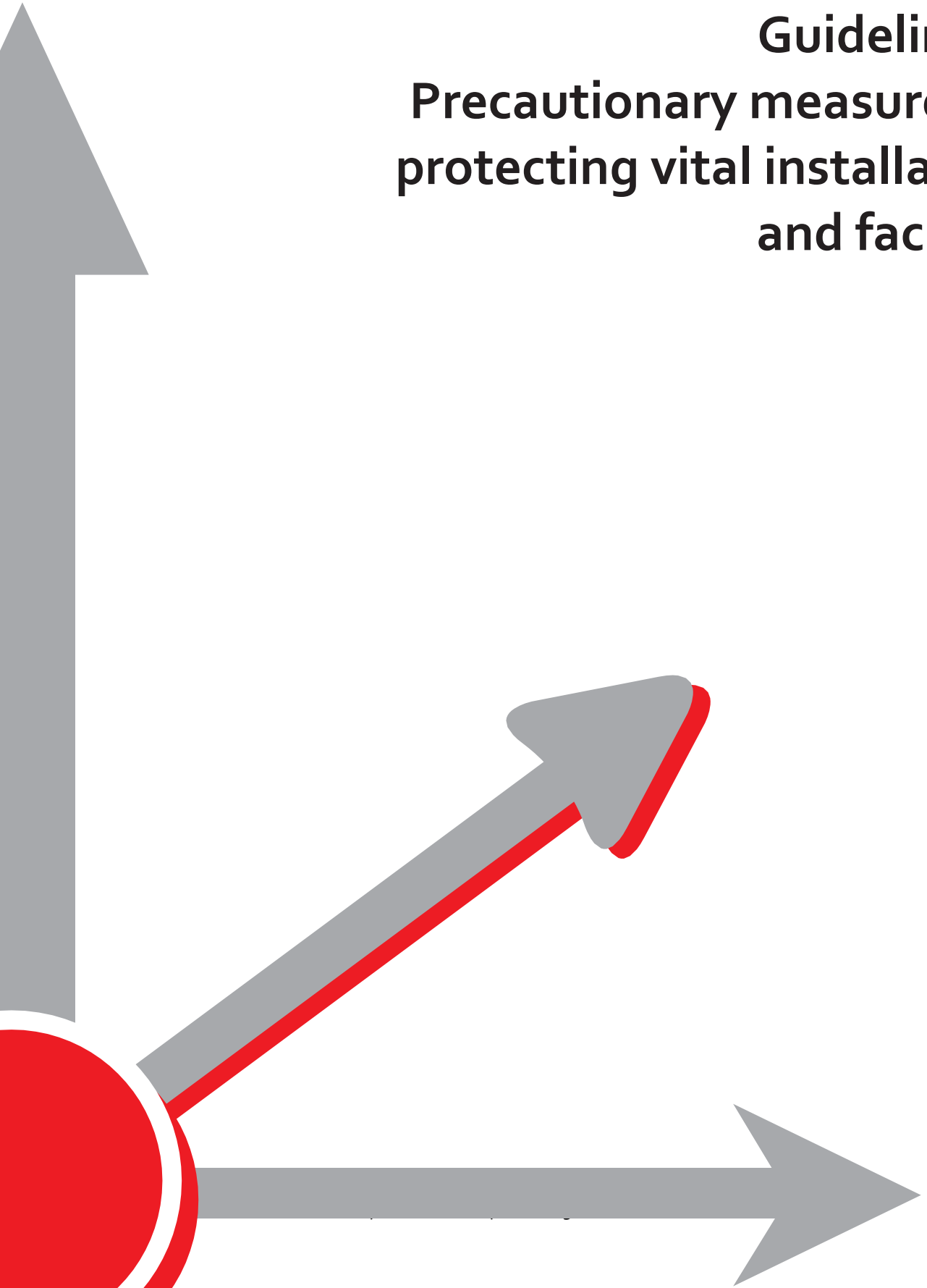
euralarm

Guideline on Precautionary measures for protecting vital installations and facilities



Changes revision table

Date	Rev #	Paragraph /Page	Change
November 2025	1.0		First release

FOREWORD

This document is intended as a general guidance and is not a substitute for detailed advice in specific circumstances. Although great care has been taken in the compilation and preparation of this publication to ensure accuracy, Euralarm cannot in any circumstances accept responsibility for errors, omissions or advice given or for any losses arising from reliance upon information contained in this publication.

DISCLAIMER

This document is intended solely for guidance of Euralarm members, and, where applicable, their members, on the state of affairs concerning its subject. Whilst every effort has been made to ensure its accuracy, readers should not rely upon its completeness or correctness, nor rely on it as legal interpretation. Euralarm will not be liable for the provision of any incorrect or incomplete information.

Note: The English version of this document is the approved Euralarm reference document.

ACKNOWLEDGEMENT

In the face of growing threats to critical infrastructure and the increasing complexity of regulatory and technological landscapes, the development of this concept paper marks a significant step toward enhancing the resilience and security of vital systems across sectors.

We would like to express our sincere gratitude to the BHE Bundesverband Sicherheitstechnik e.V. for their invaluable contribution to the elaboration of this document. Their deep expertise, practical insights, and unwavering commitment to advancing security standards have been instrumental in shaping a comprehensive and actionable framework. BHE's collaborative spirit and technical leadership have ensured that this concept not only reflects the current state of the art but also anticipates future challenges. This document stands as a testament to what can be achieved through strong partnerships and shared responsibility in safeguarding our society's most essential assets.

Euralarm • Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

Table of contents

1. Introduction

In an increasingly complex and interconnected world, in which interdependence between different sectors are ubiquitous, the security of critical infrastructures is a central element of social stability and order. The protection of these vital facilities and installations, from energy and water supply to health care and communication and transport systems, is of central importance for the well-being and security of European society. Recent developments and threat scenarios show how vulnerable European infrastructures are to targeted attacks, natural disasters and technical failures.

The introduction of the European Directive on Resilience of Critical Entities (CRE or RCE) is therefore an important step towards establishing minimum uniform standards for the physical protection of these facilities. Cross-sectoral arrangements for physical protection will complement the existing IT security measures and thus create a holistic security concept. Irrespective of the fact of the implementation timeframe of national legislative procedures, the implementation of protective measures is necessary and sensible to safeguard them against all conceivable threats, be they natural events, technical failures or targeted acts of sabotage, and to ensure their functionality. Regular risk analyses and the preparation of resilience plans not only enable operators of critical infrastructures to identify and prevent potential threats, but also to sustainably strengthen the resilience of their infrastructures.

The protection of critical infrastructures requires extensive expertise and an integrative approach in which structural, technical and organizational measures are intertwined. Only through the coordinated combination of these various protective measures can the necessary security be achieved to be able to withstand both sabotage attempts and natural disasters. The combination of physical security measures such as intrusion and fire protection, perimeter security, access control systems and video technology with advanced cyber security measures is essential. This creates a comprehensive protective shield that meets the special requirements and threats of critical infrastructures.

The purpose of this document is to illustrate in practice the importance and the basic requirements for physical security and safety in the field of critical infrastructure. In view of the constantly growing threat situation and the interdependencies between the individual sectors, the security of critical infrastructures must not only be understood as a task for individual infrastructure operators. Rather, it is an all-society issue that requires the cooperation of all parties involved - from government agencies to security authorities to private companies and specialized security service providers. Only through this shared responsibility and the continuous adaptation to new threat scenarios can the security and stability of Europe be guaranteed in the long term.

2. General overview or problem definition

In recent years, the EU has introduced two key directives to improve the protection of critical infrastructure:

- the Critical Entities Resilience (CER) Directive, also known as the Resilience of Critical Entities (RCE) Directive (EU) 2022/2557); and
- the NIS2 Cybersecurity Strengthening Directive (EU) 2022/2555).

These targets aim to ensure the functioning of key services in crisis situations and to increase resilience to various threats. In addition to the specific critical properties, large parts of the economy are also directly or indirectly affected. The guidelines are presented in more detail below.

2.1 CER Directive (or RCE Directive)

The EU Critical Entities Resilience Directive (CER Directive) entered into force in January 2023 and intended to be transposed into national laws by 17 October 2024 before becoming applicable.

Any national regulations of the CER Directive for physical protection are intended to supplement the existing IT security measures. The aim is to strengthen the overall resilience of critical infrastructures to threats.

Critical infrastructures are increasingly at risk. Events with catastrophic consequences are becoming more frequent, more complex and often reinforce each other. This has been shown in the last years. Although the infrastructure is divided into different sectors, they are interlinked in such a way that there are usually dependencies between them. If failures occur in one sector, e.g. energy, IT or logistics, this can have a serious impact on other sectors and thus on the entire value chain. Nevertheless, except for the area of IT security of critical infrastructures, regulations in Europe differ from country to country, if any exist at all.

The CER Directive establishes an umbrella over energy, transport, finance, health, drinking water, sewage, urban waste disposal, information technology and telecommunications, food, space and public administration and supplements the existing rules on IT security for critical infrastructures. The starting point is all conceivable risks that could be caused by natural or humans ('all-hazard approach') - be it a storm, human error or an act of sabotage.

It specifies which companies and institutions must implement mandatory resilience measures for the physical protection and stability of the overall society and economy.

Another aim is to consider the interdependence between critical infrastructures: for example, all other sectors depend on the energy sector. Water and transport routes are also essential for the other sectors. It is therefore envisaged to set out cross-sectoral objectives: the prevention of disruptions and failures, the limitation of their consequences and the restoration of functioning after an incident.

To achieve these objectives, operators of critical infrastructure respond to the specific risks of their investments with tailor-made measures. Those are presented in so-called resilience plans. A substantial basis for this consists of risk analyses and assessments to be carried out regularly by the operators of the sectors concerned.

Operators take appropriate and proportionate measures to achieve the set objectives. Due to the diversity of sectors, measures can be very diverse. The aim is to enable operators to develop common standards in cooperation with interbranch organizations and thus to specify what is to be regarded as an appropriate and proportionate measure for their sector (e.g. energy). Minimum standards should be created and gaps closed. Existing sector-specific regulations remain unaffected.

Furthermore, national central reporting systems for significant disruptions could be expected, which would complement the existing reporting system in the area of IT security of critical infrastructures.

The cooperation of all actors in the critical infrastructure area might be institutionalized. The responsibilities of the numerous actors involved in the protection of critical infrastructures should be defined more clearly.

Irrespective of when CER directive will be implemented on national levels, the direction can be seen: in the future, a combination of physical security (e.g. by perimeter protection, access control, intrusion and fire alarm technology, video technology and alarm management) and cyber security of the systems will be required. This has a significant impact on critical infrastructure operators and security companies, as both physical security and secure network architecture and remote access expertise are required.

2.2 NIS2 Directive and NIS2 Implementing Act

The NIS2 Directive aims to ensure a minimum level of cybersecurity across the EU. It shall apply to all undertakings and entities operating critical services and infrastructures. Member States shall ensure that these operators protect their networks and IT systems against cyber-attacks.

National implementations are intended to define clear requirements for operators of critical installations and essential facilities to close security gaps and improve protection against cyberattacks.

Significant points of the national implementations are expected to be:

1. Companies concerned:
   In addition to the operators of critical installations, NIS2 focuses on particularly essential and important facilities, depending on their size and economic importance, as well as certain federal facilities.

2. Extended sectors:
   In addition to the classic critical infrastructure sectors, such as energy, health and water, NIS2 also covers larger parts of the economy, such as manufacturing and the digital sector. This means that entities outside the previously regulated critical sectors can also be covered by the new cybersecurity requirements.

3. Scope of action:
   Among other things, the directive requires the concerned entities to take comprehensive measures for cyber security and risk management that cover the entire company. This includes, for example, a reporting obligation for security incidents.

4. Obligation to provide evidence:
   Critical infrastructure operators must prove within defined intervals (e.g. 3 years) that they comply with the requirements of the Act. For important institutions, there should be documentation obligation and random checks by the authorities in order to ensure the effectiveness of the security and safety measures taken.

5. Member State supervision and sanctions:
   The NIS2 Implementing Act asks for national implementation of the supervisory authority for the companies concerned, which in future will have to fulfil certain requirements (e.g. registration, proof and reporting obligations, etc.). If minimum requirements are not met, companies may face heavy fines, which vary depending on the violation and size of the company. Fines may be between 100,000 and 10 million euros or up to 2 percent of global sales are imposed, whichever is higher. These sanctions are intended to ensure that the prescribed cybersecurity measures are consistently implemented.

The following graph shows the different objectives of the above-mentioned guidelines at a glance:

High common level of cybersecurity across the Union

NIS2 is the minimum level of cyber security in the EU. Companies operating critical services and infrastructure in the EU are regulated by the member states.

Resilience of critical entities

CER is the resilience baseline for operators of critical services in the EU. These operators are regulated nationally and risks and implementation by the EU are monitored.

An example of the national implementation for Germany is presented in the graph below.

Focus: Cyber Security and Information Technology
Affected: KRITIS operators + particularly important facilities + important facilities
Object of protection: Large parts of the economy
German Supervision (BSI) + EU

Focus: Physical Security and Resilience
Affected: KRITIS operator
Object of protection: Critical installations
Supervisory Authority (BBK)

2.3. Impact on security technology service providers

The CER and the NIS2 directives are expected to have far-reaching effects on the requirements for installers and planners of physical security systems:

1. Holistic security concepts and 'hybrid' approaches

   Providers of physical security technology are required to integrate their products into holistic security concepts. The combination of physical protection measures, such as access control with their cyber security requirements, must be considered - i.e. this access control must be integrated into secure network structures.

   This means that e.g. Access control systems can no longer be considered in isolation but must be closely linked to IT-based monitoring systems and contingency plans. This is the only way to ensure comprehensive protection that is tailored to the requirements of the NIS2 and CER directives.

2. Advice on increasing resilience and appropriate protective measures

One of the central expectations of security service providers is the ability to competently advise operators of critical infrastructure on the selection of the right security measures. Resilience, i.e. resilience towards threats and the ability to quickly recover from disruptions, plays an essential role here. Providers must therefore be able to prepare individual needs analysis that are tailored to the specific risks of the respective institution. This includes recommending protective measures that not only address current risks but are also prepared for future threats.

3. Risk assessment and proportionality of measures

The CER and the NIS2 directives presuppose that security measures are based on sound risk assessment. Providers of physical security systems must therefore be able to embed their products and services in an overall risk analysis process. They should carry out an accurate risk assessment together with operators and, where appropriate, public authorities and develop solutions that are proportionate and tailored to the specific context of the critical infrastructure concerned. This process also requires the inclusion of organizational measures, such as the training of security personnel or the establishment of clearly defined access and intervention protocols.

4. Technical standards and consideration of normative standards and guidelines

A key requirement for suppliers is compliance with the 'state of the art'. Physical security and safety systems must comply with the latest technical standards and consider all relevant normative standards and guidelines to meet the expected requirements of the CER and the NIS2 directives. Consequently, companies should continuously adapt and keep their technology up to date to prevent manipulation, intrusion and sabotage. This also includes security measures such as advanced authentication for access systems, encrypted communication channels and modern alarm systems. It is important to ensure that the solutions are resilient to both the latest physical and IT-based threats.

3. The security concept

3.1 Description

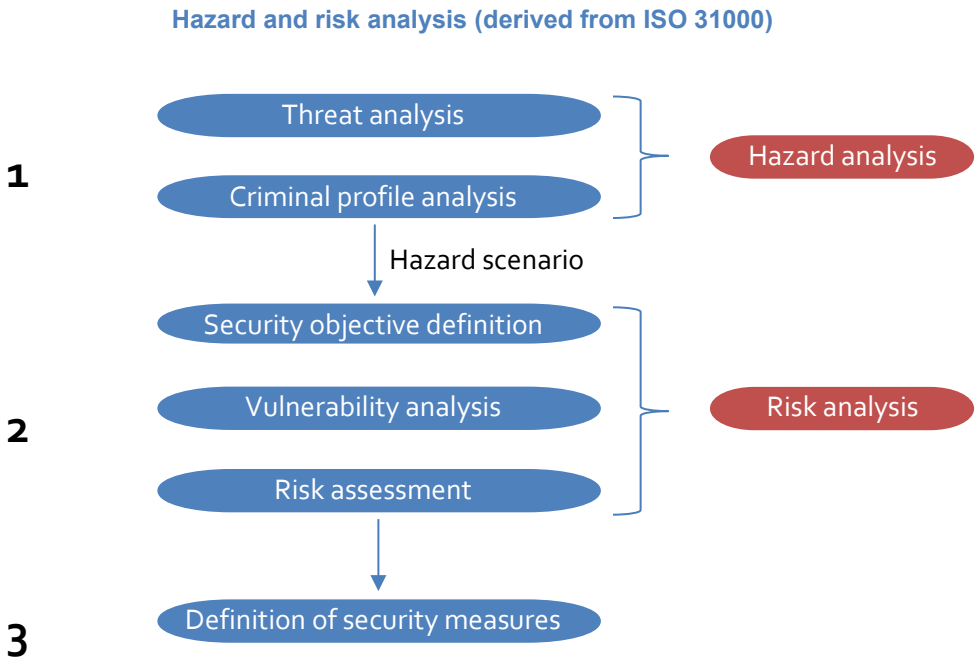
"Without a concept, everything is nothing!". This statement makes clear, not only for operators of critical infrastructures, that the preparation of a security concept, considering the structural, organizational and personnel security, is essential before any planning and projecting of a security-related system. Such a concept forms the basis for a qualified and targeted execution of security technology. An electronic security system will only have an optimal impact, if - like a gear in a complex gearbox - it is optimally matched to all other adjacent specific areas:

- structural security (e.g. perimeters, security doors and windows)
- organizational security (e.g. definition of intervention measures), and
- personnel security (e.g. quantity and quality of security staff)

A security concept makes it possible to measure and evaluate security and based on this, to derive efficient and necessary measures. Such a concept should not only be created once initially but must be continuously adapted and updated, e.g. in the event of a change in the risk situation, structural modifications or technical changes in use. Many security standards define this necessity as an operator's obligation or as a client's obligation, i.e. the operator must create and update the concept jointly or with the support or approval of the bodies involved, such as authorities, insurers, planners and installers.

This is particularly essential for critical infrastructure facilities, as changing threat situations and perpetrators' approaches can continually require new assessment criteria. This continuous improvement process is derived from the general risk management standard ISO 31000.

In recent years, these typical approach and structure for the development of concepts have been derived for the security industry.



3.2 Standards and guidelines

Apart from ISO 31000 for risk management, there are no significant specific standards for security concepts. Rather, in all essential standards and regulations for security technology (see other chapters) and in adjacent specialized areas, such as personnel safety, the urgent necessity of a safety or security concept is emphasized as well as

- operator/client obligations (e.g. inspections),
- qualifications of the acting persons (e.g. competent person)
- minimum content; and
- defined security levels.

These could be, for example, the

- series of standards for all security & hazard alarm systems (e.g. EN 50131 & upcoming EN 50749),
- for video surveillance systems EN IEC 62676-4,
- external perimeter security systems (e.g. CLC/TS 50661-7),
- Emergency and Danger Response Systems (e.g. upcoming EN 50726)
- etc.

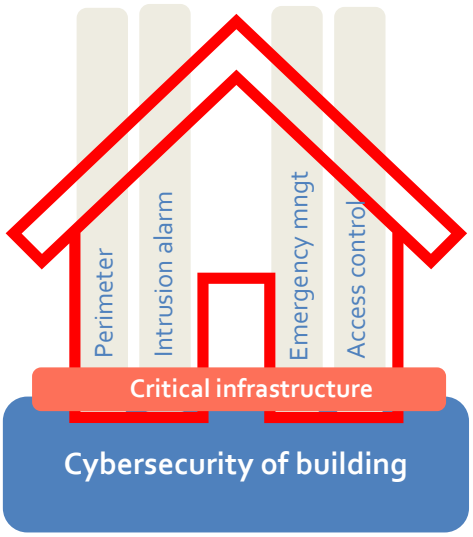
Document	Type	Titles	Publication	Validity
ISO 31000	General requirements, not subject-specific	Risk management - Guidelines	2018-02	International
EN IEC 31010	General requirements for risk assessment, not subject-specific	Risk management - Risk assessment techniques	2024-12	International

4. Minimum requirements for physical security

This chapter outlines the necessary minimum requirements that must be covered in the various security-related disciplines to ensure the physical security of a critical infrastructure.

Physical Safeguards

- External perimeter security systems
  - Physical protection and detection
- Access control systems
  - Access control and access protection of entrances and exits, driveways, barriers and locks
- Intrusion alarm systems, fire alarm systems and video surveillance systems
  - Protection of buildings and terrain - Detection
- Emergency management systems
  - Emergency management (standard procedures)
  - Implementation of organizational measures - even in crisis situations
  - Predictive overview of the security situation and 'Systemic health'



4.1 External Perimeter Security

4.1.1. Description

External perimeter security represents the outermost component of an effective security concept for a property. It often consists of a combination of mechanical security measures and an External Perimeter Security System (EPSS). The mechanical security encompasses protection-objective-compliant planning and deployment of fences and barriers as mechanical obstacles. The EPSS is an external detection system that fulfils a similar function to an intrusion detection system within a building. It serves to detect intrusion attempts into external areas outside of enclosed buildings and is installed within the perimeter.

Deter, detect, delay and document. Through early warning upon approach to a facility or during unauthorized and often forcible entry, resistance time can be significantly increased. Furthermore, a EPSS has a deterrent effect on opportunistic offenders. In almost all cases, the EPSS is combined with a video surveillance system to verify events and distinguish between genuine and false alarms.

The primary function of an external perimeter security system is therefore to ensure the integrity of the legal boundary, around the clock. It must therefore be specifically tailored to the mechanical barrier (ditch, wall, fence, hedge, etc.). Additional requirements arise from the threat profile and the general protection objective of the facility.

The requirements for a EPSS deployed to secure critical infrastructure are therefore typically set significantly higher than for standard perimeter security in the commercial or industrial sector. In addition to climbing over fences, crawling under, breaking through, or specialized movement methods such as belly-crawling, and rolling are among typical approaches that complement the threat profile.

4.1.2 Standard and guidelines

The standardization of external perimeter security is currently shaped by the European standard series of the European Committee for Electrotechnical Standardization (CENELEC), CLC/TS 50661 series. Additional national standards often apply.

Note: In the following table, possible standards related to mechanical security measures (fence, wall, outrigger construction, etc.) are deliberately omitted.

Document	Titles	Publication	Validity
CLC/TS 50661-1	Alarm and electronic security systems - Part 1: External Perimeter Security Systems - System requirements	2018	CENELEC members

4.1.3. Minimum requirements for critical infrastructures

External perimeter security systems requirements are divided into two different categories according to CLC/TS 50661-1

- EPSS self-protection and
- EPSS performance.

'EPSS self-protection' is a measure of the extent to which an offender contemplates sabotage of the security system. Critical infrastructure installations should be assigned to the intrinsic protection class '4'. Due to the perpetrator profile, a multi-stage attack is also likely. In a first step, the detection system can be decommissioned or at least disturbed. This disturbance must be detected and reported extensively.

Highest classifications of performance category are intended for installations that are more complex or require greater operational flexibility. Only from performance category 'B' are two levels of alarm provided, e.g. "pre-alarm" and "alarm". Due to better control of the intervention, this should be provided for in a EPSS for critical infrastructure installations.

	Recommendations for PSS in critical infrastructure areas
EPSS self-protection	Intrinsic protection class 4
EPSS performance category	Performance category B or higher
Detection technology	Multiple detection with two detection systems, each with a physical different operating principle in accordance with the recommendation of DIN VDE V 0826-20
Perpetrator profile to be considered	Breaking through, climbing over, crossing, loitering around
Emergency power bridging time	Depending on requirements and intervention time

4.2 Access control

4.2.1. Description

Access control systems are key in the protection of critical infrastructures, as they specifically regulate and monitor access to particularly vulnerable areas. Its main function is to grant access to security-relevant areas only to authorized personnel and at the same time to prevent potential unauthorized access, and can keep a timestamped record of transactions, flag denied attempts, etc. For operators of critical infrastructure, it is of the utmost importance to achieve the best possible level of protection and to benefit from the advantages of modern technical systems.

At the same time, transparency must be created and 'legacy' removed. Mechanical keys, for example, can be passed on, easily lost or copied without authorization which causes a permanent security risk. In addition, replacement can quickly become expensive in the event of key loss. The use of a lost/stolen key is not logged or noticed. To meet a higher security level, additional or alternative biometric detection methods can be used for verification or authentication in critical facilities. An intelligent electronic access control system provides an effective remedy and can be more cost-effective over the entire life cycle, as operating costs are significantly different to pure mechanical systems.

Individual or group-specific access rights are used to determine who has access when and where. At the same time, security managers receive a comprehensive overview of all access events as well as notifications if access points are opened, passed or manipulated without authorization. This can bolster protection against theft, vandalism, sabotage and economic espionage. In the event of loss or theft of access card or key, immediate action can be taken. By deleting permissions in real time, the object is never unprotected. In addition, access rights can always be updated during operation and, for example, provided with flexible access times.

Efficient electronic access management saves considerable resources, creates flexibility in handling and ensures an overview with detailed real-time data. In addition, security procedures can be automated, and operating costs can be reduced. Many everyday functions and reactions to incidents can be handled without manual intervention. This saves time, makes maintenance more efficient and reduces personnel requirements on site.

The various integration options with third-party systems are also advantageous. The possibilities range from classical security systems such as video surveillance systems, perimeter protection, escape route control and physical security information management (PSIM) to room management, time recording, occupational safety instruction systems, presence notification and building management. Fire alarm systems can also interact with the access control system. The fire alarm control panel could trigger appropriate escape door controls, for example.

4.2.2. Standards and guidelines

The access control technology is covered by EN IEC 60839-11 series of standards.

Note: The following list deliberately makes no reference to any standards related to mechanical protection (door, lock, fittings, etc.).

Document	Titles	Publication	Validity
EN IEC 60839-11-1	Alarm and electronic security systems - Part 11-1: Electronic access control systems - System and components requirements	2013 + AC 2015	CENELEC members
EN IEC 60839-11-2	Alarm and electronic security systems - Part 11-2: Electronic access control systems - Application guidelines	2015 + AC: 2015	CENELEC members
EN IEC 60839-11 full series	See IEC catalog of standards		

EN IEC 60839-11-1 sets out the requirements for access control systems. For this purpose, the requirements to be fulfilled are listed in 4 security levels. Requirements cover, for example: access point interface, alerts and signalling (display, alarm, logging), threat signalling, overriding, system self-protection and power supply.

4.2.3. Minimum requirements for critical infrastructure

The classification in one of the 4 security grades according to normative Annex A of EN IEC 60839-11-2 is carried out by the operator according to their safety and organizational requirements and a previously carried out risk analysis, if necessary, together with the security provider. High security areas of critical infrastructures must be implemented primarily at security grade 4. Risk analysis is not part of the standard, but guidance is provided.

In the event of security incidents, the system shall automatically and software-controlled activate the following processes:

- Blocking access to hazardous areas
- Closure of access points (e.g. locks)
- Opening pre-determined emergency doors
- Triggering of alarms, especially for rescuers

4.3 Intrusion Alarm System (IAS) or Hold-up Alarm System (HAS)

4.3.1. Description

Intrusion alarm systems (IAS) and Hold-up alarm systems (HAS) play a central role in the protection of critical infrastructure and serve the comprehensive security of buildings and systems. These security systems provide precise, fast and effective detection and reporting of intrusion or robbery situations and are indispensable for the protection of highly sensitive areas.

Intrusion alarm systems are technical systems that are familiar with intrusion attempts and manipulations at an early stage and trigger alarms. A variety of sensors are available to detect potential intruders, e.g. motion detectors, glass break sensors or magnetic contacts on windows and doors. These systems continuously monitor all sensitive areas of critical infrastructure, providing an effective line of defence. In the event of an incident, IASs automatically initiate measures, which usually include alerting a security control centre or the responsible security forces. This enables rapid response to threats to counter attempts of unauthorized access to security-relevant information or assets.

Hold-up alarm systems complement IASs by being designed for manual alarms in emergency situations. HASs enable personnel to trigger a targeted alarm in the event of an attack or threats from third parties.

These systems often consist of strategically placed panic buttons or mobile triggers and are designed in such a way that they can be discreetly used to enable immediate action. When an HAS is triggered, a rapid alarm is transmitted to security forces, which is particularly important for areas with public traffic or for critical control

centres and control rooms.

By being able to give an alarm in acute threat situations, HASs contribute to the prompt security of personnel and to ensuring operational functionality.

The detection and response times must be closely coordinated to be able to intervene quickly in the event of security-related incidents, such as intrusions. Especially in critical infrastructures such as substations, which play an essential role in the power supply, such an incident can have far-reaching consequences. For instance, a stolen cable harness not only leads to financial damage but can also have a serious impact on security of supply. Hospitals, utilities or other vital facilities could be cut off from the power supply, creating serious risks. In this case, the intrusion or hold-up alarm system serves less to protect against classic theft. Its primary purpose is to detect sabotage or other attacks on critical infrastructures at an early stage and to enable a direct response, for example by security services or the police.

4.3.2. Standards and guidelines

The following standards and guidelines are relevant for intrusion and Hold-Up alarm systems:

Document	Titles	Publication	Validity
EN 50131 full series	Alarm systems - Intrusion and Hold-up systems	See CENELEC search page (Keyword : "50131" Committee : "CLC/TC79")	CENELEC members

4.3.3. Minimum requirements for Critical Infrastructures

For objects belonging to the critical infrastructure category, professional perpetrators must be expected in many cases, with particular reference to organized crime, extremists and terrorists. Therefore, the use of Security Grade 3 components in accordance with EN 50131 or higher (if available) is strongly recommended to ensure more comprehensive protection against overcoming and sabotage. Examples are motion detectors with integrated masking detection, magnetic contacts with integrated external field monitoring and transmission paths to the alarm receiving point with DP4 (Dual-Path-4) technology.

The combination of different detection technologies can significantly increase the resistance to attempts to overcome the system. The standards mentioned do not only refer to the devices but also contain specifications for their professional installation. An intrusion alarm system (IAS) or hold-up alarm system (HAS) should be installed in a place that is neither visible nor accessible to unauthorized persons to ensure protection from sight and access.

4.4 Fire alarm systems (FAS)

4.4.1. Description

Fire alarm systems for critical infrastructures are to be understood in the context of this document in such a way that buildings, plant parts or even racks/cabinets etc. are supervised in a protective target-oriented manner in addition to the already existing building regulations requirements.

This is mostly done with the help of so-called special technology, i.e. not only with the classical point-type automatic fire detectors.

Interaction with extinguishing systems as well as the possibility of triggering actions based on pre-set rules and pre-alarm information is usually described in the security concept beyond the normative area.

4.4.2. Standards and guidelines

In the case of fire alarm systems, in most countries local regulations or standards apply when connected to public fire brigades. If insurance specific requirements are considered, very often additional requirements must be implemented.

4.4.3. Minimum requirements for Critical Infrastructures

The selection of available construction products or the possibility of individual system adaptation in accordance with the applicable standards and regulations should already be discussed in the fire protection concept (fuse concept).

While aspirating smoke detectors have become established for monitoring transformer rooms and equipment surveillance, linear smoke detectors in various configurations (2D/3D) can be applied for large monitoring areas. The deployment of video technology for the detection of fire and smoke, or the use of pure thermal monitoring systems, could be feasible depending on the risk analysis. System components that are not certified or harmonized as construction products may be employed if their use is necessary to achieve the protection objective and they are listed in the relevant standards. This also applies when these components are not included in a system according to EN 54-13.

The monitoring of junction boxes, data cabinets and computer systems, power supply equipment and associated emergency power supply requires a high degree of expertise.

4.5 Video Surveillance Systems (VSS)

4.5.1. Description

To ensure the long-term security of critical infrastructure, video surveillance systems in addition to other security technologies offer the added benefit of making sensitive and/or confusing areas or rooms visible from a (large) distance. At the same time, the actual events onsite (also across locations) can be observed and recorded at the same time.

The intelligent interaction of the various security systems with modern video surveillance technology, whose systems work together in a networked manner, results in great potential for crime prevention, as it is possible to identify suspected perpetrators at such an early stage that they are already detected before entering sensitive areas by means of video technology.

If the video surveillance technology is additionally equipped with bidirectional audio technology, a control centre or a 24-hour emergency call and service control centre can remotely address the alleged perpetrators. In most cases, this deters an offender from entering or proceeding to the sensitive area.

The requirements for a VSS to secure a critical infrastructure are therefore usually much higher than for a standard video backup in the commercial or industrial sector. It is therefore strongly recommended to work according to the current state of standards when securing critical infrastructures.

4.5.2 Standards and guidelines

The standardization of video surveillance technology is regulated by the EN IEC 62676 series of standards.

The most important standard in this series is EN IEC 62676-4, which describes the application rules for video surveillance systems in security applications. Among other things, it describes details on the topics of design, selection, planning, construction, image quality verification, operation and documentation.

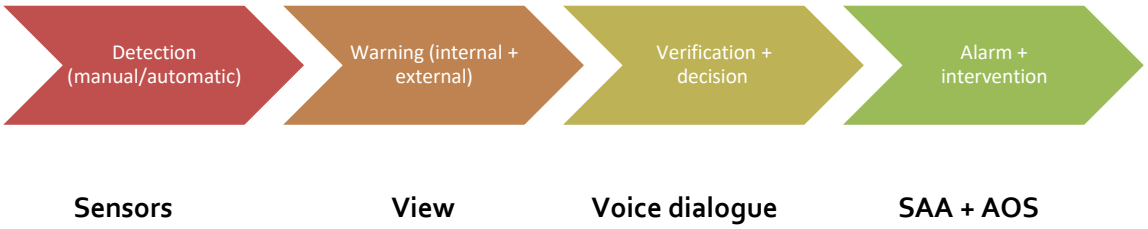
Document	Titles	Publication
EN IEC 62676-1-1	Video surveillance systems for use in security applications - Part 1-1: System requirements - General	2014
EN IEC 62676-1-2	Video surveillance systems for use in security applications Part 1-2: System Requirements – Performance requirements for video transmission	2014 + AC: 2015
EN IEC 62676-4	Application Rules for Video Systems in Security Applications	2025
EN IEC 62676 full series	See IEC catalog of standards	

4.5.3. Minimum requirements for Critical Infrastructures

The revised version of EN IEC 62676-4 (IEC publication available since October 2025) explicitly addresses the definition of security grades. Depending on the sector and subsector of critical infrastructure, the standard recommends different security grades, which are presented in a table.

4.6 Communication chain

The following diagram illustrates the communication chain from the detection until the intervention for Emergency and Danger Response Systems (EDRS). This chain is further detailed in the following sub-sections.



SAA: System Activation Alarm
AOS: Authorities and Organisations with Security responsibilities

4.6.1. Description

Communication in the event of a crisis is of central importance for the rapid and effective management of the situation. Especially in times of crisis, communication systems must be highly available to all reporters (EN 50726-1: devices, systems, or individuals that identify and communicate the occurrence of an emergency or danger event) and decision-makers. At the highest security level, a communication system that is independent of all other systems and self-sufficient, with its own redundant network, should be available. At the medium security level, redundancy is not necessary, and at the low security level, an existing security network can be used instead of a separate network. The decision on the relevant security level is made as part of a risk management process.

An established communication concept is used in every organization.

The main tasks of the communication systems used therein are to support all processes in order to ensure smooth operation, as well as to quickly and effectively remedy malfunctions in the operating processes. These disturbances can be of a technical nature or affect the health and safety of employees. Through various preventive measures, such intra-organizational disturbances can be reduced to a minimum.

Regarding potential national legal requirements, the existing communication concept of an organization may need to be reviewed and adapted, considering all conceivable disturbances caused by external factors.

The interferences (attacks) regarding the type of execution and the associated extent of damage to be considered in the communication concept for damage management must be determined on a case-by-case basis by a risk assessment in a risk management process (see chart).

Each incident requires a decision on the nature and scope of the measures to be taken. Many questions are of particular importance, for example:

- Is the organization's existing communication structure, with its existing communication facilities, capable of bringing about quick and well-founded decisions on measures to be taken?
- Is the existing communication infrastructure available in the event of an incident?
- Are there any priorities for incident communication?
- Is there an emergency communication infrastructure?
- How long is the emergency communication infrastructure available in the event of a power outage?
- How to make the right decision in case of simultaneous fire alarm (evacuation) and containment alarm, what happens in the event of a terrorist attack if both events are reported at the same time?

These and many other questions must be answered in the context of risk management for an Emergency and Danger Response System (EDRS). It is required to implement a 'risk management file' in accordance with EN 50726-1.

In many critical infrastructure relevant organizations, emergency and danger response systems have been installed over recent years to be able to make quick decisions in the event of a crisis and to significantly reduce the extent of damage.

The reaction time to an incident has a great influence on the extent of damage. The shorter the reaction time, the faster countermeasures take effect and the shorter the duration of the disturbance.

Incident Response Time = **Total time to Report Incident + Contact Availability Officer + Investigate and Verify the Situation + Decide + Initiate Countermeasures + Assistance from Authorities and Organizations with Security Responsibilities**

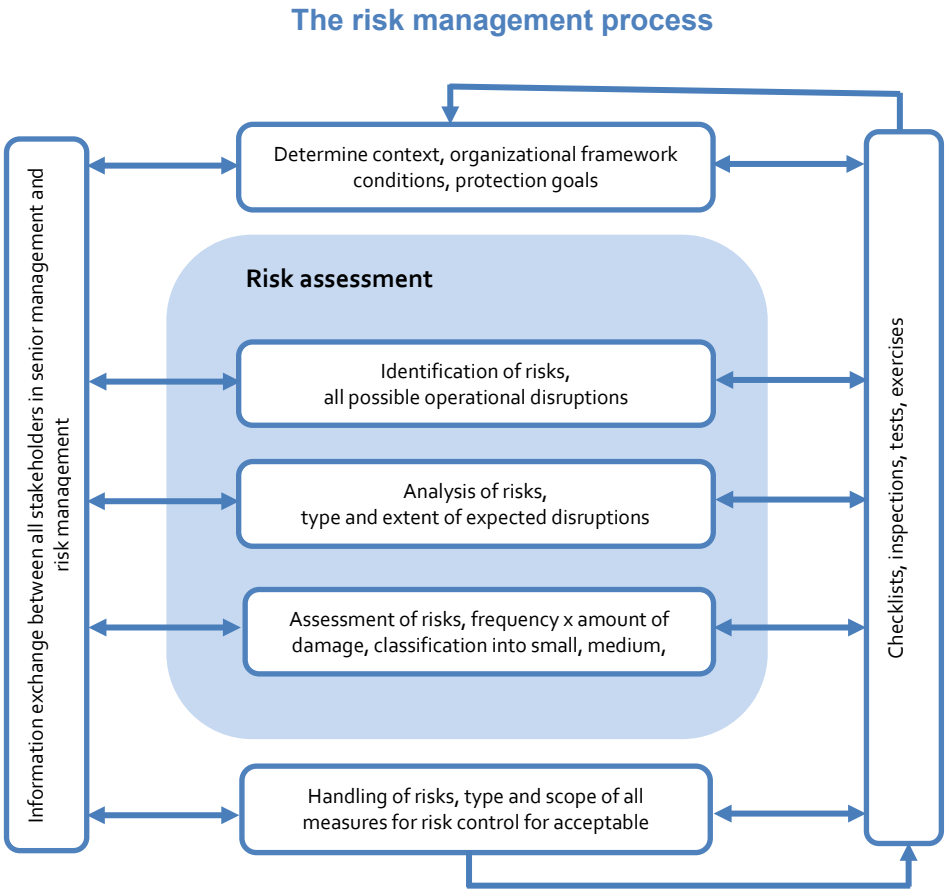
One way to reduce the incident response time is to reduce it to the reporting time if appropriate countermeasures are automatically initiated by incident notifications. However, this carries the great risk that false incident reports are not filtered out and thus cause damage. In addition, in the case of simultaneous occurrence of dangers with countermeasures, such as a terrorist attack report and a fire report, the wrong countermeasure might be initiated, and the proportionality of the countermeasures would not be taken into account.

Another possibility for minimizing the incident response time is optimal crisis-disaster-case communication along the entire event chain from the incident notification to the initiation of countermeasures. As a result, false incident reports can be filtered out, situational correct countermeasures can be initiated, and proportionality can be considered.

Which crisis and incident response is required in the form of data, information, language and alerting in conjunction with the corresponding organizational needs in individual cases cannot be determined on a blanket basis but must be determined as part of a risk management process (see chart).

The risk management process for an EDRS is an essential part of EN 50726-1:2024. The standard describes the requirements for an emergency and danger response system (EDRS) in conjunction with the required organizational communication along the event chain and concludes with the forecast of the expected residual

risks. The residual risks apply on the assumption that all identified technical and organizational measures for risk control are implemented and complied with in accordance with the risk-co-management file drawn up.



4.6.2 Standards and guidelines

Document	Titles	Publication
EN 50726-1	Emergency and Danger Systems Part-1 Emergency and Danger Response System (EDRS) Basic requirements, duties, responsibilities and activities.	2024-05
EN IEC 62820-2	Building intercom systems - Part 2: Requirements for advanced security building intercom systems (ASBIS)	2018-01
EN IEC 62820-3-2	Building intercom systems - Part 3-2: Application guidelines - Advanced security building intercom systems (ASBIS)	2018-06
EN IEC 31010	Risk management - Risk assessment techniques	2019
prEN 50726-2	Emergency and danger systems, Part 2: Emergency and Danger Response Systems (EDRS) – Particular requirements for all hazard approach	in preparation
prEN 50726-3	Emergency and danger Systems – Part 3: Emergency- and danger-response-systems (EDRS) – Risk management file and examples for applications	in preparation

4.6.3 Minimum requirements for critical infrastructure

The minimum requirements for an emergency crisis communication system result from the risk management process according to EN 50726 Part 1 and Part 3, whereby it must be checked very carefully whether the low security level is suitable for a critical infrastructure application. If it is nevertheless used, the 'voice communication' feature of security level 2 is mandatory to minimize the residual risk.

5. Cybersecurity through resilient transmission technology as well as secure routers and networks

5.1. Secure networks/routers and resilient transmission technology

5.1.1. Description

Security technology requires maximum reliability and protection against failures or attacks, especially in critical infrastructures and sensitive areas. EN 50136 plays a central role here, as it defines requirements for the transmission of alarm messages via networks.

This standard specifically refers to alarm transmission systems that ensure communication between intrusion detection, fire detection, access control systems and alarm receiving centres.

To ensure maximum resilience, secure routers and networks are crucial. The resilience of a system describes its ability to remain robust against external influences such as cyber-attacks, technical faults or network congestion and to maintain the required functionality. The aim should therefore always be to establish a safe and redundant transmission path so that both the transmission paths and the transmission times can be monitored in accordance with the applicable standards and directives.

5.1.2 Standards and guidelines

In the field of alarm transmission technology, there are several standards and directives that are relevant at both European and national level. These standards and guidelines define the requirements for the planning, installation, operation and monitoring of alarm transmission systems.

Apart from any national standards, the following European Standards shall be considered, depending on the applicability:

Standards	Title
EN 50136-1	Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems
EN 50136-2	Alarm systems - Alarm transmission systems and equipment - Part 2: Requirements for Supervised Premises Transceiver (SPT)
EN 50136-3	Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)
CLC/TS 50136-10	Alarm systems - Alarm transmission systems and equipment - Part 10: Requirements for remote access
EN 54-21	Fire detection and fire alarm systems - Part 21: Alarm transmission and fault warning routing equipment
EN 50131	Alarm systems - Intrusion and hold-up systems

5.1.3. Minimum requirements for Critical Infrastructures

1. Power supply

   Transmission technology must be protected against voltage drops and power outages, which can be ensured by an uninterruptible power supply.

   In addition, the power supply unit of the transmission device should be continuously monitored so that any malfunctions are reported to a permanently occupied body. Such a power supply unit should meet the requirements of EN 50131-6 Grade 4.

2. Redundant transmission paths

   Transmission technology which has at least two independent transmission paths should only be used, e.g. a wired IP transmission path and a radio-based IP transmission path (mobile).

   Both transmission paths should be fully emergency powered and have end-to-end monitoring to the alarm receiving centre.

3. Sabotage / Tamper Protection

   The transmission technology must be adequately protected against mechanical damage or sabotage, e.g. by robust housing, cover contact, drill-through protection or tear-off protection.

4. Surge Protection

   As part of the risk analysis, it is recommended to consider whether additional surge protection is required. This applies, among other things, to the 230V power supply, external mobile phone antennas, or any other kind of connection.

5. Cybersecurity

   Only specially designed protocols are to be used for the alarm transmission, which corresponds to the current state of the art.

   The device used should also be certified according to the applicable cybersecurity requirements.

   It is recommended to use devices that have been developed according to the principles of 'Security by Design' and 'Security by Default' and that have state-of-the-art protection measures in place against Denial of Service (DoS) attacks.

   Remote access should only be carried out via services and infrastructures that comply with the state of the art in accordance with EN 50710 and CLC/TS 50136-10.

Use of certified equipment:

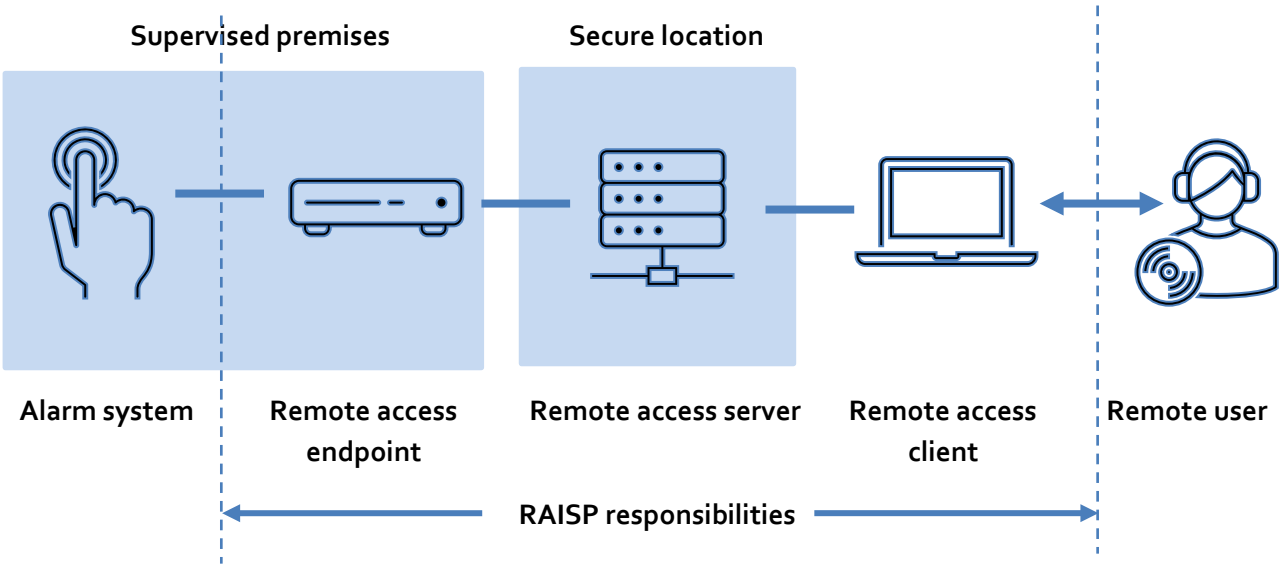
The transmission equipment used should be tested and certified according to EN 50131-10, EN 50136-2 and EN 54-21.

Installation recommendations for intrusions in the Critical Infrastructure area		
Intrusion	ARC according to EN 50518	
Transmission device incl. power supply unit	Approval according to EN 50131, grade 4	
Cybersecurity standard	Compliance with existing national directives	
Transmission routes	Dual-Path 4 (permanent connections only)	
Transmission protocol	Compliance with existing national directives	
Key generation	Dual alarm receiving point (PK03)	By transmission (PK04)
Transmission systems	Two transmission networks with closed user group (no access from the public network)	
Emergency power bridging time	On the object side for at least one transmission path; 60 hours	
Remote access options	According to EN 50710 / CLC/TS 50136-10 on closed-group transmission systems	
Certifications	EN 50131-10, EN 50136-2, EN 54-21	
Password security	E.g. according to the state of the art only passwords with at least 8 characters, uppercase and lowercase letters, numbers and special characters	

5.2. Remote Access and Remote Services

- EN 50710 regulates "remote services"
- CLC/TS 50136-10 regulates "remote access infrastructure"

The two standards apply to all security- and safety-related systems described in this document.
CLC/TS 50136-10 'Requirements for Remote Access' regulates the technical infrastructure for secure remote access connections and overall responsibility on the remote access infrastructure. It defines the performance, reliability, integrity and security features of a remote access infrastructure. A remote access server takes over the central function of the remote access infrastructure. The operator of the remote access infrastructure shall assume overall responsibility, including for cybersecurity.



EN 50710 lays down requirements for the provision of secure remote services. These are specifically designed for fire safety systems and security systems in general and more specifically for each type of system.

A risk assessment shall include permitted operating procedures and protective measures. Responsibilities are regulated between the provider of the remote service and the client.

6. Cybersecurity requirements for products

It is not only in the context of critical infrastructures that increasing attention must be paid to the cybersecurity of the products used. New legislations are currently being passed, which must be implemented by the manufacturers of the products. Users and installers should pay attention to the implementation of the cybersecurity goal, especially around critical infrastructure.

6.1. CRA - Cyber Resilience Act

Critical Entities Resilience (CER) Directive and NIS2 Directive focus on organizational and operational resilience. The CRA adds a technical layer of protection by ensuring that the digital products used within these infrastructures are secure by design. The Cyber Resilience Act was published in the Official Journal of the European Union by Regulation (EU) 2024/2847 on 20.11.2024 (see Regulation - 2024/2847 - EN - EUR-Lex).

The regulation entered into force on December 10, 2024, and its main obligations will apply from December 11, 2027. Vulnerability reporting requirements apply from September 11, 2026.

For the first time, the CRA describes the cybersecurity requirements for digital products across industries. This includes hardware as well as software.

There are exceptions only for non-commercial open-source projects and industries in which there are already more extensive regulations, such as medical devices. These requirements are particularly important for manufacturers as they need to ensure that their products meet the new standards.

Below you will find the most important questions and answers about the CRA.

Do the requirements of the CRA have to be met?

Yes, the CRA extends the scope of the CE mark. Without fulfilling the requirements, the products can no longer be sold in the EU internal market. This applies not only to manufacturers but also to traders and importers who wish to place goods on the EU internal market.

What requirements need to be implemented?

The CRA stipulates that the information security of a product must be ensured throughout its entire life cycle. This includes principles such as 'Security by Design' and 'Security by Default', as well as ensuring the confidentiality and integrity of the data processed and transmitted. Manufacturers are required to report discovered vulnerabilities and fix them with security updates. In addition, the maintenance of a Software Bill of Materials (SBOM) is mandatory.

SBOM documents which commercial and free software components are contained in software products. It makes dependencies on third-party components transparent and thus helps manufacturers, security researchers and professional users to monitor vulnerabilities.

How long is the product life cycle?

According to the CRA, the life cycle of a product with digital elements starts at the time of placing on the market and is valid either for the expected lifetime of the product or for a period of five years from the date of placing on the market, whichever is shorter.

What are the penalties?

Failure to do so will result in severe financial penalties and a ban on the sale of the product on the European market.

Why should we deal with the issue now?

Establishing the necessary processes takes time and several cycles of experience. Aspects such as a secure development process, security by design and security by default should be implemented at an early stage to ensure compliance with the later published harmonized standards.

Are there specific provisions in the CRA addressing concerns for critical infrastructures?

The CRA is (amongst other objectives) intended to facilitate the compliance of digital infrastructure providers with the supply chain requirements under NIS 2 Directive by ensuring that the products that they use for the provision of their services are developed in a secure manner and that they have access to timely security updates for such products.

For that purpose, categories of critical products are listed in the CRA: Hardware Devices with Security Boxes, Smart meter gateways, Smartcards or similar devices (this list is likely to be extended in the future). They have a cybersecurity-related functionality and perform a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products with digital elements through direct manipulation. Furthermore, those categories of products are considered to be critical dependencies for essential entities.

For those reasons, such products are, as a minimum, subject to an EU-type examination (third-party conformity assessment by a Notified Body) and might, in the future, be subject to a European cybersecurity certification scheme developed under the Cyber Security Act (CSA), like e.g. the European Common Criteria-based cybersecurity certification scheme (EUCC). Also, the mandatory notification of actively exploited vulnerabilities intends to ensure that the CSIRTs designated as coordinators, and ENISA, have an adequate overview of such vulnerabilities and are provided with the information necessary to fulfil their tasks as set out in NIS 2 Directive.

6.2 RED (Radio Equipment Directive)

The RED prescribes cyber security in Section 3.3. The requirements can be fulfilled by the manufacturers through a self-assessment and declaration of conformity with a harmonized standard (EN 18031 series) or after verification by a notified body.

All products that support wireless standards such as WIFI, Bluetooth or Zigbee are affected by the directive. This means, in a broader sense, that, for example, machines connected to the internet must not have 'harmful effects on the network or its operation' and the protection of personal data must be ensured.

6.3. Products from safe origin/transparency Supply chain

New or revised standards increasingly oblige manufacturers to monitor the origin of both digital and physical components of their products. As already mentioned, the Cyber Resilience Act requires the maintenance of a Software Bill of Materials. External software or software stock parts, so-called libraries, must be documented and checked. This is done either by the supplier's obligation to report and correct security gaps as quickly as possible, or by their own efforts, when integrating open-source projects, to check them for errors or security gaps.

The usual use of libraries in software projects is therefore no longer easily possible. In the event of a security breach, the company is obliged to provide authorities and customers with qualified information, in some cases within 24 hours of becoming aware of it. In addition to reporting, an assessment of the severity of the incident must also be carried out.

The same applies to hardware components. For example, certain non-European companies are coming under increasing scrutiny and there are instances of blocking the use of these products in the critical infrastructure environment; e.g. back doors can also be inserted into the products via the hardware - in some cases, it is difficult to prove/disprove whether a device is "phoning home".

The network and the networked devices are the basis for overall security. The product is only as secure as the weakest link in the chain. In other words: the most unsecure supplier is critical to the security of the product. Therefore, the entire supply chain must be considered. European Standards are designed to ensure the reliability of the components used. Labels such as 'Made in Europe' are therefore likely preferred or maybe given greater importance.

7. Selection of suitable specialist companies

Professional and qualified advice and support for Critical Infrastructure operators by companies specializing in security and safety technology is of crucial importance for the effective and targeted protection of critical infrastructure.

At this point, it is particularly important to warn against unqualified or even dubious companies that try to sell the critical infrastructure operators a superficially cheap technology quasi 'off the shelf'. Such systems are usually unsuitable, as the individual requirements of the device to be protected are not considered. Unfortunately, operators often realize too late that these 'standard solutions' do not meet their specific security needs.

To ensure that security and safety systems are fully functional when required, they must not only be installed by specialist companies, but also regularly maintained by them.

The use of incorrect products and/or incorrect or inadequate planning of the security technology often leads to malfunctions in practice.

National regulations (authorisation schemes) and certification schemes shall be considered when choosing a suitable specialist company.

Publication date: November 2025

Euralarm
Gubelstrasse 22
CH-6301 Zug (Switzerland)

Swiss Commercial Registration No: CHE-222.522.503

E secretariat@euralarm.org
W www.euralarm.org