RECOMMENDABLE

Commend Whitepaper on the new EN 62820 Directive

EN 62820
ADVANCED SECURITY
BUILDING INTERCOM

Communication that saves lives

Why incident response plans (IRP) are essential

Whether in companies, government agencies or public institutions – the need for reliable security technology is at a record high. It's a busy time for security professionals, especially where emergency and threat response communication is concerned.

RECOMMENDABLE

Commend Whitepaper on the new EN 62820 Directive

Lost in risk?
Guidance and assistance in accordance with EN 62820

Status quo

We are living in a time that is characterised by insecurity. Extremism and terrorist threats have become regular topics in the media. Killing sprees and other attention-seeking acts of violence have left deep marks on the population. Many people are understandably concerned – and persons in positions of responsibility are no exception. But unlike private persons, **managers, executives and security directors** have special social responsibilities that come with their roles as professionals. **They are called upon to ensure the best possible protection of their staff during working hours and at their place of work.** As a restul, they are required to take safety precautions in the interest of everyone within their scope of responsibility. This includes anyone from visitors in an office complex to customers in a shopping centre or patients in a hospital. In addition to taking all these precautions, barrier-free access has to be maintained in all relevant areas.

Vague ideas

The applicable legal requirements for executives are getting more and more specific: many international work protection laws, as well as the upcoming **European Directive EN62820**, already require employers to **provide an individual written threat analysis** for every area of activity within their company. This includes interviews with employees to determine their subjective awareness of risk scenarios. If it turns out that there are actual everyday situations where colleagues fear for their physical integrity, the employer is mandated to take appropriate countermeasures. This is where things get tricky, as **the ideas about what "taking countermeasures" involves are often quite vague.**.

In essence, this is due to many executives lacking relevant know-how. This is not meant to criticise them in any way. Those with key responsibilities in less technical areas simply do not have the knowledge necessary to translate identified security shortcomings into the proper technical equipment to eliminate them.

Even the best executive can feel overwhelmed when faced with questions such as, "Do we need a new **video surveillance system?**", "Should we get new **fire alarms?**" or "What about **access control?**". This is because, depending on the area of application, these issues may involve rather complex risk scenarios for a range of different target groups. Airports or railway stations, for example, have a large number of employees working in different locations and areas of activity at the same time, in addition to being frequented by many hundreds of passengers in multiple buildings. This often leads to rash decisions and grasping at every straw that promises to step up the current level of security. Be careful, however. If you approach the problem this way, you will run the risk of overreacting – using a sledgehammer to crack a nut, so to speak. This is because, taken in their context, **threat situations and risk scenarios** are **highly individual**, requiring a multiplicity of **specific factors** to be taken into consideration.

For that reason it is highly advisable to consult with a competent provider early on so they can support and guide you through the planning process.

How should you proceed?

German standard as a guideline

Governmental departments, official bodies and boards of trustees in many countries provide guidelines for business executives on how to handle work-related security issues. However, the main focus of these guidelines is usually on organisational issues and business processes. Technical aspects are usually treated only superficially and/or incompletely. For example, these documents typically provide general notes on resistance classes for doors and windows, or guidelines on intruder alarm systems. However, crucial aspects such as fail-safe emergency communication are completely omitted. The same applies to standards that are seek to improve security in residential and non-residential buildings. Where technology is concerned, their focus is exclusively on fire protection.

In Germany, which ranks as one of Europe's leading promoters of technical risk management, the **VDE 0827** standard already provides **clear guidelines** for business executives on how to implement security measures and how to select the proper technical equipment. The guidelines provided by this standard were **also used as a basis for the new EN 62820 standard,** which is currently being introduced throughout Europe. With its comprehensive set of rules, this standard describes, for example, the **technical systems** suitable for **calling help, triggering alarms, warning affected persons and transmitting instructions** in individual security threat scenarios. EN62820 also helps security managers to take all the measures that are required of them by law. Of course, the mere existence of a standard does not make its recommendations compulsory, but there are laws and directives that do.

The legal situation

How does this seeming contradiction work out in practice? Like this, for example: **In the event of a worst-case scenario that involves personal damage, the official investigators will verify if everything humanly possible has been done to avert danger and to minimise damage.**

With this in view, the "duty of care" as required by numerous laws enforces compliance with relevant norms and standards and may lead to criminal prosecution if an incident does happen. In other words, **wherever a law refers to "duty of care" or "technical regulations", this implies a liability to ensure compliance with relevant technical norms and standards.** This is why many regional building regulations today require that "building systems are to be constructed and maintained in such a way that public safety and law and order are not endangered. Applicable technical regulations intended to ensure these requirements are to be followed." ...or, for example: "Each entrepreneur shall ensure that the building work complies with the accepted technical rules of engineering and required documentation."

EN 62820
ADVANCED SECURITY
BUILDING INTERCOM

RECOMMENDABLE

Commend Whitepaper on the new EN 62820 Directive

The proper solution for emergencies

Finding appropriate technical equipment

To avoid misunderstandings, it is important to remember that the new rules of application are intended only to ensure the best possible support of organisational processes for firms, government agencies and institutions. They do not provide any rules of conduct for specific incidents such as a killing spree. This is because many firms and institutions have their own crisis management concepts. For this reason, the focus should rather be on implementing these individual concepts with the help of stable, fail-safe incident response plans (IRP). The challenge, then, consists in finding an appropriate technical system whose solutions provide added value in crisis situations. This includes the effective support of the most essential crisis intervention routine: assessing situations and alerting security services or police forces.

Multi-functional intercom systems are ideally suited for this purpose. They are designed to support each item on the emergency and threat response agenda with latest-generation technology. Each system is different, as its composition depends on the assessment of the underlying technical risk management (see info box for details).

The key factor in deciding on technical equipment is security level as determined by way of a risk analysis. "Security Level 1" applies in low-risk environments with limited requirements. "Security Level 2" is recommended for environments involving a medium level of risk. "Security Level 3" is appropriate for potential high-risk areas. The different system solutions all share the same basic structure: The core element of a powerful IRP consists of an industrial-strength intercom server as the system's control centre. Connected to a (potentially unlimited) number of strategically positioned query point terminals and building alarm equipment, the server functions as an interface to all relevant security technology components, such as video surveillance or loudspeaker systems, and the telephone network.

1| Alarm

→ Who can trigger an alarm?

→ Where are the "IRP hotspots"?

→ Which emergency call terminals are available?

2| Verification

→ Who verifies the alarm?

→ What is the response procedure in case of an alarm?

→ How are security warnings communicated to affected persons?

→ Which additional systems have to be controlled (e.g., CCTV, loudspeakers, access control,..)?

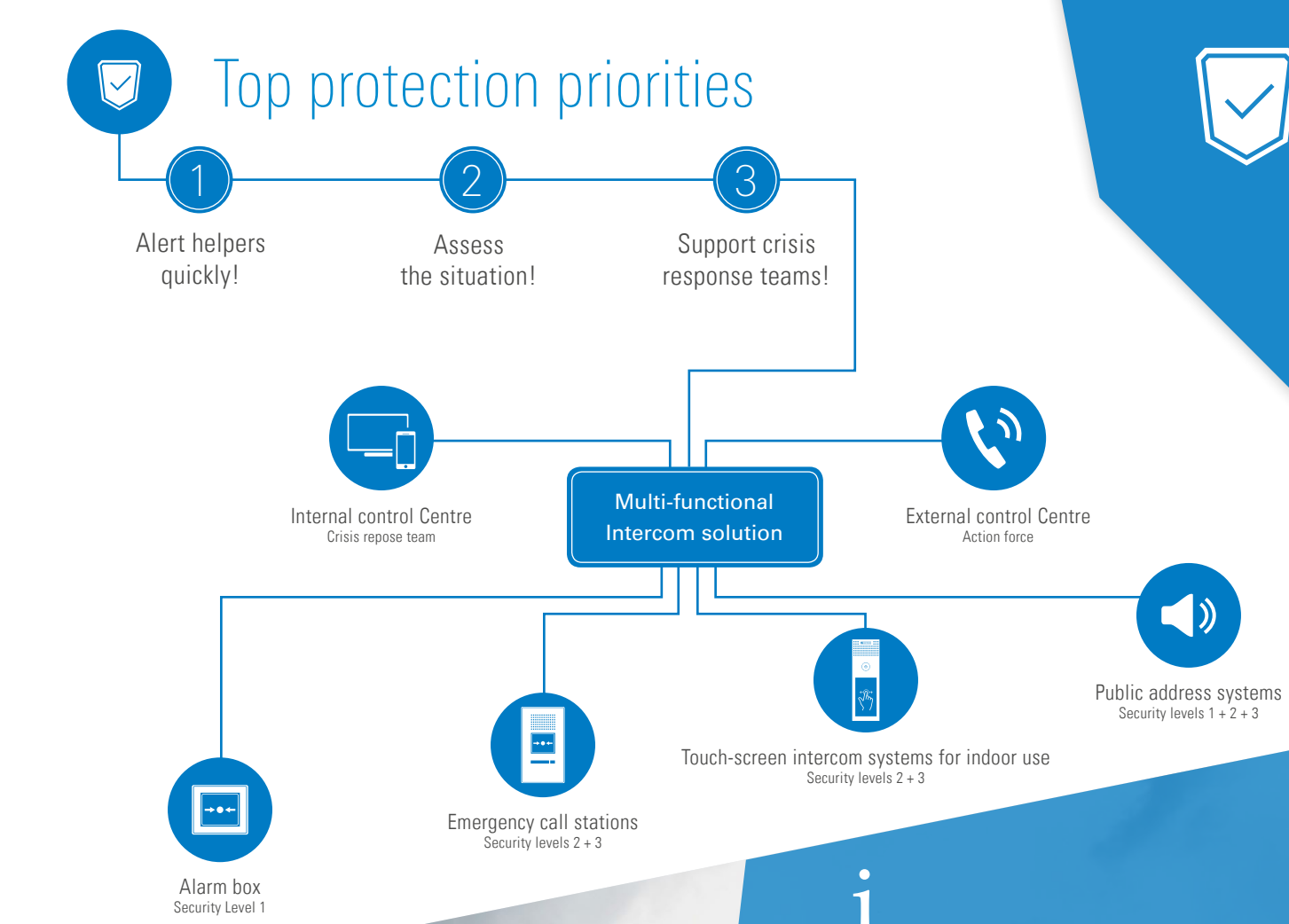
→ Will the appropriate security services be alerted?

→ Which information will the security services require?

→ How can the members of an internal crisis response team coordinate with each other?

Top protection priorities

1. Alert helpers quickly!
2. Assess the situation!
3. Support crisis response teams!



4| De-escalation

5| Aftercare/Prevention

Technical risk management:

The new **EN 62820** standard calls for a technical **Risk Manager** to determine the **required security level** and for the solution to be implemented accordingly. This defines how the technical equipment will support the firm or institution in managing a dangerous situation or emergency.

It is therefore essential that concrete requirements and protection goals are defined right at the beginning of each planning stage. This allows for individual adjustments, as a primary school requires a different solution than a synagogue, for example. **Deciding early on which functions are needed** will **help** to **keep the costs within the limits** of what is technically necessary, and it will allow existing technical systems to be incorporated into new concepts. Once the technical equipment has been selected, it has to be integrated into the organisational processes.

A risk manager will only have achieved his/her main objective when all crisis-specific processes have been improved.

Functionality and added value in everyday situations

Functionality in emergency situations

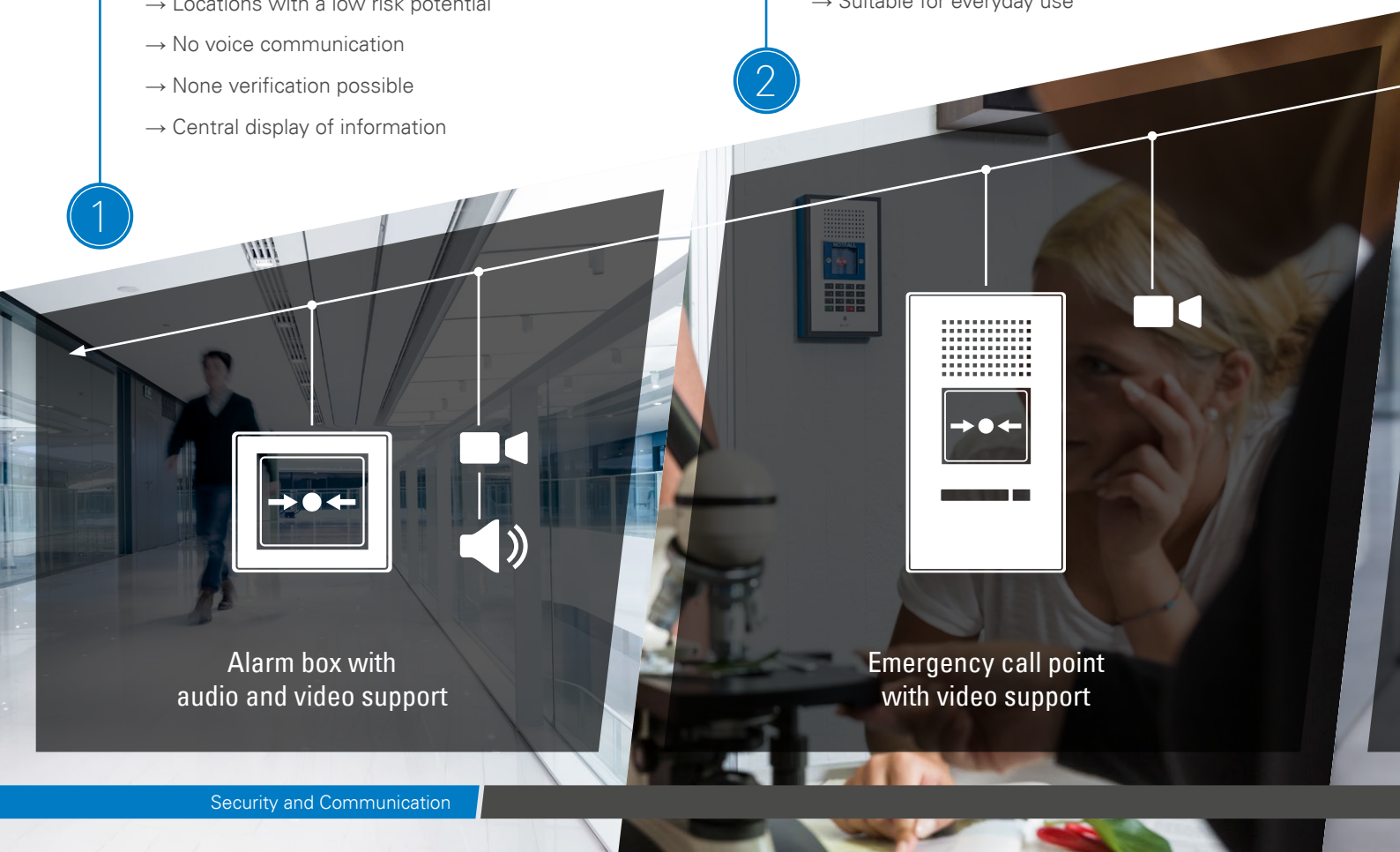
A crucial factor is a **bi-directional intercom system**, i.e., one that provides direct voice communication connection between a caller and the appropriate control centre. This is because an instant communication line via loudspeakers and microphones is essential for **verifying and prioritising alarms, and for coordinating appropriate countermeasures.** Even if the person who triggered the alarm is unable to respond, the staff at the control centre can still **monitor the situation at the other end of the line acoustically over the microphone** and take the necessary steps. Their response may involve anything from calling the police to establishing direct contact with a potential perpetrator over the intercom line. Moreover, this **acoustic verification by control centre staff also helps to prevent costly false alarms**.

„IRP Hotspot 2“

→ Locations with high risk potential
→ Voice communication
→ Activation of external cameras
→ Confirmation
→ Self-monitoring (24/7)
→ Vandal resistant
→ Ultimate availability
→ Suitable for everyday use

“IRP Hotspot 1”

→ Locations with a low risk potential
→ No voice communication
→ None verification possible
→ Central display of information



Security and added value

IRP arrangements that are based on latest intercom technology have a unique advantage: they **can be used efficiently for everyday communication tasks**. After all, it is for a good reason that the Standards Committee rates systems as particularly useful if they can not only be used in an emergency but also in everyday situations. This is because experience shows that people must be fairly familiar with specific technical equipment before they are sufficiently confident to use them in an emergency. One example are intercom systems in school classrooms, which can significantly improve regular day-to-day communication throughout the school premises. Systems like these can also be used for sounding the break signal, **making announcements**, **providing information**, **coordinating security drills**, or **issuing situation-specific instructions**. A tailored intercom system can also add significant value where internal communication at industrial plants and production facilities is concerned – e.g., when it comes to improving communication between control stations and other work areas. Besides, **operators are certain to benefit** from a practical side effect: the systems' versatility and **suitability for multiple purposes makes for a highly efficient investment** (think "indirect profitability").

Smart indoor touch-screen terminal with integrated video camera

3 → "IRP Hotspot 3"

→ Locations with high risk potential
→ Voice communication
→ Integrated video communication
→ Enhanced crisis communication
→ Self-monitoring (24/7)
→ Ultimate availability
→ Modular and multi-functional, suitable for day-to-day use

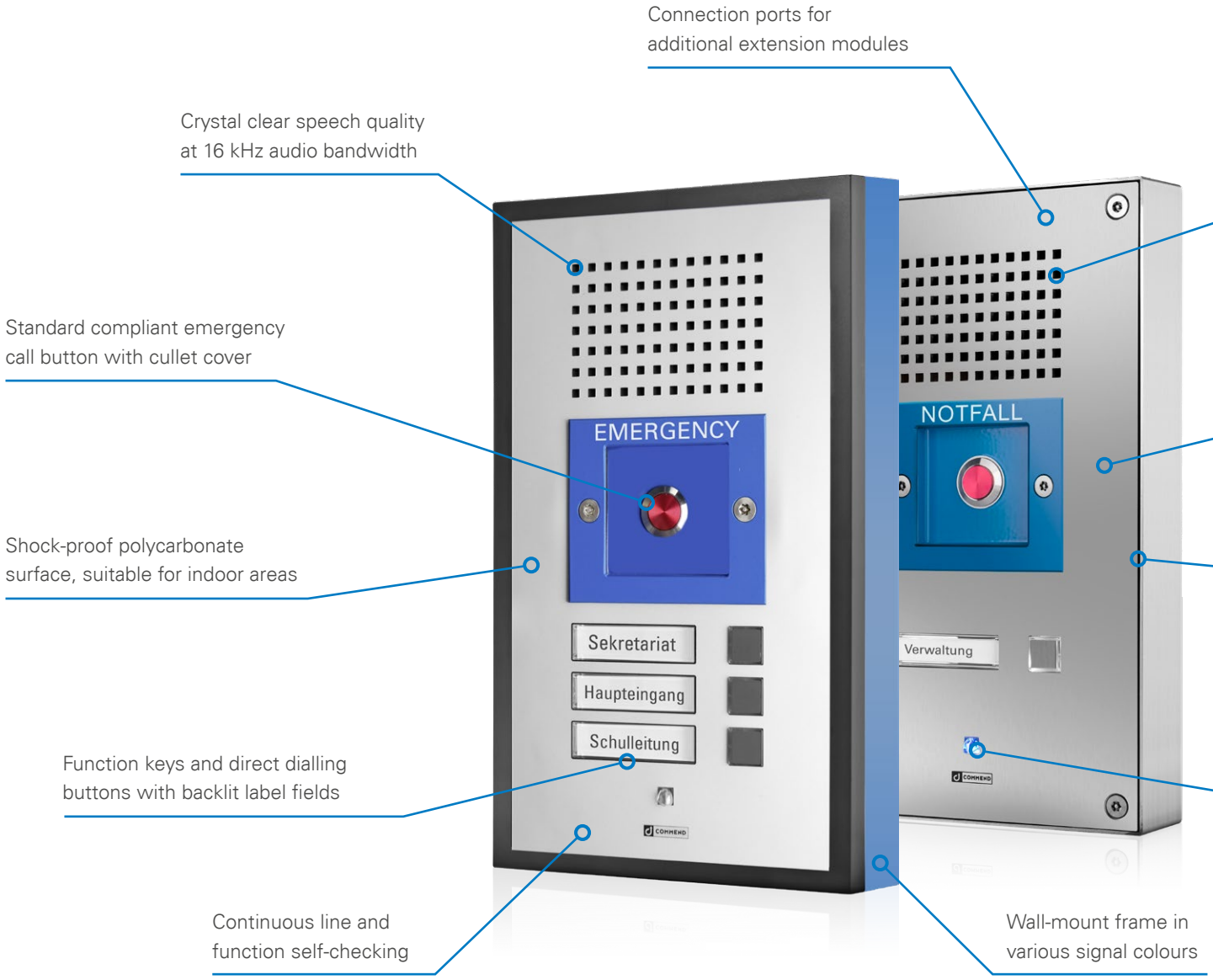
RECOMMENDABLE

Commend Whitepaper on the new EN 62820 Directive

Beyond the usual standard

When it comes to quality, it's the details that count

Additional specifications in terms of equipment are imposed by external requirements on the hardware components – for example, if the devices are to be installed outdoors or indoors. The following example of a **standard-compliant intercom station for indoor use** illustrates some essential key features: Customers should verify that the devices are capable of **continuous self-monitoring** to ensure their **constant availability and functionality**. Another important feature is **resistance against vandalism**, e.g., through specially reinforced front panels. Polycarbonate is a proven and reliable material for this kind of intercom station. An additional "**poke protection**" is also good to have. The intercom station should also be designed to prevent the ingress of dirt or dust. Remember: the larger the call button the easier it'll be to operate in an emergency.



A perfect partner

When implementing an emergency and threat response system, service partners can be especially helpful, as they can guarantee **products and services from a single source**. All security managers are therefore well advised to **find a single-source solution provider** – someone who can support and guide you from the concept phase through all stages of the planning process. An isolated building security platform is of little use – just like a dedicated evacuation solution that cannot be utilised for anything else. Instead you should select a provider who can supply the terminal devices as well as the server components, interfaces and easy-to-operate user surfaces. If your provider can also offer **a high level of availability and quality**, all the better. Besides, you should ensure the availability of **standardised interfaces to third-party systems** so you can integrate your existing components into your new system. Ideally, your offer should include a **visualisation feature** to enable you to **custom-configure** central components such as **control desks** to suit your user needs. Please note: Innovative service providers will already offer you the option of integrating **mobile subscriber units** into the network via **emergency applications**. In this age of mobile devices, a feature like this will improve your system's security communication capabilities by several magnitudes.

Poke protection and special sabotage-proof screws

Vandalism-resistant high-grade steel surface, suitable for outdoor installation

Protected against ingress of moisture, dirt and dust

Electret microphone for hands-free talking (max. speaking distance: 7 m)

RECOMMENDABLE

Commend Whitepaper on the new EN 62820 Directive

7 Hints for security managers

1. Find a single-source solution provider.
2. Consult with your provider early on so they can support and guide you through the planning process.
3. Make sure they can also offer you a high level of availability and quality of their solutions.
4. Focus on solutions that include the terminal devices as well as the required server components, interfaces and easy-to-use user surfaces.
5. Ensure the availability of standardised interfaces to third-party systems so you can integrate your new system with your existing components.
6. Verify that the solution includes a visualisation feature that enables you to custom-configure central components such as control desks to suit your user needs.
7. Request the ability to integrate mobile subscriber units into the network via emergency applications. In this age of mobile devices, a feature like that will improve your system's security communication capabilities by several magnitudes.

Contact our specialists to learn more about **technical risk management** and the **advantages and possibilities** of an emergency and threat response system.

We are looking forward to your visit and will be happy to assist you with our professional expertise.