Annex D.8: Global Physical Security Technical Standards

Objectives

This document describes the technical security measures to protect Zalando people, data, facilities and operational business. It is prepared to support the development and maintenance of security concepts, risk assessments and security surveys.
Due to the wide range of relevant aspects, it is not intended to be a stand-alone guide for e.g. Zalando facilities, confidential/critical data rooms or high value areas. It must always be understood and exercised in consideration of all applicable standards and local codes.

The intent of this Global Physical Security Technical Standard Document (installation) is:

- To provide a clear definition of basic classifications of a typical Zalando facility environment;
- To define the design criteria to be used in the design, construction and maintenance of security measures of these spaces;
- To give direction regarding the design of the elements stated, but not to specify that requirement in detail;
- To be used in concert with all applicable standards and local codes;
- To serve as a reference tool for architects, engineers, contractors and other project team members for projects related to technology spaces.

The Global Physical Security Technical Standards Document for Zalando facilities are not intended to be a stand-alone guide for building security measures of Zalando facilities. Document named SIGPhysicalSecurityStandardV1 (available for Zalando management only) is inseparably linked and from it this document was created. Where a requirement listed in this document differs from that listed in an applicable standard, the more stringent requirement shall be followed. The standards listed may not apply to every geographic region. All designs shall be reviewed by a qualified technology design specialist of the Zalando Security Team to ensure conformance with applicable policies, codes, standards and practices. The security manager of Zalando, in corporation with the Project Manager(s), are responsible for the sign-off of security concepts and for a later acceptance after the implementation of security solutions.
Based on the Global Physical Security Technical Standards Document and Remodel Standards the Security Manager of Zalando will finally determine the project specific security measures mandatory, recommended or optional to be applied to each of the security project areas and their boundaries. The following principles have to be taken into account as decision criteria for a right and economical security concept:

1. Increasing the resistance time. Sometimes referred to as 'target hardening', the principle creates a series of barriers that take time to breach. The barriers designed for any facility should be seen as an onion skin – several layers of defense in depth. This is also known as intrusion protection.
2. Detection of malicious intent. Any target hardening must come with appropriate detection measures. Without detection a criminal may achieve his goal without being noticed – regardless how much time it would need. Detection and hardening must be balanced such that the time from detection to successful attack is less than the reaction time (i.e. the time local security staff or police forces will need for an intervention).
3. The document named SIGPhysicalSecurityStandardV1 (available to Zalando management only) is inseparably linked from which this Global Physical Security Technical Standards Document was created.

The design of security concepts performed by the Zalando Security Team will also contain the Risk Assessment of the location of the building. Security measures will be recommended based on the Risk.

Risk Assessment means a systematic appraisal and is used to evaluate the strengths, weaknesses, opportunities, and threats, in order to achieve a rating of the adequacy of security measures in place and to act as a basis for decision that a location is suitable for a Zalando facility and which security layers have to be considered and implemented.

As global contact please always use Zalando Security Manager contact details in relationship with security concepts/projects for new and existing Zalando facilities.

Please note this document is the intellectual property of SIG EMEA who have allowed Zalando the use of this document. Nothing our of this document may be copied or reproduced by 3rd parties without approval in writing from SIG EMEA. SIG EMEA is based on the Albert Verweystraat 46, 2202 NP, Noordwijk, Netherlands with Dutch company registration number 62101501)

SECTION 1: Greenfield Security Standards

Content

1. Perimeter needs:

1.1. Fencing.

The fence around the Zalando facility should comply with TAPA.
A good sample fence to utilize in future is the Nylofor 2m43 height fence from Betafence as used in the GF5 Lodz facility
The fence has anti-tamper security bolds which secures the fence with the mounting poles.
Furthermore the fence is rigid, has a small maze and is coated for oxidation protection

The advised model for the fence is a fence similar to above, complying to TAPA standards

TAPA regulation calls for:
* Fencing encloses entire facility including cargo handling and shipping and receiving yard.
* Fencing height is 8 feet / 2.4 meters or higher <OR> 6 feet / 1.8 meters and installed with an electronic (climb-over/tamper) warning system.
* Fencing regularly inspected for integrity and damage.
* Fencing maintained in good condition.
* Gate(s) manned or electronically controlled.
* Multi-tenant/Multi-story warehouses docks are fenced and access controlled.

The whole outline of the Zalando perimeter needs to be fenced as well as the demarcation line between the employee car park and the Truck / Logistics part. The fencing should be placed in a way that employees can only enter the facility on the designated entrance points. Gates / entrances can be strategically positioned on points where required. These entrance points are described in the next chapter (1.2)

1.2. Gates and perimeter entrances

The Gates in the fence (where applicable) will have to conform to the standard of the fence itself (see 1.1)
There can be one or more entrances for cars and trucks to enter onto the Zalando perimeter where there will be a boom barrier entrance to control access to the parking area / Zalando logistic area. The barrier will be positioned behind the fenced area in a way that a sliding gate of the fence can be used to close down the entrance area to prevent further vehicle access to the perimeter.
This sliding gate again has to comply with the standards of the fence itself (see 1.1) and has to have a manual - key switch override accessible from the outside. Next to this this sliding gate has to have a fire interface override (automatic and/or manually openable in case of fire alarm)
Where required automatic or manual fence gates have to be applied for fire truck entrance routes along the fencing (outside the normal entrance points for employee cars and trucks).
Where required key lock or access reader controlled fence doors can be implemented for pedestrian access.

The car / truck entrance points will be controlled by means of a boom barrier in normal day situations. Each boom barrier entrance / exit will be controlled by the following electronic measures:

1. ANPR system (automatic license plate recognition system).
   For this device the following cabling is required:
    1. A CAT6 cable from the ANPR unit to the boom barrier.
    2. An 8 core signal cable (8x0,22cy) from the ANPR unit to the boom barrier.
    3. A fiber connection cable from the central equipment room (ie server room inside the office space) to the boom barrier. Please note the fiber provided has to comply with the network cabling requirements to ensure the connection works over the provided distance and is ground /external rated cable when passing through the ground / external environments etc.
    4. A power connection by means of local un-switched mains at the boom barrier
2. Intercom system.
   For this device the following cabling is required:
    1. A CAT6 cable from the Intercom unit to the boom barrier.
    2. An 8 core signal cable (8x0,22cy) from the intercom unit to the boom barrier.
    3. A fiber connection cable from the central equipment room (ie server room inside the office space) to the boom barrier. Please note the fiber provided has to comply with the network cabling requirements to ensure the connection works over the provided distance and is ground /external rated cable when passing through the ground / external environments etc.
    4. A power connection by means of local un-switched mains at the boom barrier
3. Access control system (Card Reader)
   For this device the following cabling is required:
    1. A CAT6 cable from the Card reader unit to the boom barrier.
    2. An 8 core signal cable (8x0,22cy) from the Card reader unit to the boom barrier.
    3. A fiber connection cable from the central equipment room (ie server room inside the office space) to the boom barrier. Please note the fiber provided has to comply with the network cabling requirements to ensure the connection works over the provided distance and is ground /external rated cable when passing through the ground / external environments etc.
    4. A power connection by means of local un-switched mains at the boom barrier

Above calls for a dedicated fiber connection for each device, so 3 in total per boom barrier. For above cable infrastructure item 4 for the various devices may be combined in a single mains connection for all devices as long as the mains is capable (sufficient amperage) to provide mains for all related equipment (plus power for the boom barrier as well when this will be added). Furthermore the boom barrier has to have sufficient room to house the required fiber switch convertor as well as the power supplies and access panels for the ANPR, Intercom and access readers. Alternatively a separate external cabinet may be used directly connected to the boom barrier when there is insufficient mounting space in the boom barrier.

1.3. External Camera's

To enable a correct position for multiple external cameras, we need to create the flexibility to position cameras in a way they can monitor strategic points such as fencing, gates, entrances and parking space areas.

To create this flexibility we require the following cable requirements to each projected lamp post on the perimeter:

1. A fiber connection cable from the central security equipment room to each lamp post (at around 4m height). Please note the fiber provided has to comply with the network cabling requirements to ensure the connection works over the provided distance and is ground /external rated cable when passing through the ground / external environments etc.
2. A power connection by means of local un-switched mains at each lamp post (at around 4m height)

This way later on each lamp post can be used to mount a camera by mounting a local power supply on that lamp post together with a fiber convertor.

1.4. External Guard Houses.

On the perimeter one or more external guard houses can be positioned. These external guard houses function as check points for visitors, employees and / or truck drivers. Typically a guard house can be equipped with the following security equipment: Access reader, Intercom Post, Panic button, Intrusion devices, release buttons / controls for the barriers and camera's. For this reason the guard houses need to be prepared with sufficient cabling for connecting and controlling these security devices. Anti -ramming protection must be placed around the guard house.

We require the following cabling requirements to each external guard house:

1. Four dedicated fiber connection cables from the central security equipment room to each external guard house (each security device group will have its own dedicated fiber, in this case one for access, one for intrusion, one for intercom and one for cameras). Please note the fiber provided has to comply with the network cabling requirements to ensure the connection works over the provided distance and is ground /external rated cable when passing through the ground / external environments etc.
2. A power connection by means of local dedicated mains group for the security equipment at each external guard house

For the guard house access control door, intercom, camera or intrusion device follow the cable requirements as mentioned in chapter 4.

1.5. Other External Objects.

On the perimeter one or more external objects can be positioned such as water / power / technical buildings. These external buildings can be equipped with the following security equipment: Access reader, Intercom devices, Intrusion devices, camera's etc. For this reason, the other external objects need to be prepared with sufficient cabling for connecting and controlling these security devices.

We require the following cabling requirements to each other external object:

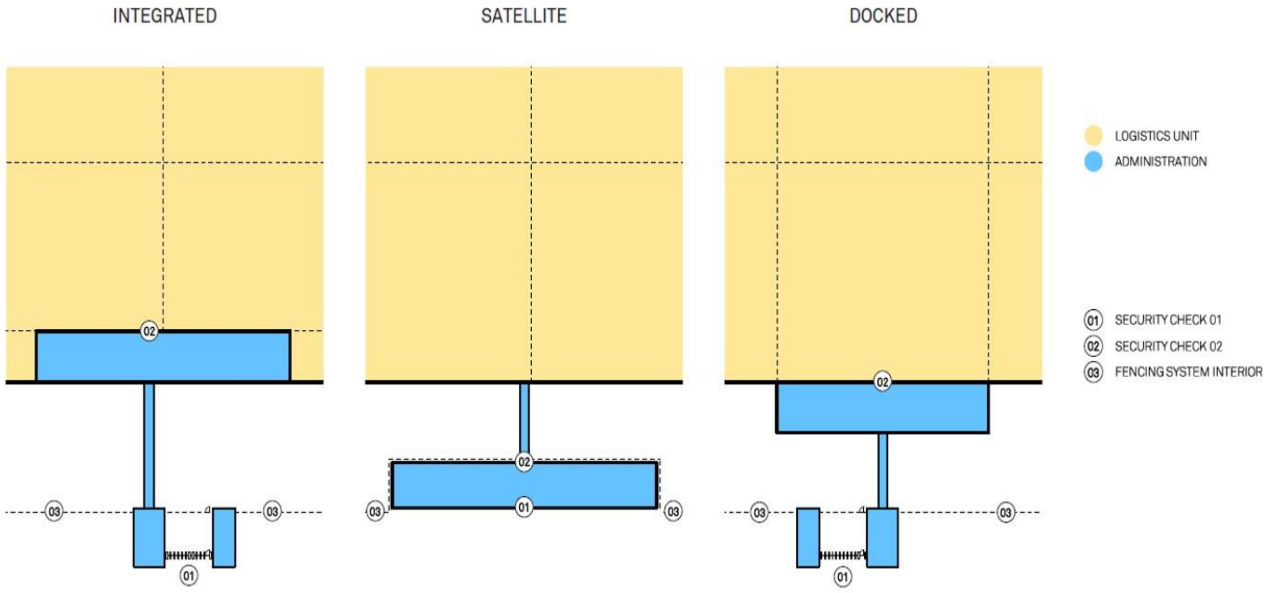
1. Four dedicated fiber connection cables from the central equipment room (ie server room inside the office space) to each other external object (each security device group will have its own dedicated fiber, in this case one for access, one for intrusion, one for intercom and one for cameras). Please note the fiber provided has to comply with the network cabling requirements to ensure the connection works over the provided distance and is ground /external rated cable when passing through the ground / external environments etc.
2. A power connection by means of local dedicated mains group for the security equipment at each other external object

External tourniquets will be covered in the next chapter (chapter 2)

2. Various Layouts and office space needs on the facility:

2.1 various office space layouts

Zalando can have various office space layouts in relation to the logic centers as shown below:



The major difference between these office layouts relates to entrance to the office building, where tourniquets to enter the office block are either external or internal. With it, the cabling has to be adjusted to whether the tourniquets are external (i.e. use fiber) or internal (i.e. use CAT6). Further cabling requirements is given in the next chapters. For the remaining part the security requirements remain the same for the office part of the building.

2.2 Perimeter doors

Depending if a perimeter door is a regular traffic door or a door only for escape purposes, this door will either be equipped as access control door (regular traffic) or as monitored intrusion door (emergency escape only). In all cases a camera will be placed on a strategic position to monitor the traffic coming through the door.

2.3 Perimeter windows

On Ground floor level openable perimeter windows the windows will receive a contact connected to the intrusion system.

2.4 Internal access controlled doors

The following doors will be equipped inside the office as an access controlled door:

- Doors leading to office spaces (generally each office on the 2nd floor of the office block but also the stair house doors and lobby doors leading to the office space)
- Doors leading to kitchen areas (i.e. the demarcation between the general Zalando break area and the dedicated kitchen area or the door for kitchen goods delivery)
- Doors which provide access to IT rooms (i.e. server rooms)
- Doors which provide access to Security Rooms (i.e. security equipment room or guard / soc / visitation rooms)
- Doors which provide access to Special rooms (like nursery room)

2.5 Reception area

The Reception area will be equipped with panic buttons connected to the intrusion system for emergency situation and with Intercom post to answer intercom calls when required. There will also be release buttons positioned in the reception area to manually control the wide lanes (swing gates) for passage with large goods, handicapped people, cleaning team etc.

2.6 Main entrance area tourniquets access controlled

The main entrance area will control the entrance of employees and visitors by means of (internal or external) speed stiles / tourniquets. The amount of speed stiles / tourniquets is based on the amount of traffic which can occur at that facility. The entrance and exit to these speed stiles / tourniquets will be controlled by means of in and out reader. Tourniquets must fail open upon fire alarm / manual override in the direction of the escape route.

2.7 Warehouse entrance area tourniquets access controlled

The warehouse entrance area will control the entrance of employees and visitors by means of speed stiles / tourniquets. The amount of speed stiles / tourniquets is based on the amount of traffic which can occur at that facility. The entrance and exit to these speed stiles / tourniquets will be controlled by means of in and out reader. Next to this the warehouse tourniquets will have a random generator to select random passing people for visitation. Tourniquets must fail open upon fire alarm / manual override in the direction of the escape route.

2.8 Visitation area

The visitation area will be equipped with panic buttons connected to the intrusion system for emergency situation and the doors to the visitation areas are access controlled.

2.9 Elevators

The general and goods elevators will be equipped with a reader to control access to the various floors.

2.10 Internal cameras

Next to each perimeter door which will be monitored with an internal camera, the other positions where cameras will be strategically placed are:

- Tourniquet areas (varies between 3-5 cameras)
- Bridge to warehouse camera (facial recognition)
- Balcony areas
- Entrance to kitchen area
- Entrance to IT room area
- Entrance to guard office area
- Reception areas
- Entrance to office areas

2.11 Security rooms

As indicated earlier the security rooms will be equipped with access controlled doors, but inside the rooms there will also be control equipment for the security system installed. Furthermore an intercom post will be installed for answering intercom calls and as indicated earlier the doors will be monitored by means of camera.

2.12 Intrusion motion detectors, Arm – Disarm units

In various strategic points motion detectors and arm-disarm panels will be mounted within the office building. The motion detectors will be projected in a way to create a high success rate of capturing motion on attempted break in during lock down hours. The related arm and disarm units will be projected in a way to have the most efficient layout for arm and disarm points.

3. Warehouse needs

3.1 Loading bays

The loading bays will be equipped with roller shutter door contacts to monitor if the loading bay shutter is opened or closed. Loading bays will be monitored generally in groups of 3 by a camera looking towards the bay and a PIR motion detector covering detection over the group of 3 loading bays

3.2 Perimeter doors

Depending if a perimeter door is a regular traffic door or a door only for escape purposes, this door will either be equipped as access control door (regular traffic) or as monitored intrusion door (emergency escape only). In all cases a camera will be placed on a strategic position to monitor the traffic coming through the door.

3.3 Access controlled doors in the warehouse

The following doors will be equipped inside the warehouse as an access controlled door:

- Doors leading to high profile office spaces (generally inside the warehouse there are some offices which require a card reader)
- Doors leading to logistic truck driver office (the entrance to that logistic office is controlled from both the warehouse side as well as truck drivers waiting area side)
- Doors which provide access to IT rooms (i.e. server rooms)
- Doors which provide access to high value areas (i.e. high value caged areas / pick areas)
- Doors which provide access to Special rooms (like technical rooms, workshops etc)
- Doors which provide access to (external) break areas (from warehouse to internal break area and from external break area to internal break area)

3.4 Motion detection in the warehouse

The motion detectors in the warehouse are strategically positioned to capture motion mainly around perimeter entrances such as described at the loading bay (1 detector per 3 loading bays) Furthermore motion detectors need to be placed at perimeter doors and perimeter windows.

3.5 External break areas

The external break areas are fenced of to prevent employees wondering of to the Zalando perimeter.
For H&S reasons these contained areas do have emergency escape doors which need to be monitored with a door contact by the intrusion system. Furthermore a camera will be positioned to strategically overlook the contained are with escape door(s). Please note access controlled doors situated on an escape route need to have a door override in place for emergency situations

3.6 High value caged areas

The high value caged areas require an additional layer of security, which is established by a access controlled door providing access and several strategic positioned cameras to monitor the entry and (escape) exit points. (Escape) exit points must be secured with a door contact connected to te intrusion system and alarmed with a local door sounder. When escape routes are created between the high value caged area and normal picking area, those doors need to be constructed in a way that small high value goods cannot be passed i.e. underneath the door. We advise a 2 door interlock system on these position which are caged. The caged area needs to be equipped with a fine maze fencing in a way small high value goods cannot be passed from the high value caged are to the normal logistic area.

3.7 Perimeter windows in warehouse offices

Perimeter windows in the warehouse either need to be secured by glass break detectors or motion sensors covering these windows connected to the intrusion system

3.8 Truck driver entrance doors

Truck driver entrance doors are to be equipped with an access control reader to enter into the truck driver waiting area. During logistic office hours these doors will be programmed to be in unlock state, so the truck drivers can freely enter the waiting area.

3.9 Logistic offices

The logistic office in the warehouse is to be secured with an access control reader to enable entrance into the logistic office from either the warehouse or the truck driver waiting area
Furthermore these offices need to be secured with panic buttons, motion detectors / glass break detectors and an arm/disarm keypad connected to the intrusion system

3.10 Cameras inside the warehouse

Next to each perimeter door which will be monitored with an internal camera, the other positions where cameras will be strategically placed are:

- Loading bay doors (generally 1 camera per 3 loading bay doors)
- Passage points between Hall 1 and Hall 2 and between Hall 3 and Hall 4
- High value caged areas monitoring the access controlled entrance door and emergency escape route doors
- Break areas monitoring who is entering the break area (or uses the override button as escape route) as well as externally overviewing the caged area and the escape doors from that area
- Entrances from the office / bridge into the warehouse

4. General cabling requirements for security devices in the office and warehouse

All the cables must be clearly marked on both ends with an unique identifier.

For each camera connection the cable requirement will be:

1. A dedicated CAT6 cable from the central security equipment room to each camera position. Depending the cable length as defined within network environments, the cable may pass through one or more dedicated switches. The nearest switch to that camera must have PoE capability to power feed the camera over the dedicated CAT6 cable. At head end and /or switch end the cable needs to be terminated on a patch strip within the security equipment cabinet / switch cabinet (clearly marked with unique identifier) and on the camera the cable needs to be terminated to a dedicated RJ-Box (clearly marked with unique identifier) within one meter of the camera position

For each intrusion device (i.e motion detector, panic button, glass break detector, door contact, siren etc.) door the cable requirement will be:

1. A dedicated 8 core signal cable (8x0,22cy) from the nearest i/o intrusion module to the door contact(s) of the monitored door. The cable length may not exceed the maximum length as defined within the intrusion system environment. Where possible the doors need to be prepared of factory to contain the intrusion door contact(s) plus cabling tube preparation to pass via door frames / dry walls etc.
2. The i/o modules are connected to each other and the main intrusion panel via a RS485 data bus where again the maximum cable length may not exceed the maximum length as defined within the intrusion system environment.

For each access controlled door the cable requirement will be:

1. A dedicated 12 core signal cable (12x0,34cy) from the nearest access control module to a junction box at the access controlled door positioned on the secure side of the door where possible out of sight (i.e. above false ceiling).
2. From the junction box single cable runs of 8 core signal cable (8x0,22cy) will have to be made to each access controlled door elements such as the door contact(s), the lock (Abloy EL460 orEL560 lock), override devices and door alarms (sirens) where applicable of the access controlled door. The cable length may not exceed the maximum length as defined within the access system environment. Where possible the doors need to be prepared of factory to contain the intrusion door contact(s), lock chase outs with hinge transfers etc. plus cabling tube preparation to pass via door frames / dry walls etc.
3. A dedicated CAT6 cable from the reader position to the nearest access control module. The cable length may not exceed the maximum length as defined within the access system environment.
4. The access modules are connected to each other by means of network cabling (or RS485 where feasible).

For each access controlled tourniquet / speedstile the cable requirement will be:

1. A dedicated 12 core signal cable (12x0,34cy) from the nearest access control module to a junction box inside each tourniquet / speedstile device.
2. A dedicated CAT6 cable from the reader position to the nearest access control module. The cable length may not exceed the maximum length as defined within the access system environment. (note: a speedstile / tourniquet has entrance and exit readers)
3. The access modules are connected to each other by means of network cabling (or RS485 where feasible).
4. A dedicated 8-core signal cable (8x0,22cy) from the central emergency release contact (must be in place already from fire H&S perspective) to minimal 2 emergency release units, to enable emergency releases during emergency situations
5. A dedicated 8-core signal cable (8x0,22cy) from each turnstile gate (positioned for goods transport, cleaning team, handicapped access etc.) to the reception desks (serving the turnstile area) to enable manual release in both directions on these gates

For each intercom unit the cable requirement will be:

1. A dedicated CAT6 cable from the central equipment room (ie server room inside the office space) to each intercom position. Depending the cable length as defined within network environments, the cable may pass through one or more dedicated switches. The nearest switch to that intercom must have PoE capability to power feed the intercom over the dedicated CAT6 cable. At head end and /or switch end the cable needs to be terminated on a patch strip within the security equipment cabinet / switch cabinet (clearly marked with unique identifier) and on the intercom end the cable needs to be terminated to a dedicated RJ-Box (clearly marked with unique identifier) within one meter of the intercom position

SECTION 2: Technical Design

Content

5. Installation Standards for Field Hardware – Intercom Technology (ICOM)

5.1. ICOM – Intercom Technology

5.2. ICOM – Intercom Desk Station – i.e. Office Reception Desk

5.3. ICOM – Intercom Door Station with Camera – i.e. Visitor Entrance

5.4. ICOM – Intercom Door Station without Camera – i.e. Visitor Exit

6. General Building Perimeter and Interior Requirements for Zalando Facilities

6.1. Access Controlled Rooms which are containing Critical Data – MDF Rooms.

6.2. Location of MDF Rooms

6.3. MDF Room Entrance Doors (Access Controlled Doors)

6.4. External Walls of MDF Rooms

6.5. Internal Walls of MDF Rooms

6.6. Apertures within Internal Walls of MDF Rooms

6.7. Roof Areas of MDF Rooms

7. Zalando Security Cabling Standard for the connection of Field Hardware

7.1. General Cabling Requirements

7.2. Cable Types

8. Zalando AutoCAD Standards and typical design

1. Installation Standards for Field Hardware – Central Security Equipment/Interfaces:

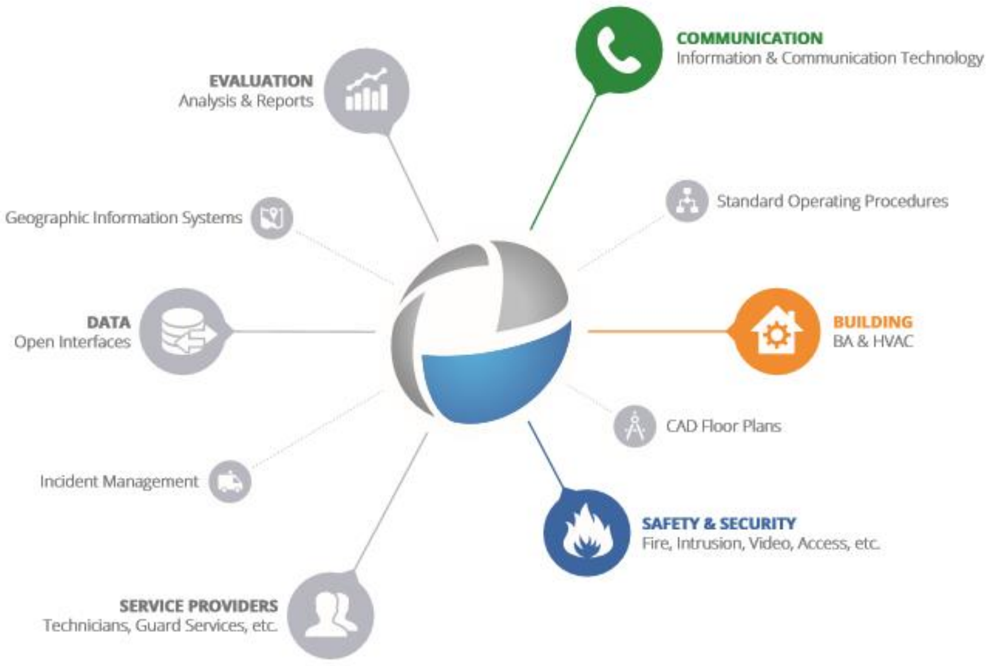
1.1. Central Security Equipment/Interfaces for the Connection of Security Field Hardware (PSIM)

The Zalando Physical Security Information Management Platform can be configured and deployed with a combination of functions such as access control, ID management, alarm monitoring, intrusion detection, digital video management, credential enrollment & authentication, networked visitor control, CCTV control, and automatic data exchange with HR or other source data systems. In the field interfaces are required to connect e.g. access control card reader, alarm contacts and other security systems to the Zalando PSIM (Physical Security Information Management) Software Platform.
NOTE: Zalando only will accept the original devices from the chosen security systems which interfaces with their chosen PSIM system.

For their facilities and as a corporate standard, Zalando has chosen the Advancis Winguard system to serve as their PSIM solution. The Security Field Hardware chosen must be capable to interface with this PSIM system.

Physical Security Policy Approved Security System: *Controlled Areas must be supervised and secured with an approved electronic security system. All security devices connected to the system must be certified for use with it by the manufacturer of the system.*

PSIM Layout

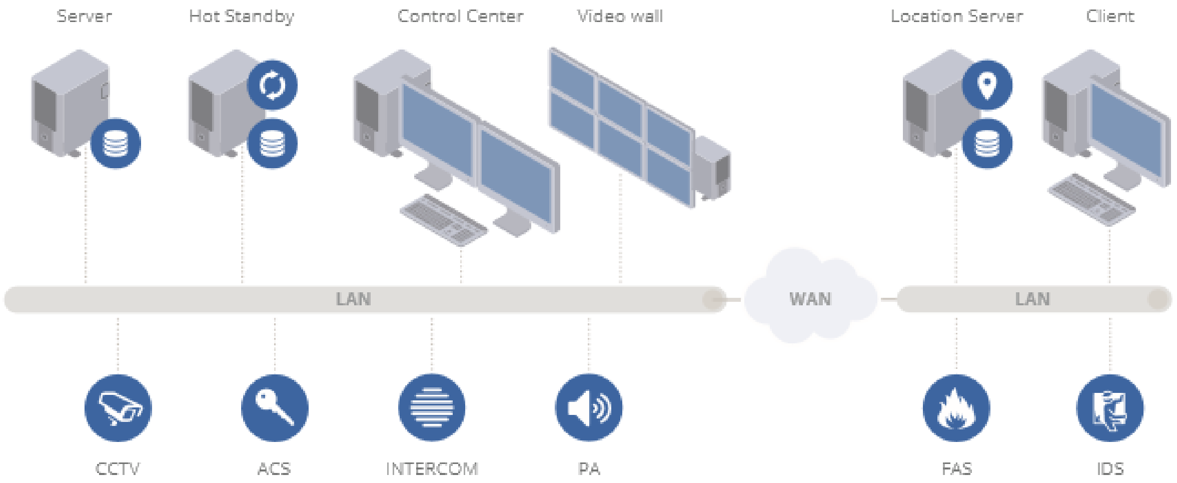

COMMUNICATION
Information & Communication Technology
EVALUATION
Analysis & Reports
Standard Operating Procedures
Geographic Information Systems
DATA
Open Interfaces
BUILDING
BA & HVAC
CAD Floor Plans
Incident Management
SAFETY & SECURITY
Fire, Intrusion, Video, Access, etc.
SERVICE PROVIDERS
Technicians, Guard Services, etc.

1.2. Multi Sites

The Zalando SIM Platform can be configured and deployed to cover multiple locations, in a way that multiple Zalando facilities can be managed from a central chosen location (Control Center). With it, it is essential that the various Zalando facilities follow the same design and system standards as chosen by Zalando to make the integration between the various facilities, chosen system and central management platform seamless. The various facility systems will be connected over the corporate Zalando network.

1.3. Servers and accessibility

The Zalando SIM Platform will be enterprise based. With it the PSIM will have a Central server and a hot standby server. The central control center will have access to these servers and full management access rights. Where required also a location server with a local client (/local rights) can be installed and configured.
This setup provides Zalando the most flexibility in managing their security platform.



2. Mechanical security and Electronic Access Control System (EACS)

2.1. Mechanical security measures

There will be a variety of points inside the Zalando facility which require to be secured mechanically among which gates, emergency escape doors, windows etc. When these elements needs mechanical security elements only, it is important these elements are secured with mechanical locking hardware which are rated as high secure within the industry. Next to this the local standards and regulations have to be met in installing these devices such as: panic overridable where needed, amount of locks and position in relation to the width of door / window / gate etc. The ultimate aim for choosing the class and amount of mechanical locking hardware required, is to delay an attempt of break in as long as possible, have an early as possible detection (which will be covered by the electronic measurements which will be put in place) of the attempt and have a response time which is faster as the delay created.
All elements in a total mechanical locking solution work together, with it all has to be rated equally such as the lock armor plates, the cylinder (which in example may not excel from the armor plate more as 3mm) etc. It's therefore essential mechanical locking hardware is delivered and installed by a qualified lock vendor who can make the correct assessment for the required locking hardware.

2.2. Cylinders and Key locking plan

Manual keys are to be kept to a minimum and need to be centrally managed / registered. Keys, mother-keys and combinations are stored securely; In case non-electronic devices are used (no Zalando badge), the keys and master-key must be kept in a secure location. The Zalando security team will provide and plan the amount of cylinders and keys required and will manage the key locking plan. Generally the key locking plan consist of a master key, around 6 group keys and individual keys in each group. For electronic secured doors by means of an electronical access control system (ACS) the aim is to use as much as possible electronic mortice locks. This way these locks can be operated / overridden by means of a key. Therefore in these ACS controlled doors the delivery of the cylinder and it's key management is the responsibility of the Zalando security team and not included in the scope of the EACS vendor.

2.3. Electronic Access Control System (EACS)

To manage and control access to general traffic doors, Zalando will require an Electronic Access Control System (EACS) to be implemented. The EACS will allow Zalando to create several layers of security to provide controlled access to certain areas by authorized personnel only. The access levels which can be assigned in the EACS will create the zone layers which Zalando wants to create in their facilities. The EASC is generating alarms when access controlled doors are opened without authorized entry or exit

Zalando requires an EACS which complies to the following specifications, where Nedap AEOS is their preferred choice of product:

SOFTWARE APPLICATION

The access control system shall function as the single platform for at least access control. It shall be accessible through a web based user interface via the local area/wide area network, without requiring specific system client software to be installed on workstations.

All software shall be based on a single codebase and not be produced as a customer specific solution. The system application software shall run in Linux and Microsoft Windows server environments and support industry standard relational database management systems conforming to the ANSI-SQL 92 standard.

Upgrading the system shall not affect the functioning of integrations; 'old' integrations must remain functioning with a newer software version that includes new interfacing functionality. The system shall allow to integrate with third party systems including Physical Security Information Management (PSIM), Video Management System (VMS) and intrusion detection. It shall allow to interface with Human Resource Management (HRM) systems, Integrated Workplace Management Systems (IWMS), room booking systems, IT monitoring systems and building automation and control systems.

The system shall offer a generic flexible interface, where incoming and outgoing commands and events can be freely defined and translated to integrate third party devices. This shall support IP and serial RS232 protocols and also function when the server is unavailable.

The system shall allow for easy and unlimited expansion in terms of data and devices, at any given time in the future without performance loss or the need to adjust system software.

The system shall support hard segmentation to provide a single system on a site shared by multiple tenant organisations. This shall allow each organisation to have their own separated domain and configuration. The system shall support varying degrees of segmentation. This shall not lead to having to duplicate hard- or software, including card readers.

EVENTS AND ALARMS

The system shall provide an audit trail for all events and alarms and for all system and administrator user actions, for which it shall log all changes to all fields, including the value before and after a change. For each system user, the system shall allow to filter which logged events and alarms are accessible.

The system is capable to offer a fully customisable map of buildings and their floor plans to display selected security critical locations and devices. The map shall visualize the real-time state of security devices and alarms including their location. From this map, the system shall be able to control (activate/de-activate) devices connected to the access control, intrusion detection or IP video surveillance systems.

The system shall offer a database interface for multiple suppliers of generic commercial database reporting tools as well as for multiple suppliers of open source database reporting tools. It shall allow these database reporting tools to use all event and cardholder information in the database. The system is capable to offer a database export (ODBC) interface for third party time and attendance reporting tools.

IDENTITY AND ACCESS MANAGEMENT

The system shall distinguish between the following cardholder types: employees, visitors, contractors and vehicles. The system shall allow to add any type of information fields to cardholders (including vehicles) at any time by creating user defined fields. It shall allow to automatically respond on data entered in user defined fields.

The system shall be compatible with multiple manufacturers of ID-scanners and card printer software and shall support the use of desktop card readers and digital signature pads for cardholder enrolment.

The system shall link authorisations to cardholders (which can be persons or vehicles), not to the access card held by the cardholder, and allow a cardholder to possess multiple access cards. All access cards shall be inactive, unless assigned to a cardholder.

The system shall automatically block the original access card if a replacement for an access card has been assigned to a cardholder and shall automatically inform the concerned cardholder by sending a message. The system shall be able to automatically block cardholders whose access cards have not been used for a definable period of time, as soon as their employment finishes (by interfacing with the HR system), based upon a pre-determined event and if the validity of their data has expired (e.g. passport or certifications).

The system is capable to automatically update authorisations of cardholders if one or more defined criteria and rules are met, using conditional constructs including ‘if’, ‘and’, ‘or’, ‘greater than’, ‘less than’, ‘equals’, ‘then’ logic.

The system is capable to allow for verification using PIN code and multiple types of biometrics, and shall support biometric readers of multiple manufacturers. Verification shall function seamlessly at all access points if the server is unavailable.

The system shall provide anti-pass back (APB) to prevent people from entering selected zones and access points by re-using an access card from a cardholder that did not previously leave the concerning zone/access point. APB shall function seamlessly when the server is unavailable.

The system shall provide visitor management.

The system is capable to offer a native integration with third party lift systems for destination control, to manage which specific floors cardholders are authorised to access. This shall be effective, even if the server is offline.

The system shall be able to manage authorisations for access of vehicles and be capable of using ANPR, UHF and RFID to identify vehicles.

The system shall indicate which cardholders are present on site and in which specific zone.

The system shall restrict the maximum number of cardholders present in zones and prevent individuals from being alone in selected zones, even if the server is offline.

The system shall be able to restrict the number of movements of selected cardholders.

The system is capable to provide access to selected access points which shall only be granted if 2 authorised cardholders scan their access card at the same card reader within a definable time, even if the server is offline.

The system is capable to prevent individuals from being alone in selected zones, even if the server is offline.

The system is capable to allow to grant access to selected zones only if a selected cardholder (the manager) is present in that zone, even if the server is offline.

The system is capable to automatically send selected persons a message if there are fewer first aiders present than a defined minimum (e.g. 1 first aider per 50 cardholders). This shall not require a person to carry multiple cards.

SECURITY AND EMERGENCY

The system shall allow to open (unlock) or close (lock) predefined access points manually by pressing an emergency button and automatically in response to a fire alarm or intruder alert. This shall function seamlessly if the server is unavailable. In response to an activated crisis situation, the system shall automatically print a list with all cardholders present in each zone.

The system shall be able to define security scenarios (e.g. crisis scenarios and increased threat levels) that shall be activated and deactivated manually and automatically in response to nominated events. An activated security scenario shall allow to automatically lock or unlock selected access points and automatically activate or deactivate different authorisations, anti-pass back and verification for selected cardholders.

The system is capable to provide guard tours with predefined checkpoints for guards on surveillance.

ACCESS CARDS AND DOORS

The system shall be able to simultaneously operate multiple access card technologies, including: Mifare Classic, Mifare DESFire, Legic Advant and Prime, Access cards using 2.45 GHz, UHF, Magnetic stripe, Barcode and QR-code.

The system shall support the synchronisation of access points (airlock) allowing a secure passage by preventing cardholders from passing a second access point before the first access point is closed. The number of access points within one specific airlock shall be unlimited. The precise functionality of an air lock shall be changeable by remotely adaptable software and without the need to change hardware. The system shall allow to turn airlocks on and off remotely from the user interface. Operational continuity of airlocks shall be guaranteed if the server is unavailable.

The system shall support wireless online locks of multiple manufacturers. Wireless online access points shall offer the same functionality as wired online access points. The system shall use a single database and GUI for wired and wireless online access points.

The system shall support all wireless locks that comply with the OSS Standard Offline protocol. The system shall use a single database and GUI for wired and wireless offline access points.

The system is capable to allow to manage long term lockers (assigned to a selected cardholder for a definable period) and short term lockers (for one time use for any authorised cardholders). It shall use a single database and GUI for the management of lockers and access control.

FIELD HARDWARE

Controllers shall be able to perform multiple security disciplines, including access control. The precise functionality of controllers and their inputs and outputs shall be determined by remotely adaptable software. Adapting the functionality of the controllers and their inputs and outputs shall not require exchanging or changing hardware or wiring.

Controllers shall be able to connect third party card readers using the Open Supervised Device Protocol (OSDP), Wiegand protocol, IP protocol and RS485 communication. A migration to other card technologies shall not result in the need to change controller hardware.

Controllers shall be capable of containing a SAM for storing DESFire keys and digital certificates and shall allow updating the DESFire keys and digital certificates remotely via a secure, encrypted connection.

In normal operation, requests for access to an access point shall be processed by the controllers, without needing to consult the server. Events generated shall be stored in the server database. If the server is not available, controllers shall be able to cache at least 100.000 events.

Controllers shall be able to communicate with each other (peer-to-peer) and process signals from any device (such as controller expansion units, readers and doors) connected to any other controller connected to the network, even if the server is unavailable. This shall ensure functionality including anti-pass back, biometric and pin verification, lift destination control, occupancy limit, two person rule, minimum occupancy rule, manager first and airlocks function seamlessly if the server is unavailable.

Controllers shall be compatible with Power over Ethernet (PoE) IEEE 802.3af standard, PoE+ IEEE 802.3at standard as well as 12-27 Volt DC power supply.

The system shall allow the expansion of controller capacity using controller expansion units (adding card readers, inputs and outputs) and I/O expansion units (adding inputs and outputs) that use the intelligence of the controllers. They shall connect to a controller using RS485 bus wiring.

Card readers shall allow to read Mifare Classic and Mifare DESFire cards and use all available Mifare Classic and Mifare DESfire card technologies simultaneously. Card readers shall be capable of being updated, configured and migrated to other card technologies remotely. They shall be capable of simultaneously reading the UID (CSN), encoded sector data and application data (file data).

Card readers shall be capable of functioning as a transparent reader for Mifare DESFire access cards, meaning no Mifare DESFire keys are stored on card readers.

Card readers shall support RS485 (encrypted using TLS1.2 and plain protocol) and Wiegand communication and shall protect against relay attacks with a Frame Waiting Time (FWT) of 5 ms or less.

2.4. EACS - Readers

Each Access controlled door must be equipped with a InveXS MD(K)170B or ConveXS MD80F (or equivalent design / data) card reader mounted on the exterior wall (depending on the location and available surface area for mounting). The reader must be configured to read the Mifare Desfire encrypted Zalando cards. The reader should be installed on the handle side of the door at 110 centimeters (44 inches) above the ground and be attached to a recessed electrical junction box. (If local circumstances will not allow the installation of a recessed built-in card reader a surface mount version can be accepted but this need to be authorized in advance by the Zalando security team.)
To enable location status of cardholders in the facility, the perimeter doors which provide entrance / exit at the facility will be equipped with card reader in and card reader out. In combination with anti-pass back functionality this will enforce the card holders to book in and out of the facility, to provide an accurate mustering list in case of evacuation events of the facility
An additional layer of security will be applied at the MER/SER/IDF/MDF or other high security rooms upon indication of Zalando security team, which require a Keypad Card Reader (such as the MDK170B or equivalent) for entrance. This keypad reader requires a combination of a badge and an unique user pin code for access validation.

The Zalando preferred readers and it's specs are:

Nedap Readers

- Modern design, optionally with touch keys or screen
- Suitable for all commonly used access control systems and technologies.
- Wiegand output, RS485 or RF modulator communication
- For indoor (InveXS) and outdoor (ConveXS) use
- Adaptable – Interoperable with a growing range of technologies (currently Base Mifare Desfire EV1 configuration for Zalando

Various available types:

Nedap InveXS MD170B Reader (Mifare Desfire EV1)

- Modern design, unique combination of card reading technologies.
- Designed for door applications requiring a small footprint card reader
- Suitable for all commonly used access control systems and technologies.
- Wiegand output, RS485 or RF modulator communication
- Supports Mifare Desfire EV1 credential technologies.
- For **indoor** use
- Detection range Mifare Desfire EV1: Approx. 1cm

Nedap InveXS MDK170B Reader (Mifare Desfire EV1)

- Modern design, unique combination of card reading technologies.
- Can be used **with key pin** combination and access control card, or just card or pin.
- Designed for door applications requiring a small footprint card reader
- Suitable for all commonly used access control systems and technologies.
- Wiegand output, RS485 or RF modulator communication
- Supports Mifare Desfire EV1 credential technologies.
- For **indoor** use
- Detection range Mifare Desfire EV1: Approx. 1cm

Nedap ConveXS MD80F Reader (Mifare Desfire EV1)

- Modern design, unique combination of card reading technologies.
- Designed for door applications requiring a small footprint card reader
- Suitable for all commonly used access control systems and technologies.
- Wiegand output, RS485 or RF modulator communication
- Supports Mifare Desfire EV1 credential technologies.
- For indoor and **outdoor** use
- Detection range Mifare Desfire EV1: Approx. 1cm

2.5. EACS - Locks

The preferred locking mechanism for access controlled doors is an electric solenoid mortise lock with a built in Request-To-Exit Switch (REX). The product that meets this requirement is the Assa Abloy EL series. An equivalent electric solenoid/motorized lock can be accepted but need to be authorized by Zalando security team. Site must use this product or an equivalent product that offers all the same design features. To ensure a correct installation and preparation of the door which will receive this lock, it is strongly recommended these works are carried out by a certified M&E contractor. Where possible, on new build facilities, the Zalando security team will try to have the doors prepared for these lock by the door manufacturer, which are new and still to be delivered to site

Installation Notes (preferred choice):

- Requested locking mechanism is an electric motorized security lock with a built in Request-To-Exit Switch (REX), panic function, self-locking deadbolt.
- Connection of REX contact on the REX input of the access control module. Required line supervision with resistors (1K series).
- Deadbolt contacts are providing an additional security feature and are recommended for connection on the Access Control system especially for perimeter doors leading to outside of the building. Connection the deadbolt contact (locking status) on an input of the access control module. Required line supervision with resistors (1K series).
- The product that meets this requirement is the ASSA ABLOY EL466, EL566 Security Lock. If local laws and regulations don’t allow this please contact Zalando Security Team.
- Equivalent products which are offer the same design features are accepted but need to be authorized by Zalando Security Team.
- Further solutions like door strikes or magnetic locks (mag locks) are accepted but need to be authorized by Zalando Security Team.
- Standard Strike Time: 5 Seconds (to be set in the programming)

Alternative:

- Electric Door Strike with REX monitoring contact, 12 or 24 VDC (only Interior Room Doors, where an electronic mortise lock Installation is not feasible)

- Electro Holding Magnet (MAG Lock), 12 or 24 VDC (Interior Room Doors - min. 3000N / Exterior Building Doors - min. 5000N & only where an electronic mortise lock installation is not feasible)
Note: MAG locks have to be mounted on the interior wall side of the secured room.

In case an alternative lock (door strike or magnetic lock) is used, it is essential a request to exit button is installed on the exit side (unless there is an exit reader).
In case there is no free egress available on the access controlled door (e.g. door strike installed with fixed knob on the exit side, mag lock installed, or out reader installed), it is essential an emergency door override unit is installed, which is monitored for activation by the EACS.
These elements will be covered under topic 2.6 EACS – Door Contact(s), Rex and BGU

2.6. EACS – Door Contact(s), REX and BGU

Each door must be equipped with a magnetic Door position switch (door contact) that has been mounted in a recessed position that cannot be seen from either side of the door when the door is in the closed position.

Installation Notes:

- Each door must be equipped with a magnetic door position switch (door contact) Magnetic door contacts on double wing doors can be wired in series and connected to only one alarm input.
- Monitoring of door status (open / closed)
- Connection to access control module
- Required line supervision with resistors (1K series – access Standard)
- Requested as a recessed built-in version. If local circumstances will not allow the installation of a recessed built-in contact a surface mount version can be accepted but need to be authorized by Zalando security team.
- Overhead contracts of synthetic material are preferred above aluminum

Request-To-Exit (REX) devices are required on every door to shunt the alarms as the door is opened from the inside of the secured space/room. The preferred method to achieve this is an Electric Mortise lock with a built in REX as outlined above. However, when a motorized lock can’t be used, a REX Button must be installed on the interior wall exit side, on the handle side of the door at 110 centimeters (44 inches) above the ground and be attached to a recessed electrical junction box (surface mounting the REX button, directly to the wall is not preferred).

Installation Notes:

- When an electric motorized security lock with an integrated door handle REX contact can’t be used, a REX Push Button must be installed. An alternative locking device which requires a REX push button is a door strike or a magnetic door lock (MAG-Lock).
- Connection of REX contact on the REX input of the access control module. Required line supervision with resistors (1K series).
- A REX Push Button needs to be attached to a recessed electrical junction box, installed on the handle side of the door, so the inside of the secured space/room.
- Assembly height: 110 centimeters (44 inches) above ground.

Alternative Solutions:

- REX, Request to Exit Motion Detector (e.g. T-REX). In exceptional cases and in coordination with a representative of Zalando Security Team a Request-To-Exit motion detector will be allowed. It's not permitted to use REX Request to Exit Motion Detectors in combination with perimeter access control doors which are leading to the outside of the building or in combination with access control for rooms with critical or highly confidential/confidential Data.

Emergency Override's (BGU) devices are required on every EACS door (also tourniquets, speedstiles etc.) which does not have a mechanical means of exit. This BGU is to prevent people being locked inside an access controlled area when the EACS system fails. It is therefore important that the access control doors which require this override safety have a fail-safe lock installed. A Fail-safe lock opens when the power is cut to the lock (in other words, the lock requires power to be locked). The BGU must be installed on the interior wall exit side, on the handle side of the door at 110 centimeters (44 inches) above the ground and be attached to a recessed electrical junction box (surface mounting the BGU device, directly to the wall is not preferred).

Break Glass Override Device / Emergency Exit Push Button

- The power cut-off switch of the emergency exit push button needs to disconnect the locking device from the access control system on a direct way so that the locking device will not be powered anymore and unlocked.
- The device shall be mounted on the interior wall, installed on the handle side of the door
- Assembly height: max. 44 inches (110 centimeters) meters above ground (push button height)

- A status monitoring switch (double pole, double throw) must also be installed and connected on an input of the EACS. In the case Emergency Exit Push Button will be pushed an alarm needs to be generated. If this functionality is not available or not to implement ask Zalando security for an approval to work without it.

Alternative Solutions (i.e. standard in Germany):

- Emergency Exit Terminal Unit according to EU Standard – EU DIN EN 179 and DIN EN 1125 (legislation demand in e.g. Germany)
- The power cut-off switch of the emergency exit terminal unit needs to disconnect the locking device from the access control system on a direct way so that the locking device will not be powered anymore and unlocked.

2.7. EACS – Door sirens and key overrides.

Door sirens are required to be installed on all access control doors and on all site perimeter doors (in combination with a door contact). The purpose for the siren is to sound when the access controlled door is held open (over 45seconds) or forced open (opened without a valid entrance / exit event). A perimeter door can be a physical external perimeter door leading to the outside, but can also be an internal door leading to an emergency escape route or 3rd party space. Perimeter doors without access control readers must at least be secured with a door contact / siren combination. These doors will be referred to as Monitored Point (MPT)

Installation Notes:

- Door Sounders/Sirens shall be used to indicate unauthorized entry and exit on access controlled doors. To allow a fast intervention of guards in case of an incident
- Connection to an auxiliary output of the EACS.
- In case of a perimeter door which has no access control installed a door contact/siren needs to be installed which is connected to an in-/output of the AECS
- Minimum sound level 100dB - 120dB
- Assembly height: minimum 10 feet / 3 meters above ground

Key override-Bypass. In case a monitored perimeter door is also occasionally used as transport door, a key override switch must be installed which will allow the local user to override the door sounder. The switch must be installed on the exterior wall, on the handle side of the door at 44 inches (110 centimeters) above the ground and be attached to a recessed electrical junction box (surface mounting is allowed in liaison with the Zalando security team).

Installation Notes:

- Assembly height: 44 inches (110 centimeters) meters above ground

2.8. EACS – Central Equipment – Housing and Power Supplies

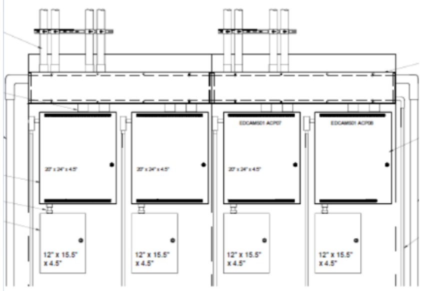
Zalando accepts the majority of (CE approved) Power Supplies/Charger to contain and power Interfaces to connect Security Field Hardware for Access Control, Camera system and Intrusion Detection.
The current version of the chosen Access Control Hardware shall always be the bases of the installation of Access Control specific equipment and security system field hardware within an Zalando facility infrastructure.
Zalando prefers to have the Security Equipment centrally mounted in example in the central MER/SER/IDF/MDF room. The maximum cable lengths allowed for a functional system prevails above the preference to have all security equipment mounted centrally.

Installation notes:

- Housing
  - Standard housings of EACS etc. is allowed
  - Rack mounted or wall mounted solution may vary per facility
  - Tamper switch
  - Network and UPS backup provided by Zalando
  - For onboard Power supplies an local backup battery is required
- Power Supply / Charger
  - 12 VDC or 24 VDC power limited output (depending the system needs)
  - Built-in charger for sealed lead acid or gel type batteries (Optional ABT-12)
  - Automatic switchover to standby battery when AC fails
  - AC input and DC output LED indicators
  - AC fail supervision (form C contacts)
  - Low battery supervision (form C contact)
  - Low battery disconnect prevents batteries from deep discharge
  - Thermal overload protection
  - Short circuit protection
  - Primary circuit switch for incoming 115 VAC or 230 VAC

To avoid that unauthorized people can have access to area housings and power supplies/chargers the cabinets always shall be installed in rooms which are separated from public areas (e.g. office). The minimum height of cabinets shall be 2 meters (6 Foot). Measure point is the bottom edge of the cabinet.

Sample central housing and power supply installation wall mount:



2.9. EACS – Turnstiles / gates

To create a demarcation line between reception area (front of house) and office area (back of house) Zalando may choose to have turnstiles / gates installed in this area.
This will prevent employees and visitor to enter directly into the office area. The amount of barriers varies per site and will be determined based on the traffic rate in this area and each barrier will be controlled with an in and an out reader connected to and controlled by the EACS. (with anti-pass back functionality)
A separate gate will be installed as well controlled by reception for delivery of goods or people with disabilities who cannot pass through the standard turnstiles.

Sample:

Installation Notes:

- Each gate must be capable to handle incoming as well as outcoming traffic
- Monitoring of gate status (open / closed)
- Connection to access control module (readers must be installable in or on the gate)
- Separate in / outwards swinging gate, reception controlled, for goods delivery or people with disabilities.
- Fail safe open function (gate must fail open in case of power cut / fire alarm etc.)

Zalando requires a random visitation search feature in the configuration of their access system. This means randomly a cardholder has to be selected during the exit event of a speed lane. The exit needs to be decline and an visible and audible alarm needs to be triggered as indication the person has been randomly selected for a visitation search

3. Intrusion Detection / Security Devices

3.1. Intrusion Detection System (IDS)

This specification defines the requirements for an Intruder alarm system range which can deliver the security needs for Zalando, where Honeywell Galaxy is their preferred choice of system.

The following is a summary of the minimum specifications for the control panel range.

- 16 multi-state detection circuits on-board the standard control panel
- Expandability capability up to 520 detection circuits
- Capability for 32 independent areas (partitions or groups)
- Capability for 1000 users
- Intruder Event log Capacity of 1500 events
- Independent Access event log capacity of 1000 events
- 7 switching outputs on-board the standard control panel capable of switching 400mA each
- One relay output on-board the standard control panel capable of switching 1A @ 30v DC
- Capability for 67 independent weekly schedules, each with 28 on/off events
- 67 independent holiday schedules, with 32 holiday periods
- Schedule driven auto-arm for each area (partition or group)
- Lockout schedule capability to prevent disarming during secure periods
- Capability for voltage substitution detection on the detection circuits
- Full diagnostics monitoring of all detection circuits and power supplies
- Automatic scheduled reporting capability of diagnostic information
- Communication capability over PSTN, Ethernet, GPRS and ISDN
- Wireless sensor capacity for 198 sensors
- Bidirectional communication for all wireless sensors for message delivery confirmation
- Agile-routing capability for all wireless sensors to provide wireless-path redundancy
- 32 channel Bi-directional audio capability with 10 second pre-alarm per channel
- Access control capability for 64 doors each with Wiegand card readers/PIN pads
- Schedule controlled user rights for door access
- Door access rights controlled per system area (partition or group) with automatic blocking for armed areas
- Secure remote Servicing capability for configuration and remote maintenance
- Full range of system peripherals including Color, Graphical, Touch-screen user interface
- Full compliance to En50131 at Grade 3 level plus communications compliant to Grade 4 level, ATS 5

The System must consist of a centralized control panel which contains all the configuration settings and system control authority. The system must have the following minimum specifications:

System functionality

Zone input circuits for detection points:

Zone input circuits are multi-state analogue detection circuits which allow connection of conventional alarm sensors or wireless detection inputs which are individually identified.

The system shall have 16 on-board, zone input circuits with an upgrade path to 520 zone inputs circuits. All zone input circuits must have fully configurable system responses.

Each wired zone input circuit must be capable of full supervision using an end of line resistor plus contact resistor to detect the following states:

Zone short circuit
Zone low resistance
Zone Closed (Normal)
Zone high resistance
Zone Open (Alarm)
Zone Fault
Zone masked
Zone Open circuit

It must be possible to enable certain circuits with voltage tamper detection to detect if an attempt has been made to bypass the zone input circuit by substitution of the circuit with a voltage source

Each Wireless zone must use two-way communications with transceiver modules. There must be the capability to use multiple transceiver modules to provide alternate paths to each sensor. The system shall monitor the signal level on each path to maintain the strongest two-way route to each sensor.

Each zone must have full programming capability of the following attributes:

- Function (or Zone Type. The complete list of zone functions is shown in Table 1)
- Descriptor (16 alphanumeric characters)
- Chime Attribute (Chime effect, enable/disable)
- Omit Attribute (Zone can be omitted, enable/disable)
- Part Attribute (Zone included in part arm, enable/disable)
- Response Time (Fast or slow)
- Custom SIA (SIA format mnemonic for alarm signaling)
- Activity Monitor (Check for zone activity in the dis-armed state)
- Resistance Select (Resistance windows of the zone)
- Group (Assignment of zone to Galaxy Group)
- Wireless sensor programming and signal strength

Area control (Partition or Group control)

The system must have the option to be configured to have up to 32 fully independent areas (partitions or groups). Each area must be capable of being armed independently. Each system user must be capable of having authority to one or any combination of areas

Every zone on the system must be assigned to one area only. Certain zone types such as Keyswitch and Exit Terminate (Push To Set) zones must have the configuration ability to assign additional areas that their function will also affect for shared entrance areas.

There must be configurable logic to allow multiple areas to arm at the same time but to hold off common lobby areas from arming if all the surrounding areas are not armed or not currently in the process of arming yet.

System users

The system must be able to be configured to have up to 1000 users. Each user must be able to have a variable authority level to govern rights to arm, disarm and reset the system following alarms. Each user must have separate assignment of arm/disarm control and access control rights. Each user must have the ability to be programmed with a PIN code up to 6 digits long plus an Access control card up to 40 bits long.

Event log

The system must be able to generate an event log of all events which took place at the system

Outputs for signalling and control

The control panel shall have at least 7 high-current (400mA) switched-negative outputs, one relay output capable of switching 1A at 30V DC and at least 6 low current signal outputs. There must be an upgrade path to allow at least 260 outputs to be configured on the system.

Timers and Scheduling

The system must have multiple independent timer schedules which run on a weekly cycle. Each weekly cycle must have the capability to program at least 28 events (on and off switches).

The schedules must be able to be assigned to control the following system events:

Auto arm/disarm
Arming monitor
Output control for electrical switching
Activity control of user profile for arming/disarming restrictions
Access control profile restrictions

<u>Automatic system Diagnostics</u>

The system must have comprehensive self-diagnostics and reporting sufficient to have full visibility of the current health and trends on the system.

The system must be able to record the following system health data:

Status of every system power supply including:

Output voltage
Output voltage history (minimum and maximum)
Output current
AC mains Input Status
Battery charge status
Battery presence status
Battery load test status

The status of every zone input on the system including

Circuit loop resistance for wired zones
Resistance history (minimum and maximum in the closed/normal state)
Signal strength from every wireless sensor
Signal strength history for each sensor (minimum and maximum)
Activation history in the disarmed state for detector operation checking

The system must be capable of being configured for periodic transmission of the self-diagnostic information to the remote management software. The remote management software must be capable of generating a report, automatically, for each installation which will highlight all the areas where the measurements are outside spec or where there is trend where the measurements are drifting significantly.

<u>Communications</u>

The system must be able to communicate over the following media

PSTN, Analogue telephone lines
ISDN Telephone lines
Ethernet WAN and LAN connections

Each of these media must allow for alarm signaling and Remote Servicing

Wireless sensor capability

It must be possible to install up to 8 transceiver interface modules in order to allow use of wireless sensors and user control 'keyfobs'. The system must accept an incoming message from any sensor via any transceiver interface.

Wireless communication must be two-way with the system delivering an acknowledge reply to each message from a wireless sensor or keyfob. The system must allow for intelligent routing of the acknowledge signals so that the reply is sent only from the transceiver interface which has the strongest reception of the original signal.

Wireless keyfobs must give user feedback on arming command status and must be capable of showing the armed status of the system upon request

The wireless sub system must meet the requirements of EN50131-5-3 to Grade 2 level.

Access Control

The system must be capable of controlling up to 64 doors. Access through the doors must be restricted to users who have access rights to those specific areas of the building at specific times. The system must not allow access to an area which is armed to avoid false alarm activation.

It must be possible to define rights for users to disarm or arm areas of the building using their access control card at a door control reader.

Remote Servicing

A PC software suite must be available to service installed systems from a remote, centralised location. This package must have the following capabilities:

- Centralised database for storing site data for at least 100,000 configured installations
- Ability to have up to 32 operators accessing the database, simultaneously, via a client browser application across a local or wide area network.
- Ability to have up to 64 remote systems connected to the database simultaneously via a communications server application
- Ability for the communications server to accept incoming connections from remote systems, automatically, even when no operator is active on a client browser.
- Choice of Communication Media
    - Ethernet TCP/IP
    - RS232 Serial Interface
    - PSTN
- Full Audit trail log of activity in accessing the database
- Connection log of all remote, installed systems which are connected to the database
- Ability to define scripts to make mass updates to groups of accounts to roll out a common change across many installed systems

Operator Features include:-

- Creating/Open of system accounts
- Printing account information
- Copying account information to new accounts
- Real-Time control of remote systems via virtual Keypad Operation
- Upload data from installed systems
- Download data to installed systems
- Off-line programming of all aspects of installed system configuration
- Rolling back panel programming data to a previous, saved version
- Mimic Panel display of system status in real-time
- Diagnostics indication of installed systems' health
- Event log display
- Event log filters
- Ability to set time and date
- Initiate connections to installed systems
- Copying of event log data
- Printing of installed system data
- Printing of event log
- Automatic generation of detailed system health status reports using uploaded diagnostic data

Compliance and Approvals
The product must be independently tested to the following directives and standards:
R&TTE 99/5/EC
EN50131-3: 2009 security grade 3, environmental class II

The product must be suitable for use in systems designed to comply with EN50131-3:2009:

- Security Grade: 3
- Environmental Class: II
- Power Supply Type: A
- Alarm Transmission System: ATS2=D2, M2, T2, S0, I0

The control panel must be compatible with the relevant parts of the following standards:

EN50131-1:2006+A1:2009 Alarm systems – Intrusion systems – General requirements (grade 3).
EN50131-6:2008 Alarm systems – Intrusion systems – Power supplies (grade 3).
PD6662:2010 Scheme for the application of European Standards for intruder alarm systems.
BS8243: 2010 Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions - code of practice.

Appendix 1 – System Peripherals

The following peripherals must be available for system design:

User Interfaces

Standard keypad for programming and user control

- Stylish design
- 32 (2 x 16) alphanumeric backlit LCD display
- Tamper protection
- Tactile backlit rubber buttons
- Full system control
- Addressable
- Can be connected directly to the system databus at distances up to 1,000 m from the control panel
- Arm/Disarm with PIN and/or optional proximity tag
- Easy installation
- Self learn capability for proximity tags

TouchCenter Keypad with Prox tag reader

- ¼ VGA TFT Touchscreen keypad
- Graphical icons for end user control
- Engineer access and control capability
- Plastic enclosure
- Lid and mounting tamper protection
- Can be connected directly to the panel up to distances of 1,000 m
- Integrated proximity reader for arm/disarm capability
- Self learn capability for proximity tags
- Dual action functionality, simple arm/disarm operation removes the need for PIN entry

Self contained single door controller

- Proximity Door Control Unit
- Connects directly to peripheral data bus
- Monitors the status of one door
- Able to control a door lock and request to exit button directly
- Can be used to arm/disarm with Prox Card/Tag
- Addressable
- Intended for Internal use or External use

System Expansion

Zone & output extension module

- Connects directly to peripheral data bus at up to 1000 m from the control panel
- Addressable
- 8 zone input circuits with voltage tamper protection
- 4 transistorised outputs
- Lid and surface removal tamper protection

Intelligent Power Supply Range

- EN50131-1/EN50131-6 Grade 2 or 3 compliant
- Total capacity 2.75 A
    - Rating dependent upon grade selected and battery capacity
    - RS485 communication support
    - 8 zones/4 outputs

Wireless transceiver portal or Gateway

- Wireless transceiver providing support for wireless sensors and keyfobs
- Comprehensive wireless diagnostics, testing and monitoring functionality
    - Low battery
    - Programmable supervision
    - Jam detection (interference)
- Centralised programming mode via system keypad
- Walk test automatically logs the signal strength of each zone
- Full signaling of RF status

Wireless sensor portfolio

The following wireless sensor types must be available for system design:
10m PIR sensor
12m Dual-Tech microwave & PIR sensor
Magnetic door contact
Shock sensor
Audio glass-break detector
Smoke sensor
Carbon Monoxide sensor
Flood and temperature sensor

Wireless sensor must have a typically battery life exceeding 3 years.
Sensors must have an open field transmission range of 2km.

3.2. Intrusion Detection Devices / Security Devices

Security Devices: Security devices such as Motion Sensors, Glass Break Sensors and Tamper Switches are the least visible part of the electronic security system and at the same time, the most important part as they provide a second layer of access control and redundancy if the primary access control device fails. To work effectively, they need to be correctly installed and periodically tested.

Magnetic Window / Door Contact

Window and door contacts are used to monitor the open or closed position of a door or window. The contact will provide an early detection state in case the window or door is forced open and will warn the employees upon arming the system when not all doors or windows having such contact are physically closed

Installation Notes:

- The Zalando security team will indicate specific windows and/or doors which must be equipped with a magnetic contact
- Monitoring of window / door status (open / closed)
- Required line supervision with resistors (1K series & 1K parallel)
- Requested as a recessed built-in version. If local circumstances will not allow the installation of a recessed built-in contact a surface mount version can be accepted but need to be authorized by the Zalando security team

Roll-Up Door Contact / Overhead Door Contact

Roll-Up / Overhead door contacts are used to monitor the open or closed position of a such doors. The contact will provide an early detection state in case the door is forced open and will warn the employees upon arming the system when not all doors having such contact are physically closed

Installation Notes:

- Each roll up door (overheads) that opens, must be equipped with a magnetic contact
- Monitoring of roll up door status (open / closed)
- Assembly height: if possible above roll up door (alternatively on the floor)
- Required line supervision with resistors (1K series & 1K parallel)
- Requested housing material: synthetic material

Acoustic Glass Break Detectors

Glass Break Sensors. Glass Break Sensors (GBS) are designed to detect a breach involving the breaking of a glass panel. Only Glass Break Sensors with the dual detector technologies of Acoustic and Shockwave may be used. Sites deploying GBS' are also required to maintain a specialized testing device design specifically to test the type of sensors in use at the site.

Installation Notes:

- Acoustic glass break detectors are required as secondary alarm device (second security layer) to protect building or floor entrance doors with glass panes. Additionally they should be used to protect windows within building areas where motion detectors cannot be used or within high risk areas for early detection purposes.
- The detector shall be mounted on ceilings and walls in close proximity to the glass panes and listen for sound frequencies associated with glass breaking.
- The detector should have a minimum detection radius of 8 meter.
- The detector shall be optimized for premises single- and multiple-glazed with simple window glass
- For the commissioning of the detector a test by using the glass breakage simulator is required
- Depending on the type of glass and the presence of a window film or plastic interlayer an acoustic glass break detector may is not suitable. The installer is responsible for the correct selection of the detectors and for the decision to use an acoustic glass break detector as secondary alarm device.

Motion Detector PIR / DUAL

Motion Sensor: Motion Sensor (also called a Motion Detectors) must be installed at any site that is expected to close for any part of a day or week. The detectors are designed to detect any movement within their field of "vision" and then trigger an alarm.

Installation Notes:

- Motion detectors are required as secondary alarm device (second security layer) to protect the internal building perimeter. They are especial suitable for large buildings because there is no guarantee that all building areas steady can be secured by security guards twenty-four hours a day year round.
- Motion detectors should be armed (unmasked) during the time after operation hours (in the night, on weekends) and only disarmed (masked) during the periodically guard tours of the security guards

- Each exterior door (also overhead doors, etc.) must be within the clear and full field of vision of a detector
- Each exterior window area until a high of 32 feet / 10 meters above ground must be within the clear and full field of vision of a detector
- Detectors with multiple sensor technologies may be used with Microwave/ Passive Infra-red being the preferred combination
- DUAL Detectors are in any case required for buildings areas which have no-suitable climatic conditions (e.g. warehouse dock areas, server rooms or office rooms with air condition, etc.).
- The detector shall be suitable for conventional connection technology
- The detector shall be equipped with an anti-mask (AM) monitoring contact which should be wired in line with the alarm contact. Additionally it should have a Walk Test functionality to perform a functional control and a detection range check.
- Due to various application areas the detector shall be suitable for wide angle, vertical curtain and long range detection optics.
- Please note: DUAL-Microwave Detectors which work within the following frequency ranges are not permitted.
    - 2.4 GHz IEEE 802.11b/g/n
    - 3.6 GHz IEEE 802.11y
    - 5 GHz IEEE 802.11 a/h/j/n

  Non-critical are devices which work above the 6 GHz frequency range.
- Assembly height: a max. 8 feet / 2.50 meters above floor
- No flush mount box, connection occurs directly
- Connection to an input of a LNL1100 input module
- Required line supervision with resistors (1K series & 1K parallel)
- A tamper switch must also be installed and connected on an alarm input of a LNL1100 input module.

  Note: If several single tamper switches are securing different housings of an Alarm Device Unit then these switches shall be wired together in line and shall be connected to only one alarm input.

Alarm Sounder/Siren with Strobe Light

Alarm sounders/sirens and Strobes provide audible and visual verification of an alarm

Installation Notes:

- Sounders/Sirens shall be used to indicate the detection of an intrusion. To allow a fast intervention of guards in case of an incident, an alarm a strobe light must be added or integrated.
- Only necessary if building areas are not equipped with door sounders which could be linked to an intrusion detection alarm.
- Minimum sound level 100dB - 120dB
- OFFICE AREA: Maximum sound level 60dB
- Strobe color – red. An alternative color is permitted when local building codes are requiring the red color for other security and safety systems e.g. fire alarm systems.
- Assembly height: minimum 10 feet / 3 meters above ground
- A tamper switch must also be installed

4. Video Management System (VMS) and Cameras (CAM)

4.1. VMS – Video Management System

The preferred choice of VMS for Zalando is the Genetec Omnicast solution. The specifications for the VMS are listed below.
The storage capacity has to be determined based on the total amount of camera's, the frame rate per second (min. 7 fps), the storage resolution (min. 1Mp resolution) and the live recording time (when motion detection recording and / or event recording is applied).
Zalando wants to achieve a storage time of 30 days and requires a overcapacity of 15% on the calculated storage.
Zalando also requires and interfaceable analytics solution with their VMS for which their preferred choice is Kiwi Software.

General VMS Requirements

A. The VMS shall be based on a true open architecture that shall allow the use of non-proprietary workstation and server hardware, non-proprietary network infrastructure and non-proprietary storage.

B. The VMS shall offer a complete and scalable video surveillance solution that shall allow cameras to be added on a unit-by-unit basis.

C. The VMS shall interface with analog-to-digital video encoders and IP cameras and with digital-to-analog video decoders, hereafter referred to as digital video servers (DVS). The VMS shall support DVS from various manufacturers.

D. The VMS shall integrate DVS using the DVS native SDK or using the following industry standards to interface to the DVS:
1. ONVIF

E. All video streams supplied from analog cameras or IP cameras shall be digitally encoded in H.265, H.264, MPEG-4, MPEG-2, MJPEG, MxPEG, Wavelet or JPEG2000 compression formats and recorded simultaneously in real time.

F. All audio streams supplied from IP video servers shall be digitally encoded in g711 (u-law), g721, g723, or AAC compression formats and recorded simultaneously in real time.

G. Each camera's bit rate, frame rate, and resolution shall be set independently from other cameras in the system, and altering these settings shall not affect the recording and display settings of other cameras.

H. The VMS shall be able to use multiple CCTV keyboards to operate the entire set of cameras throughout the system, including brands of cameras from various manufacturers and including their PTZ functionalities (i.e.: Pelco keyboard controls Panasonic dome or vice-versa).

I. The VMS shall be able to retrieve and set the current position of PTZ cameras using XYZ coordinates.

J. The VMS shall support PTZ camera protocols from multiple manufacturers, including analog and IP protocols.

K. The VMS shall arbitrate the user conflict on PTZ usage based on user levels per camera.

L. The VMS shall support the following list of CCTV keyboard protocols:
1. American Dynamics 2078 ASCII, and American Dynamics 2088 ASCII
2. Bosch Autodome, Bosch Intuikey.
3. DVTel.
4. GE ImpactNet.
5. Panasonic, Pelco ASCII, Pelco KBD-300, and Pelco P.
6. Radionics.
7. Samsung SSC-1000.
8. Video alarm.

M. The VMS shall support the following list of joysticks and control keyboards:
1. Axis 295.
2. Axis T8310 Video Surveillance Control Board.
3. Panasonic WV-CU950 Ethernet keyboard.
4. Any USB joystick detected as a Windows Game Controller.

N. The VMS shall allow for the configuration of a time zone for each camera connected to a DVS. For playback review, users shall have the ability to search for video based on the following options:
1. Local time of the camera.
2. Local time of the SSM.
3. Local time of user’s workstation.
4. GMT Time.
5. Other time zone.

O. Audio and Video storage configuration for the SSM shall either be:
1. Internal or external IDE/SATA/SAS organized or not in a RAID configuration.
2. Internal or external SCSI/iSCSI/Fiber Channel organized or not in a RAID configuration.
3. Within the overall storage system, it shall be possible to include disks located on:
   a. External PCs on a LAN or WAN.
   b. Network Attached Servers (NAS) on a LAN or WAN.
   c. Storage Area Networks (SAN).

P. The SSM shall not limit the actual storage capacity configured per server.

Assumptions on the system:

The architecture is to be based on streams of 4Mbps, considering no multicast on the network to redistribute the streams to the workstations as worst case.

The servers are dimensioned for integration of Kiwi Security Analytics and the needed redirections of the streams to the dedicated servers from the archivers.

Where required, propose Survision cameras for ANPR as the custom integration in GSC is done through Genetec middleware ‘SmartDevice’ and enables the possibility to manage opening of gate, white list of plates, and investigation on plates captured.

Software proposition:

In terms of software, Security Center should consists of:

- Omnicast professional for required amount of camera connections
- Sipelia SIP Intercom management for required amount of intercom connections
- Mobile application client connections (@ required amounts)
- Security Desk and Web Client connections (@ required amounts)
- SDK connection for the integration with KIWI Security analytics and ANPR from Survision
- 1Y of SMA

On the side of analytics, the analytics package should consist of the following packages of Kiwi Security :

- Required amounts for Face Collector for 1 video channel (perpetual license). Automatically detects and extracts faces from a video stream.
- Required amounts for Intrusion Detector for 1 video channel (perpetual license). Automatically detects persons or vehicles intruding into critical areas. Includes weather filters.
- Required amounts of Privacy Protector for 1 video channel (perpetual license). Patented solution for privacy protected video surveillance by pixelization of humans and vehicles in real-time.
- 1Y Service Level Agreement on these analytics.

Servers and Workstations:

Zalando prefers Dell Hardware where allowance needs to be made for identical servers with embedded storage for the CCTV system and identical dedicated servers for the video analytics.
Each CCTV server is should be equipped with sufficient storage in RAID5 to cover the needed storage for all cameras for 1 month plus 15% over capacity.

Server configuration for CCTV:

- PowerEdge R730xd for Intel v4 CPUs
- Chassis with up to 12, 3.5" Hard Drives and 2, 2.5" Flex Bay Hard Drives
- Intel Xeon E5-2609 v4 1.7GHz
- 2x 8GB RDIMM, 2400MT/s,
- Windows Server 2012 R2, Standard Edition, 2 Socket, 2 VMs
- PERC H730 RAID Controller, 1GB NV Cache
- Required amount of 8TB 7.2K RPM SATA 6Gbps 512e 3.5in Hot-plug Hard Drive
- 2x 300GB 15K RPM SAS 12Gbps 512n 2.5in Flex Bay Hard Drive
- Dual, Hot-plug, Redundant Power Supply (1+1), 750W
- Broadcom 5720 QP 1Gb Network Daughter Card
- Broadcom 5720 DP 1Gb Network Interface Card
- Dell EMC QSYNC Bezel for PE R730XD
- ReadyRails™ Sliding Rails With Cable Management Arm

Server configuration for analytics

- PowerEdge R330 for Intel v6 CPUs
- 3Yr ProSupport and Next Business Day Onsite Service
- Dell EMC 1U Standard Bezel
- Intel Xeon E3-1220 v6 3.0GHz, 8M cache, 4C/4T, turbo (72W)
- 4x 8GB (1x8GB) 2400MT/s DDR4 ECC UDIMM
- 2400MT/s UDIMMs
- Performance Optimized
- 2x 300GB 10K RPM SAS 12Gbps 2.5in Hot-plug Hard Drive,3.5in HYB CARR
- DVD+/-RW, SATA, Internal
- Single, Hot-plug Power Supply, 350W
- ReadyRails™ Sliding Rails With Cable Management Arm
- Windows Server® 2016,Standard,16CORE

4.2. CAM – IP-Camera Technology

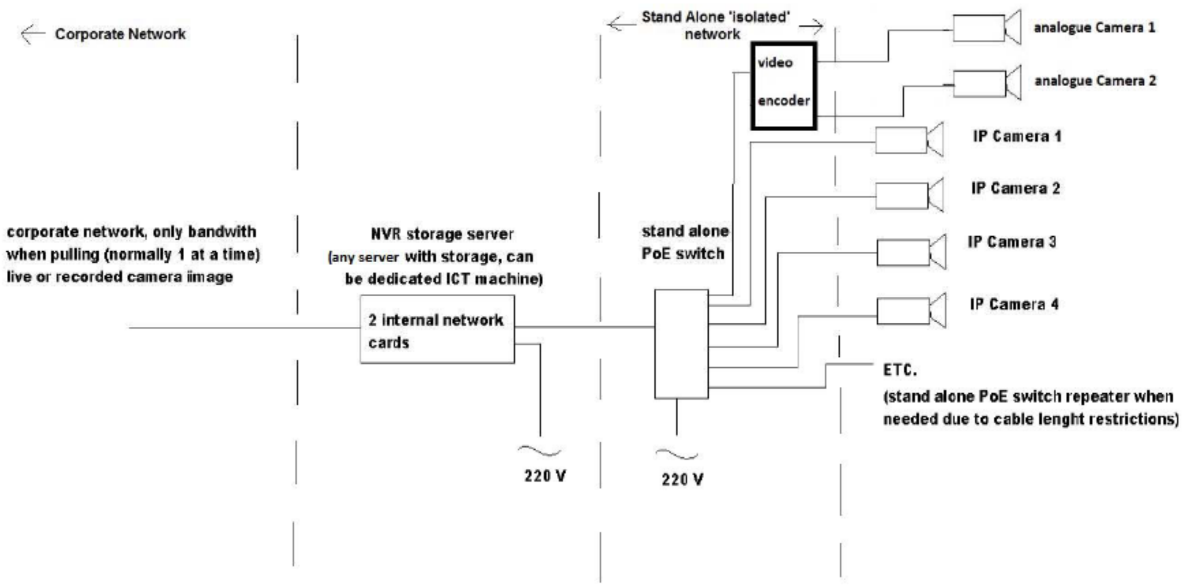
Each exterior door must be under the surveillance of an IP camera. This translates into one camera per door including the emergency exits. Also specific building areas such as reception-, security-, dock-, high value areas, MDF, IDF, etc. have to be supervised by cameras.

Installation Notes:

- As a standard one camera shall monitor one single door
- Under favorable circumstances one camera maybe can be used to view on multiple doors when those doors (or i.e. turnstile) installation are placed within an area of 4 meter wide.
- The IP camera needs to have a clear and full unobstructed view on the door(s).
- The entire door(s) surface must be captured by the lens of the camera
- Minimum Picture Quality Standard: The camera shall be positioned and pre-adjusted on such a way that the camera field of view allows recognizing or identifying a person which is passing through the door.
- Assembly height: minimum 10 feet / 3.00 meters above floor, below concrete or false ceiling
- Within hall areas with a ceiling higher than 13 feet / 4.00 meters a wall mount adaptor with a length of 5 feet / 1.50 meter shall be used to install the camera with the necessary distance to the door.
- The IP camera needs to have a minimal resolution of 1MP
- The IP camera must have day/night capability (true filters) where IR support may be required in areas where there is no permanent light support for the camera.
- External cameras need to have sufficient power for heaters, external suited housing (IP rated) and vandal proof housings
- Zalando security team may choose 360 degrees IP cameras or PTZ cameras where required

4.3. CAM – Network Architecture and using existing infrastructure

Standard on new installations, Zalando would require a CAT6/7 cable infrastructure to be delivered for the IP cameras. To prevent loading the Zalando network itself, the cable infrastructure for the IP cameras must be approached as a standalone network dedicated for these cameras. This network will be connected to the NIC of the recording unit, and the second NIC in the recording unit will be connected to the Zalando corporate network.
In this configuration the Zalando network bandwidth will only be used when from remote locations live or recorded video streams are reviewed. As this is typically one or a selection of few cameras the total bandwidth for these video stream over the Zalando network will stay minimal.


Corporate Network
Stand Alone 'isolated' network
video encoder
analogue Camera 1
analogue Camera 2
IP Camera 1
IP Camera 2
IP Camera 3
IP Camera 4
corporate network, only bandwith when pulling (normally 1 at a time) live or recorded camera image
NVR storage server (any server with storage, can be dedicated ICT machine)
2 internal network cards
stand alone PoE switch
ETC.
(stand alone PoE switch repeater when needed due to cable lenght restrictions)
220 V
220 V

In case Zalando has an existing analogue camera system and infrastructure which they want to upgrade to IP cameras (or utilize analogue cameras where they are still of sufficient quality), video Palun's or video convertors can be chosen, which i.e. can convert PoE network connections to coax and vice versa. This solution has the preference from Zalando to safe on having to replace the existing analogue camera infrastructure for a new network cable infrastructure. Naturally the existing cable infrastructure has to be of sufficient quality when utilized for a (converted) IP network infrastructure.

4.4. CAM – PoE Power Supply / PoE Switches for IP Cameras

Installation Notes:

- Network connection point for a camera will be connected to a standard (gigabit) PoE Switch which is normally installed and placed on one of the building IDF's.
- The Contractor has to provide a complete documentation of each planned IP camera (camera type, IP address data, etc.).
- The Contractor has to take over the full responsibility to confirm the IEEE 802.3af standard in connection with the camera, the PoE switch and cable between the camera and the PoE switch.
- The maximum distance between switch and camera is the same as the Ethernet standard, 295 feet / 90 meters
- The contractor has to allow for sufficient power per port in relation to the power consumption for each cameras (note external cameras or PTZ may consume more power because of the heaters on board or motors which create PTZ motion, a high PoE outlet may be required for those cameras)
- The power consumption of a standard IP camera with PoE Device Class 3 can be between 6,49 and 12,9 watts.
- In case an IP camera has higher power consumption as the standard (more than 15.4 watt /e.g. IP PTZ cameras) a High Power PoE Adaptor (Midspan) has to be connected between switch and camera.

4.5 CAM – General Installation Requirements for Internal IP Cameras

Installation Notes:

- Inlets to IP network cameras have to be carried out with RJ45 connection unities. RJ45 jack (female) by using a patch cable.
- Connected to the nearest MDF/IDF PoE Network Switch with RJ45 plug (male) via 19“ patch panel within network enclosure.
- Internal lighting must provide sufficient illumination to allow CCTV supervision; camera motion detection and post event investigation to work properly even at night. Visible lighting has an additional deterrent effect and is therefore recommended over IR lighting.
- By the connection of a camera on ceiling (e.g. concrete) the accessibility of the connection is to be guaranteed.
- All data cables for cameras and connection points (e.g. RJ45 connection unities) needed to support any part of the camera system that are located below a false ceiling, or are otherwise located below 10 feet / 3.2 meters must be <u>completely, not visible</u> contained within metal or hard plastic security conduit (rigid or flexible) for protection against mechanical impact, tamper or vandalism. Connection unities which are open accessibility have be protected by metal or hard plastic covers or boxes.

5. Installation Standards for Field Hardware – Intercom Technology (ICOM)

5.1. ICOM – Intercom Technology

An IP Intercom System shall be installed to provide a possibility for e.g. visitors to ask for access to specific exterior or interior building areas. The IP intercom may be used to allow visitor entrance by means of remote door release, but only when a visual verification can take place (video intercom in combination with line of sight at the remote released door) or where it concerns a low risk access (i.e. carpark entrance). The IP intercom must have the ability to interface with SIP / VOIP phones.
The preferred solution for Zalando is Stentofon

5.2. ICOM – Intercom Desk Station – i.e. Office Reception Desk

- Base intercom station as desktop version
- With gooseneck, handset or build in microphone
- With monitor when video intercoms are applied
- Built-in loudspeaker
- Interface keypad which can be used for:
  - to call multiple intercom stations in the system
  - to open the barriers, doors etc. (Note – required feature: Connection in line with an card reader interface output to ensure authorized opening of the barrier, door etc.).

5.3. ICOM – Intercom Door Station with Camera – i.e. Visitor Entrance

- IP door station module
- Color flush mount camera, 1/4" Interline CCD-Sensor
- Built-in microphone and loudspeaker
- Call button(s) module which shall be used to call the reception desk station and/or alternative desk station(s).

5.4. ICOM – Intercom Door Station without Camera – i.e. Visitor Exit

- IP door station module
- Built-in microphone and loudspeaker
- Call button module which shall be used to call the reception desk station and/or alternative desk station(s).

6. General Building Perimeter and Interior Requirements for Zalando Facilities

6.1. Access Controlled Rooms which are containing Critical Data – MDF Rooms.

As in Zalando the security risk lays mainly in their critical data, we have expanded on the physical security standards of the MDF rooms. The same may be applied i.e. IDF rooms.
NOTE: A Security Manager of Zalando has to be consulted for a proper design and construction of new MDF Rooms. The involvement of Zalando security is also required in connection with the upgrade of existing MDF Rooms to meet the standard requirements and the security level which is necessary to achieve.

6.2. Location of MDF Rooms

- All MDF Rooms should be located within the already existing and secured building perimeter of Zalando facilities.
- MDF Rooms should have dedicated access doors. They should not be part of the access route to other rooms.
- If a room is located in an area where there is vehicle movement (e.g. facing outside wall) the room must be protected against unintentional ramming by either sufficient wall construction or with posts.

6.3. MDF Room Entrance Doors (Access Controlled Doors)

- The door shall be break-in-resistant and rated at the fire rating required by insurers (minimum 60 minutes rating is recommended) and must bear the fire rating stamp.
- Where permitted, all entrance doors to the MDF should be configured as fail-secure. Access must be controlled. However, local codes will prevail. The architect should consider the location of the MDF, the position of the MDF doors, and egress paths to minimize the necessity of fail- safe egress scenarios involving the MDF.
- Locking hardware should be configured to permit free egress in the event of a fire emergency or similar emergency scenario.
- Automatic door closers are required on all doors with card readers, electric locking devices, and/or door contacts.
- For more details also see the Chapter: Electronic Access Control System (EACS).

6.4. External Walls of MDF Rooms

- Where sufficient standoff of vehicles cannot be guaranteed by the fence line and unauthorized vehicles could reach a critical infrastructure at ground floor level, the external walls must be constructed to withstand an attack using vehicles. The required thickness and reinforcement of the walls depends on the landscape, probable velocity and impact angle and assumed scenario in terms of used vehicles.
- External walls of MDF Rooms must provide sufficient resistance against intrusion. The resistance time must be balanced with detection capabilities and reaction time. As a rule of thumb, brick walls > 240mm and concrete walls > 200mm provide sufficient resistance.

- Supplementary strengthening to existing insufficient walls must be internally, slab to slab and can be achieved e.g. by fitting composite panels of sheet steel and compressed timber boards such as plywood or Stirling board. The timber boards must be glued to the steel sheets. The panels must be welded to fixed top and bottom steel channels and the panels must be welded together on the vertical butt joints. An example construction which would be sufficient as an external wall (i.e. where existing walls would provide near to zero resistance) is shown in the diagram below:

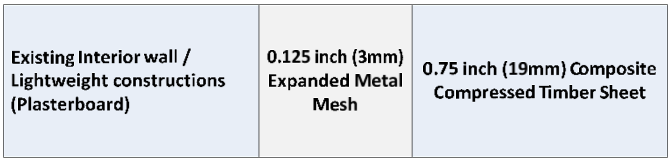
Existing Insufficient External Wall	0.125 inch (3mm) Steel	1.5 inch (38mm) Composite Compressed Timber Sheet	0.125 inch (3mm) Steel	1.5 inch (38mm) Composite Compressed Timber Sheet	0.125 inch (3mm) Steel

- Additionally to the supplementary strengthening the fact of existing insufficient walls is require that the complete surface inside of internal walls must be covered by DUAL motion detectors which have to be connected to the alarm system. Also lightweight constructions walls shall be supervised by cameras from the inside of the MDF Room to provide fast analytic options in case of a motion detection alarm.

6.5. Internal Walls of MDF Rooms

- Internal walls are walls around MDF Rooms or infrastructure components which cannot be accessed directly from outside of the building. Where internal walls around MDF rooms or infrastructure rooms can be accessed from third parties (e.g. other tenants) they have to be treated as external walls regarding intrusion protection.
- In general the recommended construction standards for internal walls are the use of the same measurements and materials as required in connection with external walls. In all other cases and as a minimum internal walls must provide the same resistance time as their entry doors.
- Lightweight constructions under use of e.g. plasterboard walls will require that supplementary strengthening must be fitted internally and run slab to slab. The strengthening could comprise panels constructed from expanded metal mesh such as expanded steel and composite compressed timber boards such as plywood or Stirling board. These panels would be screwed through to the main supporting pillars of the existing wall. The recommended grade of expanded metal mesh should confirm a maximum aperture size of 0.2 inch (50 mm) by 0.2 inch (50mm). Minimum diameter of bars shall be 0.12 inch (3mm).

- A possible composite construction is shown in the diagram below:



Existing Interior wall / Lightweight constructions (Plasterboard)

0.125 inch (3mm) Expanded Metal Mesh

0.75 inch (19mm) Composite Compressed Timber Sheet

- Additionally to the supplementary strengthening the use of lightweight constructions is require that the complete surface inside of internal walls must be covered by DUAL motion detectors which have to be connected to the alarm system. Also lightweight constructions walls shall be supervised by cameras from the inside of the MDF Room to provide fast analytic options in case of a motion detection alarm.

6.6. Apertures within Internal Walls of MDF Rooms

- Apertures with a free area greater than 20cm x 20cm must be closed. Where air condition ducts are fed through apertures they must be properly fixed such that they cannot be removed with simple tools (screw driver) or barred with steel bars inside.
- If apertures are required because of e.g. air ventilation reasons between the MDF Room and e.g. an air condition/climate room the apertures have to be secured with an expanded metal mesh. The recommended grade of expanded metal mesh should confirm a maximum aperture size of 0.2 inch (50 mm) by 0.2 inch (50mm). Minimum diameter of bars shall be 0.12 inch (3mm).
- For detection purposes, the complete metal mesh surface inside of the MDF Room area must be covered by DUAL motion detectors which have to be connected to the alarm system.

6.7. Roof Areas of MDF Rooms

- Roofs on ground floor levels or those roofs that are accessible from adjacent buildings must be treated as external walls.

7. Zalando Security Cabling Standard for the connection of Field Hardware

7.1. General Cabling Requirements

Security cable installation in in- and exterior areas has to follow local regulations and to confirm all Zalando in related standards (e.g. IT, Engineering, Security Standards) in relationship with:

- supply of cable
- laying with appropriate required distances, in combination with any mounting kits, in cable trays, suspended ceilings, raised floors or walls
- laying in cable tubes, pipes, conduits, channels, etc.
- break-troughs or drillings at walls
- installation in flush mount junction boxes
- installation in surface mounted junction boxes or cabinets
- complete documentation

All cables, wires and connection points (e.g. RJ45 connection unities) needed to support any part of the security systems that are located below a false ceiling, or are otherwise located below 10 feet / 3.2 meters must be completely, not visible contained within metal or hard plastic security conduit (rigid or flexible) for protection against mechanical impact, tamper or vandalism. Metal or hard plastic cable channel/trunking systems are only allowed if they can be closed, locked and sealed permanently to avoid unauthorized access to security cables.

All cables and wires of Physical Security - or Loss Prevention Systems must be separated from high power cables at any part of the cable route. Any signal interconnection which could cause a disturbance in the security system has to be prevented (e.g. installation of separation plank in cable trays, etc.).

With the exception like CCTV cameras or intercoms, no security cabling or wiring shall run on the exterior side of a facility.

Rebuild of fire prevention is incumbent upon the security contractor. (where cables need to pass walls etc. the fire protection needs to be restored after to its original specification)

Cable labels are to be carried out absolutely accordingly.

- Meeting Zalando naming convention

A measurement must be carried out to confirm the effectiveness of data lines.

- Complete measuring protocols have to be provided.

115V / 230V power supply connections for central equipment must be secured individually with a suitable breaker.

To all enclosure of the central equipment a potential balance with sufficient cable is to be intended.

Where junctions need to be made (to be prevented where possible, preference is to have single, non-interrupted cable runs), the junction needs to be soldered and protected with shrink sleeve when 2 cables are joined together, or alternatively a junction box needs to be installed when joining several cables. The junction box and its joints inside need to meet industry standards and cables inside needs to be clearly labeled.

7.2. Cable Types

Installation cable 6x2x0,6mm or 4x2x0,6mm (minimum 8 cores, AWG 18/22) as J-Y (ST) Y or freely of halogen J-H (ST) H standard.

- Use with intrusion detection system – motion detectors, magnetic door contacts, magnetic window contacts, distributor/junction boxes, etc.

Installation cable 10x2x0.6mm or 6x2x0.6mm (minimum 12 cores, AWG18/22) as J-Y (ST) Y or freely of halogen J-H (ST) H standard.

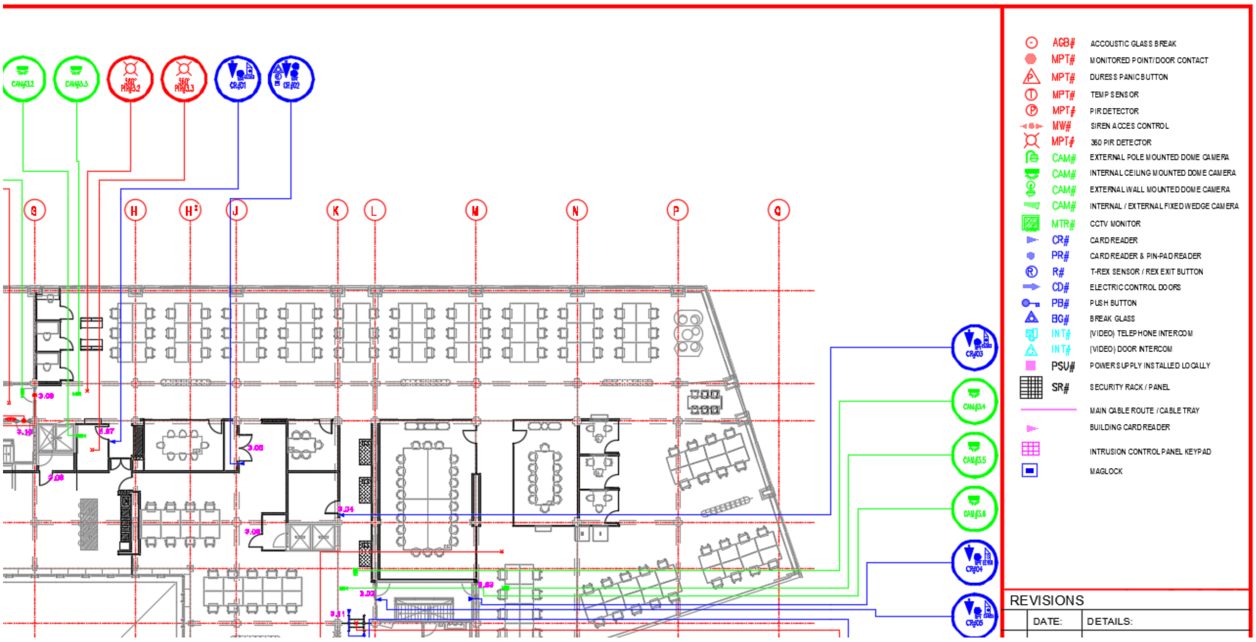
- Use with access control or escape doors – door distributor/junction box

Data cable .S/FTP 4x2xAWG23 (8 core AWG 18/22 for card reader is also possible)

- Use with Access Control – Card Reader - at most allowed segment length is 360 feet / 110 meters
- Use with IP Video – IP Camera - at most allowed segment length is 295 feet / 90 meters
- Use with VoIP - IP- Intercom - at most allowed segment length is 295 feet / 90 meters

8. Zalando AutoCAD Standards and typical design

Sample typical layout design


G
H
H'
J
K
L
M
N
P
Q
AGB# ACCOUSTIC GLASS BREAK
MPT# MONITORED POINT/DOOR CONTACT
MPT# DURESS PANIC BUTTON
MPT# TEMP SENSOR
MPT# PIR DETECTOR
MW# SIREN ACCES CONTROL
MPT# 360 PIR DETECTOR
CAM# EXTERNAL POLE MOUNTED DOME CAMERA
CAM# INTERNAL CEILING MOUNTED DOME CAMERA
CAM# EXTERNAL WALL MOUNTED DOME CAMERA
CAM# INTERNAL / EXTERNAL FIXED WEDGE CAMERA
MTR# CCTV MONITOR
CR# CARD READER
PR# CARD READER & PIN-PAD READER
R# T-REX SENSOR / REX EXIT BUTTON
CD# ELECTRIC CONTROL DOORS
PB# PUSH BUTTON
BG# BREAK GLASS
INT# (VIDEO) TELEPHONE INTERCOM
INT# (VIDEO) DOOR INTERCOM
PSU# POWER SUPPLY INSTALLED LOCALLY
SR# SECURITY RACK / PANEL
MAIN CABLE ROUTE / CABLE TRAY
BUILDING CARD READER
INTRUSION CONTROL PANEL KEYPAD
MAGLOCK
REVISIONS
DATE:
DETAILS:

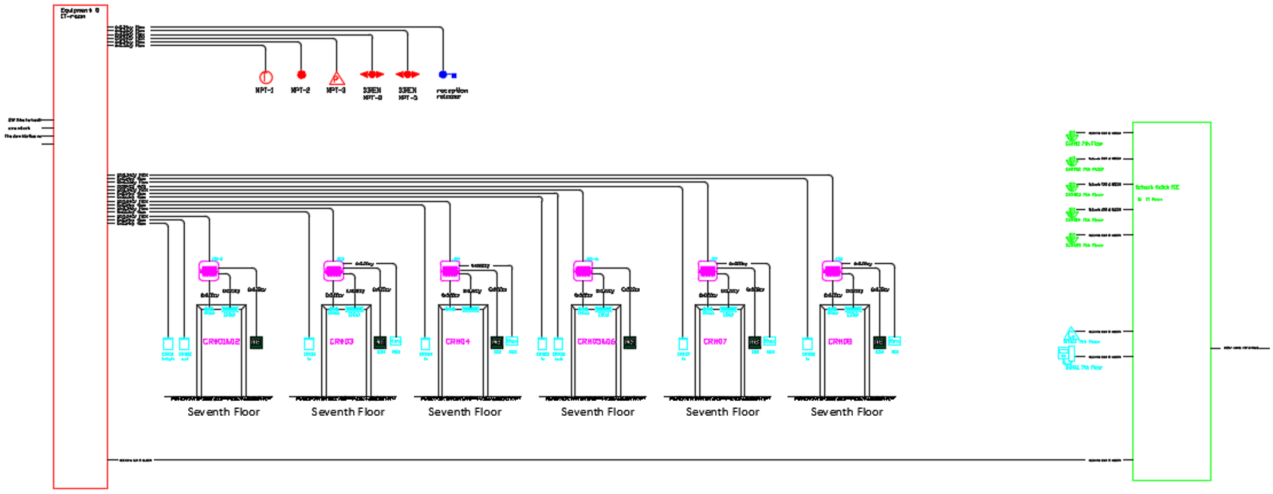
In a floorplan layout design drawing the following symbols and colors shall be shown:
Green circles and symbols represent the camera system
Blue circles and symbols represent the access system
Red circles and symbols represent the intrusion system
Magenta circles and symbols represent intercom system and general system items

A legend will be present indicating the symbols and what they represent

Typically Zalando will design the floorplan as follows:

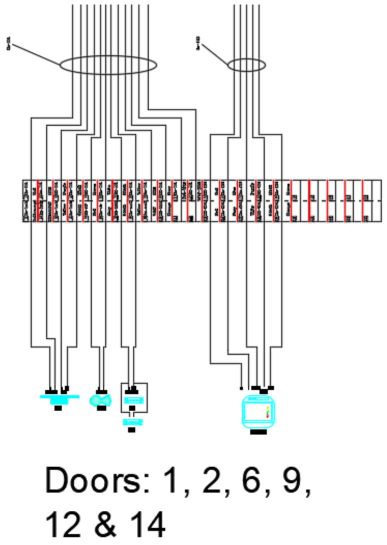
- Main traffic doors (or tourniquets) leading in/out of the main facility will receive an in and out reader (with anti-pass back enabled) to register people on and off the facility (also to have mustering reporting tools available).
- Internal traffic doors leading to higher secure zones will receive an in reader
- Internal doors to highest secure zones (e.g. MDF) will receive a in reader plus pin
- Each perimeter door which is not an access door will receive an door contact
- The access doors will receive a sounder which will sound upon door forced or held open; the monitored perimeter doors will receive a sounder which will sound when the door is opened
- All monitored perimeter doors and access doors leading to a higher security zone will be monitored by means of a camera (to identify who entered through that door)
- Perimeter may be monitored by means of external cameras
- Areas vulnerable to intrusion will be secured with intrusion detectors
- Main entrance doors for visitors which have access control will be equipped with a video intercom

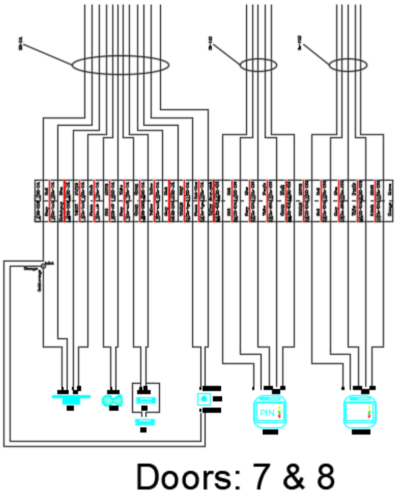
Sample generic system schematic



The generic cabling schematic will show the cable types and quantities which run between the main equipment and the field equipment

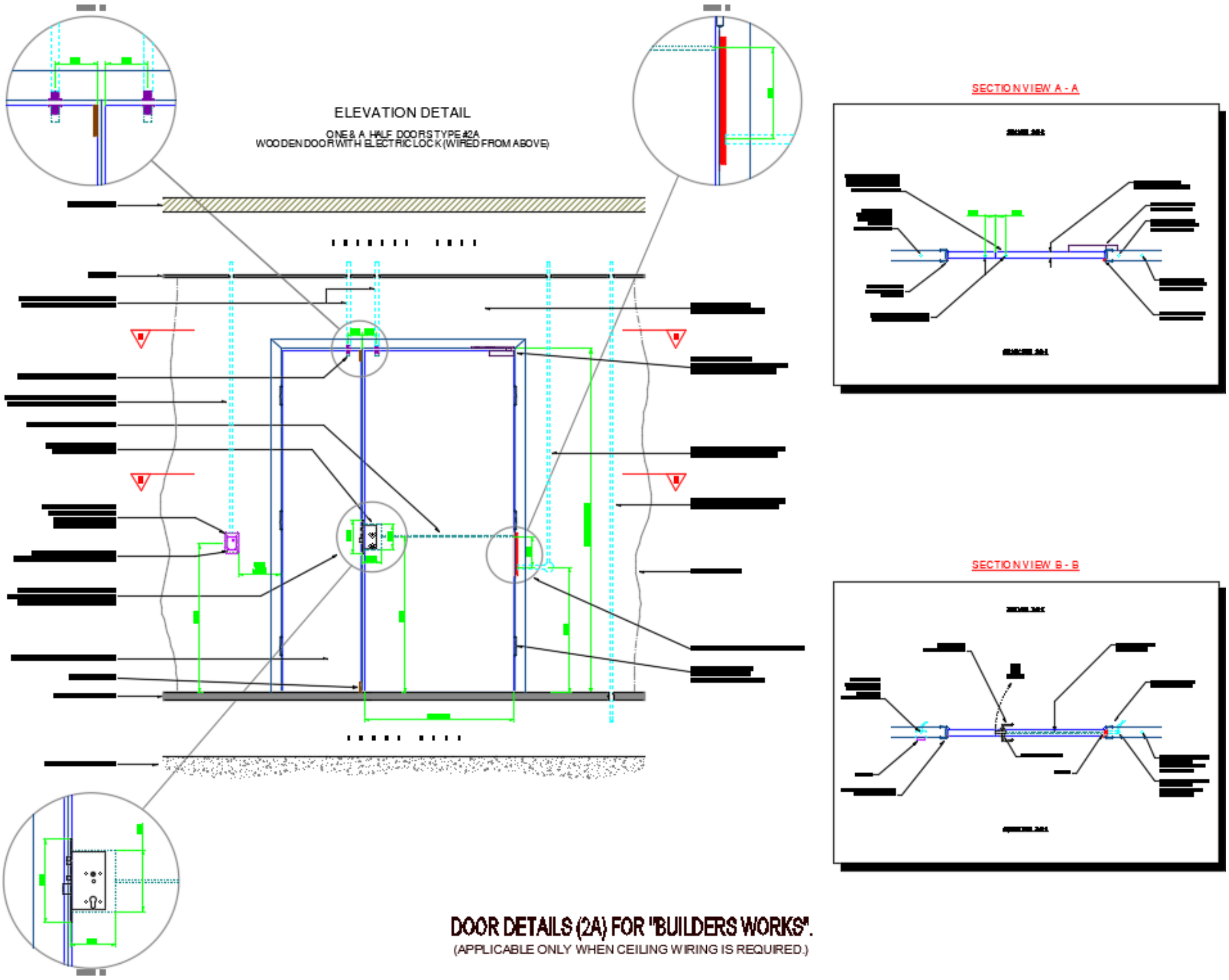
Sample detailed schematic





The detailed schematics will show wire termination details of devices to main equipment and/or cable junction boxes

Sample elevated door plans


ELEVATION DETAIL
ONE & A HALF DOORS TYPE #2A
WOODEN DOOR WITH ELECTRIC LOCK (WIRED FROM ABOVE)
SECTION VIEW A - A
SECTION VIEW B - B
DOOR DETAILS (2A) FOR "BUILDERS WORKS".
(APPLICABLE ONLY WHEN CEILING WIRING IS REQUIRED.)

The elevated door plans will show details of the equipment installed around a door, containing info such as mounting heights / distances etc.

This concludes the technical standards document. Please contact the Zalando security team on any unclarities for further explanation. This technical standards document will be under continuous review and may be adapted over time to the latest industry standards.