, EnOcean, or KNX-RF. These technologies each have their own security features, often employing encryption such as AES-128 or AES-256 to safeguard data.

To keep wireless BACS networks safe:

- Always implement strong encryption and authentication for wireless communication, adhering to the latest standards.
- If a device or system can't support secure communication (such as strong passwords or encryption), its use should be reviewed, and risks should be assessed. Try to limit or replace insecure devices as soon as possible.
- Only allow known and approved devices to connect to the wireless network. Set up access controls on devices, such as Wi-Fi access points.
- Check for possible wireless interference from other devices and networks, especially in the 2.4GHz band (used by Wi-Fi, Zigbee, etc.). Plan and test carefully to prevent disruptions.
- Determine which systems should have priority in using specific frequency bands to prevent BACS devices from being affected.
- If interference can't be resolved by adjusting settings, think about switching to a different wireless technology or frequency.
- Physical obstacles, such as steel walls or special windows, can interfere with wireless communication. Plan building layouts and test wireless coverage before deployment.
- Avoid using wireless communication in areas with high interference, outdoors, or where frequency conflicts cannot be resolved.

By following these guidelines, BACS wireless networks will become more secure, reliable, and less vulnerable to disruptions from other technologies or environmental factors.

5.2.11. INF.14.A17 Use of Mobile Networks for BACS

When integrating mobile networks into Building Automation and Control Systems, it is crucial to fully utilize their security features. Direct, unregulated IP-based communication with BACS components over public mobile networks like 5G or Sigfox should be strictly avoided.

BACS components should only be connected to public mobile networks when absolutely necessary for operational needs, following a thorough assessment of this requirement. If public mobile networks lack proper network segmentation, an Application Layer Gateway should be used to isolate IP communications. The use of coupling elements with firewall features is recommended to protect mobile networks linked to Building Automation and Control Systems

Security features vary depending on the mobile technology used; therefore, it is essential to evaluate whether a specific technology meets security needs before selecting it. When connecting via public mobile networks, organizations should ask about the provider's security measures (including encryption) and add extra encryption if needed to safeguard sensitive data. BACS devices often connect to cloud services or external providers through embedded SIM cards; these links must be secured with firewalls, allowing only temporary, device-initiated access.

Low-Power Wide Area Networks (LPWAN), initially designed for IoT applications, are now being increasingly implemented within BACS. These networks enable low-power devices, such as battery-operated sensors, to transmit data over extensive distances to a designated gateway.

5.2.12. INF.14.A18 Communication Interfaces to External Systems

Communication between the Building Automation and Control System (BACS) and external systems should occur only through clearly defined interfaces with specified cybersecurity features. The communication must be authenticated and encrypted. The number of interfaces to external systems should be limited to what is necessary.

When Building Automation and Control Systems (BACS) need to connect with external systems, such as facility management, office IT, or other external networks, consider the following points:

- Document all connections and dependencies between BACS and outside systems.
- Limit and control communication to specific interfaces, protocols, and systems.
- Avoid unnecessary external communication. Allow it only in exceptional cases.
- If BACS shares resources (such as networks or directory services) with other systems, establish clear rules for availability, security, and access rights.
- Specify who is responsible for changes and maintenance on shared resources.
- Include any third parties involved with shared resources in these agreements.

5.2.13. INF.14.A19 Use of Dedicated IP Address Range for BACS

Dedicated IP address ranges should be assigned specifically for Building Automation and Control Systems (BACS) and must be separated from those allocated to office IT or other operational technology (OT) systems. It is essential to identify which parts of the address range will be used for static IP assignments and to specify which BACS components require static addresses.

IP addresses should be assigned systematically and logically to represent the associated building and device type. When devices use DHCP for automatic address assignment, it's essential to distinguish between dynamic and static address ranges. Since most BACS devices operate on static addresses, careful planning is vital to avoid conflicts.

In situations where network segments are duplicated across multiple buildings, use Network Address Translation (NAT) or similar methods to prevent address conflicts. Recognize that protocols specific to BACS, such as BACnet and KNXnet/IP, may only utilize parts of the network; therefore, addressing planning for these network areas is also recommended. In summary, managing IP addresses for BACS helps ensure separation, clarity, and efficient administration.

Certified KNXnet/IP Routers and Interfaces are compatible with DHCP. However, KNXnet/IP clients, such as visualization systems, may not consistently support DHCP functionality.

5.2.14. INF.14.A20 Broadcast Communication

In OT networks for building automation, minimize broadcast traffic at OSI Layers 2 (Data Link) and 3 (Network) to avoid overload; preferably, use unicast or multicast whenever possible. Use broadcasts only when necessary and properly segment the network.

Configure BACS routers to prevent forwarding broadcasts unless specific subnets require them. Devices that require broadcasts should be on a shared subnet, isolated from other devices sensitive to broadcast traffic.

5.2.15. INF.14.A21 Ensuring Displayed and Control Values are Up to Date

For remotely monitored building control systems, it must be clear whether displayed data—such as values or status—is current. The system should detect outdated critical data and either alert users or activate a fault response to protect occupants and the building. Simulated or "frozen" data should be flagged or trigger an alarm as required.

Most KNX devices can send key values like temperatures and valve positions cyclically. They can also monitor communications, and if an update isn't received within a set period, they switch to a predefined fault position to safeguard occupants and the building.

This functionality can be applied to monitoring systems, which may observe the cyclic transmission of key values or monitor fault signals sent by KNX devices as part of communication monitoring. As field-level twisted pair devices, KNX devices do not include a user fault notification service. However, they offer adequate services that allow for monitoring by supervisory systems.

5.2.16. INF.14.A22 Self-sufficiency as a Security Principle

Building Automation and Control System, subsystems, and system segments should be designed to operate independently according to their protection requirements, even if connectivity to the main BACS fails. These systems or segments should be built to minimize critical dependencies on central BACS components, other subsystems, or system segments. In case of a connection failure, a BACS is expected to remain operational for a specified period, as determined by its required protection level.

It is crucial to identify all dependencies among control silo systems, their devices, and any connected systems. The minimum operational duration and functionality required for each system to function independently should be determined.

Some BACS and IoT devices require uninterrupted internet access. If a device cannot function without an internet connection for the necessary duration, alternative products or establishing a secure, dedicated internet connection for BACS should be considered.

This security design principle is also a fundamental element of KNX System Design.

5.2.17. INF.14.A23 Robust Components

Depending on operating conditions, durable components should be used in Building Automation and Control Systems (BACS), especially in challenging environments. If such durable components are unavailable, appropriate compensatory measures should be implemented.

The KNX Standard requires that certified KNX products have a minimum useful life of 10 years.

5.2.18. INF.14.A24 Time Synchronization

Components and systems connected should use synchronized time if required for automated measurement, control, and regulation. Building Automation and Control Systems (BACS) that are connected should also share the same time. If the Building Automation and Control System (BACS) spans multiple buildings or sites, time synchronization must be ensured across all of them.

If real-time communication is needed within a Building Automation and Control System (BACS), native BACS Point-to-Point, multicast, or similar methods — such as native KNX communication — should be used for time synchronization instead of relying solely on NTP (Network Time Protocol).

5.2.19. INF.14.A25 Status Logs

Security-related runtime events and device availability must be logged for BACS critical devices. An appropriate monitoring plan should be developed and implemented. The availability and key parameters of BACS-related components should be continuously monitored. If errors or set limits are reached, these should be automatically reported to the operating organization. The BACS should at least trigger alarms if systems fail or if essential automated control functions are unavailable. It should also specify which security-related or other events should automatically generate alarm messages. Status reports and monitoring data should only be transmitted over secure communication channels.

This requirement is usually addressed at the automation or management level, with KNX supplying the field-level events to be monitored.

5.2.20. INF.14.A26 Change Logs

In addition to the requirement to log status changes, security-related events should also be logged. All configuration changes to technical building systems. This includes software or firmware updates, which must be recorded. It should be specified which log data is collected in a central logging system. Since changes may involve wiring, physical modifications, or configuration adjustments made with external protocol-specific configuration tools, obtaining valid logging data directly from the BACS itself may not always be possible. Instead, it may rely on commissioning and site reports generated by installers,

maintenance staff, and system integrators. Log data should only be transmitted over secure communication channels.

For KNX standard systems, configuration changes are made using ETS, which keeps a record of all modifications.

5.2.21. INF.14.A27 Emergency Planning

Regularly assess how Building Automation and Control Systems (BACS) impact emergency planning. Establish guidelines to minimize disruptions if BACS components fail due to technical issues or cyberattacks. Emergency plans should include contact information for maintenance staff and their authorized levels for managing emergencies.

Outline procedures to sustain essential operations during BACS failures and document restart plans for all systems, specifying the restart order.

Consider emergency and fault recovery procedures beyond the defects period and maintenance contract term, since building control systems should last over 10 years. Suppliers may cease operations or contracts may lapse during this time. For KNX systems, long-term support is ensured as long as a valid ETS project and project passwords are maintained.

5.3. Requirements for Critical Systems with Enhanced Cybersecurity Needs

These additional requirements provide enhanced security. Consider them if you need higher protection, based on your risk assessment.

KNX systems are typically not used for applications requiring high security.

5.3.1. INF.14.A28 Dedicated Physical Network for BACS

For greater protection, Building Automation and Control Systems (BACS) networks should be physically isolated. Connections to external cloud services should be established through dedicated, tightly controlled internet access. Furthermore, connections to untrusted networks, including the internal office network, should be blocked in accordance with the protection requirements of BACS.

5.3.2. INF.14.A29 OT-Network Segmentation

To protect specific building systems with higher security requirements, such as health and safety systems or security systems, a separate OT network segment should be considered to keep them isolated. This allows for monitoring and controlling communication.

5.3.3. INF.14.A30 Dedicated Time Server for Critical Systems

For enhanced security, provide a dedicated time server for BACS or individual building subsystems. This server should utilize GPS or another time source, in addition to NTP.

6. Conclusion: A fault-resilient BACS system also has good resilience against cybersecurity risks.

The first line of defense against cybersecurity threats is a well-designed and fault-resilient building control system. If the system is well-segmented, there are no central points of failure, and the control functionality is distributed and kept as local as possible. This approach minimizes vulnerability and enhances the overall security of the automation solutions, such as those offered by ABB's KNX systems. Ensuring robust segmentation and local control can significantly reduce the risks associated with cyberattacks.