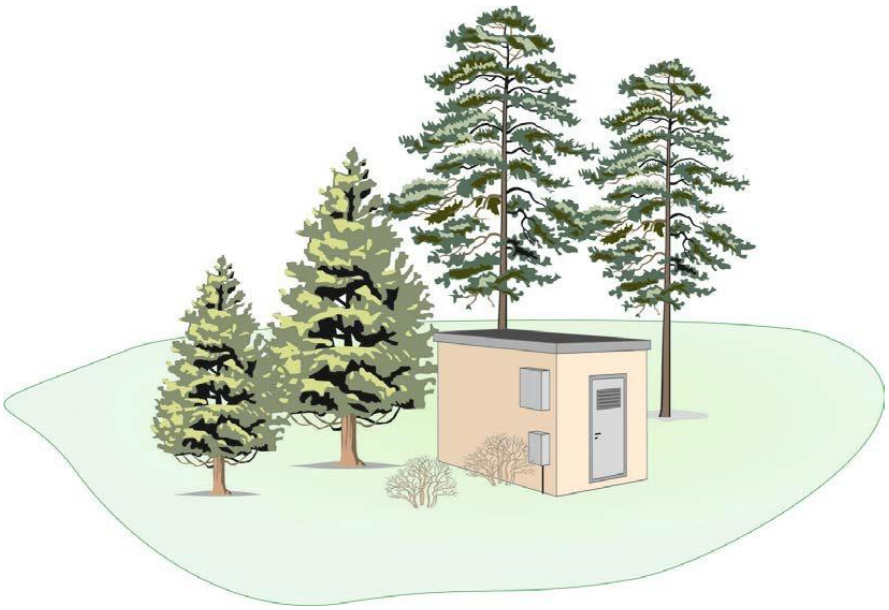
Instructions for Robust Fiber

Sub-appendix 4.1

Robust sites for digital critical infrastructure protection

Ver 1.3.2



CONTENTS

1. INTRODUCTION

This sub-appendix is a guide with minimum requirements for how a robust Site should be supplemented with the aspect of protection and functions for extended operating time to be able to handle electronic communication in the event of Extraordinary events. The minimum requirements include both requirements for new construction and requirements for rebuilding an existing facility.

The sub-appendix also contains recommendations and examples of solutions.

2. DEFINITIONS

Uninterruptible power supply
UPS, "uninterruptible power supply" takes over the power supply in the event of interruptions in the external electrical network for a limited period and acts as a filter against disturbances in the network. The size of the batteries and consumption, respectively, determines how long interruptions can be handled.

Operations center
Location for monitoring and control of electronic communications networks. Often referred to as the Network Operation Center (NOC).

Extraordinary event
Extraordinary event refers to such an event that deviates from the norm, involves a serious disturbance or imminent risk of a serious disturbance in important societal functions and that requires urgent action by a municipality or a region. The Act on Extraordinary Events (LEH) (2019: 925).

Extended operating time
Extended operating time means that the Site must have an operating time of at least 10 days after an interruption in the Site's external power supply has occurred.

Alarm center
Activities at alarm companies for receiving alarms and initiating action.

Critial operations at societal level
Operations that can cause societal disruptions in the event of disruptions or loss of operations. There may also be activities needed to deal with an ongoing societal disturbance.

The concept includes the facilities, nodes, infrastructures, and services that are of crucial importance for maintaining important societal functions.

3. THREATS

This refers to events that affect the access to, and the function of, a Site. The threats shall be checked when information about changes regarding threats is communicated from PTS (PTSFS 2020: 1 5§).

External threat

- Accidents:
  - Weather (PTSFS 2020: 1 5§)
    - Storm (Wind)
    - Lightning strike
    - Heat wave (high temperatures)
    - Extreme cold
    - Skyfall.
  - Floods (precipitation, moisture).
  - Fires (vegetation fire and fire in a building).
  - Landslides.
  - Third party
    - Accidental excavation of cables
    - Accidental disconnection of connections.

  Note. See also "Katastrof natur/miljö" https://www.msb.se/sv/amnesomraden/skydd-mot-olyckor-och-farliga-amnen/naturolyckor-och-klimat/).

- Physical attacks / serious criminal activity / terrorism:
  - Sabotage (PTSFS 2020:1 5§).
  - Intrusion (PTSFS 2020: 1 5§).
  - Excavation of cables.
  - Other external impact (PTSFS 2020: 1 5§).
  - Fire.
  - Destruction or theft of equipment.
  - Water damage.
  - Electromagnetic radiation (see electromagnetic threats below).

- Electromagnetic threats (EM threats), electric and / or magnetic fields that are strong enough to affect electrical / electronic devices and systems):
  - Lightning strike.
  - Solar storms.
  - Electrostatic disorder (EDI).
  - Electromagnetic Interference (EMI).
  - Radio Frequency Interference (RFI).
  - Electric network transients.
  - Electromagnetic pulse (EMP).
  - Direct injection (to conduct strong current pulses directly on electrical or data cables in a building).
  - Intentional Electromagentic Interference, IEMI (High Power Microwaves HPM).

  Note. See also https://www.msb.se/sv/publikationer/centrala-beredningsgruppen-elektromagnetiska-hot-cbg-em-hot--forum-for-informationsspridning-och-samverkan-om-em-effekter/ and https://www.regeringen.se/regeringsuppdrag/2020/07/uppdrag-till-elsakerhetsverket-och-forsvarsmakten-att-utreda-elektromagnetiska-storningar-pa-totalforsvarets-verksamheter/

internal threat

- *Serious criminal activity (refers to threats from own organization):*
    - Corruption of information assets.
    - Unauthorized copying of software.
    - Unauthorized use of equipment.
    - Manipulation of networks, hardware and software.
    - Illegal or unauthorized handling of information.
    - Theft of information.
    - Eavesdropping on information.
    - Disclosure of sensitive information.
    - Receipt and use of information from unreliable sources.

- *Downtime:*
    - Inaccessibility of staff / staff loss.
    - Lack of goods and services for maintenance and repair.
    - Loss of power supply (external).
    - Excavation of cables.
    - Loss of ability to monitor and control.
    - Deficiencies or errors in troubleshooting functions
      Improper use of equipment.
    - Faults in equipment (devices and systems).
    - Conductive disturbances (see electromagnetic threats).
      Loss of functions for indoor climate.
    - Dust, Corrosion and frostbite.
    - Network and hardware overload.
    - Thermal radiation.
    - Presence of shortcomings in preventive work.
    - Presence of deficiencies in management functions.
    - Contamination e.g., radiological, or biological contamination.
    - Major accident occurs.
    - Limited access to technology location due to external circumstances.

4. SECURITY LEVEL FOR EXTRAORDINARY EVENTS

4.1 Overall requirements

The technical and organizational measures that the provider of public communication networks or publicly available electronic communication services shall take in accordance with chapter 5. Section 6 b of the Electronic Communications Act (2003: 389) is regulated in the Swedish Post and Telecom Agency's regulations on requirements for operational reliability PTSFS 2015: 2 and 2020: 1.

The Operational Safety Regulation divides assets into five classes (A-E) based on the number of active connections that may be subject to disruption or interruption because of the asset ceasing to function normally

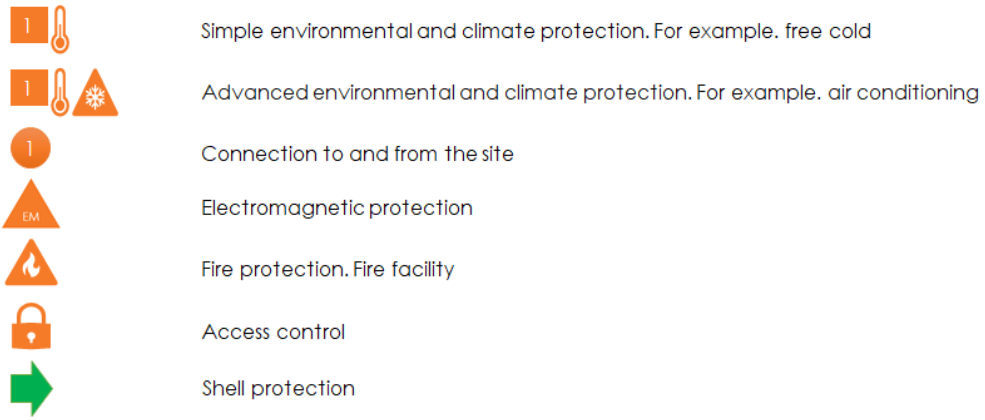
For the facilities (Sites) that manage these assets, based on the importance of the Site in the electronic infrastructure, the guide defines a number of security levels with complementary protection measures focusing on protection and functions for extended operating time in the event of extraordinary events.

The protective measures for each safety level are defined in section 5. DESCRIPTION OF PROTECTIVE MEASURES.

4.2 Security level for Site regarding handling of Extraordinary events

The security level that a Site must obtain is denoted by **"S"** and is determined by the Site's importance in the electronic infrastructure.

Explanation of symbols



Security level

S0. Small local significance the site handles nodes for a local area with a limited number of connected customers. The site can handle the placement of systems and equipment for critical operations and activites without privacy protection by mounting in electronics racks.

Image: Security level S0 - Site of small local significance

S1. High local significance the site handles nodes for a local area with connected customers, customers with critical operations and facilities for mobile radio. The site can handle the placement of systems and equipment for critical operations and activites to a limited extent.

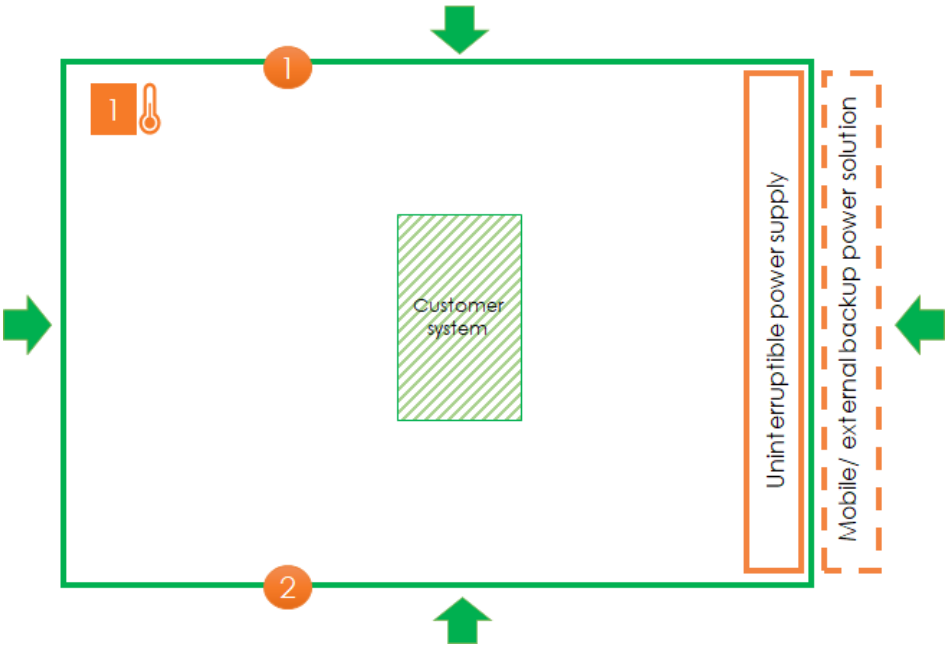


Image: Security level S1- Site with high local significance

S2. High importance the site handles a central strategic node within a geographical area. The site handles inbound and outbound traffic for a geographical area such as a municipality. The site can handle placement of systems and equipment for critical operations and activites by placing electronics racks in, for the business' own section, with burglar alarms and passage systems.

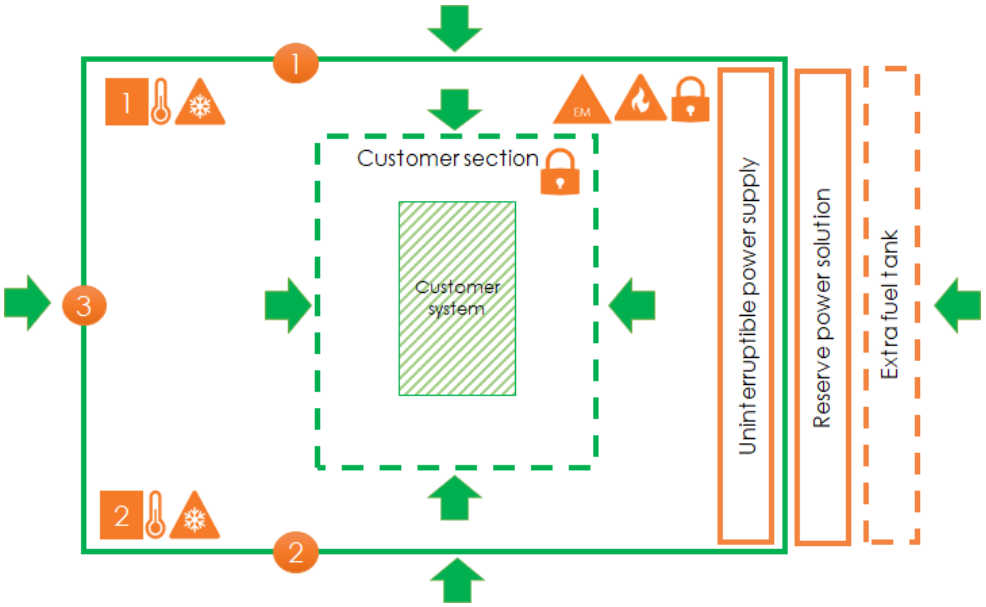


Image: Security level S2 - Site of high importance

S3. Crucial importance the site handles traffic that is part of the regional or national electronic infrastructure. The site can handle the placement of systems and equipment for critical operations and activites by placing electronics racks in, for the business's own, privacy-protected space with mechanical protection, tamper protection, burglar alarms and passage systems.

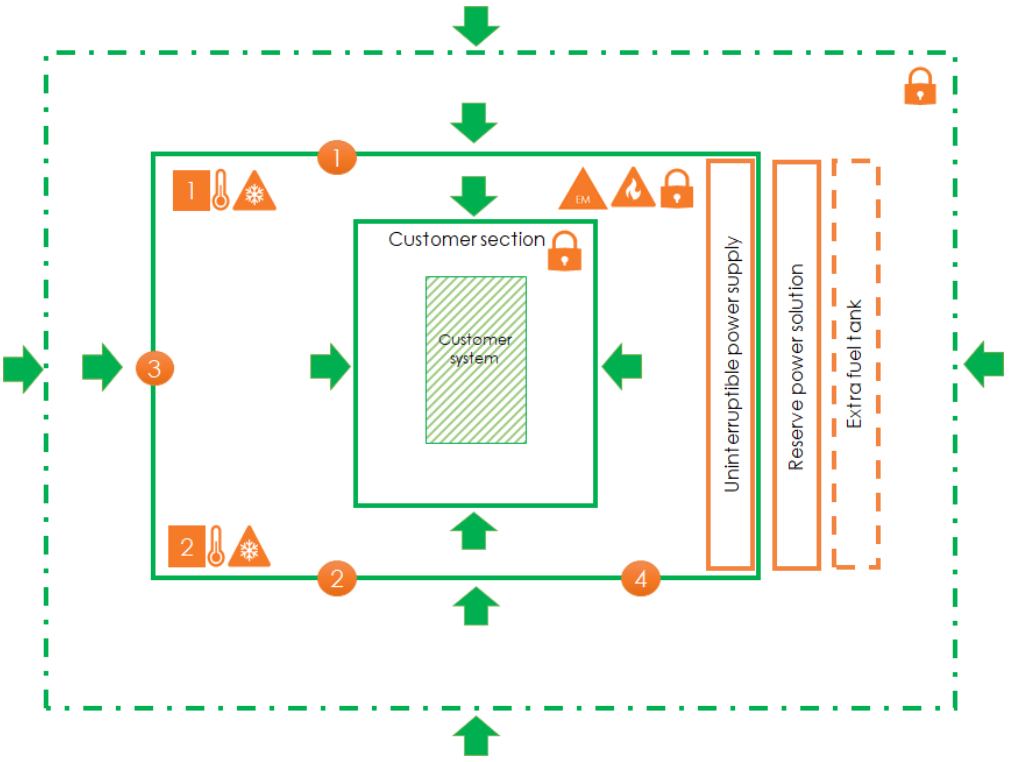


Image: Security level S3 - Site of crucial importance

5. DESCRIPTION OF PROTECTIVE MEASURES

In the case of new construction, the level of physical protection is determined by the level of security established for the planned Site and an RSA to ensure the established level of security and any additional measures.

For existing Sites, and when auditing facilities for connecting for customers for critical operations and activites, an RSA shall be implemented which shall form the basis for an action plan for supplementing the necessary protection measures to obtain a current level of protection for the Site.

The protection measures required for robust Sites to be able to handle electronic communication in the event of Extraordinary events are based on the Swedish Theft Protection Association's standards for Mechanical Burglary Protection (protection class 1–3) and for Design and installation of burglary and assault alarms (alarm class 1–4).

The safeguard measures cover the following areas and are defined for each Site in *Chapter 6 SITE PROTECTIVE MEASURES*.

5.1 Site area

The geographical area of the site.

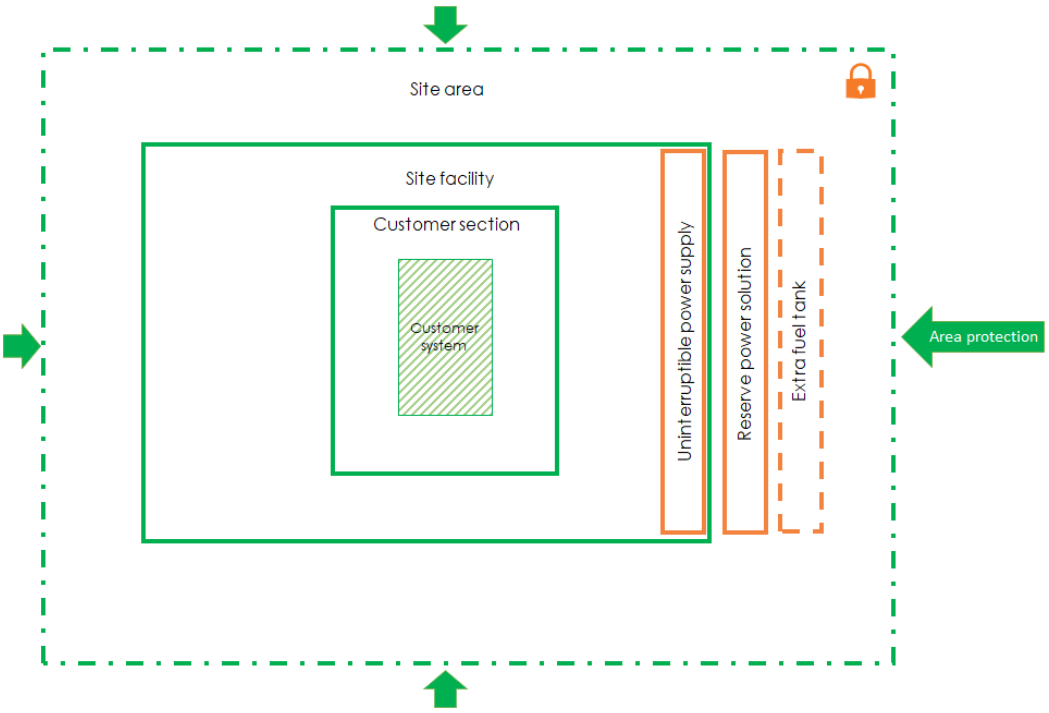


Image: Site area

5.1.1 Area protection

The area protection consists of mechanical and electronic protection. The purpose of the area protection is to protect property, material, and equipment within a fenced area and to prevent or impede access to premises within the fenced area. The area protection also marks a limit for unauthorized access.

Mechanical area protection
The mechanical area protection consists of:

- *Area fence / wall.*
  - According to SSF 200: 4 Chapters 2.7 and 4.6.
- *Gate / gate / door.*
  - Gate design according to SSF 200: Chapter 4 4.6.
  - Lock according to SSF 200: Chapter 4 2.7.

Electronic area protection

The electronic area protection consists of several different sensors and systems for monitoring, burglar alarms and access control. System selection is based on completed RSA.

Overall requirements

- The electronic area protection systems must always be connected to the system's uninterruptible power supply.
- The systems for electronic area protection must be functionally monitored from the Operations Center and / or the Alarm Center.

Burglar alarm
Alarm system type 1 shall include sensors for:

- Gate / gate / door.
- Security installations.

Alarm system type 2 shall include sensors for:

- Gate / gate / door.
- Fence (option).
- Internal area.
- Security installations.

Installed alarm system must be able to:

- Activate any camera recording.
- Integrate with access control systems.
- Handle alarm sensors individually.
- Transfer alarms to Operations Center and / or Alarm Center.
- Local operated.

Camera surveillance
To determine the cause of an alarm, camera surveillance can be used and include:

- Gates.
- Fence.
- Internal area.

Installed camera surveillance system must be able to:

- Connect to Operations Center and / or Alarm Center.
  Be monitored from the Operations Center and / or Alarm Center and locally at the facility.
- Start camera recording on command from the Operations Center and / or Alarm Center and locally at the facility.
- Be operated from the Operations Center and / or Alarm Center and locally at the facility.

Note. The possibility of using cameras where the camera recording can also be started with detected motion must be considered.

Access control

- Access control shall take place through access control systems with logging, identification, and access control at the personal level (PTSFS 2015: 2 § 13 Measures regarding access and access and amendment PTSFS 2020: 1 §13).

- The access control system must always be part of a separate access zone where the group of people who have a pronounced need for access to the zone is part of a separate access group.

5.2 Site building

A Site can either be realized as a stand-alone building or as an integrated part of another suitable building. In this section, the Site is treated as a detached building.

5.2.1 Shell protection

The shell protection consists of mechanical and electronic protection. The purpose of shell protection is to protect property, material, and equipment within a building and to prevent or impede access to premises within the building. The shell protection also marks the limit for unauthorized access.

Mechanical protection
Consists of the building's enclosing surfaces, windows, doors, hatches, grilles if necessary, at windows. For mechanical burglary protection, the Swedish Theft Protection Association's standard SSF 200: 5 applies.

- **Protection class 1**:
  The enclosure surface shall provide protection against burglary, and make it more difficult to remove stolen goods, for activities with no or little amount of property / assets liable to be stolen or other protection value.

  The enclosing surface must be made of concrete, stone, or lightweight concrete. Reinforced rule constructions with, for example, sheet cladding or thin steel sheet can also be accepted.

Addition
Windows must not be on the wall or in the door of Site with protection class 1.

- **Protection class 2:**
  The enclosure surface shall provide protection against burglary, and make it more difficult to remove stolen goods, for activities with a larger amount of property / assets liable to steal or other protection value than class 1.

  The enclosure surface must be concrete cast or masonry. Sheet steel between double building boards and which are joined and fastened to studs can also be accepted. As a rule, stronger plates, and thicker sheet steel than protection class 1 are required.

  Addition
  Windows must not be on the wall or in the door of Site with protection class 2.

- **Protection class *3:***
  The enclosure surface shall provide protection against burglary, and make it more difficult to remove stolen goods, for activities with a focus on theft-prone property / assets or other protection value.

  The enclosure surface must be concrete cast or masonry. Sheet steel is usually required on both sides of a reinforced rule construction. Simple steel plate can be allowed if reinforcements are made and specific assemblies are applied.

  Addition
  Windows must not be on the wall or in the door of Site with protection class 3.

  Note. The need for bollards as protection against sabotage must be considered in detached buildings.

Electronic protection

The electronic protection consists of several different sensors and systems for monitoring, alarms and access control. System selection is based on completed RSA.

Note. The need for bollards as protection against sabotage must be considered in detached buildings.

- **Overall requirements**
  - All systems for electronic protection must be connected to the plant's uninterruptible power supply.
  - The systems for electronic protection must be functionally monitored by the Operations Center and / or the Alarm Center.

- **Alarm**

  Burglary alarms including equipment, installation and documentation must meet requirements in accordance with the Swedish Theft Protection Association's rules SSF 130: 8. The rules include requirements for design of the the facilities, installation, adjustment, testing, facilities owners, facilities caretakers, test operation and documentation.

  The rules classify the facilities into four alarm classes depending on the need for protection for what is to be monitored.

  - Alarm class 1 Alarm monitoring is performed as internal pre-protection with at least 2 volume detecting sensors and may be switched on and off by locking bypass at the entrance to the room.

  - Alarm class 2. Alarm monitoring is performed as shell protection, (protection of openings in the Site's enclosure surface), supplemented with internal pre-protection with at least 2 volume detecting sensors. The function of the alarm system must be monitored. Connection and disconnection take place via control panel.

    Note To avoid mistakes with connection of alarms, automatic connection with pre-alarm function can be used.

  - Alarm class 3. The monitoring is designed as shell protection, (protection of openings in the object's enclosing surface), supplemented with internal volume protection, except for hygienic and windowless spaces smaller than 4 m2. The highest requirements for tamper protection are placed on the control panel and actuators. Bypassing must be done with button or short bypass switches in so-called shared assembly. Card bypass switches must be combined with a keypad with a personal code. The actual alarm transmission (eg to security companies / guards) must also be monitored.

  - Alarm class 4. Class 4 The alarm monitoring is performed as shell protection, (protection of openings in the object's enclosing surface), supplemented with internal volume protection for all spaces. The highest requirements for tamper protection are placed on the control panel and actuators. Bypassing must be done with button or short bypass switches in so-called shared assembly. Card bypass switches must be combined with a keypad with a personal code.

  Installed alarm system must be able to:
  - Handle alarm sensors individually.
  - Activate camera recording.
  - Integrate with access control systems.
  - Transmit alarms to operations center and / or alarm center.
  - Be locally operated inside the front door and be able to control the entire facility.

- **Camera surveillance**
  To determine the cause of an alarm, camera surveillance, such as ordinary images, infrared images, or thermal imaging, should be used and include:

  - Doors.
  - Windows.
  - Inside building.

  Installed camera surveillance system must be able to:

  - Connect to the Operations Center and / or Alarm Center.
  - Be monitored from the Operations Center and / or Alarm Center and locally at the facility.
  - Start camera recording on command from the Operations Center and / or Alarm Center and locally at the facility.
  - Be operated from the Operations Center and / or Alarm Center and locally at the facility.

  Note. The possibility of using cameras where the camera recording can also be started with detected motion must be considered.

- **Access control**
  - Access control shall take place through a passage control system with logging, identification, and access control at the personal level (PTSFS 2015: 2 § 13 Measures regarding access and authorization and amendment PTSFS 2020: 1 §13).
  - The access control system must always include a separate access zone where the group of people who have a pronounced need for access to the space is part of a separate access group.

5.2.2 Electrostatic protection

Electrostatic Discharge (ESD) is a sudden flow of electricity between two objects with different charges.

- Installation floors with antistatic carpet (also called computer floors) should be used, with a height of at least 400 mm above the underlying floor.

  If installation floors are not used, an antistatic floor covering must be used.

- All racks / cabinets / wall plates / cable ladders etc must be connected to the equipotential bonding rail.

- When working with installed electronics, anti-static bracelets must be used.

5.2.3 Electromagnetic protection (EM)

Magnetic fields pose a threat to conductive materials such as electrical wires, metal wires, electronics, etc. Magnetic fields can affect electronics by disrupting software (requiring a reboot or requiring software to be reloaded) or destroying hardware depending on strength and duration. The disturbances can enter a building both through walls and via metallic pipes (such as electricity or water pipes), or are generated by power supplies or other faulty equipment inside the walls. Below is an overview of electromagnetic interference that can affect socially important infrastructure and various types of protection.

Electromagnetic interference

- Natural sources of electromagnetic fields
    - Lightning strike.
    - Solar storms.
      Also causes induced currents, (GIC), in power lines, railways, pipelines, etc. Electrical wiring (requires high current to be noticed, but equipment with low EMC can be affected even in small fields).
- Accidental interference
    - EMI (Electromagnetic Interference).
      Interference that occurs in electronic equipment due to transmissions from or faults in other electronic or electrical equipment.
    - Electric network transients.
      Electricity network transients can arise in the event of disturbances / connections on the electricity network and via electrical installation propagate into the Site.
- Intentional disturbances
    - EMP (ElectroMagnetic Pulse).
      Electromagnetic pulse caused by a nuclear detonation.
    - IEME *(Intentional EMI, intentionally generated electromagnetic interference)*
      - Interference transmission.
      - HPM *(High Power Microwave, short-lived pulses of electromagnetic radiation with very high peak power)*.
    - Direct injection
      Direct injection means that someone conducts strong current pulses directly through a wall or via equipment inside the facility or via electrical or metallic data cables in a building.

Note. See also
https://www.msb.se/siteassets/dokument/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/utbildningsmaterial-elektromagnetiska-hot/introduktion-till-avsiktliga-elektromagnetiska-hot-mot-samhallsviktig-verksamhet-och-kritisk-infrastruktu.pdf

Protection against electromagnetic disturbances

Protection against radiant disturbances

- Reinforcement structures in exterior walls, ceilings and floors must be connected and connected to the facility ground to obtain EMC protection.
- Sensitive and critical equipment must be placed some distance into the building or in a screened room with the walls clad with sheet metal. (For example, concrete exterior walls provide approximately an attenuation of 10 dB attenuation, while bricks provide a very small attenuation).
- Känslig elektronik ska vara skärmad, d.v.s innesluten i metalliska skal som stänger ute det mesta av den inkommande strålningen från HPM-källor.

  Sensitive and critical electronics must be shielded, i.e., enclosed in metallic shells that block out most of the incoming radiation from HPM sources.

Protection against conductive disturbances

- Transient protection must be present on all incoming metallic cables.
- Incoming cables from the outside must pass through the base or base plate and the bushings must be sealed with protection for EMI and EMP.

Protection against antagonistic threats

- An attacker should not be able to get too close to sensitive equipment.
- An attacker should not be able to access a connection point.

5.2.4 Fire protection

Overall requirements
The fire protection must be designed with reassuring robustness so that all, or large parts of the protection are not knocked out by individual events or stresses. The fire protection must handle:

- Direct fire, ie. brand inuti Sites.
- Indirect fire, ie. a fire outside the Site, whereby the fire protection in the Site's enclosing area constitutes the fire cell boundary.

Note. See also https://www.boverket.se/sv/PBL-kunskapsbanken/regler-om-byggande/boverkets-byggregler/brandskydd/brandklasserd-for-ytskikt/

Fire technical class

- The site must constitute its own fire cell and meet fire technical class at least EI60. See also chapter 5.2.7 Sectioning.
- Steel doors that at least meet the Site's fire technical class must be used.
- All cable and pipe penetrations must be fire-proof in accordance with the fire technical class applicable to the Site.
- In the event of difficulties in minimizing fire load or similar situations, higher fire safety classes such as R60 / 90D must be investigated.

Note. See also Boverkets byggregler (2011:6) – föreskrifter och allmänna råd.

Fire alarm

- The site must be equipped with an automatic fire alarm with adapted fire gas ventilation.
- If there is a ventilation system, the ventilation ducts must be fitted with fire dampers connected to fire alarms.
- The function must be maintained even in the event of a power failure.
- The alarm system must be functionally monitored by the Operations Center and / or the Alarm Center.
- Fire alarms must be transmitted to the Operations Center and / or Alarm Center.

Note. See also the Fire Protection Association's rules for fire alarms, SBF 110: 8.

Extinguishing system

- The site must be equipped with an automatic extinguishing system with aspirating / sampling fire detection.
- The extinguishing system must be functionally monitored from the Operations Center and / or the Alarm Center.
- All doors must be fitted with emergency knobs on the inside.
- Equipment for automatic extinguishing systems must be placed in a separate room.

Note. See also https://www.msb.se/sv/publikationer/vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/

5.2.5 Environment and climate protection

Overall requirements

- The site must be equipped with systems for regulating ventilation, cooling and humidity.
- The systems must be functionally monitored from the Operations Center and / or the Alarm Center.
- To avoid overheating, condensation and short circuits, the site temperature should not be allowed to vary outside the temperature limits +18 ° C to +25 ° C with a relative humidity of 40–55%.
- Temperature alarms must be present and transmitted to the Operations Center and / or Alarm Center.
- Humidity alarms must be present and transmitted to the Operations Center and / or Alarm Center.
- The amount of air supplied must create an overpressure in the Site to prevent dust and dirt from being "sucked" into the Site. The design of the Site and the manufacturer's recommendations must be dimensioning for the technical characteristics of the facility.
- Ducts for air upply must be equipped with smoke detectors connected to fire dampers or automatic fan stops or another solution to minimize the risk of contaminating the indoor environment with air from the external environment, eg. fire smoke, chemical emissions, etc.
- Condensers used to regulate the climate in the system must be placed outside and protected by placement high above the ground and "burning in".
- Sound absorbers or suspended ceilings should be avoided so as not to bind or collect dust.

Redundant cooling system

- Redundant cooling units with separate cooling circuits must be present to ensure continuous operation.

5.2.6 Diversity

- Redundant connection of optical cables with separate cable path and cable entry.

5.2.7 Sectioning

Sites where installed equipment has specific requirements for protection must be able to be divided into separate security zones.

Security zones

- *Permission zone*
  Protected / alarm-classified space for equipment with different requirements for access protection or shell protection.
  If sectioning with shell protection is used, all areas must be shielded, including crawl spaces, ventilation ducts and under installation floors.

- *Fire cell / Fire section*
  Separate fire cells / fire sections with requirements for a fire technical class that deviates from the Site's class or to reduce the requirements for the size of the fire extinguishing system and the amount of extinguishing agent. If cells / sections are used, all areas must be handled, including crawl spaces, ventilation ducts and under installation floors in accordance with the defined protection class.

- *Climate zone*
  Separate climate zones with requirements that deviate from the Site's environmental and climate protection.

5.2.8 Electrical installation

Uninterruptible power supply

The site must be equipped with uninterrupted power.

- The lighting, other electrical outlets or other general power in the Site must be supplied from a group separate from UPS. Separately secured distributors (PDUs) must be used in stands.
- Interruptible Power Supply (UPS) type on-line must be used.
- For Redundant power supply 2 (see section Redundant power supply), duplicate / redundant UPSs that supply duplicate UPS- centrals must be used.
- Each UPS (if doubled) must have its own battery.
- UPS batteries should be valve regulated and should have a life expectancy of at least 5 years.
- The batteries must be dimensioned to ensure electricity during the time required for controlled shutdown of the equipment or manual start of reserve power, however at least 10 minutes. Consider future expansion when dimensioning.
- Installation and operation must be handled in accordance with IEC 62485-2.

Redundant electric power supply

The site shall have redundant electric power supply as below.

Redundant electric power supply type1

- Electric power supply including main switch, control panel and reserve power system in accordance with the **text under headline Reserve power system.**

Redundant electric power supply typ 2

- Two separate electric power supplies including main circuit breakers, control panels and reserve power system in accordance with the **text under headline Reserve power system.**

Reserve power system

The site must be equipped with a reserve power system. If a mobile backup power system is used, the same requirements apply as for a permanently mounted system.

- Reserve power must be placed in a separate room.
- A building or device for reserve power must be located within area protection.
- Reserve power must also supply air conditioning, lighting and constitute general power in the Site.
- Reserve power systems must be functionally monitored from the Operations Center and or the Alarm Center.
- Reserve power placed in a container must at least meet the requirements in SSF 200: 5 for sheet metal walls.
- Logbook for diesel tank must be available.
- Maintenance routine including periodic operating tests (automatic or manual) must be in place.

Note. See also https://spbi.se/wp-content/uploads/2019/03/SPBI-dieselbra%CC%88nsle-till-reservkraftverk-2019.pdf

Operating time

- *R1*
    - The minimum requirement for operating time for reserve power systems is 10 days, which is realized by refueling. Devices for filling fuel tanks should be fitted with locks in at least lock class 3.
- *R2*
    - The minimum requirement for operating time for reserve power systems is 10 days, which is realized without refueling.

5.3 Operating alarm

- Function monitoring and operational alarms must be handled via TCP / IP connections to the Operations Center and / or Alarm Center.
- Connections for function monitoring and operating alarms must be redundant.

5.4 Radio system Radio in the site area

- Radio system located within the area protection to the Site is given the protection that is designed for the current system.
- The mast must be placed so that it cannot damage vital parts of the system in the event of a mast failure.
- The radio system must be implemented in accordance with the Swedish City Network Association's document "Guidance - Fixed Radio Networks" or similar.

6. SITE PROTECTION MEASURES

The level of security set for a Site governs the level of physical protection.

Below are protection measures for each level of protection. **Overall requirements in accordance with Chapter 5 *DESCRIPTION OF PROTECTIVE MEASURES* apply to all Sites and are therefore not specified in the table.**

Sites with security level S0 must be handled in accordance with Appendix 4. Robust Site and Node.

Site protection measures	S1 High local significance	S2 High importance	S3 Crucial importance
Area protection			
- Area protection			
– Mechanical area protection	No	RSA	Yes
– Electronic area protection	No	RSA	Yes
– Burglar alarm	No	RSA	Yes
- Alarm system	No	Type 1	Type 2
– Camera surveillance	No	RSA	Yes
– Access control	No	RSA	Yes
Site building			
- Shell protection			
– Mechanical protection	Appendix 4	Protection class 1	Protection class 2
- Electronic protection			
- Alarm	Alarm class 1	Alarm class 2	Alarm class 3
- Camera surveillance	Option	Option	Yes
- Access control	Yes	Yes	Yes
- Electrostatic protection			
- Floor, Rack, cabinet, personell	Yes	Yes	Yes
- Protection against electromagnetic disturbances			
- Radiant disturbances	RSA	Yes	Yes
- Conductive disturbances	RSA	Yes	Yes
- Antagonistic threats	RSA	Yes	Yes
- Fire protection			
– Fire technical class	EI60	EI60 alt. R60/90D	EI60 alt. R60/90D
– Fire alarm	No	Yes	Yes
– Extinguishing system	No	Yes	Yes
- Environment and climate protection			
– Redundant cooling system	-	Yes	Yes
- Diversity			
– separate cable path and cable entry	2	2	2
– Demands that should be implementet with new building sites	-	3	4
- Sectioning - Security zones			
– Permission zone	No	Yes	Yes
– Fire cell / Fire section	No	Yes	Yes
– Climate zone	No	Yes	Yes
- Electrical installation			
– Uninterruptible power supply	Yes, 4 hour	Yes, 1 hour	Yes, 1 hour
– Redundant electric power supply	Type 1	Type 2	Type 2
– Reserve power system	R1 – External	R1 - 10 days	R2 - 10 days
- Operation alarm			
– Equipment	Site	Site	Site
– Larm receiver	NOC	NOC, Customer	NOC, Customer

7. RSA

Risk and vulnerability analyzes must be managed In accordance with:

- Sub-appendix 4.1.1 RSA Robust Site for socially important digital infrastructure.
- Sub-appendix 4.1.2 Routine and guidance for Risk and Vulnerability Analysis (RSA).

8. ENVIRONMENTAL ASPECTS

8.1 A sustainable telecom society

Hydrogen-powered fuel cells with water vapor as the only emission may replace diesel-powered reserve power generators and batteries. Fuel cells can be used for different types of telecom systems both as a replacement for batteries or as a reserve power generator.

In Sweden, there are some test plants with outputs from 1 kW up to some 5 kW. An advantage of fuel cells is that they produce direct current and telecommunications stations usually use equipment that uses 48 VDC.

It is important that the special positive properties of the fuel cell can be used to achieve environmentally smart technical solutions:

- High efficiency at low effects.
- Fuel flexibility, opportunities to use different types of fuels. For example, hydrogen, methanol, and diesel.
- Low emissions.
- Low noise level and no visible or disturbing exhaust fumes.

Together with Telia Sonera, the Swedish Post and Telecom Agency carried out long-term tests on various types of fuel cells in 2005–2008 but has resumed the project to build some pilot plants together with operators.

Read more at:
https://pts.se/sv/bransch/internet/robust-kommunikation/atgarder/faltprov-av-bransleceller/

The use of hydrogen fuel cells is not only a carbon-neutral emission, but the prices of fuel cells have come down to a level which means that they can offer a diesel-powered reserve power alternative.

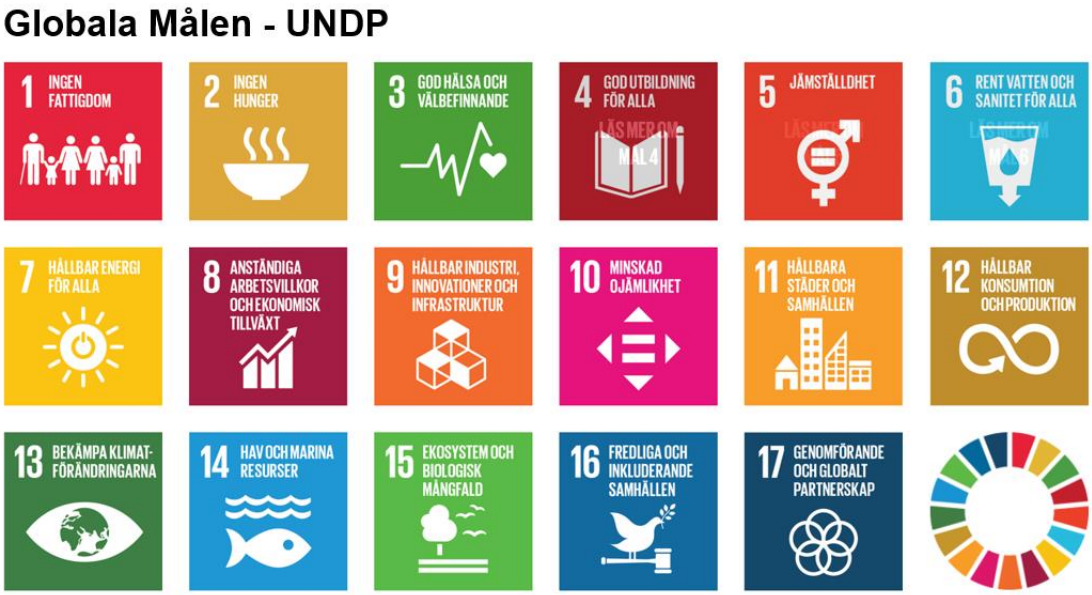
There are challenges to work on. Above all, access to hydrogen is currently (2020) limited to a few cities that have hydrogen factories. This makes the technology vulnerable from the perspective of fuel supply. The alternative is for operators to create their own fuel.

Nevertheless, the aspects of working with renewable energy in the transition to hydrogen fuel cells are the only possible future solution as our fossil fuels are running out in the world and we must find an alternative to today's spare units and work to create an environmentally friendly future-proof solution for telecom facilities.

Furthermore, there are other alternatives that also need to be tested and looked at more in telecom, such as wind power and solar cells as alternative electricity sources.

8.2 Sustainable reserve power

The UN's Global Goals program has led to a trend towards more sustainable energy supplies and the fight against climate change on a broad front. Innovation and development have led to new modern internal combustion engines with significantly lower emissions and they are now used to advantage as reserve power engines.



In addition, several interesting new liquid fuels have recently been developed, which replace fossil fuels. Today, there are various fossil-free fuels manufactured here in the Nordic region.

A good fuel for a spare plant is, for example, HVO100. This is because the fuel can withstand storage for a very long time. HVO100 reduces emissions by:

- 33% lower levels of fine particles.
- 9% less nitrogen oxides (NOx).
- 30% less hydrocarbons (HC).
- 24% lower carbon monoxide (CO) emissions.
- reduced levels of polyaromatic hydrocarbons (PAH).

As it is fossil-free, it is also CO2-neutral, i.e., no net addition of CO2 to the atmosphere.

REFERENCE DOCUMENT

https://www.msb.se/sv/publikationer/vagledning-for-fysisk-informationssakerhet-i-it-utrymmen/

https://www.msb.se/elektromagnetiskahot

https://www.svk.se/siteassets/aktorsportalen/sakerhetsskydd/dokument/fysiskt-grundskydd--en-vagledning-for-elbranschen.pdf

https://www.svk.se/siteassets/aktorsportalen/sakerhetsskydd/dokument/vagledning-fysiskt-omradesskydd-for-elanlaggningar.pdf

Lag (1998:150) om allmän kameraövervakning.
Lag (1990:217) om skydd för samhällsviktiga anläggningar.
Säkerhetsskyddslagen (1996:627).
Lag (1974:191) om bevakningsföretag.
Personuppgiftslagen (1998:204) PUL.
Lag (1983:1097) med vissa bestämmelser om larmanläggningar m.m.
Lag (1974:194) om bevakningsföretag.
Vägledning fysiskt områdesskydd för elanläggningar