SAUTER
Für Lebensräume mit Zukunft.

IT Security in Building Automation

White Paper

Document number: D100236537
Revision: 03
Version: 01

Im Surinam 55
4058 Basel
Switzerland

Tel.: +41 61 – 695 55 55
Fax: +41 61 – 695 55 10
www.sauter-controls.com
info@sauter-controls.com

Document number: D100236537
Revision: 03
Version: 01

Contents

List of changes

Date	Rev./Ver. issue	Change	Section	Page
03/2021	03/01	General revision		

List of figures

List of symbols

Information

Information relevant to handling the product.

Call to action

The reader is called to action.

Internet link

Reference to links or applications on the internet.

Warning instruction

Warning instructions are written in front of the action.

Structure

Nature and source of the danger

Consequences

- Action required

1 Executive summary

The topic of IT security in building automation (BA) is no longer a pipe dream that can be easily circumvented. The IT landscape has changed radically in recent years. In addition to the general accessibility of BA solutions via the Internet, two other massive changes have taken place in recent years. On the one hand, the virtualisation of applications and outsourcing to the cloud has led to new solutions but also new providers. And on the other, the rapid growth of the IoT “Internet of Things” has led to incredible amounts of new devices and data, exponentially increasing the need for Internet communication and access to cloud services.

Where recently BA could be seen as an isolated solution, full integration with many other equipment systems and devices is now required. This is also bringing about a change in user behaviour and expectations. Overall, this leads to a proliferation of attack opportunities for cyber criminals.

However, in contrast to general IT applications, with building automation it is not just data which is at risk. Since BA systems are physically connected to the technical equipment of the building (ventilation, lighting, doors, access control systems), any attacks can compromise the security of the building itself.

The actual risk each building faces is project-specific and greatly depends on its vulnerability and on the scope and depth of the BA.

The measures used to protect a BA system are of three fundamental types: Protection of individual devices / PCs / software, protection of the IT infrastructure, i.e. networks and network access, and lastly protection measures in the processes.

Protective measures for devices / PCs / software already start with the manufacturer. IEC 62443-3-3 provides a list of requirements for which manufacturers should provide solutions. The protective measures for the IT infrastructure and the remaining measures for the devices / PCs / software are implemented by the installation contractor, with clients, general contractors and specialist planners setting out the general conditions, particularly the cost framework, in their tendering specifications and bills of quantities. There are both international standards (IEC-62443 etc.) and recommendations from national associations, especially for critical or strategic systems.

The efforts to ensure IT security extend throughout the development process of a system, from the manufacturing of the components, via project engineering and commissioning through to maintenance and operation. An adequate standard of security can only be achieved if all those involved play the part required of them. The security precautions must be proportionate to the risks. And risk analysis is essential.

This white paper, “IT Security in Building Automation”, provides an overview of the individual security measures that can be taken. The diagrams and illustrations contain additional information on the various threats. For a

systematic approach, standard IEC 62443 is recommended. Local recommendations or regulations must also be considered. The use of specialised experts is recommended.

The white paper only deals with the aspect of IT security against unauthorised external intervention or attack. It only refers to the other aspects – IT availability and the technical safety of the HVAC system itself – when necessary in order to minimise the negative effects of the control system failing.

2 Introduction / general information

This white paper, entitled “IT Security in Building Automation”, only deals with the aspect of IT security against unauthorised external intervention or attack. The aspect of IT availability (where security means never failing, never crashing, redundancy etc.), which is often regarded as a part of this topic, is not discussed here. The safety of the HVAC system itself (e.g. emergency power supply, hardware lockouts, redundant design of system components etc.) is also only referred to when necessary in order to minimise the negative effects of the control system failing.

The reason why IT security in building automation (BA) is increasingly important and relevant lies in technological development. For some time now, automatic control engineers have been using ever smarter components at increasingly lower hierarchical levels. PLCs and automation stations have long since become industry-specific microcomputers with embedded operating systems. Consequently, they communicate largely using the standard IT technologies. Even the field devices follow the trend towards ever more integrated intelligence with increasingly high-quality communication technology. Similarly to room operation, where private mobile devices (BYOD) or new control concepts with voice assistants (e.g. Amazon Alexa!, Google Nest Hello etc.) have become popular. These new approaches (cloud, AI) require additional interfaces and protocols (WiFi™[1], Bluetooth®[2], LoRaWAN®[3], Web API, MQTT, OPC and many more) which in turn offer additional attack opportunities.

The development of BA in the last 10 to 15 years has been characterised by standardisation and opening. The ability to integrate systems from different manufacturers has become a major selling point. Systems used to be proprietary in every respect and communication between them was difficult or impossible, but at the turn of the millennium, network, protocol and object standards were defined, opening the systems up to each other.

Using shared IT standards for communication, it became possible to integrate building automation into the existing business IT structures of a building. The use of the internet became established for remote communication, opening up almost unlimited communication opportunities for BA.

All these innovations have presented customers and operators of building automation systems with huge benefits in the form of increasingly better functionality, virtually unlimited communication options and complete freedom of choice for new projects and upgrades.

However, these very positive developments have brought a new dimension of vulnerability to BA. This is largely the same as for general IT applications.

---

[1] Wi-Fi®, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, and other marks are trademarks of Wi-Fi Alliance.

[2] © 2021 Bluetooth SIG, Inc

[3] LoRa, LoRaWAN®, Copyright © 2021 LoRa Alliance®

But unlike general IT applications, BA systems are physically connected to the technical equipment of a building (HVAC systems, lighting, access control, fire doors etc.), which means there is an additional dimension as regards the consequences of this vulnerability. This is because unauthorised access might not “merely” result in data being altered or manipulated, but can impinge on technical equipment in the building that is relevant to security and safety. Where criminal intent is involved, the consequences can be serious.

The risks posed by this vulnerability largely depend on the type and utilisation of the building. Not all buildings are of equal interest to attackers or as seriously affected.

If the building automation system is “only” connected to the HVAC (heating, cooling and ventilation) systems, the risks are likely to be much lower than if it is also connected to systems such as lighting, access control and door control. It is also clear that the risk to smaller, non-public buildings is not the same as it is to centrally located, heavily frequented or particularly security-sensitive buildings such as airports and railways stations. With such buildings, the intended threat can range in extreme cases to digitally assisted acts of violence or terror.

Therefore, the security precautions must be proportionate to the risks. A specific risk analysis is essential for every project.

Certain fundamental measures are required in all systems. Here a strategy of defence-in-depth, i.e. the use of multiple protective measures and technologies, is generally recommended. However, maximum security is only possible with a great deal of effort and expense. Even then, absolute, 100-percent security is almost impossible, in building automation as in any other system.

3 Elements of IT security in building automation

The security of network-based building automation (BA) can be improved using protective measures on two basic levels.

Just as people in towns can protect themselves by locking doors of their houses as well as by securing the city gates, precautions for BA systems can be taken on the individual devices (automation stations, PCs etc.) and/or with access to the relevant networks. And just as it is best to lock the city gates securely and not let the danger into the town in the first place, protecting the network access points is probably the more important aspect for BA. However, even city gates and walls are never 100% tight, and dangerous subjects can also come from inside the city. In the same way, protection of individual BA devices is essential.

Good results can only be achieved by making efforts on both levels together.

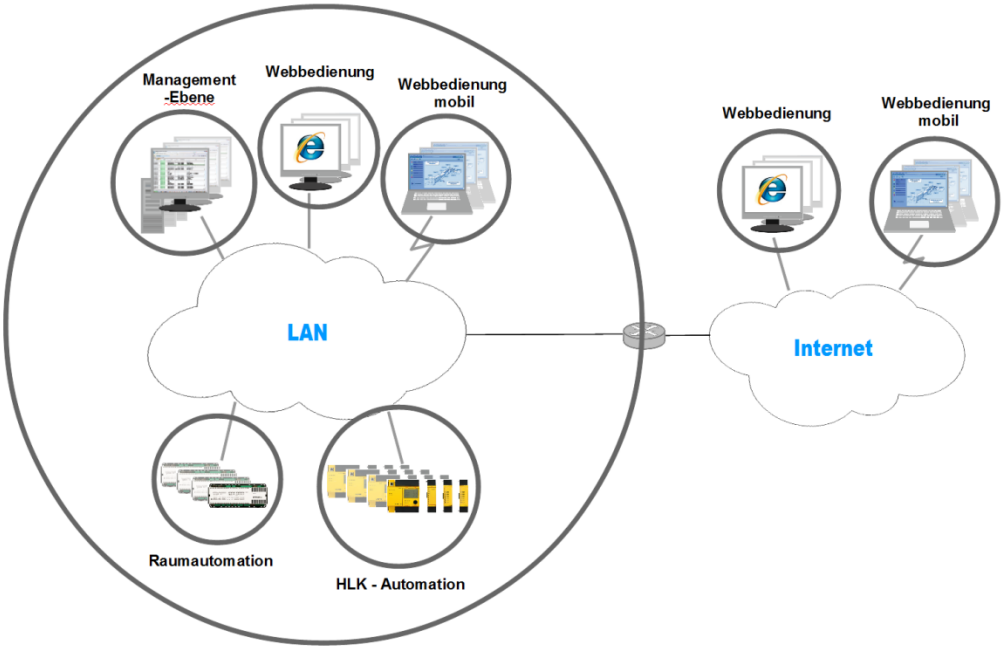

Fig. 1: Areas and networks of the BA system

In the service life of a BA system, the measures on the individual device / software level already begin with the product manufacturer, who implements a wide range of protective measures at the factory. These might include a password-protected access permission system, support for encrypted communication, internal firewalls or other measures.

These pre-installed protective measures on the device / software level must then be completed and configured when the system is installed and commissioned. The system of access permissions must be set up, the default users must be deleted and the devices may have to be re-hardened.

During this phase, purchased computers must be protected against malware (with an anti-virus program) and hardened as much as possible.

The manufacturer of the BA equipment usually has very little or only indirect influence over the measures on the IT infrastructure level, in other words the networks, subnetworks and access to them. These are planned and implemented by the installation contractor of the BA system (usually together with the IT officers of the customer, building operator or general contractor). The installer decides whether the BA system, or at least the automation level, should be run on a dedicated BA network, whether an internet connection is needed for remote communication, how the network is subdivided, which security measures such as firewalls and VPNs are used for the access points, and how any WiFi networks are protected. The general contractors and specialist planners specify the functional requirements and the cost framework.

IT security efforts continue throughout the service life of the system. As described above, they begin with the manufacturer of the equipment and programs, and continue through project engineering, implementation and commissioning of the system. But even after that, during operation, ongoing IT security requires constant work from maintenance and operating staff.

The required standard of security can only be achieved if all those involved play their part.

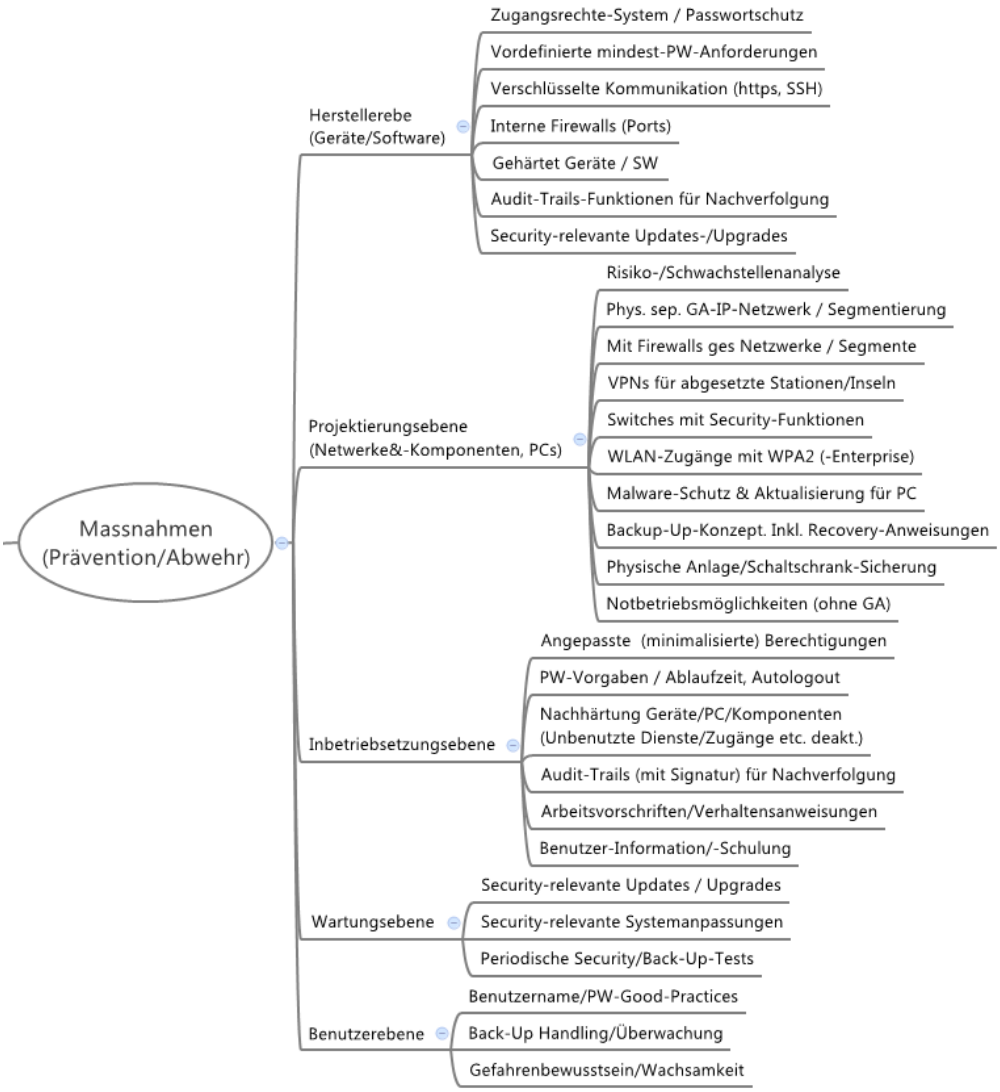

Fig. 2: Measures based on responsibility level

3.1 Elements on the manufacturer level

The devices affected are those with an (embedded) operating system (automation stations, network devices, intelligent sensors, smart actuators), as well as the software for the management system (SCADA/ML/BEMS software, and energy analysis and energy management software).

As a manufacturer, SAUTER has based the development of modulo 6 on IEC 62443-3-3 in order to integrate measures and solutions for cyber security. Document [1] is a guideline for this. The measures include:

identification / authentication and access rights

On both modulo 6 and SAUTER Vision Center, the web server user accounts can be configured with different authorisation levels and password

requirements. Changing the default password is mandatory on modulo 6 stations.

Usage control

Thanks to the integrated Access Control List, access from other participants in the network can be both explicitly permitted (whitelist) and explicitly prevented (blacklist).

Logging

The web server embedded in the modulo 6 stations stores all user actions in the form of an audit trail. This means that all user interventions can be traced back. This is similar to SAUTER Vision Center, where even higher requirements in accordance with FDA Cfr 21 Part 11 are supported.

Integrity check

The Building Data Integrity Solution (modu615-BM) is a solution that periodically checks the integrity of the data at all stations in a system. In the event of an integrity breach, an alarm is triggered and, if necessary, the original configuration is reloaded to the affected station. This solution uses a blockchain concept, encryption (TLS) and 2-factor authentication as standard functions.

Quick response to events

In the event of an integrity breach, an alarm is triggered and the original configuration is reloaded to the affected stations if required.

Encryption

The use of TLS is standard in modulo 6. All protocols that support this offer options such as the web server with https. Furthermore, BACnet/SC is integrated so that BACnet no longer communicates in plain text, but only with pre-registered stations that also support BACnet/SC. BACnet/SC uses TLS and is only available in encrypted form.

Network separation: 2 network interfaces

This allows, for example, the automation station to be connected to the corporate IT network and access to the web server, as well as access to cloud services such as the Meteo server or the email server for the automation station, while at the same time, physically separated, the building automation with BACnet/IP is operated on a separate network. This limits the data flow effectively.

Backup/Restore

This primary functionality is supported by the complete tool chain. This function restorably backs up both the configuration and the control program. With the Building Data Integrity solution, this restore can even be performed automatically if an unauthorised change is detected.

Availability

The internal architecture of modulo 6 stations prioritises the control functions over all other tasks, so that if the interfaces are overloaded (e.g. in the event of misconfiguration in the BACnet network, or a DoS attack on the web server), these interfaces are shut down, the affected interface is blocked, and the control continues to function fully.

3.2 Access permission system and password protection

Naturally, all devices and software products that are accessed by users (web servers, configuration interfaces etc.) must be equipped with a configurable access permission system with password protection.

The data interfaces which the devices and software products use to communicate with their data sources must also be protected from unauthorised access with a suitably verified ID. (This applies to the data sources of the energy analysis and management software, for example.)

Security can also be greatly improved if the password protection supports advanced functions such as minimum password complexity, automatic logout for inactivity, a lockout period after a predefined number of failed login attempts, or a regular PW expiry period.

Furthermore, when determining access rights, access should be limited to the bare minimum – i.e. only display as much as necessary (need-to-know) or only offer as much as necessary (least functionality).

Predefined minimum PW requirements

The password complexity, automatic logout, lockout period and regular PW expiry period are elementary features for effective protection.

Manufacturers should provide these functions in their products so that they can be configured during commissioning according to the security level of the system. If the manufacturer permanently programs the minimum requirements on its products and they can no longer be adapted to the security level of the system later, they might be set too high and be inconvenient to use.

However, it does make sense that at least the admin user with default PW set up by the manufacturer can be or – even better – has to be changed after a preset operating time or criterion. Many of the most widely reported hacker attacks are based on precisely this deficiency. The default PW was not changed after commissioning, and lists of these passwords for various manufacturers can be found on the internet.

Encrypted communication with https, SSH

For secure communication, the products must be able to use TLS-secured communication (https, SSH) for their web servers and configuration interfaces. Thus, in addition to the encryption of the communication, the communication participants are also reliably identified (by certificates, if operated with a Public Key Infrastructure, PKI).

Internal firewalls (ports)

All network-capable devices of a system (usually with a Linux operating system) should be protected with a factory-installed and preconfigured firewall. This means that all ports not used for regular operation are inaccessible. On software products too, ports that are not used or required should be inaccessible in the as-delivered state, in other words after a standard installation. For optimum adaptation to the infrastructure security concept, the port numbers used for the various services should remain freely configurable. It is also recommended that only the effectively available ports give a positive response to a port scan, and all others no response at all.

Hardened devices and software

All the required devices and software products must be hardened before delivery. This means that all services and access points that are not required should not be installed or should be disabled ex-works. Standard IT functionalities such as Telnet (Port 23) or FTP (Port 20) offer hackers additional, widely known ways into the building automation hardware. Encrypted variants should also be used here (SSH, FTPS).

Audit trail functions (with signature)

For retrospective analysis of genuine attacks, as well as false alarms (caused by incorrect operation or playing around), all systems should support audit trail functions (recording user activity) if possible. These not only help to find out who the attacker was or caused the false alarm, but also identify any damage or effects that need to be rectified.

For reliable tracing of genuine attacks, these recordings should be protected with a signature, so that they cannot be changed either deliberately by skilled hackers or accidentally by careless investigators.

Security-relevant updates and upgrades

Like any other types of IT, techniques for attacking IT systems constantly develop at a rapid pace. This means that all affected products must be regularly updated and upgraded. Manufacturers of BA products must therefore provide security updates and upgrades for them, as well as the necessary distribution channels.

Elements on the project engineering level

During the project engineering phase of a building automation system, the IT infrastructure and its security elements are among the items that are specified. The task is to define aspects such as the topology (for the networks and subnetworks), the protective measures for access points and the protective measures on the management level to be installed on the PC.

In addition, measures should already be planned at this stage for dealing with possible disruptions (resulting from an attack).

The general contractor and specialist planners have an important say at this stage. Their tender specifications and bills of quantities state the technical requirements and cost framework which ultimately make the security measures possible in the first place.

Analysis of risks and weaknesses

A risk analysis is the basis for engineering suitable defensive measures. Because the risk is not the same for each type of building and BA system, a project-specific risk analysis is essential. This determines the extent of the security measures. The influencing factors include the vulnerability of the building and the scope of the BA functions (HVAC, lighting, (fire) doors, access control systems etc.).

Physically separate BA IP network / segmentation

Because modern BA systems use the IP standard (OSI layer 3) as a basis for practically all their communication, it is naturally tempting to try and save money by using the existing IP network infrastructure that is normally present in the building. However, this is obviously not the best solution for the BA system in terms of IT security. Not only are there issues with performance and availability, but the protection of the networks cannot be optimally adapted to the requirements of the BA system, because the requirements of other applications also have to be taken into account. As well as this, such shared use of the network infrastructure means there are many users and possibly additional access points, with the ensuing risks to the BA network.

Networks and segments protected by firewalls

Protecting all network access points with firewalls is one of the most important and effective ways to increase IT security against unauthorised access. The firewall checks all incoming network packets before forwarding them, based on the addresses of the sender and recipient, and the services used.

Firewalls with additional monitoring functions further increase security. These FWs not only check the address information of the incoming packets, but other criteria as well. For example, they analyse the content of the packets (deep packet inspection, DPI) before they allow them access to the network.

There are also firewalls which filter outgoing data traffic. This puts up additional obstacles to malware that is not detected by the affected devices.

Finer segmentation can be used to make networks more secure. Subdividing a LAN like this means that the boundaries of the resulting subnetworks can also be protected with firewalls. The extent of the damage from infected machines can therefore be more effectively restricted within the LAN.

These days, firewalls are often integrated with the router in a single device. Firewall functions are also being taken over by increasingly intelligent switches. All three functions are being merged into devices with ever more powerful hardware.

VPNs for remote stations and units

Connecting remote stations or units to the BA system using a VPN (virtual private network) substantially increases overall security.

The VPN establishes an encrypted channel between the remote station or unit and the system’s internal LAN or segment. As the name implies, the remote station or unit is virtually integrated in the LAN or segment. The communication is encrypted and the identity of each VPN user is verified with a password. If the encryption (TLS) uses a certificate (from public key infrastructure) for identification, it is almost impossible for unauthorised persons to intercept this access or misuse it for their own purposes.

Protecting remote stations with VPN is not only worthwhile for very remote stations (WAN/internet), but also for stations in other segments of large networks.

Switches with security functions

Switches with integrated security functions are particularly useful when despite the risks described above, an existing network infrastructure is to be used both by the BA system and by other users. These can greatly enhance the security of the BA components connected to the jointly used network by filtering data traffic to each individual user. The switch ensures that each user only receives the data packets that are actually intended for it.

More advanced switches are also able to compile selected network users (for example the BA users) into a VLAN. This means they communicate within their own virtual network and are only visible and accessible to the other network users if this is explicitly permitted using a router or firewall.

Some of these switches can also be configured manually using whitelists and blacklists. During commissioning, these lists are used to permanently define which devices (based on their MAC address) can and cannot be connected to which port. This prevents external computers from connecting to the BA network.

WLAN access with WPA2 (Enterprise)

If (mobile) devices are to be used which will be connected to the system via WLAN (wireless LAN), only a WLAN (WLAN router) which supports the WPA2 (Enterprise) standard provides a suitable, up-to-date level of security.

With the WPA2 security standard, communication is encrypted according to the Advanced Encryption Standard (AES).

Unlike WPA2 without “Enterprise”, where the same password is used for all users (pre-shared key), the “Enterprise” version supports individual passwords, either from user accounts (LDAP/Active Directory, RADIUS) or via certificates (from public key infrastructure).

WPA2 and particularly WPA2-Enterprise, when used with sufficiently long and complex passwords and WPS disabled, are currently regarded as very difficult or virtually impossible to crack.

Malware protection & update for PC

As well as network protection, during the project engineering phase it must also be specified which malware protection is to be installed on the management PCs. To ensure that it remains effective, a practicable update concept must also be defined.

Malware protection disables known computer viruses, worms, Trojans etc., and deletes them if possible. Because only known malware can be detected, it is important to ensure that the protection is regularly updated.

Backup concept with recovery instructions

It goes without saying that a BA system requires a suitable backup system.

The BA system will probably no longer function after an attack, and this will have consequences for the use of the building. This means the function must be restored, possibly in a great hurry. A pre-existing, clearly defined procedure with (tested and practised, see below) step-by-step recovery instructions is an invaluable help if this happens.

Because the backup files usually also contain copies of highly sensitive data, it is important that the engineering already includes a concept for how they can be reliably and securely kept. Particular attention must be paid to system configuration information or user administration data, for example, which can be extremely useful to skilled hackers.

Physical system / control cabinet security

The physical security of the system, control cabinets and communication equipment not only serves to prevent malicious attacks, but also prevents careless access by unauthorised persons.

In the context of IT security, the most important aspect is to protect the physical points of access to the devices, control cabinets and communication equipment. There must be no unauthorised access at all to Ethernet, USB and configuration ports on devices such as PCs, automation stations and routers, regardless whether they are assigned or not.

Emergency operation options (without BA)

In the event of an attack with effects on the functionality of the BA system, local operating and indicating units on the AS and other systems themselves can perform important rescue tasks.

The same also applies for hardware lockouts on the technical installations (e.g. fan must not run when the damper is fully closed etc.).

Elements on the commissioning level

During the commissioning phase, the specifications from project engineering for IT security must be implemented and completed. All parameters relevant to security (user permissions, password requirements, ports etc.) must be configured and wherever possible, the protective measures must be tested. For subsequent operation and maintenance, update subscriptions must be set up and future users trained.

Tailored (minimised) user rights

During commissioning, the users and user groups are set up for all the relevant devices, PCs and systems, and their rights are defined. The better and more precisely the rights are adapted (i.e. restricted/minimised) to the tasks of the users/groups, the smaller the risk – the risk of targeted attacks as well as the risk of unintentional operating errors. The “need-to-know” / “least functionality” principle fundamentally applies here: in other words, only allow access to those data and functions that are necessary for the user, and none beyond this.

Modification of user rights becomes even more important when we think of illegally obtained login data (user name and PW) or users leaving devices or PCs without logging out.

PW specifications/expiry time, auto logout

Many devices, operating systems and programs include the option of setting these parameters. How complex does a password have to be? What restrictions are to be set? How often must users change their passwords? How long can a user be inactive before being automatically logged out? The risk analysis determines how strictly these requirements are set.

However, an overall, practical view must be taken. User-friendliness competes with security here, and it is worth remembering that as the scope of the password requirements grows, so does the difficulty for users. If passwords are overly long and complicated, frequently have to be changed and there are too many to remember, the more likely it is that users will have to write them down. Users also have passwords at home, some of which their family members need to know, and others which they must not be allowed to know. Each system they use has its own password rules. At some point it becomes impossible to remember all professional and private passwords, and the result is password lists on smartphones, keeping them in freeware

password managers of dubious security levels, or even on pieces of paper under keyboards.

Hardening devices, PCs and components

After completing the installation and configuration of all relevant elements, security can be further increased by hardening all devices (Linux) and PCs. What this means is removing or at least disabling all unused services, access points, user accounts, processes and programs. Only the elements that are actually necessary for operation should be left on the devices. The leaner the system, the harder it is for hackers to find tools that they can use.

PCs are particularly affected. Other devices (such as automation stations) should have been pre-hardened as far as possible by the manufacturer (not co-compiled).

Audit trails (with signature) for tracing

If a malfunction occurs, permanently available, active audit trails are enormously important. Not only are they used for monitoring, but in the event of an error, they can also make it much easier to restore the system or data.

The logbooks may have to be activated and configured during commissioning. At the very least, they must contain all user actions, modifications to data and, of course, all switching and adjustment operations.

They can also be set up for operating systems in databases and routers. This makes monitoring even more effective.

Because skilled hackers will no doubt try to remove their traces from the audit trails, it may be necessary to protect them with a digital signature for sensitive systems. The digital signature protects the recordings with a signature code and prevents any subsequent changes to them.

When configuring the audit trails, their long-term treatment must also be considered. How will they be prevented from becoming too big? Do they have to be regularly backed up? How long does the data have to be kept?

Standard operating procedures

Definitive and tested standard operating procedures (SOP) for IT security should be in place on two levels by the time the system goes into operation. First, there should be one for normal operation, which helps to ensure that all safety elements are functional at all times and constantly updated. There should also be one for the occurrence of an attack or disturbance, with procedures and information on identifying the problem, limiting the damage and dealing with the situation.

The SOP for normal operation might consist of workflows and checklists, and a reminder function from a calendar is also useful. When properly observed, it ensures that all security-relevant elements are maintained: Is the malware protection up to date? Are all security-relevant updates of programs and operating systems installed? What security measures have to be carried out

for newly installed or added elements? Have backups been made and correctly saved, and is restoration regularly tested? Did whoever was responsible for checking the procedure do so? These standard operating procedures are a key component in the overall effort to prevent or minimise risks.

If an incident occurs which affects the functionality of the BA system, the system will probably be partially or completely out of action in these circumstances. In the worst case, this can have serious effects on the use of the building. The function of the BA system will then have to be restored in a hurry. Existing, clearly defined and practicable procedures including step-by-step instructions then become an invaluable aid. As well as help on restoring the function, they can contain essential information such as reporting paths, telephone numbers, escalation levels and immediate measures.

User information and training

During day-to-day operation of the BA system, IT security can only be optimal if all of those involved play their allotted part. The human factor, which not only means those in charge of maintenance but also the users and operators, is very important.

If the system is correctly set up with all the appropriate security mechanisms, the people involved are probably the largest potential risk.

Incorrect operation of the system itself (playing around, experimenting), incorrect use of security mechanisms, inappropriate use of access data and other data, careless use of communication devices, naivety (email, phishing etc.), are probably the greatest dangers.

As well as training on technical matters, which is essential for correct operation of all the system’s safety mechanisms, it is crucial to make staff aware of the potential risks and sensitise them to possible dangers

If the IT security topics are dealt with in a special training course (separately from the other topics), they are given more weight. Occasional refresher courses help maintain awareness of the topic even after long periods without any incidents. Instruction for new staff should not be forgotten either.

The topic of behaviour and recovery from damage therefore deserves its own training block.

Elements on the maintenance level

Hackers are constantly developing ways to attack IT systems, so defensive technologies develop in response. The BA system may also develop.

The purpose of maintenance (in the context of IT security) is to regularly look after all the installed elements of IT security, update them and, if necessary, adapt the system to the latest developments.

Security-relevant updates and upgrades

All devices and programs, and especially the PCs and their malware protection, and communication equipment such as routers and VPN devices must be regularly maintained with the available updates. This is the only way these security mechanisms can keep up with the constantly developing hacking technology.

In some cases, technical development may mean having to upgrade to newer or more comprehensive versions.

Security-relevant system adaptations

The hardware and software installed in BA systems tend to have much longer life cycles than commercial IT products.

Changes to IT threats and IT security can make it necessary not only to maintain the existing security measures, but also to implement larger, wider-ranging system adaptations.

Periodic security/backup tests

To ensure a high level of effectiveness, the security measures must be checked at predefined intervals and tested as far as possible.

The procedures in the event of an attack or disturbance should also be regularly practised. This particularly applies to restoring the system from backups. Backups sometimes turn out to be unusable when it comes to the crunch.

At regular intervals, security reviews should take place to check whether system operators and users observe (IT) security procedures.

Elements on the user level

As has been stressed here several times, a BA system can only maintain a high level of IT security if all those involved with it perform their security-related tasks throughout its service life. In particular, this means the users during day-to-day operation. If any irregularities occur, they should be the first to notice them.

User name and PW recommendations

As mentioned above, the required password complexity is specified and adapted to the system-specific risk by the manufacturer or at the latest during commissioning.

However, the users are also obliged to choose passwords that are as difficult as possible to crack. This means that they should never contain obvious elements such as their names, the names of their partners or children, date of birth, and so on. There are hackers (as well as IT enthusiasts) who write algorithms to crack passwords by comparing them with such items of personal data.

Above all, it is the length, more than the complexity, that makes a password secure. Prose sentences are also very well suited, provided they are not well

known quotes or sayings. They have the great advantage of being easier to remember (e.g. “1 x Sauter always Sauter” or “my darling is the best”).

Naturally, good PW habits also include never writing them down or letting other people use them.

Backup management

Automated backup procedures must be monitored to ensure that they are correctly and completely executed. If necessary, external media must be replaced. Their effective usefulness must be periodically tested (see above).

Because the backup files usually also contain copies of highly sensitive data, they must be kept in a suitably secure place. Particular attention must be paid to files with system configuration information or user administration data, for example, which can be extremely useful to skilled hackers. Engineering documents such as system topologies, security concepts etc., including all their copies, are also very useful information for an attacker with bad intentions and must be kept appropriately protected.

Risk awareness and alertness

As mentioned above, BA system users must be taught about all the potential risks as part of dedicated IT security training courses. It is extremely important to raise their awareness and encourage them to be alert. Anomalies and unusual occurrences must be recognised and taken seriously.

As so often, humans are the main risk. Techniques such as phishing, fake program updates and even conversations can all be used in attempts to gain access to sensitive data, system information, and user names and passwords with high levels of authorisation.

Processes and audits

Various organisations are active in this area. For example, the IEC 62443 standard is a good reference and very closely related to the ISO 27000 series. These references look at various aspects of security, from product development, through the entire life cycle of products, to discontinuation. But also the processes, the product development, the product users, such as system integrators, and finally the end users are considered. Cyber security affects everyone who comes into contact with the products and systems. It is important to define clear objectives and to use the means to this end. IT security is an always-on process and must be able to adapt to recurring and changing threats.

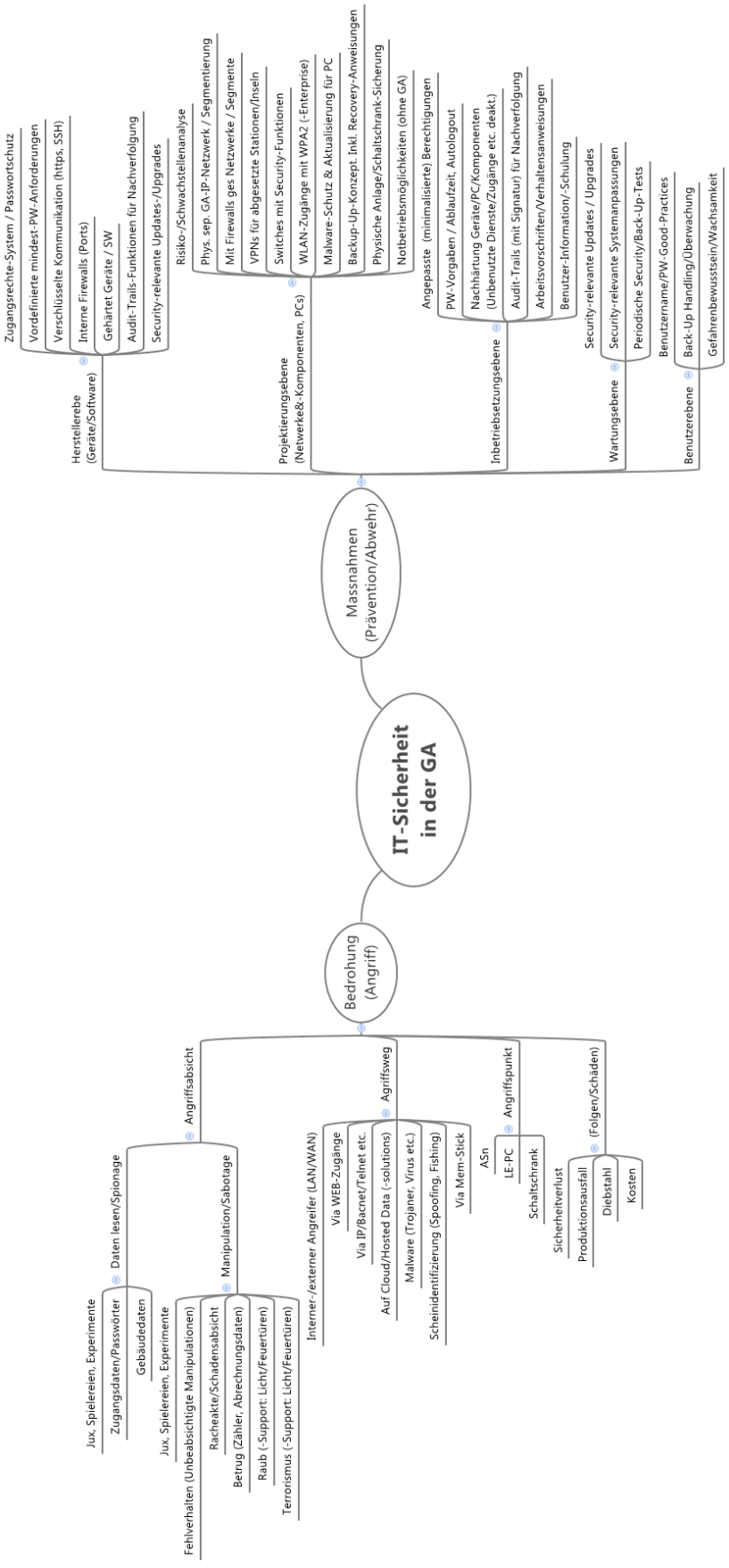

Fig. 3: Threats and countermeasures of IT security for the BA

4 Conclusion

The range of actions for the IT security of a BA system is enormous. There is a world of difference, from doing nothing right up to taking every conceivable precaution. Every level is possible, from “any average IT specialist can get in” to “almost impossible or not worth the effort, even for expert hackers with serious intentions”, with corresponding workloads and costs!

Assessing the individual risk of each project is essential. Here too, the range is enormous. For many buildings, the risk is not much more than users playing with the technology, messing around and trying things out. There is certainly a very high, very serious risk to buildings with valuable items or where enemies are at large, or for important public buildings with a high level of vulnerability.

Basic safety measures with the state of technology usual for the industry are urgently recommended for all buildings. They help prevent most attacks and the type of playing around mentioned above. They can also help prevent incorrect operation and software errors, which can never be ruled out, and are still the most frequent cause of malfunctions.

As so often, the human factor is very important. Operator accesses with permanently logged-in user, passwords under the keyboard, borrowed passwords, unchanged plant administrator accesses, in short: lack of care, lack of risk awareness, lack of vigilance! This can be helped by providing regular information and specific training.

The author

Franklin Linder, El.Ing. is a technical editor at SAUTER Head Office in Basel. He has 20 years of experience in the development, operation and marketing of building automation systems.

Company portrait

As a leading provider of solutions for building automation technology in ‘green buildings’, SAUTER provides pleasant conditions and a sense of well-being in sustainable environments. SAUTER develops, produces and markets energy-efficient total solutions and offers a comprehensive range of services to ensure that buildings are operated with optimal energy usage. Our products, solutions and services ensure high energy efficiency throughout the entire life-cycle of a building, from planning and construction through to operation, in office and administrative buildings, research and educational establishments, hospitals, industrial buildings and laboratories, airports, leisure facilities, hotels and data centres. With over a century of experience and a track record of technological know-how, SAUTER is a proven system integrator, with a name that stands for continuous innovation and Swiss quality. The recipient of awards for the best automation system and the best energy service, as well as eu.bac and BTL certifications for products, SAUTER provides users and operators with an overview of energy

flows and consumption, enabling them to track the development of their costs.

5 Bibliography and list of sources

[1]	VDMA, V. D.-u. (2021-02). VDMA 24774:2021-02. IT security in building automation. VDMA, German Engineering Federation.
[2]	IEC International Electrotechnical Commission. (2013-08). Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (1.0 ed.). Geneva, Switzerland: IEC, Geneva, Switzerland.
[3]	VDMA, German Engineering Federation. (2016). Security in Automation – Profiling IT security standards for mechanical and plant engineering. Product and know-how protection. Berlin: HiSolutions AG. From https://industrialsecurity.vdma.org/documents/16227999/16499033/1492086887896_INS_NAM_2016_Industrial_Security_IEC62443.pdf/c2e80bdb-c820-42cb-b3cc-fedd68571e1e
[4]	ZVEI, German Electrical and Electronic Manufacturers' Association. (2017). Orientation guide for manufacturers IEC 62443. Frankfurt am Main: ZVEI. Retrieved from ZVEI, Zentralverband Elektrotechnik- und Elektronikindistrie: https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2017/April/Orientierungsleitfaden_fuer_Hersteller_IEC_62443/Orientierungsleitfaden_fuer_Hersteller_IEC_62443.pdf
[5]	Cybersecurity for modulo 6. An Overview. Implementing IEC 62443 for Building Automation.2019-11, 5th Revision, Fr. SAUTER AG. https://extranet2.ch.sauter-bc.com/wp-content/uploads/sites/13/2020/01/1071060-26.pdf

6 List of abbreviations

Abbreviation	Term
e.g.	for example
gen.	In general

7 Index

L

M

O

P

R

S

T

U

V

W