

**BRANCH:** Technical security

**THEME:** Concept of integrated safety system (PSIM) for  
QEMETICA production facility

# **1. General information**

## **1.1. Subject of the study**

The subject of the study is the development of the concept of an integrated security system (PSIM) for the QEMETICA production facility. The concept of the integrated security system includes:

- Description of the safety management system including its operating principle,
- Functional and conceptual description of the security system,
- Structural description of the security system including:
  - graphic application description,
  - layout description,
  - Description of object navigation (layout and action plans),
  - Description of procedures for actions and activities,
  - description of alarm events ( filter configurations and alarm priorities),
  - report description,
  - Description of authorization management mechanisms,
  - description of integration capabilities,
- Functional and conceptual description of the transportation service system (YMS),
- Structural description of the YMS system including:
  - graphic application description,
  - layout description,
  - Description of object navigation (layout and action plans),
  - Description of procedures for actions and activities,
  - description of alarm events ( filter configurations and alarm priorities),
  - report description,
  - Description of authorization management mechanisms,
  - description of integration capabilities,
- SSP integration description,
- Description of expansion and integration with CCTV,
- Description of expansion and integration with SKD,
- Description of expansion and integration with SSWiN,
- Description of expansion and integration with alarm broadcasting system,
- Description of expansion and integration with key management system,
- Description of integration with the PROMAN system,
- Description of integration with the TMS system,
- Description of integration with SAP,
- Description of security system equipment and YMS,
- Description of the limit devices of the above-mentioned security systems and YMS,
- A list of all equipment necessary for the proper operation of security systems and YMS, as well as their number and locations,
- Description of the construction and mechanical safeguards required to be implemented,
- Description of the necessary procedures and instructions for implementation,
- Functional requirements of the PSIM security management system.

## **1.2. Acronyms**

|                   |                                                                                                                |
|-------------------|----------------------------------------------------------------------------------------------------------------|
| VSS system        | - video surveillance system (video surveillance system) SSWIN                                                  |
| system            | - burglary and assault signaling system                                                                        |
| KD system         | - Access Control System T&A                                                                                    |
| System            | - working time registration                                                                                    |
| system SSP system | - fire alarm system                                                                                            |
| PSIM system       | - Security systems integration and management system (PSIM).<br>Physical Security Information Management PSIM) |
| YMS system        | - transport service system                                                                                     |
| AKPiA             | - control and measurement apparatus and automation                                                             |

## **2. Safety management system (PSIM)**

### **2.1. Operating principle of PSIM**

The security management system is a vendor-neutral, vendor-independent platform that allows full integration of different types of security, such as SKD, VSS, SSWIN, SSP, etc. The platform allows these systems to be operated, alarms to be processed and acknowledged from one or more central operating stations. This involves fully informing operating personnel of events by means of text, graphics, video preview, as well as providing guidance on countermeasures accompanying the presentation of the alarm message. Such information can be displayed on the screen, as well as printed. The platform is neutral to the systems it integrates. It functions on a plane independent of the manufacturers of the security systems it integrates. This means that any security system in a facility can be integrated with a security management system. The platform consists of a computer system that supervises and controls the actuators and integrated systems. An overarching control panel and, at the same time, a supervisory and control system is used to collect and protocol incoming alarms and any other information from the integrated subsystems. In addition, it prepares and transmits all necessary information to supervisory personnel or intervention services. The system supports the staff in the event of an alarm by performing the following functions:

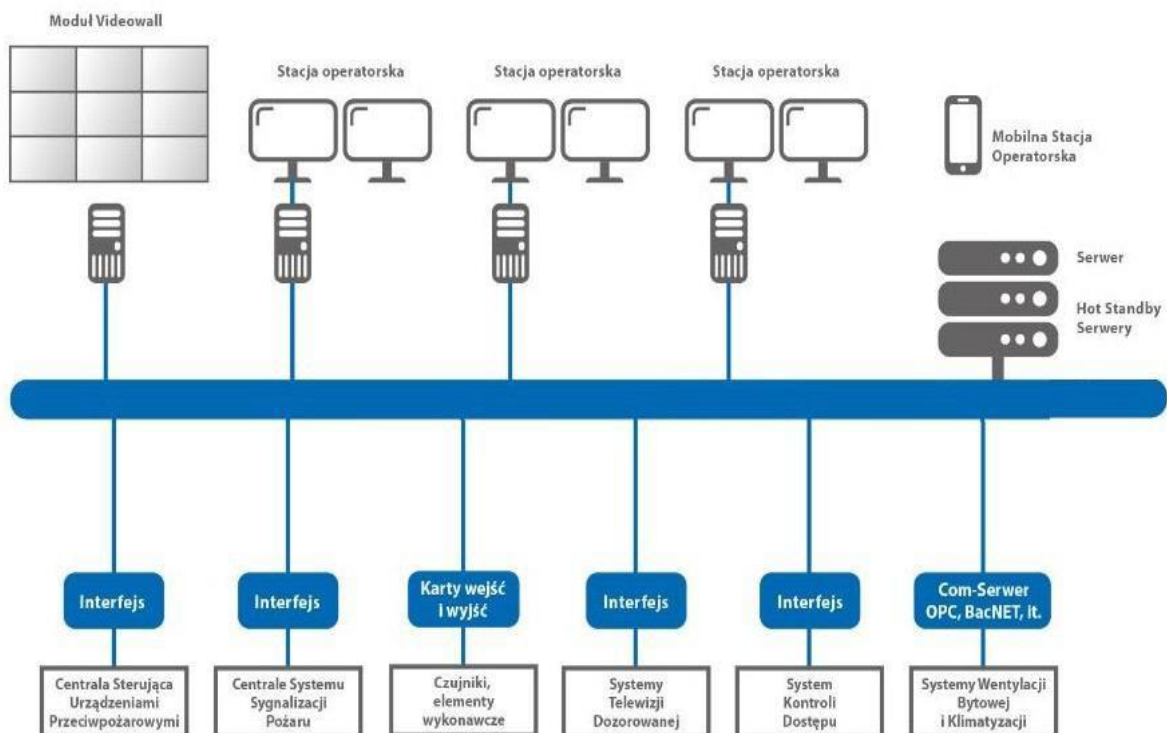
1. Early recognition of the threat with an alarm system,
2. Quickly inform the staff of the arrival of an alarm,
3. Provide proposals for actions and possible countermeasures appropriate to the type of threat,
4. Ordering the processing of events, taking into account the priority of the alarm,
5. Relieve staff of routine activities (background work),
6. automatic documentation of events,
7. Simplifying the operation of often very numerous technical systems and control panels,
8. Provide a graphical overview and detailed site plan including the location of sensors, access roads, evacuation routes, etc.,
9. automatic control devices security devices such as alarm sirens, cameras, etc. through the subsystem,
10. requesting confirmation of alarms by staff as well as taking action and documenting all actions.

The security management platform provides rational, decisive and seamless processing of all incoming information in the event of an emergency. Using an integrated graphical interface with prepared plans in the event of an alarm, the location of the alarm can be quickly located. By properly configuring the system, all data regarding the event, such as: evacuation routes, partitions, distances or evacuation zones, can be visualized, processed and transmitted to the emergency services. Technical data such as: sensor number, type of alarm, location of the event, address, rooms, etc. can be easily integrated in text format. Guidance for intervention services can be included in the text

or special notes describing the activities undertaken. You can use a list of responsible persons with up-to-date phone numbers or addresses, and reach for archived documentation, such as manuals, warranty cards, service logs.

## 2.2. Functional description of the PSIM system

The security systems integration and management platform has a client-server architecture. The entire system is installed on a central server, to which signals from all integrated systems and devices installed at a facility or group of facilities descend. Thanks to the client-server architecture, the operator can log into the system from anywhere, just a network connection to the server where the PSIM System is installed. This allows the creation of distributed systems managed from one central location. The system has a modular design allowing it to be freely expandable, modifiable and scalable in case of phased implementation or the need to integrate other external installations such as those related to production supervision areas. The safety management system collects and analyzes signals about the states of systems integrated with it. All integrations are implemented at the hardware level through interfaces with software that translates the protocol of the device in question, or through direct contact connection. The figure below shows an example of a conceptual diagram of the operation of a safety systems interference-management platform.



The system can be expanded to any number of workstations, The platform works in the form of a web browser hence it is possible to log into the system from anywhere in the building from any device (laptop, computer, PDA). Depending on the type of device from which the operator logs in, the type of rights assigned to the operator, individual operator stations are created, which allows, among other things, the creation of dedicated service stations.

Based on the site's security concept, the site's security regulations and the investor's requirements, a list of events and action procedures is established. "Events" are messages sent from integrated systems to the PSIM system. For each "event," different levels of importance are assigned depending on the message in question. To relieve the burden on PSIM operators, routine and statutory reports can be defined in the system so that they are automatically processed and logged without the involvement of operators. The event list can be dynamically modified at any time. When developing an event, the security systems integration and management system assists the operator not only with detailed situation plans with the alarming element in question, but also automatically executes defined procedures and guides through an algorithm for handling the situation. Among other things, the task of automatic operating procedures is to define links between subsystems in order to receive complete information from the alarmed location. The following are examples of automatic action procedures defined between systems:

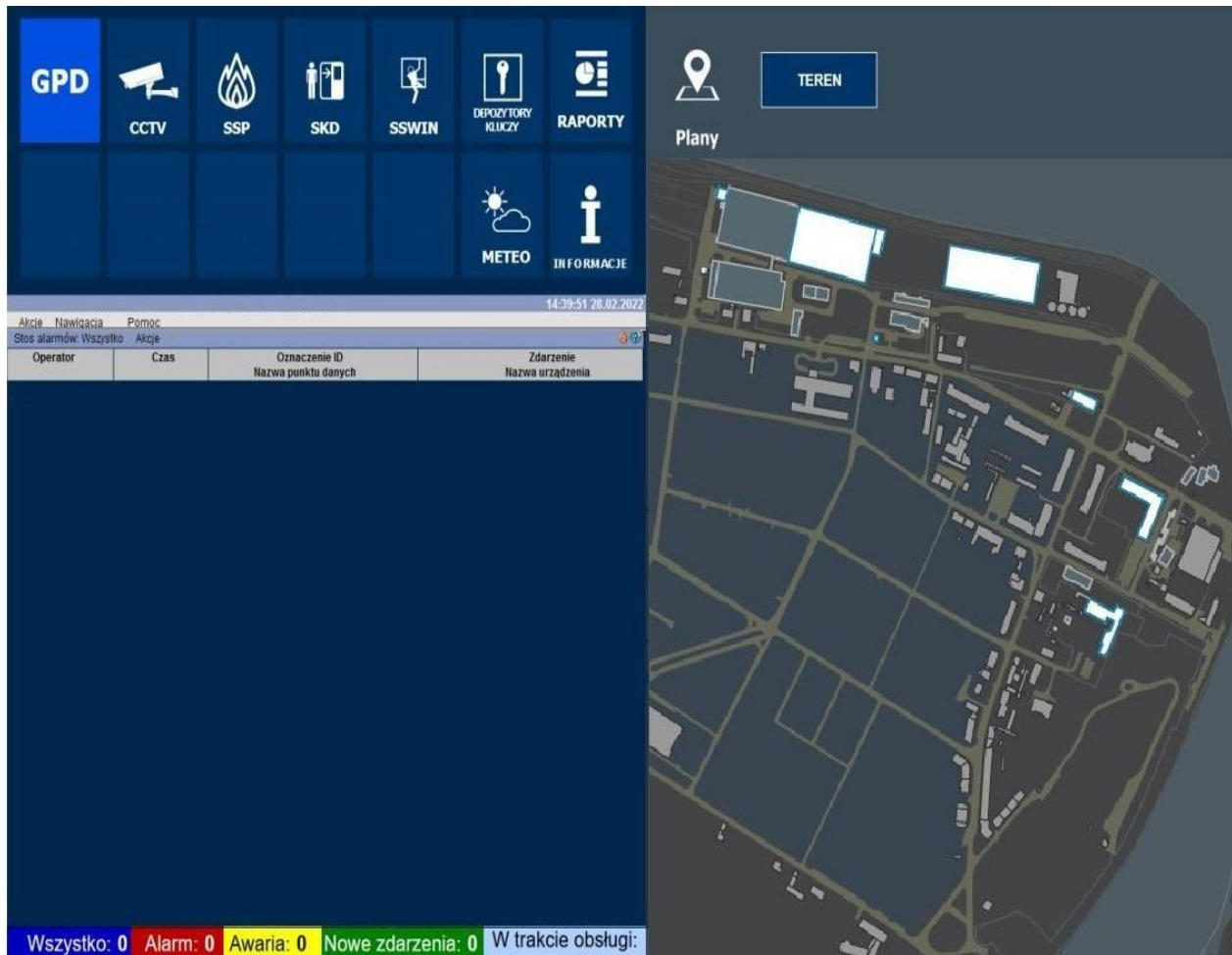
- In the event of an alarm from a passage supervised by the access control system, the monitor of the PSIM operator unit displays the image from the camera supervising the passage in question. The alarm may relate to a forcible entry, use of an unauthorized access card or leaving a door open.
- In the event of an alarm from the fire alarm system, the monitor of the PSIM operator unit displays the image from the surveillance camera of the particular zone where the alarm occurred.
- In the event of an alarm from an intrusion alarm system, the monitor of the PSIM operator unit displays the image from the surveillance camera of the area where the alarm occurred.
- In the event of an alarm from the fire alarm system, the passages supervised by the access control system located on the escape routes are released.

The PSIM system allows you to create multi-level access to the program for individual users. This gives you the ability to give appropriate privileges to individual users. From full control of the system through device control to event handling. The security systems integration and management system allows you to control integrated systems from the program level. By using the flexible capabilities of the system, the way the integrated systems are operated and monitored can be adapted to the knowledge and skill level of the operators. This allows a new employee to respond instantly and seamlessly in a critical situation.

### **2.3. Graphic application description**

The graphic application allows the use of the following types of graphics: bitmaps + SVG vector graphics - graphic plans, outlines or situation plans are presented in vector form, thus allowing the presentation of any scale, in the best way to support the intervention services. The sensors of the integrated systems are applied to the plans in layers, so the operator can fade out individual layers and supervise only those that interest him at the moment.

Sensors are represented by symbols of various arbitrary sizes and shapes. When an event occurs, the sensor changes its color to match the type of event. In addition to indicating the status with different colors and shapes, in addition, its most important data can be displayed for each sensor on the site plan.



The layout consists of two main windows. The first shows the main navigation menu and the alarm stack. The second features the site's floor plan. The navigation menu consists of freely configurable shortcuts most often referring to integrated security systems, reports or other information data. Underneath the navigation menu shortcuts, an alarm stack is displayed, which displays messages relating to occurring events.

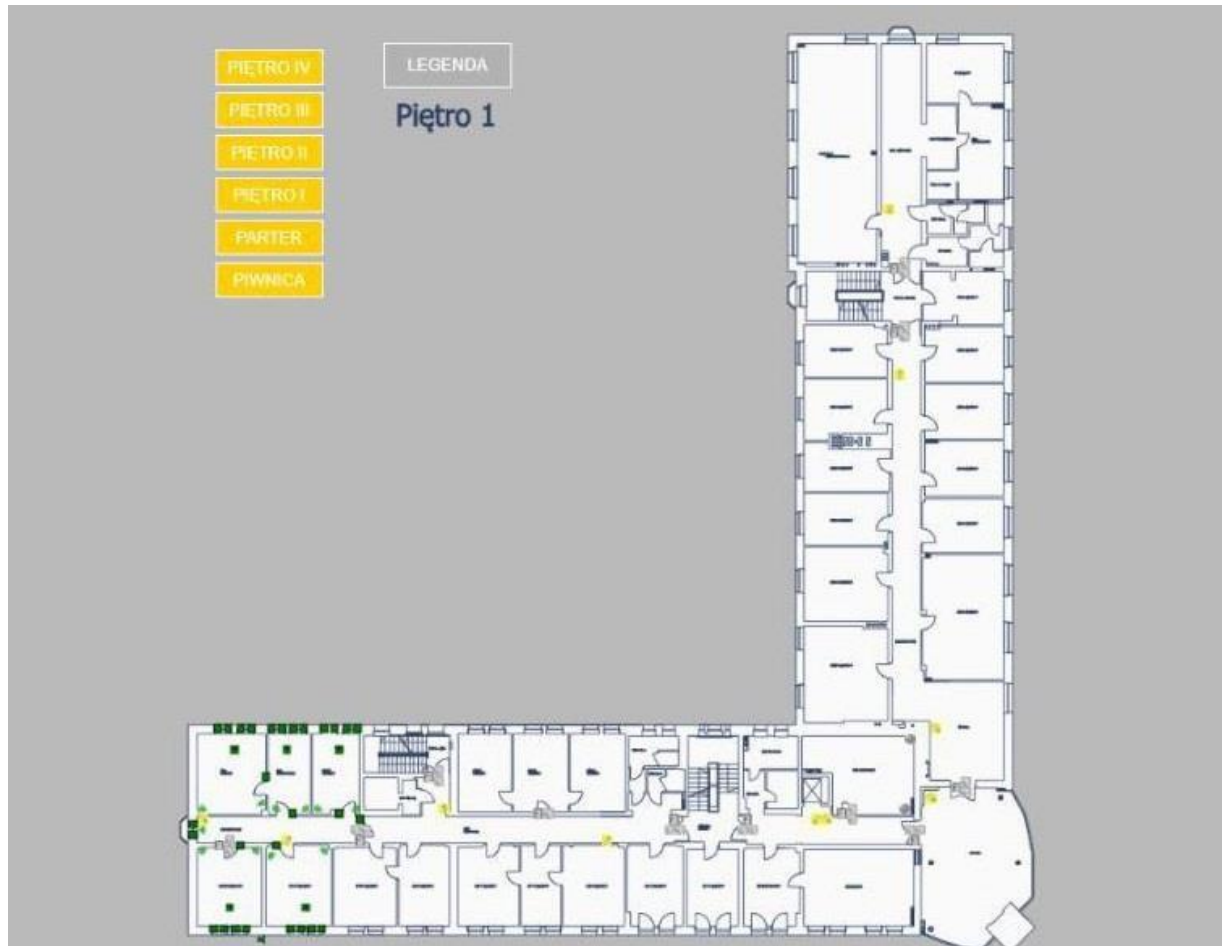
The navigation windows are differentiated for each operator. Depending on the level of authority held, a given user will have access to certain

security systems and data collected in the PSIM system. Authorization levels for user data should be determined at the system implementation stage.

Object navigation through the layout is performed by pressing given buttons in the navigation menu, events occurring in the alarm stack or objects in the site layout. In the case of the navigation menu, when you click on a given navigation shortcut, a window will be launched with the given security system, report or other function for which it has been configured. The window that will open when the selected button is pressed is freely configurable at the programming stage. This makes it possible to create any appearance of the window with the selected scheme or division of a particular security system.

If you select an event from the stack, a window with the alarm event in question will be launched. The window that will open when the selected alarm event is pressed is freely configurable at the programming stage. This makes it possible to create an appropriate algorithm for dealing with the occurrence of a given alarm event. In the case of navigation on the site plan, it can be done in several ways depending on the configuration at the system programming stage. It is possible to select an individual object or building from the navigation

plan, i.e. the plant map, or open a window with plans, where it will be possible to select the building whose plan is to be opened. After displaying an underlay of a particular building, it is possible to select a particular floor of the building and designate from which security system the elements are to be displayed. The next photo shows an example of a site plan view after selecting a building.



## 2.4. Description of emergency procedures and events

Procedure procedures are entered into the system as algorithms consisting of individual actions to be performed, which can be combined. Procedural algorithms contain not only the order and descriptions of the actions to be performed, but also phone numbers and details of the people to be notified.

The specific procedures to be implemented should be agreed with the developer at the system implementation stage.

A single action denotes a step to be performed, e.g. "send security to verify the alarm" or "notify the head of security." The same actions are repeated more than once when developing action procedures. To simplify the development of action procedures, such actions are entered only once and can be used repeatedly in action algorithms. The operator, through the action plan, is informed what action to take in the event of a specific event. To this end, the individual actions of the plan are clearly and transparently presented and must be effectively executed by the operator before the event can be removed from the alarm stacks. The individual actions with which the employee is familiarized can be either manual or automatic. Manual actions can include an additional text description detailing the task to be performed. The system, through an automatic action, can take designed actions on its own. Such an action could be to present an image from a camera that covers the location where the alarm event occurred, automatically unlock the door, automatically call the crisis center, send an sms or email message or send any acceptable control command to the external system.

The processing of an event involves a series of actions performed by the user. A list of these actions is displayed on the screen and includes the next steps of handling the event report depending on the type of threat. The set of steps can be designed by the administrator in a very elaborate version and automatic interactions of the integrated systems are possible. Selecting an event for processing, the user sees a situation plan with only the alarming sensor, its description, the time of receiving the alarm report and the previously described action procedure, as well as the automatic actions performed. When developing individual action plans, the operator gives the results of the performed actions. In addition, he can add a comment. The operator can interrupt the development of the event and resume it again. All information regarding the event and its elaboration is logged and archived in the system. An operator with the appropriate authorization can review the activities performed during an emergency event.

The alarm stack contains a list of events that have been received or their handling has not yet been completed - an example view below.

| Operator | Czas                | Nazwa punktu danych | Zdarzenie | Tekst zdarzenia | Nazwa urzadzzenia |
|----------|---------------------|---------------------|-----------|-----------------|-------------------|
|          | 14.02.2019 11:39:35 | Strona Lewa         | Alarm     |                 |                   |
|          | 14.02.2019 11:39:35 | Strona Lewa         | Alarm     |                 |                   |

Wszystko: 2

Alarm: 2

Awaria: 0

Sterowanie: 0

W trakcie obsługi: 0

Each occurring event is assigned to a category represented by the corresponding color. The event categories are voluntarily configurable, this makes it possible to set display priorities for given events depending on the categories in which they are located. This makes it easier to handle events related to alarms and failures, at which an immediate operator response is needed. Events are entered into the so-called alarm stack according to their assigned priority with an audible notification and displayed on the screen until the system operator finishes processing them. The displayed events can be sorted according to the time of occurrence of the alarm and the category in which the alarm is located. In addition, events occurring in the alarm stack can be sorted using user-defined filters.

## 2.5. Description of reports

The security systems integration and management platform automatically records information about incoming reports, procedures performed and operator comments. The historical data stored by the system can be reported and analyzed according to various criteria and printed on print forms.

The method of reporting to be implemented should be agreed with the developer at the system implementation stage. An example of the generated event report is shown below.

| Lp.     | Wpłynięcie zdarzenia | Nazwa punktu danych      | Komunikat(y)                                               | Przebieg                                                                     |
|---------|----------------------|--------------------------|------------------------------------------------------------|------------------------------------------------------------------------------|
| 1024696 | 23.04.2019 15:54:26  | POŁĄCZENIE Z INTERFEJSEM | Awaria('client did not connect'): POŁĄCZENIE Z INTERFEJSEM | 15:54:54 (MASTER) Obsługa rozpoczęta<br>15:54:55 (MASTER) Obsługa zakończona |
| 1024697 | 23.04.2019 15:54:26  | POŁĄCZENIE Z CENTRALĄ    | Awaria('client did not connect'): POŁĄCZENIE Z CENTRALĄ    | 15:54:49 (MASTER) Obsługa rozpoczęta<br>15:54:53 (MASTER) Obsługa zakończona |

Reports from the archive make it possible to assess the condition of the facility, quickly locate faults and make appropriate repairs. A simple and clear history of events (e.g., the number of reported fire hazards, failures), presented in the form of a graph for set periods of time, informs the administrator and service technician of the need to service a particular system. Various reports can be generated in the system depending on the operator's expectations. Reports can be generated manually and by using timed driving. Timed driving can be configured to generate a report of all events or events for specific categories or specified electronic security systems on specific days or every specified time. This makes it possible to regularly run reports on alarm events occurring in individual buildings or systems.

## 2.6. Description of authorization management mechanisms

The system has multi-level access to individual functions combined with authorization codes, which allows different levels of interference in the system (from full control, through control of devices, to handling events), but also identification of people and registration of their work. Below is an example of the system login screen.



Depending on the privileges granted, a given system operator can interfere with the security systems integration and management platform to a limited extent. Individual operator privileges are individually configured depending on the competencies and position of the individual employee. The user can be restricted in access to individual security systems. Examples of restrictions include access only to events affecting the alarm stack, access to ESBs occurring only in a given area, or inability to rip footage from the video surveillance system.

Individual users are identified in event and handling reports. This provides later verification of who handled an event, when they handled it, and whether they completed handling it.

## 2.7. Integration opportunities

The security systems integration and management platform is neutral to the systems it integrates, functioning on a plane independent of the manufacturers of the security systems it integrates. The platform integrates with the systems in question through a dedicated protocol or an open protocol.

Regardless of who manufactures a particular system, it can be integrated into a PSIM system. While comprehensive solutions with products from a single source simplify design and installation, they contain limitations, as not all vendors have the individual systems and equipment on offer. The ability to incorporate "third-party" (from different manufacturers) technologies is becoming an important criterion for selecting a PSIM system.

The following list shows examples of what systems from different manufacturers can currently be coupled with PSIM:

- systems signaling fire, burglary i systems alarming of danger,
- Surveillance TV (video matrix switchers with camera control, IP technology),
- Access control systems including RCP systems, key depositories,
- Communication systems, public address systems, DSO, intercoms,
- Controlling the work of guards,

- Elevators - status indicators and communication with the cabin,
- Paging systems - analog and digital alarm systems,
- electrical equipment, power switchgear,
- radio and telephone voice communication systems - the latter with automatic caller identification and location,
- time synchronization systems,
- control of gates and barriers,
- lighting control,
- Two-state control - automatic shutdown of equipment and machinery,
- Switching on exhaust or suction, control of flaps and ducts,
- Building and manufacturing automation systems.

To ensure the consistency of the database and the correct management of the PSIM system, install a system server with PSIM management software and database. Realize the server as a virtual server. Hardware resources for the server shall be secured by QEMETICA. The minimum requirements and technical parameters recommended by the manufacturer for the server are presented in the following section.

### 3. YMS transport service system

One of the more effective methods of minimizing potential threats to the security objective is the efficient management and verification of the authorization of persons and vehicles to enter, leave, stay on the premises of the Plant. Important in this process is the elimination of unauthorized granting of access and the authentication of the source ordering the granting of access.

In order to streamline the process of granting authorizations, it is recommended to implement software for avigation, management of the pass system and issuance of access control cards. It is also necessary to report the appointment of an Information Security Administrator to the General Inspector of Personal Data Protection for registration, and to fulfill the obligations under the provisions of the Personal Data Protection Act of August 29, 1997.

The software should meet the following requirements and handling algorithms:

- I. Charter of an external company
  1. System suitable for large amounts of data We store data min. 6 years.
  2. Creation of a Business Database
    - 2.1. Full company name
    - 2.2. NIP
  3. The place of generating the application - entering data
    - 3.1. By an External Company
      - 3.1.1. Data can be entered into the system directly by an external company - the site outside secured and encrypted with HTTPS protocol - secured with a login and password (at the stage of contracting, the QEMETICA inspector applies for a login and password, which is given by the system administrator)  
- certificate purchase.
    - 3.2. By QEMETICA Security Department
      - 3.2.1. Based on the data sent by an external company (in accordance with security requirements).
  4. Fields required on the application.
    - 4.1. Reference - assigned at the time of application registration
    - 4.2. Date of application - entered at the time of application registration
    - 4.3. External Data Entry Company -
      - 4.3.1. entered automatically by the system after logging in by a person from an external company authorized to enter data
      - 4.3.2. in the case of an application issued by the QEMETICA Security Department - a blank field
    - 4.4. External data entry person -
      - 4.4.1. entered automatically by the system after logging in by a person from an external company authorized to enter data
      - 4.4.2. in the case of issuing an application by the QEMETICA security department - a blank field
    - 4.5. QEMETICA department handling the contract
    - 4.6. Applicant Inspector QEMETICA -.

- 4.6.1. Selected from the book in the case of data entry by EXTERNAL COMPANY,
- 4.6.2. in case of data entry by QEMETICA Inspector - entered automatically by the system
- 4.7. Accepting manager - automatically assigned to the Department - automatically entered after selecting the department symbol.
- 4.8. Contractor - data of the company applying for the issuance of passes - drop-down menu. Company selected from the Company Database - entered by QEMETICA inspector.
- 4.9. QEMETICA contract number
- 4.10. Company name - Subcontractor if any, otherwise Contractor selected from the Company Database
- 4.11. Description of the work performed (from the contract)
- 4.12. Contact person from the company (who supervises the contractor)
- 4.13. Contact phone
- 4.14. From
- 4.15. To
- 4.16. Date of Tenant Acceptance
- 4.17. Date of approval QEMETICA Security Department
- 4.18. List of persons
  - 4.18.1. External company card number
  - 4.18.2. Card issue date
  - 4.18.3. Card return date
  - 4.18.4. Name
  - 4.18.5. Name
  - 4.18.6. Position
  - 4.18.7. ID Number - when creating an application, the system checks:
    - 4.18.7.1. Correctness of the Personal Identity Card Number
    - 4.18.7.2. Whether the person does not already have an EXTERNAL COMPANY or GUEST card issued 4.18.7.2.1. If the person has an active EXTERNAL COMPANY card
      - 4.18.7.2.1.1. for the person entering data from an external company- a pop-up window stating the person has an active card- contact QEMETICA Security Department and Checkbox- let the application through?
      - 4.18.7.2.1.2. For the person entering the data QEMETICA Security Department - a pop-up window with the information the person has an active card Check box - whether to add the card number to the new application? QEMETICA Security Department has the ability to check for which company the person works.
  - 4.18.8. Photo - if you do not attach photos to the application, a pop-up box will appear that reads DO NOT ADD ALL PHOTOS - APPLY WITHOUT PHOTOS WILL SIGNIFICANTLY PROLONG THE PROCESS OF ISSUING AN ACCESS CARD.
  - 4.18.9. Additional SKD access - multiple choice drop-down list - enters QEMETICA Security Department
  - 4.18.10. Comments
- 4.19. List of vehicles ( cars without registration no. Enter on permanent material passes)
  - 4.19.1. Entry permit number

- 4.19.2. Date of issuance of entry permit
- 4.19.3. Brand
- 4.19.4. Vehicle type - drop-down menu (delivery/truck, passenger, special, trailer/trailer)
- 4.19.5. Registration number (when creating an application, the system checks whether an entry permit has already been issued for the requested car)
  - 4.19.5.1. In case it was issued
    - 4.19.5.1.1. For the data entry from an external company - a pop-up window stating that an entry permit has been issued for the car - contact QEMETICA Security Department. QEMETICA Security Department has the ability to check for which company the car is driving.
    - 4.19.5.1.2. For the introducer of the QEMETICA Safety Department - a pop-up window indicating that an entry permit has been issued for a particular car. The inspector writes in the comments what company the car is driving for.
- 4.19.6. Justification for entry
- 4.19.7. Comments
- 4.20. List of people (foreigners)
  - 4.20.1. Card number EXTERNAL COMPANY
  - 4.20.2. Card issue date
  - 4.20.3. Card return date
  - 4.20.4. Name
  - 4.20.5. Name
  - 4.20.6. Type of identity document
  - 4.20.7. Identity document number
  - 4.20.8. Country of origin
  - 4.20.9. Photo in case of not attaching photos to the application a pop-up window stating NOT ADDED ALL PHOTOS - APPLY WITHOUT PHOTOS WILL SIGNIFICANTLY PROLONG THE PROCESS OF ISSUING AN ACCESS CARD.
  - 4.20.10. Additional SKD access - multiple choice drop-down list - entered by QEMETICA Inspector
  - 4.20.11. Comments
- 4.21. Comment
- 4.22. Number of EXTERNAL COMPANY passes issued including blocked and paid (based on company name)-with the ability to enter a (sortable) detailed report containing:
  - 4.22.1. Name
  - 4.22.2. Name
  - 4.22.3. Card number EXTERNAL COMPANY
  - 4.22.4. Status
  - 4.22.5. Card expiration date
  - 4.22.6. Signature - with a link to the application. The application can be opened only by the QEMETICA Security Department.
  - 4.22.7. The report should be able to be modified according to the set criteria.

- 4.23. Number of issued entry permits by passenger cars, vans/trucks, special vehicles (based on company name) - with the possibility to enter a (sortable) detailed report containing:
  - 4.23.1. Brand
  - 4.23.2. Registration No.
  - 4.23.3. Entry permit number
  - 4.23.4. Signature - with a link to the application. The application can be opened only by the QEMETICA Security Department.

The report should be able to be modified according to the set criteria
- 4.24. Number of EXTERNAL COMPANY passes issued to foreigners including blocked and paid (based on per company name) - with the ability to enter a (sortable) detailed report including
  - 4.24.1. Name
  - 4.24.2. Name
  - 4.24.3. Card number EXTERNAL COMPANY
  - 4.24.4. Status
  - 4.24.5. Card expiration date
  - 4.24.6. Signature - with a link to the application. The application can be opened only by the QEMETICA Security Department.
  - 4.24.7. The report should be able to be modified according to the set criteria
  - 4.24.8. Attach file
- 4.25. Attach file
5. Fields visible on the application when creating the application:
  - 5.1. In the case of data entry by an external company
    - 5.1.1. External company entering data - entered automatically by the system
    - 5.1.2. Person from external company entering data - entered automatically by the system
    - 5.1.3. QEMETICA department handling the contract
    - 5.1.4. Requesting QEMETICA Inspector - selected from the book
    - 5.1.5. QEMETICA contract number
    - 5.1.6. Company name - Subcontractor if any, otherwise Contractor selected from the Company Database
    - 5.1.7. Description of the work performed (from the contract)
    - 5.1.8. Contact person from the company (who supervises the contractor)
    - 5.1.9. Contact phone number
    - 5.1.10. From
    - 5.1.11. To
    - 5.1.12. List of persons
      - 5.1.12.1. Name
      - 5.1.12.2. Name
      - 5.1.12.3. Position
      - 5.1.12.4. ID Number - when creating an application, the system checks: 5.1.12.4.1. Correctness of the Personal ID Number

- 5.1.12.4.2. whether the person does not already have an EXTERNAL COMPANY or GUEST card issued
  - 5.1.12.4.2.1. If you have an active EXTERNAL COMPANY card.
    - 5.1.12.4.2.1.1. pop-up window stating the person has an active card - contact QEMETICA inspector and Check box - let the application through?
- 5.1.12.5. Photo in case of not attaching photos to the application a pop-up window stating NOT ADDED ALL PHOTOS - APPLY WITHOUT. PHOTOS WILL SIGNIFICANTLY PROLONG THE PROCESS OF ISSUING AN ACCESS CARD.
- 5.1.12.6. Comments
- 5.1.13. List of vehicles ( cars without registration no. Enter on permanent material passes)
  - 5.1.13.1. Brand
  - 5.1.13.2. Vehicle type - drop-down menu (delivery/truck, passenger, special, trailer/trailer)
  - 5.1.13.3. Registration number (when creating an application, the system checks whether an entry permit has already been issued for the requested car) In case a pop-up has been issued stating that an entry permit has been issued for the car - contact QEMETICA Security Department, which has the ability to check for which company the car is driving.
  - 5.1.13.4. Justification for entry
  - 5.1.13.5. Comments
- 5.1.14. List of people (foreigners)
  - 5.1.14.1. Name
  - 5.1.14.2. Name
  - 5.1.14.3. Type of identity document
  - 5.1.14.4. Identity document number
  - 5.1.14.5. Country of origin
  - 5.1.14.6. Photo in case of not attaching photos to the application a pop-up window stating NOT ADDED ALL PHOTOS - APPLY WITHOUT. PHOTOS WILL SIGNIFICANTLY PROLONG THE PROCESS OF ISSUING AN ACCESS CARD.
  - 5.1.14.7. Comments
- 5.1.15. Comment
- 5.2. Fields visible QEMETICA Security Department - has the ability to edit all fields when verifying data sent by an external company
  - 5.2.1. Signature - assigned at the time of registration of the application by the system.
  - 5.2.2. Date of issuance of the application - entered at the time of registration of the application by the system.
  - 5.2.3. External data entry company - if entered by the QEMETICA Security Department - blank. - not editable
  - 5.2.4. External company data entry person - in case of data entry by QEMETICA Security Department - blank field. - NOT editable.
    - Phone number of the person from the external company entering the data
  - 5.2.5. QEMETICA department handling the contract
  - 5.2.6. Requesting QEMETICA Inspector - entered automatically when QEMETICA Inspector enters data

- 5.2.7. Accepting manager - automatically assigned to the Department - automatically entered after selecting the department symbol
- 5.2.8. Contractor - data of the company applying for the issuance of passes - drop-down menu. Company selected from the company database
- 5.2.9. Contract number with QEMETICA
- 5.2.10. Company name - Subcontractor if any, otherwise Contractor selected from the Company Database
- 5.2.11. Description of the work performed (from the contract)
- 5.2.12. Contact person from the company (who supervises the contractor)
- 5.2.13. Contact phone
- 5.2.14. From
- 5.2.15. To
- 5.2.16. List of persons
  - 5.2.16.1. Name
  - 5.2.16.2. Name
  - 5.2.16.3. post
  - 5.2.16.4. ID Number - when creating an application, the system checks: 5.2.16.4.1. Correctness of the Personal ID Number
    - 5.2.16.4.2. whether the person does not already have an EXTERNAL COMPANY or GUEST card issued
      - 5.2.16.4.2.1. If you have an active EXTERNAL COMPANY card.
        - 5.2.16.4.2.1.1. A pop-up window with the information the person has an active card Checkbox - whether to add the card number to the new application?
  - 5.2.16.5. Photo - if you don't attach photos to the application, a pop-up window will appear that reads NOT ALL PHOTOS ADDED - APPLYING WITHOUT PHOTOS WILL IMMEDIATELY DELAY THE ACCESS CARD ISSUANCE PROCESS.
  - 5.2.16.6. Additional SKD access -from a multiple choice drop-down list
  - 5.2.16.7. Comments
- 5.2.17. List of vehicles ( cars without registration no. Enter on permanent material passes)
  - 5.2.17.1. Brand
  - 5.2.17.2. Vehicle type - drop-down menu (delivery/truck, passenger, special, trailer/trailer)
  - 5.2.17.3. Registration number (when creating an application, the system checks whether an entry permit has already been issued for the requested car) In case it has been issued - a pop-up window informs that an entry permit has been issued for the car) QEMETICA Security Department has the ability to check for which company the car is driving.
  - 5.2.17.4. Justification for entry
  - 5.2.17.5. Comments
- 5.2.18. List of people (foreigners)
  - 5.2.18.1. Name
  - 5.2.18.2. Name

- 5.2.18.3. Type of identity document
- 5.2.18.4. Identity document number

- 5.2.18.5. Country of origin
- 5.2.18.6. Photo - if you don't attach photos to the application, a pop-up window will appear that reads NOT ALL PHOTOS ADDED - APPLYING WITHOUT PHOTOS WILL IMMEDIATELY DELAY THE ACCESS CARD ISSUANCE PROCESS.
- 5.2.18.7. Additional SKD access - from a multiple choice drop-down list
- 5.2.18.8. Comments
- 5.2.19. Comment
- 5.2.20. Number of EXTERNAL COMPANY passes issued including blocked and paid (based on company name)-with the ability to enter a (sortable) detailed report containing:
  - 5.2.20.1. Name
  - 5.2.20.2. Name
  - 5.2.20.3. Card number EXTERNAL COMPANY
  - 5.2.20.4. Status
  - 5.2.20.5. Card expiration date
  - 5.2.20.6. Reference with link to the application. Request openable only to the QEMETICA Inspector who issued it.  
The report should be editable
- 5.2.21. Number of issued entry permits by passenger cars, vans/trucks, special vehicles (based on company name)-with the possibility to enter a (sortable) detailed report containing:
  - 5.2.21.1. Brand
  - 5.2.21.2. Registration No.
  - 5.2.21.3. Entry permit number
  - 5.2.21.4. Reference with link to the application. Request openable only to the QEMETICA Inspector who issued it.  
The report should be editable
- 5.2.22. Number of EXTERNAL COMPANY passes issued to foreigners including blocked and paid (based on company name)-with the ability to enter a (sortable) detailed report including
  - 5.2.22.1. Name
  - 5.2.22.2. Name
  - 5.2.22.3. Card number EXTERNAL COMPANY
  - 5.2.22.4. Status
  - 5.2.22.5. Card expiration date
  - 5.2.22.6. Reference with link to the application. Request only openable to the QEMETICA inspector who issued it  
The report should be editable
- 5.2.23. Attach file
- 6. QEMETICA inspector
  - 6.1. Has the ability to edit all fields when creating an application
  - 6.2. When establishing a replacement - he delegates his authority to the replacement person.
  - 6.3. Notifies the process administrator of the company's entry into the Company Database
  - 6.4. Requests company login and password - when signing contract for work

- 6.5. Enters authorizations for areas covered by SKD - multiple choice field
- 6.6. Extends the expiration date of EXTERNAL COMPANY cards and entry permits
  - 6.6.1. Date pop-up window
- 6.7. Has an overview of the number of passes and entry permits issued for the Company
- 6.8. Requests expansion of authority (including approval path).
- 6.9. Does not see applications that have been completed
- 7. Issuing cards
  - 7.1. The cards are issued one at a time against a legible receipt on a digital tablet after verifying that the data matches the ID Card.
    - 7.1.1. Confirmation of receipt of the card is entered into the system
  - 7.2. The Pass Office has the ability to display the list of cards to be issued alphabetically or by companies
  - 7.3. The process of manufacturing cards EXTERNAL COMPANY.
    - 7.3.1. Scan the ID card or manually search for the person on the list
    - 7.3.2. Open the window with details
    - 7.3.3. Checking the data with the ID card
    - 7.3.4. Entering the provided photo in electronic form
    - 7.3.5. Print preview of the card - possibility to make minor editorial corrections
    - 7.3.6. Assigning a card to a person - scanning on the card reader (assign card number button)
      - 7.3.6.1. The card number appears on the print preview
    - 7.3.7. Printing a card sticker
    - 7.3.8. Putting a sticker on the card
    - 7.3.9. Re-scanning the card on the card reader - the card is unlocked and privileges are granted.
    - 7.3.10. Acknowledgement of receipt of card, familiarization with personal traffic regulations with signature of recipient on digital signature tablet
      - 7.3.10.1. Confirmation is saved in the program
        - 7.3.10.1.1. Ability to print a pass receipt
    - 7.3.11. Card issue
  - 7.4. 2 card making stations
  - 7.5. The system must be able to change the position and continue the card issuance process that has been started.
- 8. Entry permits
  - 8.1. printed from the program
  - 8.2. is received by the person who is indicated in the application as supervisor - on behalf of the company
    - 8.2.1. acknowledges receipt with a legible signature on the tablet
- 9. Card statuses
 

The system automatically changes the statuses next to the card

  - 9.1. To be issued free (the card is blocked)
  - 9.2. In preparation (blocked, but something is happening with it)
  - 9.3. Released (unlocked)

- 9.4. Locked 9.4.1.locked
  - manually
  - 9.4.2. Blocked - late application - blocks the system
  - 9.4.3. Blocked - lost, not returned - blocked manually by the process administrator, shift commander and/or system operator (necessary to write in the comment the reason for blocking the card)
  - 9.4.4. Paid
- 10. Manual card blocking
  - From card list
  - 10.1. Process administrator
  - 10.2. System operator, Shift Commander - need to enter a comment
- 11. Card blocking by the system
  - 11.1. After the deadline
- 12. Unlocking manually blocked cards (it is not possible to unlock cards blocked by the system)
  - From the list of cards
  - 12.1. Process administrator
  - 12.2. Process operator, Shift Commander - only cards blocked by himself
- 13. Damaged cards
  - 13.1. Paid
  - 13.2. Not the fault of the user - QEMETICA Security Department decides
- 14. Return of the card
  - 14.1. Scanning on the card reader - the privileges come off the card, the status changes to free to issue, the card is blocked, the person is released
  - 14.2. Ability to print confirmation of card return
    - 14.2.1. Individual
    - 14.2.2. Collective - per company
  - 14.3. Peeling off and destroying stickers
- 15. Renewal of entry cards and permits
  - 15.1. Mail to QEMETICA Inspector about upcoming expiration date of cards
  - 15.2. QEMETICA Inspector's renewal of application
    - 15.2.1. A pop-up window confirming the expiration date for card changes
  - 15.3. Assigning a new term to the application after approval by superiors
    - 15.3.1. EXTERNAL COMPANY cards renew automatically
    - 15.3.2. Printing a new entry permit - at the Security Post
- 16. Random blocking by the system to check by the guard whether the card belongs to the person using it
- 17. Blacklisted vehicles
  - 17.1. Blacklisted vehicles are not allowed into QEMETICA premises
- 18. Reports
  - Reports should be fully editable
  - The system should be able to create new complex reports.

- 18.1. QEMETICA inspector - lists of passes and entry permits issued
- 18.2. Card history
- 18.3. Search engine
- 19. Security post
  - 19.1. All employees log into named accounts
  - 19.2. Has access to all data only until the card is issued
  - 19.3. After the card is issued, he sees:
    - 19.3.1. Card number
    - 19.3.2. Who issued
    - 19.3.3. Release date
    - 19.3.4. Surname and first name
    - 19.3.5. Company
- 20. Process administrator
  - 20.1. must be able to easily edit the content of the form in each step of the process.
  - 20.2. Manages the list of users of the web portal
    - 20.2.1. Name
    - 20.2.2. Name
    - 20.2.3. Login
    - 20.2.4. Password
    - 20.2.5. Phone number
    - 20.2.6. Company - selected from the Company Database
  - 20.3. Has the ability to set up a replacement, QEMETICA inspector - with the approval of the immediate supervisor
  - 20.4. It has the ability to change the QEMETICA inspector in applications that are active.
  - 20.5. Manages the Company Database
    - The Company Database is supplemented at the request of the QEMETICA Inspector
    - 20.5.1. Full company name
    - 20.5.2. NIP
- 21. Termination date of the contract
  - 21.1. Applications may be renewed if the contract term has been changed
  - 21.2. It is not possible to change the number of a contract that has ended
    - 21.2.1. At the end of the contract term, the third-party company must return the access cards - it is not possible to renew the access cards on a new contract.
    - 21.2.2. If a new contract has been signed, a new application must be issued.
- 22. Additional SKD access
  - 22.1. After approval by the QEMETICA Security Department, the application goes to the area's subject matter administrator, who decides whether to grant authorizations
- II. Guest card
  - 1. The system will have the ability to set access groups
    - 1.1. Assignment of rights

After-hours posts issuing a GUEST card select a destination from a drop-down list - the system automatically adds the permissions necessary for the stakeholder and unlocks the card.

2. The card entitles the visitor to pass through the gate only one way, at the exit the card is collected by the guard and the visitor is released.
3. Entry permits (mandatory safety training is provided for drivers and visitors entering the site for the first time).
  - 3.1. printed from the system at the Security Post
  - 3.2. written out by hand in posts

III. Health and Safety Training

- a. The system will have the ability to implement a health and safety training application
- b. The training will consist of watching an instructional video and passing a test on health and safety news
- c. A positive result on the health and safety knowledge test is a prerequisite for being authorized to enter the site. In addition to health and safety training, it is also necessary to obtain other approvals and pass the full verification procedure provided for in the system
- d. The training can be done remotely during the process of avification and requesting entry/entry authorization to the site
- e. An OSH training order can be issued by the person reviewing the application for access to the Plant during the avocation process. In such a case, the person receives a dedicated OSH training order number before entering the Site, which he/she enters in the application, using the OSH multimedia kiosk. After passing the OHS test, the information is transferred to the system's database and an authorization to enter the Site is granted
- f. If further periodic training is required, the access card user brings the card close to the OSH multimedia reader for identification, and then undergoes the OSH training procedure. Upon its successful completion, access privileges are automatically granted to that user

### **3.1 Functional description of the system**

The transport service system is an advanced system for supervising processes and transport vehicles on the plant site. The system significantly improves the management of deliveries, increases efficiency and facilitates the control of vehicle traffic prevailing on the site. Centralized management of transport orders in the application facilitates and speeds up communication and helps eliminate errors resulting from time-consuming and complicated exchange of delivery information. Advanced delivery scheduling makes it possible to equalize warehouse loads and eliminate car queues in front of the plant. Precise scheduling of vehicle loading and unloading dates, allows optimal use of existing company resources and minimizes long waiting times for service. Transparent visualization of transport stages in warehouses and loading docks allows efficient control of vehicle traffic on the site. Built-in reporting allows you to get detailed information about the tasks carried out during the visit or the time of transport execution. The platform uses solutions from the field of information technology and logistics, and thus supports the planning of loading and unloading. It contributes to the ordering of traffic and more efficient handling of suppliers through: registrations

and control of vehicles on a per-target basis with assigned driver instructions, recording the history of activities performed on the company's premises for reporting purposes, and coordinating waiting time and access to storage ramps and other activities performed before unloading and loading.

The functionality of the system based on operator-friendly solutions and adapted to the needs, requirements and specifications of the facility. The main features of the system include:

- Arranging vehicle traffic on the site,
- Advanced reports and statistics,
- Reduction of generated service costs,
- Complete elimination of fraud.

The transport service system works by integrating with logistics systems and a platform for managing and controlling electronic security systems. Integration with logistics systems provides exchange of information on planned trips and data of drivers, vehicles which arrive at the site. Systems operating at weighing points send information to the transport service system regarding the tare of vehicles. Systems operating at warehouses and loading points send information and data regarding the unloading and loading process. The integration with the management-control platform allows for the exchange of information regarding vehicles entering and leaving the internal area of the plant, through the cameras used at the entrance gate for recognition of license plates and application of the access control system. The system, after analyzing all the data received, sends information to the PSIM system about permitting or blocking a particular transport vehicle. The PSIM system transmits the information to the access control system unit at the respective security post supervising the exit gate. A message is displayed to the operator that a particular vehicle is allowed to leave or not allowed to leave with a brief description of why the vehicle cannot leave the premises.

The transportation service system application consists of several modules, which can be freely configured at the design stage, depending on the user's needs. The first of the modules is delivery planning. The module allows you to enter a new advisory transport in case a particular transport has not been sent by the logistics systems. The scheduling module functions so that it is possible to plan the various stages of transport service and check the occupancy of the various sites used during the transport stage. The information module presents data on advisory processes. It displays messages about the number of started, pending, completed advisory processes. Depending on the rights held by the operator, it will be possible to determine which modules a particular user has access to. Distinguishing between the administrator, who has access to entire resources, and individual employees, who have access to several or only one module of the application.

A complementary element of the transport service system are the advising points otherwise known as advising kiosks. Advising kiosks provide an opportunity to confirm the arrival of a given transport. The driver, upon arriving at the site, is required to enter his or her authorization number. This is followed by a display of information regarding the transport in question, which the driver must confirm or, in the event of an error, make a correction. After

The arrival approval displays information regarding the possibility of a particular driver entering the loading area. In case the information about the arrival of a transport has not been provided by the logistics systems, the driver can enter a new transport himself by filling in all the necessary data about the transport, driver, vehicle and trailer. The transport handling system sends information regarding the manually entered transport to the logistics systems. In the event that a particular carrier requires information regarding a transport, the driver's advisory kiosk will allow documents to be scanned. The documents will be archived and assigned to individual advisory numbers.

Each transport, located in the internal area of an industrial plant, should be recorded and registered in the transport handling system. The data that should be collected and created in the transport handling system can be voluntarily configured at the system implementation stage taking into account the possibility of transferring information between systems. The basic information functioning in the system includes:

- Transport number and date of creation,
- Current status of transportation,
- Planned arrival date,
- Deadline for arrival at the checkpoint,
- Magazine,
- Type ( unloading, loading or unloading/loading)
- Material group (in the case of combined transportation separately for loading and unloading),
- Carrier data (carrier number, name, e-mail address),
- driver and vehicle data (name, phone number, vehicle registration number, trailer type, packaging (full),
- Vehicle verification information at the time of departure (driver's name, type and number of identity document),
- Delivery information, which includes transportation,
- assigned loading and unloading gate (in the case of combined transport separately for loading and unloading),
- comments added by operators.

### **3.2 Graphic structure of the system**

The first view of the graphical structure is the login window, where you need to write out the login and password. If the time to change the password is approaching, the operator's data will be displayed with a password expiration message and the number of days until password expiration. The operator will be able to skip this process or change the password. After the operator completes the login stage, the main window of the system will be displayed.

The main panel view consists of individual categories displayed as graphic buttons. When a given button is pressed, a graphical view of a given subcategory of the system will be displayed on the screen. Categories in the transport service system can be voluntarily configured at the system implementation stage, depending on the customer's needs. Depending on the authority of a given operator, it is possible to limit accessibility to particular categories. Basic categories include:

- Schedule,

- List of advisory orders,
- Reports,
- Operators,
- Current statuses

Each window of a particular category can be voluntarily configured at the stage of implementation of the system according to the customer's needs. The view can be arranged in the form of a list with individual data or in graphical form. The appearance of a particular category should be configured in such a way as to illustrate the processes occurring in the transport service system in the simplest possible way. The appearance of the application should be clear and transparent for operators.

### **3.3 Description of procedures to be followed**

Procedures of operation in the transport service system should be based on algorithms that improve the processes of handling transport vehicles residing on the premises of production plants. In order to create appropriate procedures of conduct and algorithms of operation, the system must have the ability to exchange information with other systems operating or being implemented on the premises of plants. The following are the operating procedures of the YMS system.

1. Receive data regarding scheduled transports through the logistics system. The data should include information on the avigation number, type of transport, transport company, driver, vehicle, semi-trailer and the expected date of arrival at the site.
2. When a vehicle enters the site, the system should get information regarding the entering vehicle taking into account the license plate of the vehicle, trailer and the time of entry.
3. The driver goes to the advisory desk to enter the advisory number and the missing information regarding the transport. In the absence of an advisory in the system, the driver enters all information regarding the transport. After entering the required data, the driver receives information regarding the possibility of picking up or delivering the product.
4. After receiving information about the possibility of entry, the driver goes to the weighing station to perform the taring process. After the taring is performed, the weighing system should send information regarding the tared vehicle. The information should include the time when the process was performed, vehicle data and the weighing process.
5. After the taring process is completed, the driver goes to unload or load at the designated warehouse. Information should be transmitted from the warehouse system to the system regarding the start time of loading/unloading, the amount of raw material and the end time of loading/unloading.
6. After the product unloading/loading process is completed, the driver goes to the weighing station to perform the taring process. After the taring is performed, the weighing system should send information regarding the tared vehicle. The information should include the time the process was performed, the vehicle data and the weighing process.
7. After all of the above steps are completed, the driver proceeds to the exit gate. At the exit gate, verification is made that all processes

transport service system have been implemented correctly. If the verification is positive, the system will provide information to the access control system that the trip has been allowed.

The steps described in points number 4 and 6, depending on the type of delivery, do not need to be performed. In this case, skip the process in question. The transportation service system will collect and compare the data received from the other systems during the entire advance process. For the system to function properly, it must receive information from the logistics system, the license plate recognition system, the warehouse system and the weighing system. In addition, the system must cooperate with the management and integration of security systems and the access control system.

### **3.4 Description of reports**

The YMS transportation service system should automatically archive data from the advisory processes carried out. The historical data stored by the system can be reported and analyzed according to various criteria and printed on print forms. Example In the system it should be possible to graphically present reports in the form of charts. So that, by specifying a time interval, it is possible to get information about all data collected from systems integrated with YMS. This makes it possible to generate advanced reports on transports and operators' activities, which are closely related to the data contained in the deliveries. The application should allow exporting reports in several standard file extensions. Generated reports can be automatically sent to a printing device or saved to disk.

Reports should be generated manually and using time-based control. Timing should be configurable to generate a report on all transports or transports for specific categories or specific transports on specific days or at specific times. The ability to generate reports should be included depending on the operator's privileges. In the case of people with low-level access accounts, it should not be possible to generate reports.

### **3.5 Description of authorization management mechanisms**

The system has multi-level access to individual functions combined with authorization codes, which allows different levels of interference in the system (from full control, to report generation, to view of transport processes).

Depending on the assigned authorizations, a given system operator can intervene in the transport service system to a limited extent. Individual operator privileges are individually configured depending on the competence and position of the employee. A user can be restricted in access to particular functions of the transport service system. Individual users are identified in reports and their operation. This provides for later verification of who handled or interfered with a given advance process and when.

### **3.6 Integration capabilities of YMS, PROMAN, TMS, SAP**

In order for the transport service system to function properly, the system should receive information regarding logistics, warehouse, weighing and entry and exit processes from the site (TMS, PROMAN, SAP). Therefore, it is necessary

Integration with other systems operating and implemented at QEMETICA's production facilities. Due to the fact that all systems operate in the plant industrial network, integration between systems should be performed at the software layer.

To ensure the consistency of the database and proper management of the YMS system, install a system server with YMS management software and database. Realize the server as a virtual server. Hardware resources for the server shall be secured by QEMETICA. The minimum requirements and technical parameters recommended by the manufacturer for the server are presented in the following section.

## 4. Expansion of access control system

Upgrading the access control system aims to organize the movement of people and vehicles automobile on area of plants chemical plant

QEMETICA, while at the same time being a support for security personnel in carrying out statutory obligations regarding access control to the industrial facility. Access control should cover entrances to sensitive rooms of production facilities, where interference by unauthorized persons could interrupt the continuity of production processes, and administrative buildings with special rooms. In places where the condition of the door carpentry does not allow the installation of executive elements of the access control system, the doors should be adapted to the installation of the aforementioned elements. The concept assumes the use of the existing system infrastructure for door closers during the construction of modernization works.

The KD system should be based on the criterion of recognition and registration of the user separately for entry and exit using a personalized proximity card issued in accordance with the operating instructions for the movement of people, materials and vehicles in the areas of the QEMETICA group. The access control system should include the following components:

- Access controller, supporting a minimum of one two-way controlled passage,
- power supply,
- proximity readers,
- 12-volt battery,
- emergency exit button,
- an actuator suitable for the type of controlled passage, such as a solenoid jumper with state control, gates or turnstiles,
- self-closer,
- management software,
- operator units,
- system server.

The use of the access control system for pedestrian crossings should be implemented in such a way that authorized persons personally apply access cards to the gate or turnstile reader, under the supervision of a security officer or video surveillance system. If the right of access is denied, the monitoring and security management systems record the event in the alarm event category.

The use of the access control system in the case of vehicle crossings should be implemented in such a way that drivers and passengers of these vehicles, who are authorized to enter/exit, should hand their access cards to a security officer in order to apply them to the reader and verify their granted entry/exit rights. In addition to the card-personal pass, the driver should present the card-carpass. Verification should take place on the monitor of the KD system operator unit or on the portable KD terminal. The portable KD terminal should display, among other things, a photo of the person using the proximity card, name and surname, the expiration date of the pass. In the case of positive assignment of entry/exit rights, the security officer, in addition to performing other official activities, opens the barrier or releases the vehicle barrier. In the case of denial of access rights, including placing the vehicle on the list of vehicles not authorized to enter, the security employee proceeds with the official activities specified for such situations, and the monitoring and security management systems record the event in the category of alarm events. The concept adopts a KD system based on proximity cards in the Mifare Plus standard, which is characterized by a symmetric AES-128 key and 4 levels of card security (Security Level) where SL1 level is immune to known attacks that have been

successfully carried out on cards in the Mifare Classic standard, while SL3 provides security equivalent to that of a DESFire card.

To ensure supervision of the access control system in the event of a power outage, it is recommended that network devices and control system components have power backup for 2 hours.

To ensure the consistency of the database and correct management of the KD system, install a system server with KD management software and database. Realize the server as a virtual server. Hardware resources for the server shall be secured by QEMETICA. The minimum requirements and technical parameters recommended by the manufacturer for the server are presented in the following section.

#### **4.1 Operator units of the access control system**

The operation of the KD system, including the granting of authorizations, is envisaged on PC-class operator units located in the administration building and at security posts. The operator units should be equipped with a 24" monitor. At the posts where a VSS system operator unit is envisaged at the same time, the KD software should be installed on this unit and retrofitted with an additional monitor. Additional equipment for the operator units of the access control system shall be a desktop access card reader and a stationary UPS with adequate capacity for the automatic shutdown time of the operating system.

#### **4.2 Intercoms**

There are administrative buildings on the site that receive a lot of visits from outsiders. Intercoms should be installed at the main entrances secured by an access control system in order to allow contact between people entering the buildings. The intercoms should be connected to the existing plant network and integrated with the telephone exchange. The intercom should be integrated with the existing telephone exchange so that, using a telephone, a call can be answered from the intercom.

#### **4.3 Integration of access control system**

The PSIM System will show the states of passageways at the entrance to the facility and individual rooms, as well as door lock sensors, readers and buttons at their locations on site plans and summary diagrams. From the system, the operator will control the access control doors, e.g. open momentarily, play permanently or lock the doors. For each door with readers and buttons there is a defined operating procedure, a situation plan, which will support the operator's decision in case of an incident. By integrating with PSIM, the operator will gain the ability to trigger interactions between systems. Defining automatic operating procedures and automatic controls will trigger the actions of other integrated systems, namely the user's application of a card to a reader will cause the system to show the person's data, and thanks to integration with the CCTV system, the image from the nearest camera associated with a particular sensor is called up on the monitor.

Key advantages from the point of view of rescue and firefighting operations:

- Automatically lock and unlock any door to restrict entry into specific fire zones.
- Provide the system operator with quick information about the elements involved in a fire scenario.
- Overseeing the status of elements in the collective diagrams, i.e:

- The condition of doors, areas, buildings,
  - The status of the door closure sensors,
  - The status of readers and buttons.
- For each door with readers and pushbuttons, there will be a defined operating procedure, a situation plan implementing the fire scenario for a specific fire zone.
- From the system, the operator will be able to control the access control door, for example:
  - open for a while,
  - reproduce permanently,
  - lock the door.

Added value from integration:

- Create configurable time schedules for access card users.
- Applying the card to the reader will cause the system to show a picture of the person, and then, thanks to integration with the VSS system, the image from the given camera will be called up on the monitor - the example shown allows the operator to verify whether the person has rights to the given pass.
- Entering a wrong pin will generate an alarm in the system, transmit the image from the nearest VSS camera, start a recording or take a photo.

## **5. Expansion of video surveillance system**

There is an on-site video surveillance system overseeing technological processes, the plant's production area and the external area. Access to the VSS production system is provided to operators of individual technological processes and department managers.

In order to ensure full supervision of the movement of people prevailing on the premises of the plants, the cameras of the VSS system should be installed at the access control

passages. This makes it possible to verify events occurring at a given passage.

In order to ensure effective video monitoring of QEMETICA facilities, the selection of locations and technical parameters of individual camera points was guided by the minimum image resolution in order to provide observation, recognition and identification criteria. In the case of cameras observing access control passageways, entrance and exit gates, the identification criterion should be used, which allows the identification of people entering the zones covered by the access control system. The observation criterion and the recognition criterion should be applied to camera points that are designed for surveillance of outdoor areas that do not require identification. The minimum image resolutions for each observation category are shown below:

- Minimum image resolution for observation purposes - 62.5 px/m,
- Minimum image resolution for recognition purposes - 125 px/m,
- Minimum image resolution for identification purposes - 250 px/m.

In order to ensure the supervision of the video surveillance system in the event of a power outage, it is recommended that network devices have power backup for a period of 2 hours. To ensure the consistency of the database and proper management of the VSS system, install a system server with VSS management software and database. Implement the server as a virtual server. Hardware resources for the server shall be secured by QEMETICA. The minimum requirements and technical parameters recommended by the manufacturer for the server are presented in the following section.

Cameras should be mounted respectively on: dedicated poles with prefabricated foundations, existing lighting poles and support structures, facades and structural elements of buildings and structures, suspended ceilings or walls inside buildings. The power supply to the cameras, as appropriate for the installation requirements and type, should be of PoE (802.3 af), PoE+ (802.3 at), PoE++ (implementation of PoE standard - 60W) or from a dedicated power supply.

The concept assumes the following types of cameras:

TYPE1 - fixed outdoor camera

TYP2 - outdoor fixed dome camera TYP3 - indoor fixed

dome camera TYP4 - high-speed PTZ camera

TYPE5 - indoor 360 panoramic camera°

## **5.1 ANPR license plate recognition system**

There is a high volume of truck traffic on the site associated with the delivery of raw materials needed in production processes and the collection of finished products. In order to increase the level of security and vehicle identification and control, the video surveillance system should be expanded with the functionality of recognizing license plates at key locations of the production facility. To recognize vehicle license plates, software cameras or a software module should be used in cooperation with the digital recorder unit used. The system should automatically recognize license plates of standing or moving cars. The correctness of license plate recognition using image analysis under optimal conditions must exceed 96%.

License plate recognition cameras should be placed at entrances and exits at wheel posts and at vehicle scales. ANPR cameras should be equipped with 940nm IR illuminators with a range of up to 100m. A white light filter and appropriately sized mounting spacers should be placed on the lens of the cameras. Two ANPR cameras should be used per entrance or exit. This will make it possible to recognize the license plate of a truck tractor and its trailer.

The operator of the KD system, based on the reading of automatic license plates, will receive information about the entry permit status of a particular vehicle. The software of the recorder unit should allow the creation of different variants of the system response depending on the specific category of the status of the identified vehicles, e.g. control of automatic raising of the barrier or opening of the gate.

To ensure the consistency of the database and correct management of the VSS system, install a system server with VSS management software and database. Realize the server as a virtual server. Hardware resources for the server are secured by QEMETICA.

## **5.2 VSS system operator units**

Operation of the VSS system is envisaged on PC-class operator units at the security posts, the operators of individual scales, and in the administration building.

The operator units should be equipped with a 24" monitor. Additional equipment for the operator units of the video surveillance system shall be a stationary UPS with adequate capacity for the automatic shutdown time of the operating system.

## **5.3 Registration and archiving**

Recording and management of camera images should be carried out by a specialized, dedicated recording device, hereinafter referred to as the Digital Recorder Assembly, with the ability to handle the required number of video streams of IP cameras, viewing stations, database, network communication network interfaces and for integration with the security management system. The Digital Recorder Assembly in the mode of recording video streams should record video at full resolution with a frame rate of 12 fps, excluding the cameras of the automatic license plate recognition system, for which recording at a rate of 3 fps and with a resolution of 1 MPix has been adopted. In the recording mode

alarm Digital Recorder Team should increase the number of frames of recording video streams per second twice.

Archiving of the recorded material of the Digital Recorder Unit should be min. 30 days. Storage of the Digital Recorder Complex should be made in RAID 6 standard with hard drives with a minimum capacity of 16 TB.

## **5.4 VSS system integration**

The designed PSIM system must have software and hardware interfaces for the manufacturer of the VSS cameras and DVRs used in the project. As part of the PSIM system, it is proposed to visualize cameras, monitors, DVRs and alarm outputs on site plans and summary charts according to their installation locations. The VSS system is to be able to integrate within the common PSIM management and integration platform in such a way that at the PSIM operator's station the ability to:

- Textual presentation, visualization of the status of the digital recorder assembly with the scope:
  - alerts,
  - control outputs,
  - Inputs,
  - cameras,

- monitors,
- Playback,
- registration.
- Controls:
  - cameras,
  - inputs/outputs,
  - monitors,
  - registration,
  - playback.

Key advantages from the point of view of rescue and firefighting operations:

- Elements of the integrated systems will report a report from the SSP, KD systems, which will automatically switch the cameras.
- Switch camera images by clicking, for example, on camera pictograms placed on the site plans (easier navigation through the objects than when displaying a list with the names of individual cameras).
- Automatic switching of the camera, reduces the reaction time of the operator to the events (you do not need to search for a particular camera in the list with the names of locations).
- Tracking the response of those in the fire zone.

Added value from integration:

Through integration with VSS TV, the system will be able to produce statistics related to image analysis.

- Taking pictures on demand or as a result of an event,
- Broadcasting and time-stamping,
- Free switching of cameras and monitors,
- Monitor wall management,
- Building custom monitor layouts,
- Tying monitor layouts to zones,
- Programming "presets" on PTZ cameras.

## 6. Expansion of burglar alarm system

The burglary and robbery alarm system should be used to protect buildings with a single-shift work system, technical buildings where personnel are not present during normal operation, and archive rooms in administrative buildings.

The burglary and intrusion alarm system for the internal zones of protected facilities at the Plant should be implemented based on control panels, I/O expansion modules, motion detectors, magnetic detectors and optical/acoustic sirens. Equip the SSWIN control panels with an Ethernet communication module and integrate them into the Plant LAN for central management and supervision. To centrally supervise and manage the SSWIN system, implement the SSWIN system supervision and management software on the system server.

The SSWIN system will be managed from the KD system operator unit located in the administration building. Supervision of the SSWIN system will be done from the KD system operator unit located at the security post of the main department's gatehouse.

In order to ensure supervision of the video surveillance system in the event of a power outage, it is recommended that network devices have power backup for a period of 2 hours.

## **6.1 SSWIN system integration**

The SSWIN system is to allow integration with VSS, KD, PSIM using software interfaces for information exchange and mutual interference between installations, and potential-free contacts. The PSIM operator station must be able to obtain visualization of the states of such system elements as:

- Lines
- Groups
- Readers
- Keyboards
- System states

and get the ability to control the alarm system in terms of arming and disarming the system, and arming and disarming individual groups.

Key advantages from the point of view of rescue and firefighting operations:

- View the situation in the vicinity of the room covered by the SSWiN system by linking the CCTV camera image to the SSWiN zones and tracking the behavior of the participants.
- Remote arming and disarming of the zone for rescue operations, etc.
- Define units (individuals, groups, special services) to be automatically informed of selected events by voice message, short text messages, e-mails, etc.
- Access to all events coming from the SSWiN system - they are logged to GEMOS system memory, with reporting depending on user privileges.
- Assign permissions for individual modules, plans, sensors, devices, etc.

Added value from integration:

- Supervision of the SSWiN system control panel,
- Supervision of the condition of the line,
- Status monitoring of each sensor of the SSWiN system,
- Supervision of external acoustic-optical sirens,
- Supervise the status of zones (armed/disarmed),
- Supervision of the alarm status of the control panel (tampering, intrusion, damage, etc.),
- Supervision of the status of power supply and batteries of the SWiN system,
- Through the system's parameterized inputs, monitoring will also be possible:
  - temperature sensor,
  - flooding sensor,
  - power presence.

## 7. Expansion of key management system

The existing key circulation system, which is based on a publicly accessible key board without security and detailed supervision, should be replaced with electronic key depositories. This will ensure full control and management of keys to rooms and facilities. In order to implement key circulation control, key depositories are to be installed in the administration building A and in the storage buildings, which will be integrated with the access control system. The depository will be equipped with a card reader and a numeric keypad. This will allow any authorized person to retrieve a key after applying a proximity card at the time. The depositories should be equipped with access control readers compliant with the Mifare Plus standard. The depository will be equipped with an event log, which will store information about who retrieved or deposited a key to a particular room and at what time. It will also be possible to read who retrieved the key to a particular room at any given time. The depository will be supervised and administered by dedicated management software and the PSIM security management system. The key management system will be managed from the KD system operator unit located in the administration building. Supervision of the key management system will be done from the KD system operator unit located at the security post of the main department's gatehouse.

Two key depositories should be installed. Equip the key depositories with KD readers compliant with the Mifare Plus standard.

Electronic key depositories combine secure key storage with key access management and key circulation recording. The system consists of an electronic key locker and software that records and permanently logs every key retrieval and release. The administrator of the control program - usually an authorized employee of a given system user - decides on the granting of access rights to keys to specific individuals and determines the time periods during which this access is possible. The system is ideally suited for customers who can't or don't want to give up mechanical keys, but have problems managing them and documenting their circulation. The designed system offers a modern approach to managing the circulation of keys and other objects in an enterprise and provides full control over access to business premises and documents or other valuable items deposited in depositories. The use of the system allows full identification and control of keys, deposits and employees, analysis of collected data and immediate response to emergency situations detected by the system. Electronic key depositories are high-quality devices in the form of steel boxes, which contain a control panel and a main panel with slots for storing keys. Each key is permanently connected by a metal seal to a key ring, which is locked in the individual slots of the panel. Embedded in the fob is an electronic chip that is read by the device and correlated through software with all information relating to the linked key, such as its purpose, access rights granted to specific employees, etc.

To retrieve a key from the locker, you need to log in on the touchscreen display of the control panel by applying a proximity card and/or entering an individually assigned PIN. Once the user has logged in correctly, he selects from the list of keys the one to which the system administrator has granted him access. Pressing the icon of a given key automatically opens the door to the main panel, where there are slots with locked key fobs. The previously selected key is automatically highlighted with a

colored LED - the user is guided by the device to a particular key each time. The key lock is then released and the desired key(s) can be removed from the slot and the door closed. The same procedure applies when returning the key, except that it can then be placed in any slot, as the device automatically recognizes the particular key ring.

Persons not authorized to any of the keys cannot open the depository and authorized persons, after opening the door, cannot retrieve a key they are not authorized to access, as it remains locked in its slot. Any improper actions performed at the locker can be defined by the administrator and result in an alarm being triggered. When certain procedures are performed, the cabinet transmits voice messages to inform the user when correct or incorrect actions are started or completed. Each key retrieval and return as well as other events are recorded by the software and indelibly stored on a memory card in the form of reports that the administrator can edit according to specific search criteria. The key panel can also be expanded to include a locker with lockers that can be used to store special keys of large size or any valuable items and documents. These can include cameras, tablets, data storage media or car registration cards. The configurations of key depositories and locker depositories can be tailored to individual customer expectations.

In order to ensure supervision of the video surveillance system in the event of a power outage, it is recommended that network devices have power backup for a period of 2 hours. Key depository management software should be installed on the operator units of the access control system.

## **7.1 Integration of key management system**

The key management system must be integrated into the PSIM system using a dedicated software interface for the exchange of information and mutual overrides between the rest of the facility's security installations. At the PSIM operator station, it must be possible to obtain visualization of the states of such system elements as:

- Depository closet,
- Key slot,
- System states.

And get the ability to control the depository in terms of remote cabinet opening.

Visualized system states:

- Depository cabinet glass breakage alarm,
- opening the service door,
- cabinet connection,
- no connection to the cabinet,
- cabinet doors closed,
- cabinet doors open,
- The door closed after being opened for too long,
- door too long open,
- door open without authorization,
- correct authorization,
- an unknown card was used,

- KEY AVAILABLE,
- key downloaded,
- Key turned in too late or out of time zone,
- Unauthorized downloading of the key,
- A key returned by an unauthorized person or from another locker.

Added value from integration:

- Supervise the status of all depositories from a single position;
- No need to switch between different dedicated surveillance applications - all device states visible in one unified graphical interface of the PSIM system;
- Ability to view the image from the nearest camera of the VSS system integrated in the PSIM system. When an alarm is reported by a key depository, the PSIM system will automatically display the image from the nearest fixed camera or rotate the nearest PTZ camera toward the cabinet that is the source of the alarm;

## **8. Integration of the fire alarm system**

To integrate the existing fire alarm systems located in the main department with the management and control platform of the security systems, a software and hardware interface should be used. The fire panels should be networked according to the manufacturer's recommendations, so that the entire fire alarm system is certified and has a CNBOP certificate of approval. The cross-linked control panels of the SSP system should be connected to the LAN using a dedicated converter.

The designed PSIM security management system, as a supervisory and control system, is used to collect and record incoming alarms from the fire control panel and other information from integrated subsystems in a graphical manner with location on the architectural plan. It prepares and transmits all the necessary information to supervisory personnel. With clear visualizations, it enables comfortable facility management and simplifies security procedures. Currently, supervision is carried out from the level of the fire panel, which generates information about the event

in the form of a printout, which, with the large number of sensors that are present at the site, makes it much more difficult for the operator to supervise the system.

In PSIM, the detection elements of the fire alarm system should be depicted at their installation locations on siteplans and summary charts. Action procedures will be defined for each element and detailed situation plans will be specified. Signals sent by the systems can trigger defined automatic and manual action procedures, which will be on the situation plan. In the PSIM system, it must be possible to change the observed plans, e.g. due to levels, zones, etc.

In the event of an alarm event, the fire alarm panel initiates an alarm on a small display without the ability to view the object in the fire area. This solution slows down the taking of appropriate action by the security services. The view on the PSIM platform assists the operator by displaying a detailed situational plan with the icon of the element that is currently in alarm, and then performs automatically defined procedures while guiding the operator through the algorithm for the situation.

The task of automatic operating procedures is, among other things, to trigger any interactions between integrated systems, e.g., when an alarm occurs, the image from the camera located in the immediate vicinity of the incident site is automatically presented, a situational plan with the active sensor marked is displayed, and via radio, telephone, e-mail, SMS or fax, a notification is sent to the appropriate services.

Key advantages of the PSIM system from the point of view of rescue and firefighting operations:

- PSIM system must have a CNBOP certificate, this allows the control of the control panel of the SSP system during a fire,
- Monitoring the open position of the entrance door to the facility,
- Monitoring the operation of cranes,
- Controlling the activation of message transmission by means of an audible warning system,
- Monitoring the status of emergency lighting through alarms from the SSP,
- monitoring of domestic ventilation,
- monitoring transfer flaps,
- monitoring of fire dampers on ventilation ducts,
- In addition, the fire alarm system will control the release of doors covered by access control and located on escape routes,
- Signal monitoring for fixed firefighting equipment. In

PSIM Integration System:

- Signals sent by the Fire Alarm System trigger predefined manual as well as automatic action procedures.
- The system will create charts reflecting the control matrix for each building zone.

## **9. Health and safety training system**

At present, those who visit the plants must receive training by people from the health and safety department before entering the premises. The main function of the health and safety training system is to streamline the current procedures for conducting mandatory health and safety training before entering QEMETICA's production facilities. In order to streamline the training process, it should be conducted based on microlearning through an application available on a dedicated device (kiosk or training station). The introduction of the aforementioned system will seal and streamline the training system and improve its standard.

The training point should be implemented based on a training kiosk or training station, which will be based on all-in-one computer units. The training kiosks should be located in a place that is accessible to interested parties, so that visitors can register and do the training themselves. The system should consist of registration and training scenarios to collect specific data (name, surname, phone number, email address, consent, statement, document number, etc.) for each type of visitor. Depending on the person's position and place of work, the system should trigger training in the appropriate scope. Training should take into account the risks associated with the scope of work performed in front of a given employee. In the case The system should generate training expiration dates and allow assessment of compliance with health and safety rules by a given employee. Depending on the assessment given, the employee should have training again or be banned from work. The system should allow the creation of all kinds of statements and reports on the training carried out. The graphic design of the application can be adapted to the procedures of the facility. This makes it possible to adapt the appearance of the training application to the image of the company.

Training stations at the facility of QEMETICA production plants is envisaged in the administration building, in the visitor-accessible area and at the main department's gatehouse. Operation of the OHS system is envisaged on a PC-class operator unit located in the OHS department. The operator unit should be equipped with a 24" monitor.

The EHS training system should be integrated with the PSIM system. Integrating the systems will ensure that data is exchanged between the safety systems and the OHS system. This will make it possible to assign information regarding the training possessed by specific employees. This will affect the permissions granted in the access control system, which will not allow an employee to enter the site if he or she lacks training.

If a health and safety training system is used, a 230VAC power supply and a connection to the plant network should be provided for the training stations and the operator unit of the training administrator. A server, database environment for the operation of the above-mentioned system should be provided in the plant network. The server should provide integration capabilities with the PSIM security systems integration and management system.

## 10. Protection system for control and instrumentation cabinets and switchgear

In order to increase the level of security of the cabinets of Control and Measurement Instrumentation and Automation and Electrical Switchgear, it is recommended to implement a supervision system for the Control and Measurement Instrumentation and Electrical Switchgear cabinets. To protect individual cabinets, it is necessary to use a microprocessor-based controller of environmental operating parameters of the distribution point. PPD-Controller is a microprocessor-based device for protecting and monitoring the parameters of all kinds of control cabinets, electrical switchboards, distribution points. It has the ability to integrate with security management system, video monitoring and others, which provides remote control of monitored devices. Connectivity with the device is based on encrypted TCP/IP protocol (built-in 10/100Mb connector) with access authorization, GPRS communication, can be equipped with a palette of I/O modules, sensor modules, relay outputs, communication interfaces. As part of the security of the above-mentioned cabinets, the following parameters should be monitored:

- Presence of mains power in protected cabinets (230 VAC),
- Temperature and humidity - realized through temperature and humidity sensors,
- Status opening door/wall cabinets- realized via sensors  
limit sensors installed in protected ICT cabinets.

Another element that will increase security over access to rooms where cabinets and switchboards are located is an access control system. The two-way access control system will provide information regarding people entering and leaving the premises. Thanks to the use of the KD system on the PSIM operator unit, the system administrator has the ability to quickly and easily assign individual users access to protected areas and define schedules for this access. It is possible to centrally determine the rights of individual users, immediately identify each user, control the presence of individual users in protected zones, obtain current information about events in the system, book a date (day, hours, minutes) for entering a zone and leaving it. In places where the condition of the door carpentry does not allow the installation of executive elements of the access control system, the doors should be replaced with new ones.

Use a video monitoring system in the rooms of switchgear and instrumentation cabinets. The rooms equipped with cameras of the video monitoring system allow viewing the people and activities carried out at the given AKPiA cabinets and electrical switchgears. In addition, it is possible to generate procedures on the PSIM operator unit, which when entering a room using the access control system will automatically display the image from the camera located inside this room.

If the protection system for instrumentation cabinets and switchgear is used, 230VAC power supply and connection to the plant network through ports in the PoE standard network switch must be provided.

## **11. Facilities without a connection to the company LAN**

In order to ensure surveillance of important facilities located outside the production site, they should be secured with electronic security systems. Such locations do not have a connection to the plant LAN in which electronic security systems are assumed to function. A private APN with an encrypted channel should be used to provide the connection. The private APN should be made by using an encrypted IPsec / GRE channel enabling DED, 3DES, AES encryption standards and Pre-shared Key authentication. A wireless connection is necessary to provide surveillance of facilities.

The concept is to secure these facilities with systems for access control, video surveillance and burglary and assault signaling. In the intrusion-management security system, the individual systems should be visualized. In the case of the video surveillance system, image recording should be carried out through a local DVR, and the private APN bandwidth should transmit the view from the cameras.

## **12. Procedures and operating instructions**

Procedures and instructions for operation of individual electronic security systems should be provided to the developer after completion of the work and commissioning of the system. Instructions for individual systems should include information on the system, its components and how to act in case of certain situations.

## 13. Functional requirements for systems

The section below provides a functional description and the minimum technical requirements of the systems, equipment and edge devices used.

### 13.1 PSIM system

- **technical and functional**
  - The management system must be neutral to the manufacturers of the integrated systems and equipment.
  - It is required that the PSIM system provide bidirectional control of managed systems and management information. This is understood as the ability to control integrated systems, e.g., granting permissions in the access control system, locking fire system detectors, controlling cameras.
  - It is required that the PSIM system supports information exchange with Android and iOS-based mobile users.
  - The software must have a modular design. Replacement of any software module must not stop the operation of other modules and functions of the system.
  - The following connection methods are required in PSIM:
    - Relay outputs of various devices and systems to the inputs of the integration system;
    - Integration system relays for control inputs of various devices and systems;
    - Communication port of the integrated system control panel to the integrating system controller;
    - The communication port of the integrated devices to the controller that is part of the integration system. In addition, it is required that the controllers of the integration system be able to operate in a network;
    - The communication port of the integrated system to the serial port or Ethernet jack of the integration system computer.
  - The system must operate on a computer network and provide full support via a web browser from anywhere on the network, including system administration.
  - It is required that every action performed by a user in the PSIM system can be recorded in the database.
  - The ability to configure the system with multiple workstations is required.
  - The software must be able to work in virtual environments, thus allowing visualization and integration with the management platform of the virtual environment.
  - It is unacceptable for a PSIM upgrade to disable the application server for a software upgrade or update.
  - It is required that the PSIM system supports operation in single and multiprocessor environments - making optimal use of the hardware configuration.
  - It is required to provide mechanisms for automatic and manual copying of any data locally or to a remote server.
  - The PSIM system must provide expansion to support new devices by adding a software driver to the application server.

- The ability to measure physical quantities of a continuous type (e.g. battery charging current, voltage value, temperature, pressure, etc.) is required. The ability to generate alarms based on exceeding alarm thresholds is required.
- It is required that events and responses to events be stored in an activity log, with the ability to report on them.
- It is required that the PSIM be a scalable and flexible solution, allowing functionality and capacity to be expanded incrementally - extending live software licensing without interrupting system operations.
- It is required that the PSIM system has an extensive system of access levels for individual user groups with the ability to differentiate access privileges to:
  - Reports.
  - Emergency Procedures.
  - Situation plans.
  - General settings.
  - Develop and close alarm events.
  - Closing unworked events.
    - Forward events to other service stations with differentiated permissions in the following areas: no access, read only, edit, enter new, delete.
- The ability to assign permissions individually for each element in the PSIM system is required.
- It is required that the system has the ability to assign permissions to operators with the ability to create individual service positions assigned to an operator or group.
- The ability to configure automatic routing of alarm events to appropriate workstations is required. In addition, the ability to forward the event by the user is required. In doing so, a mechanism is required to verify that the selected workstation is active. When forwarding an event, only active workstations with user ID (login) are displayed.
- The ability to freely set event categories combined with the ability to direct events to workstations is required. Color differentiation of events of each category is required.
- Events must be presented on the event list in a one-line concise form. It must be possible to edit the concise form - the ability to select the displayed data from: Ip. time and date, name (location), event, current status, priority, category, status, user is required.
- It is required to be able to set the order in which alarm events are displayed at least by (Ip., time, sensor ID, event, priority, category) ascending or descending.
- Event counters separate for events of all categories are required. It must be possible to filter the event view in the alarm list (stack) to events of the selected category by a simple operation (e.g. click).
- From a view that presents only the events of a selected category (filtered view), the PSIM system must return automatically to the view of events of all categories (unfiltered view) after a set time.

- The ability to correlate events and generate a secondary event is required.
  - It is required that the PSIM system allows filtering of active alarms for any event.
  - It is required to signal the interruption of communication with each integrated system by displaying an appropriate alarm message.
  - It is required that the PSIM system automatically returns to a working state. Necessary software components (modules) must be started automatically (e.g., operating system services).
  - It is required that the PSIM system has plans in vector format with the ability to scale the image for the entire area as well as individual buildings, zones.
  - It is required that the sensors on the plan are displayed in layers for each system, with the ability to fade out layers and defined views (slices) for an event from a particular system.
  - Editing the underlay file must not affect the content of the applied graphic layers.
  - PSIM must provide a mechanism for hiding application windows that are unnecessary at a given time. In the event of an alarm, the windows responsible for the subsystems in question must be restored to the main view.
  - It is required that all alarms be displayed in dedicated categories by location. The system must report events visually and audibly at all workstations.
  - It is required that the PSIM system has the ability to create daily, monthly, quarterly reports from the efficiency of the integrated systems.
  - It is required that the PSIM has a built-in sitemap tool, which must allow the creation of controls and functional elements using any fonts, colors, fills, images and animations.
  - It is required that the PSIM system has the ability to create individual procedures for action in case of an incident in the buildings under surveillance with the possibility of branching the procedures into further stages depending on the actions taken by the operator.
  - It is required that the PSIM system has the ability to attach any documents such as data sheets, manuals, assigned to specific operating procedures, sensors or devices.
  - PSIM must provide a mechanism for freely shaping the layout of application frames so that any content can be nested, for example, in a grid layout.
- It is required that the PSIM system has a module for entering addresses and contacts
  - base of service technicians, vehicles, etc.
    - It is required that the system has the ability to connect any device or system via a communication protocol.
    - It is required that the PSIM system has the ability to create individual operator stations for individual buildings as well as the ability to supervise all buildings from a single operator station.
    - It is required that the PSIM system allows the connection of any devices that communicate via contact (control and supervision - including fire protection devices).

- The requirement is that the PSIM system must operate in a service-oriented architecture (SOA).
- It is required that the PSIM system be created in a client-server architecture based on Microsoft.NET technology.
- It is required to provide the ability to create macros and forms.
- PHP, JavaScript and Shockwave Flash support is required.
- It is required that PSIM apply the change of style settings from the CSS form.
- It is required that PSIM has a built-in mechanism for automatic backups according to: schedule, on-demand, and by copied system fragments such as database, logs, services, configuration files, documentation, manuals, nested components.
- Online backup and incremental backup capabilities are required.
  - Database backup capability is required. Ability to restore the system from backup.
- **Certificates**
  - National Technical Assessment
    - National Certificate of Constancy of Performance
    - Certificate of Approval
    - National Declaration of Performance
- **Software licenses**
  - A perpetual license is required
  - Scalable license is required with further extensions, modules and licenses
  - Requires is required, that license PSIM is confirmed by deed license, confirming the right to acquire and use the license.
  - It is required that the PSIM license be assigned to the building facility in which it is installed.
- **General requirements**
  - The PSIM system must be independent of the manufacturers of the integrated solutions.
  - PSIM must have the ability to integrate any systems using any communication protocols.
  - The PSIM system is required to provide two-way connectivity to subsystems.
  - Must guarantee the ability to control integrated systems: locking fire system detectors, detector disconnection, fire panel reset, camera control.
  - The software must be built in a modular fashion. Upgrading or replacing any software module must not stop the operation of the other modules and functions of the system.
  - A dedicated application installed on a workstation or server is not allowed.

- PSIM must be fully administered and operated via a web browser and a PSIM system based on a dedicated application is not acceptable.
- Full management via a web browser provides independence and neutrality to the choice of operating systems and client devices.
- All functionality accessible from anywhere on the network.
- Ongoing updates to ensure browser security and performance are guaranteed by leading manufacturers Google/Microsoft/Mozilla.
- It is required that the PSIM system automatically returns to a working state. Necessary software components (modules) must be started automatically (e.g., operating system services).
- The PSIM system must have a built-in floorplan creation tool that must allow the creation of control buttons and functional elements using any fonts, colors, fills, images and animations.
- It is required that the PSIM system has the ability to create individual procedures for action in case of an incident in the buildings under surveillance with the possibility of branching the procedures into further stages depending on the actions taken by the operator.
- It is required that the PSIM system has the ability to attach any digital documents assigned to specific operating procedures, sensors or devices.
- The system must provide a mechanism for freely shaping the layout of application frames so that any content can be nested, for example, in a grid layout.
- The PSIM installation must be secured with a secure SSL connection to the server.
- It is required that the PSIM system be created in a client-server architecture based on Microsoft.NET technology.
- It is required to provide the ability to create macros and forms.
- It is required that PSIM apply the change of style settings from the CSS form.

- **Graphical user interface (GUI)**

- The PSIM system must use plans in vector format with the ability to scale images for the entire area as well as individual buildings, zones.
- It is required that the sensors on the plan are displayed in layers for each system, with the ability to fade out layers and defined views (slices) for an event from a particular system.
- Editing of the graphic underlay must not affect the content of the applied graphic layers.
- PSIM must provide a mechanism for hiding application windows that are unnecessary at any given time.

When an alarm occurs, the windows responsible for the subsystems in question must be restored to the main view.

- It is required that PSIM has a built-in sitemap tool that must allow the creation of controls and elements

Functions using any fonts, colors, fills, images and animations.

- PSIM must have a tool in the form of a built-in Graphical User Interface (GUI) designer. The GUI designer can be used to create user interfaces that are displayed on operator workstations supporting the client application.
- The GUI designer must allow the creation of interfaces that give full control over the visualization system, such as display wall technologies in the surveillance center.
- PSIM must allow the use of graphics in vector format. While vector graphics must allow the use of any colors from the full color palette.
- Devices, buttons, texts and windows can be layered with any content division.
- PSIM should have the ability to control evacuation and fire protection devices from dedicated layers (invisible to unauthorized users).
- Information windows for PSIM support must be able to contain nested documents in pdf, MS Office and read them.
- Interaction between the PSIM GUI and video walls should be seamless for the operator. It should be possible to switch live video streams for review in PSIM and to switch live video streams for representation of the current wall configuration in PSIM. The number of GUIs configured in PSIM must not be limited. All GUIs created by PSIM must be published and available immediately (subject to user privileges) in all PSIM applications on the operator's workstation.
- PSIM must allow free design of frame layouts containing dynamic and static elements.
- Frame layouts must be able to fill the entire physical screen of the monitor.
  - Frames can nest any elements such as site plans, maps, web pages, device symbols, buttons, CCTV image view windows, device function control panels, and more frames.
  - PSIM must allow defining the view and layout of windows, containing any content (maps, web pages, documents, descriptions, sensor and video panels, etc.).
- Each frame used in the PSIM system must have a selectable type:
  - Plans - contain navigation structure of situational plans generated automatically based on the folder of situational plans in the module;
  - Configuration;
  - Menu line (Settings, Operation, Reports ...);
    - Status line including selection of alarm stack filter, information on the number of alarms in each category, date and time, among others;
  - Alarm tree - contains a list of alarms (events);
  - Video stream, e.g., live camera feed;
    - Control panel - predefined dashboards for controlling integrated devices (e.g., telephone, video matrix switcher);
  - Situation plan - the box displays situation plans;
  - URL.
    - Each frame used in PSIM must be able to specify display options:

- dimensions and position -the position of the upper left corner and the width and height of the frame;
- The name of the frame - referred to by the "display in window" parameters of the situation plans;
- border - whether to show a standard border around the frame (no, if you want to "hide" the division into frames and connect them "seamlessly");
- zoom - whether buttons to zoom in and out (for HTML type plans) should appear on the plan;
- scroll bar display - if the content does not fit entirely in a given frame, then standard scroll bars appear on the edges of the frame. You can specify whether to display these bars automatically (when necessary), always (regardless of the content), or never (you can't scroll the frame's content).
- PSIM must allow the hosting of an unlimited number of frames in any layout of plans and frames with nested content.
- PSIM must provide a mechanism in the form of the ability to freely define the functions of individual procedures.
- The ability to nest arbitrary frames in a grid layout (e.g., video panels) is required. Content must be defined as device or GUI objects.
- The site plan designer must allow the use of arbitrary fonts, background colors and fills for descriptions and prompts.
- The site plan designer must allow the use of function buttons with any color, size and background graphics.
- PSIM must use global settings from CSS forms.
- The management desktop must support the following functions: Users:
  - Adding a new user account and editing it;
  - User account activation;
  - User account deactivation;
  - User account deletion;
  - Password Reset;
  - Resetting user account lockout;
  - Deleting reports;
    - The PSIM solution must allow operator and user interfaces to be displayed in Polish, English.
    - The administrative interface must be configurable and include functionality:
- Adding users,
- Management:
  - groups and schedules,
  - roles and powers,
  - device statuses,
  - maps and associations of cameras and alarms,
  - information about places and contacts.

- **Procedures**

- PSIM must be equipped with a tool for creating security policies and procedures, allowing system administrators to implement them within the system.
- PSIM must be based on a visual decision tree to enable simple configuration of procedures and policies.
- The procedure must ensure implementation: automatically or manually as part of a scenario, according to a specific schedule.
- The PSIM solution must provide a graphical user interface that allows system administrators to quickly assign a user to a group and a group of users to a security resource.
- The overriding user (group administrator) must be able to manage user permissions for the user groups they administer.
- Security resources can be grouped (e.g., within a building or a single site). Users are only authorized to work with assigned resources in single or multiple groups.
- It must be possible to program user permission changes for known and scheduled events. For example, to associate a date and time with the start/end of a set of user privileges. This period can be specified in hours, days, weeks or months.
- It must guarantee a work control module, i.e., control functions such as detector disconnection can take place only with the approval of the shift commander.
- Must guarantee a module to control the work of operators, e.g. verification of the time of the concept of the event from the alarm stack, the time from taking to closing the event.

- **Operation and powers**

- Every action performed by a user in the PSIM system must be recorded in the database.
- It is required that events and responses to events be stored in an activity log, with the ability to report on them.
- The ability to assign permissions individually for each element in the PSIM system is required.
- It is required that the PSIM system has an extensive system of access levels for individual user groups with the ability to differentiate access privileges to, not less than to:
  - Reports;
  - Emergency Procedures;
  - Situation plans;
  - General settings;
  - Develop and close alarm events;
  - Closing unworked events;
    - Forward events to other service stations with differentiated permissions in the following areas: no access, read only, edit, enter new, delete.
  - It is required that the system has the ability to assign permissions to operators with the ability to create individual service positions assigned to an operator or group.

- The ability to freely set event categories combined with the ability to direct events to workstations is required. Color differentiation of events of each category is required.
- Events must be presented on the event leaf in a one-line concise form. It must be possible to edit the concise form - the ability to select the displayed data from: lp. time and date, name (location), event, current status, priority, category, status, user is required.
- It is required to be able to set the order in which alarm events are displayed at least by (lp., time, sensor ID, event, priority, category) ascending or descending.
- Event counters separate for events of all categories are required. It must be possible to filter the event view in the alarm list (stack) to events of the selected category by a simple operation (e.g. click).
- From a view that presents only the events of a selected category (filtered view), the PSIM system must return automatically to the view of events of all categories (unfiltered view) after a set time.
- The ability to correlate events and generate a secondary event is required.
  - It is required that the PSIM system allows filtering of active alarms for any event.
  - PSIM is to allow arbitrary control of permissions to any layers to enable centralized management, the PSIM application must have a central alarm tree that receives, classifies and prioritizes all alarms in the system. The schema must be flexible and allow for the creation and deletion of custom previews and columns, where previews must be assigned to a user role, allowing detailed and multi-level access.
  - The alarm tree must include, but not be limited to, the following columns: unique ID, date and time, location, status, priority, current serving user, current serving customer, Service Level Agreement (SLA). Within the alarm tree, it should be possible to create an unlimited number of previews and counters of events that have occurred. Alarm trees must allow comprehensive formatting and filtering, allowing you to assign a color and sort order to a given priority. In addition, it must be possible to perform alarm grouping, and filters must allow the operator to efficiently manage large amounts of alarm data.
  - PSIM must allow the alarm handling process to match the implemented security operating procedure.
  - Workflow management software must be fully parameterized and capable of creating complex variable types.
  - Workflow management software must offer full control over all variables:
    - Logic tasks and activities;
    - Mathematical functions and operations;
    - Property Assignment;
    - Method call;
    - Evaluation and contingent actions;
    - Case finding.

- **Interfaces(integration protocols)**

- It is required to signal the interruption of communication with each integrated system by displaying an appropriate alarm message.
- It is required that the system has the ability to connect any device or system via a communication protocol.
- It is required that the PSIM system allows the connection of any devices that communicate via contact (control and supervision - including fire protection devices).
- PSIM must be able to receive and transmit information and events to and from devices associated with this project. This will allow full remote control of any devices and/or systems managed by PSIM. The PSIM platform must allow for seamless interoperability between security subsystems and devices, but must not replace them.
- The extent of interaction between these devices and the PSIM platform must depend on the capabilities of the software development kit (SDK) provided by each manufacturer.
- The PSIM solution must provide a calling mechanism that allows PSIM to respond to events occurring at any facility under PSIM control. In consultation with the Employer, descriptions of alarm scenarios must be provided to enable the creation of more complex alarm conditions that include a logical comparison of different calling objects.
- The system must allow control of subsystems, such as access control, to take over the access authorization function. If this is the case, it will also elevate the PSIM system to supervisor status under conditions specified at the configuration stage.
- The system, through integration with the KD access control system and the SWIN intrusion detection system, must provide the ability to count people at collection points for evacuation and count the number of people in the premises.
- The system through integration with SAP should provide the ability to lock and test items, reset the control panel, and clear alarms.
- The PSIM system must provide access to the technical documentation of the integrated systems, located with event handling, to allow a quick view for the system administrator.
- The PSIM system must guarantee compatibility to all available communication protocol updates.

- **Event handling**

- It is required to configure automatic routing of alarm events to the appropriate workstations.
- It is required to pass the event by the object user. In doing so, a mechanism is required to verify that the selected position is active. When the event is forwarded, only active posts with the user's ID (login) are displayed.
- It is required that all alarms have: notification time, notification number, system type, item number, logged-in operator.

- At all workstations, the system must report events visually and audibly.
- The ability to create individual operating stations for individual buildings as well as the ability to supervise all buildings from a single operator station.
- **Redundancy and backup**
  - It is required that PSIM has a built-in mechanism for automatic backups according to: schedule, on-demand, and by copied system fragments such as database, logs, services, configuration files, documentation, manuals, nested components.
  - Online backup and incremental backup are required.
    - It is required to backup the database and restore the system from the backup.
    - It is required to provide a server redundancy module that allows automatic switching to a backup server in case of damage to the primary server.
    - Switching to the backup server must be done with notification to the operator. For security reasons, switching to the backup server must require the user to log in again.
- **Reporting**
  - It is required that the PSIM system has a reporting module. Create daily, monthly, quarterly reports from the efficiency of the integrated systems.
  - The PSIM solution must have an integrated charting module to enable flexible reports.
  - The PSIM solution must provide a tool to visualize the information provided on the current status of the system.
  - All reports and charts must be generated as a Microsoft Office Professional application document (MS Word, MS Excel) or in Adobe Approval Portals Document Format (PDF).
  - PSIM must offer a graphical editor for selecting events from the database. Event search must be presented in the form of pie charts, line charts, bar charts allowing to reduce unnecessary information.
  - Reports should be created dynamically or manually by the user. It should be possible to display reports - on the workstation, the video wall or both at the same time.
  - Reports, charts, and operator performance information must include, but not be limited to:
    - Information on the type of events, location, time, date and action taken;
    - Information about user actions, response time to events.
- **Equipment**
  - PSIM server based on MS Server 2019/2021 operating system.
  - PSIM server must not be a dedicated server by which is meant the possibility of using any manufacturer.
  - The PSIM server must guarantee flexibility in the selection of components, subassemblies, accessories.

- The PSIM server and its components must not be certified by entities other than the hardware manufacturer.
- PSIM operator station based on MS Windows 10 operating system.
- PSIM operator station must not be a dedicated server by which is meant the possibility of using any manufacturer.
- The PSIM operator station must guarantee flexibility in the selection of subassemblies, components, accessories.
- The PSIM operator station and its components must not be certified by entities other than the equipment manufacturer.
- Requires is required, that system PSIM operated be on minimum dual-monitor stations and more with the ability to log in from anywhere.
- It is required that the PSIM system allows access to the PSIM system from the OS Android mobile application.

**Minimum requirements for PSIM server:**

- 8 Intel Xeon 2nd Generation Cores with a minimum clock frequency of 2.8Ghz
- 64GB RAM
- 600GB of SSD RAID class disk space IOPS
- Network card with a minimum bandwidth of 1Gbit/sec.
- Windows Server 2019 or better

- **Cyber Security**

- Using TLS 1.3 - AES256 encryption as a standard according to BSI specifications to secure communication between system components (e.g. Server, workstations, interfaces).
- Physical separation of PSIM and customer networks.
  - A browser-based, platform- and vendor-independent client application with a highly encrypted connection to the server (HTTPS).
  - Server-side protection and monitoring of application and data configurations against unauthorized changes.
  - Highly available server solution that provides high operational security and automatic switching to backup systems.
  - Encrypt a relational database using the AES256 encryption standard.
  - Protecting a relational database from unauthorized access.

## 13.2 YMS system

- **Preparation of deliveries**

- Storage of inbound and outbound delivery avocations, which will be referred to by tasks in the next steps of the process - avocations coming from TMS or created directly in YMS,
- Ability to advise external vehicle visits to the plant (except for logistics deliveries),
- Vehicle and driver data records,
  - The ability for drivers to register themselves (self check-in) at a self-service terminal before entering the site:
  - Choice of communication language (min. Polish, English, German, Russian),
  - Verification of driver and delivery data,
  - The ability to scan the documents required for a particular delivery, such as a tanker truck washing certificate,
  - Health and safety training implemented at the terminal,
  - issuance of a pass in the form of a proximity card with encoded advisory data,
  - pause support - the possibility for the driver to enter information about the time when he will not be available for loading,
- Alternative registration in the application by a QEMETICA employee.
  - Generate routes for driving inside the plant based on the purpose of the visit. In case of loading or unloading in several locations - selection of the most optimal loading / unloading path.
  - Directing to an outdoor parking lot or entrance gate based on advisory data and the current situation inside the plant.
- Automatic queuing of vehicles for service.
- Time window management.

- **Handling deliveries at the site**

- Recall vehicles z parking external: text message, boards synoptics, CB messages or other alternatives on the basis of:
- planned avocations for a given delivery,
- current monitoring potential delays or free loading capacity at the site,
- manual summoning of the driver by an authorized employee of QEMETICA.
- Control of barriers and traffic lights based on the read status of a particular vehicle (from a magnetic card or registration number from CCTV):
- Raising the barrier if entry is permitted,
- return to the parking lot in case of unauthorized substitution at the entrance gate, along with communication to a designated employee of QEMETICA (security).
- Handling of vehicle weighing from the terminal for self-service by the driver (entry and exit).
- Monitor travel time to designated checkpoints and dwell time at a point, such as in a warehouse during loading. Data storage and reporting in the form of Excel and dashboard.
- For multiple loading / unloading points - sending SMS messages about the next steps in the process.

- Generate an alert (to a designated QEMETICA employee) if you exceed the defined dwell time between checkpoints or arrive at the wrong service point.
  - Monitor the arrival of the vehicle at the checkpoint through the selected solution:
    - magnetic card,
    - CCTV reading of the registration number,
    - RFID gateway,
    - others proposed by the bidder.
    - Local GPS device
  - Printing of transport documents at the exit terminal after confirming the completeness of all defined steps required (e.g. loading / unloading at all points designated in the avigation, complete weighing and DMC compliance, return of pass). In case of discrepancies - alert to designated QEMETICA employee.
- **Email notifications to recipients**
    - Distribution of an email notification to the recipient of the commencement of delivery with a link to the opportunity to make a one-time complaint about the timeliness and/or quality of delivery.
    - Prepare an application that will be referred to by the link described in the section above or handle the request inside the Yard Management System. This application should be intuitive for the user with space for basic data for registration of the request:
      - cause of complaint - selection list,
      - The possibility for the submitter to add a comment,
      - The possibility of adding a photo by the submitter,
      - The claim entered by the recipient should refer in the report to the specific delivery within which the claim was registered. Such a report should be available in Excel and dynamic dashboard versions.
      - The request should go to the appropriate QEMETICA employee defined for the relationship / customer.
  - **Infrastructure**
    - Integration with IT systems as part of the data exchange defined in the business concept (ERP and/or TMS and/or weighing system).
    - Required native integration with MS Office 365 services (mailbox support)
    - In order to ensure communication between system components, it is required to implement structured network elements, in accordance with the requirements of the Employer and the general technical requirements of the LAN.
    - Communication between devices - based on TCPIP protocol.
      - Each device with a network interface must be connected to the Ordering Party's access point, prohibiting the installation of switching or packet routing devices.
      - System architecture: based on Vmware, Microsoft environments preferred (Windows Server, SQL). HA mechanisms required.

- **IT Security**

- The system should integrate with QEMETICA's existing mechanisms that implement authentication and authorization processes, preventing access for unauthorized Users and other systems that have not been previously granted the appropriate rights.
- The system should provide the ability to audit all attempts to get into the System in syslog logs with the principle of minimizing personal data.
- The system should provide for the recording of System malfunction conditions and their causes in system logs: event date, error ID, error description, etc.
- The system should include mechanisms for determining the retention time of log files along with a mechanism for archiving these files.
- The system should provide logging of all events and operations in the system log, performed by Privileged Users.
- The system should include mechanisms to prevent unauthorized users from editing and deleting log files and mechanisms to protect against overflow.
- The system should provide logging of all events and operations in the system log, performed by Business Users.
- The system should provide mechanisms to encrypt and store system logs and audit logs in a way that protects them from modification and unauthorized deletion.
- The system should be secured against vulnerabilities identified in the OWASP Top10 2017 (The Open Web Application Security Project) list, OWASP Application Security Verification Standard 4.0.1.
- Browser-based access to the System will be available using HTTPS and TLS from at least version 1.2, taking into account OWASP Top 10 configuration recommendations for known encryption algorithm vulnerabilities.
- The system must provide protection of information at rest (with data at rest) and in motion (with data in motion).
- The system in terms of source code must be free of inefficient designs, unused code fragments, unsafe designs, redundant data in the form of passwords, comments or information about the infrastructure in which the system runs.
- The system must provide for appropriate marking of generated documents to determine and confirm their authenticity.
- The system must provide SSL/TLS encryption during communication between all layers of the environment.
- The operating system, database, application layer must be hardened (hardening) by applying available configuration standards according to CIS benchmarks.
- All programming libraries, add-ons used to develop the System must be free of critical and high vulnerabilities according to CVSS 3.x (Common Vulnerability System Scoring) methodology.
- All programming libraries, add-ons used in the development of the System must be supported and developed, which is understood as meeting the condition of releasing a new version or patch within the last 6 months from when the work began

over the System. If this condition is not met, a manufacturer's statement of support and development must be provided.

- The system should pass penetration tests with a positive result (no vulnerabilities of the medium and higher risk level).
- The format of audiovisual files recorded by the system must be accepted by courts in the Republic of Poland in the event that the material has to be used as evidence in a case.
- The disk space on which audiovisual recordings will be stored must be encrypted according to the EFS standard.

- **Equipment:**

**Minimum requirements for the database server:**

- 6 Intel Xeon 2nd generation cores with a minimum clock frequency of 2.8Ghz
- 48GB RAM
- 800GB of SSD RAID class disk space IOPS
- Network card with a minimum bandwidth of 1Gbit/sec.
- Windows Server 2019 or better

**Minimum requirements for APP server:**

- 8 Intel Xeon 2nd Generation Cores with a minimum clock frequency of 2.8Ghz
- 32GB RAM
- 500GB of SSD RAID class disk space IOPS
- Network card with a minimum bandwidth of 1Gbit/sec.
- Windows Server 2019 or better

**Minimum requirements for a web server:**

- 4 Intel Xeon 2nd generation cores with a minimum clock frequency of 2.8Ghz
- 16GB RAM
- 240GB of SSD RAID Class IOPS disk space
- Network card with a minimum bandwidth of 1Gbit/sec.
- Windows Server 2019 or better

### 13.3 Access control system

- **Controller**

The AEOS Blue AP7803 controller is an advanced and cost-effective door controller. Adequate computing power combined with intelligent software components makes it possible to use all AEOS system functions in a single module. The controller's multifunctionality makes it suitable not only for use in new access control systems, but also for replacing existing systems. The AP7803's functionality is software-based, providing maximum flexibility. The product can even control restricted areas, turnstiles and elevators without



additional devices. Thanks to the software, the AP7803 can be adapted to new needs without replacing hardware. The powerful processor ensures fast execution of all operations and also allows fast data exchange with other door controllers in the network. Thanks to this solution, each door controller has full functionality even if the connection to the server is interrupted. This architecture provides an extremely efficient and scalable system.

The following are the minimum requirements for access control system controllers:

- Chassis dimensions no larger than 230 x 165 x 65 mm (H x W x D),
- Module dimensions no larger than 122 x 120 x 35 mm (H x W x D),
- Weight no more than Housing with module: ~0.7 kg, module: ~0.2 kg,
- Operating temperature range Housing: use 0°C - 45°C, storage: -30°C - 65°C
- Operating temperature range of the module: use: 0°C - 55°C, storage: -30°C - 65°C
- Relative operating humidity 20% to 90% (non-condensing),
- 800 MHz CPU controller, 256 MB SDRAM, 2 GB Flash memory,
- 10/100 Mbps Ethernet connection, RJ45,
- RS-485 bus On RS485 base (not isolated), line end selection by jumpers, support for up to 32 devices,
- PoE (Power over Ethernet ) PoE+: IEEE 802.3at:  
Readers: 500 mA at 12 VDC (used by both readers) Locks: 600 mA at 12 VDC (used by both locks) PoE: IEEE 802.3af, max. 500 mA at 12 VDC (readers only)
- External power supply  
12-27 VDC (min. 250 mA, max. 1.5 A at 12-27 VDC)  
Readers: 500 mA at Vin (used by both readers) Locks: 600 mA at Vin (used by both locks)
- Readers 2 x RS-485 or 2 x Wiegand
- Inputs

- 2x3 secured inputs (reed switch, button opening, evacuation button)
- 2 digital inputs (AC OK, discharged battery)
- Outputs
  - 2 x 1 relay (NC, COM, NO), max. 30 VDC, max. 2 A
  - 2 x 3 OC outputs (green LED, red LED, sounder, max. 20 mA each)
- Tamper detection
  - 1 optical tamper sensor
  - 1 digital input (for connection of external tamper contact)
- Status LEDs 1 status LED, 1 power LED, 2 reader LEDs
- Ethernet cable max. 100 m
- RS-485 cable 1 x 2 x 0.22 mm<sup>2</sup> shielded (100-120 Ω), max. 1200 m
- External power cable 2 x 0.5 mm<sup>2</sup> shielded, max. 5 m
- SAM socket 1x SAM socket

## • Reader

Convexs readers enable customers using an access control system to make a smooth and seamless transition to Mifare or DESFire technology. All Convexs readers are available for surface and flush mounting. AEOS can combine all frequently used reader and card technologies into one cohesive system. Systems using Nedap card technology can be easily adapted to Mifare/ DESFire cards and readers. This is because Convexs readers can be used in place of existing antennas. In addition, antenna wiring can be reused.

An additional advantage is that transitions can be deployed in controlled phases, as Convexs readers can handle many different card types simultaneously. With a wide selection of card technologies, secure data transfer between the card and the reader is achieved using CRYPTO1, triple DES or 128-bit AES encryption protocol. The configuration of Convexs readers determines functionality and performance. A configuration file is created with Aereco's software (AEOS REader COnfiguration) and inserted into the Convexs reader using AEmon software or a configuration card.



The following are the minimum requirements for access control system card readers:

- Dimensions no larger than 80× 80× 32 mm (L.× W × H)
- Weight not more than 0.2 kg,
- Power consumption 12-30 V DC, 70 mA at 12 V DC, 35 mA at 24 V DC,
- Temperature range: Operation: -20 to 55°C; storage: -30 to 65°C
- Relative humidity: from 10 to 93% (non-condensing)
- Communication:

RS485 (encryption AEOS or "plain" protocol; defined by the user)

Wiegand Data 0 and Data 1 (depending on configuration) RF modulator (120 kHz for AX1014 or AB350)

- Nedap detection range: about 8 cm; MIFARE: about 6 cm; DESfire: about 3 cm.
- Wiring:
  - Wiegand: max. 150 m; 2× 2× 0.25 mm<sup>2</sup> shielded,
  - RS485: 2× 0.25 mm<sup>2</sup>, max. 1000 m, 1× 2 × 0.25 mm<sup>2</sup>, shielded, communication only,
  - RF modulator: max. 50 m; 5× 0.25 mm<sup>2</sup> shielded, existing wiring (via Convex adapter),
- IP class Surface mounting: IP52, Flush mounting: IP54
- Certifications/approvals
  - CE: safety according to EN60950 standard
  - EMC: immunity EN50082-2, emission EN50082-1
- 24 V DC power supply, average: 19 mA, peak: 80 mA (immediately after power on or after lock/unlock)
- Connectors 2 RJ10 connectors for power and data, parallel cable connection
- Detection range ISO card with RF label 4.5 cm, wristband: 3.5 cm, keyfob remote control: 3.5 cm
- Frequency 120 kHz
- Serial channel wiring: RS485 without power supply: 1 × 2 × 0.22 mm<sup>2</sup>, shielded, max. 1000 m (depending on the reader) RS485 with power supply: 2× 2 × 0.22 mm<sup>2</sup>, shielded, max. 150 m (reader dependent) Wiegand: n× 0.22 mm<sup>2</sup>, shielded, max. 150 m (reader dependent)
- Sensor wiring n× 0.22 mm<sup>2</sup>, max. 100 m

- **Operator unit**

Minimum requirements for the KD system operator unit supporting the application AEOS:

Hardware requirements

- |              |                                                                                                                        |
|--------------|------------------------------------------------------------------------------------------------------------------------|
| • Memory     | 4 GB free for AEOS applications in addition to requirements regarding operating system and other software requirements |
| • Disk space | 50 GB free space for AEOS application and logbook AEOS server.                                                         |
| • USB ports  | One USB port free for the AEOS license key.                                                                            |

Program requirements

- |                    |                                  |
|--------------------|----------------------------------|
| • Operating system | MS Windows Server 2016/2019/2022 |
| • Browser          | Google Chrome or Microsoft Edge  |
| • AEOS             | AEOS Server+ Tools               |
| • AEOS client      | Java 11 and OpenWebStart         |

- **Access control system server**

**Minimum requirements for the access control system server:**

- 8 Intel Xeon 2nd Generation Cores with a minimum clock frequency of 2.8Ghz
- 32GB RAM
- 500GB of SSD RAID class disk space IOPS
- Network card with a minimum bandwidth of 1Gbit/sec.
- Windows Server 2019 or better

- **Software**

- The system along with the software should be freely expandable, providing scalability and modularity for phased implementation.
- The software should not have a limit on the number of identification cards in the system,
- Manage individual KD points by monitoring their status online,
- Should manage the rights of software operators with the ability to divide access to specific parts of the programs for groups of employees
- It should have the ability to create reports of all events in the system with the possibility of filtering them by: time, set time interval, card number, users, selected access control point, zone number,
- It should graphically illustrate the use of the card in the form of a photo of the user who is assigned to the ID card,
- It should have a visitor module to record the movement of visitors around the facility, The module should have the ability to enter the following data into the database: first name, last name, document number, PESEL, vehicle registration number, company, make of vehicle, purpose of visit, additional information, number of assigned ID card. In order to automate the process of entering visitors into the system, an ID card reader should be installed. The visitor module should display information about whether the employee to whom the visitor came is present at the plant. The module should also have information about the number of Guests staying at the Plant,
- Ability to view recorded events, so-called system logs,
- The system should allow multi-profiling, i.e., assigning one person to several authorization profiles,
- Provide the ability to record the operation of the entire system, to trigger certain actions upon the occurrence of certain events, such as displaying a message on the program screen, triggering an audible signal in the event of an attempt to force the door, driving an additional relay module on the client computer,
- Have the ability to filter readings (event registration), view employee transition paths, zone personnel states,
- The system should be able to graphically illustrate the distribution of readers in the building,
- The system should work with the fire and alarm control panel,
- It should signal door forcing - hardware and software, including the ability to work with an external surveillance system,

- Read registrations continuously to provide continuous access to current events in the controlled system. The system, after the start of periodic communication, is to carry out retrieval of data collected on the devices until the local data buffers on each device are emptied. At the time of downloading registrations and sending authorizations, the system should operate normally at all times (open doors for authorized persons).
- Enable control of system operation, granting rights to individual users, modification of access rules to specific rooms, preparation of reports.
- The ability for the operator to permanently lock or unlock the door at any interval.
- The application is to be able to specify additional parameters describing groups of employees.

### 13.4 Video surveillance system

- **Fixed camera of the "BULLET" type.**

The AXIS P1375-E camera is designed to be reliable in extreme conditions and climates. The camera operates in a temperature range of -40°C to 60°C (-40°F to 140°F). The IP66, IP67 and NEMA 4X rated design provides protection against water, corrosion and dust. Also available is the AXIS P13 Weathershield Extension A , which protects against snow or rain and prevents glare. The innovative design of the AXIS P1375-E provides easy access to connectors and cables, making installation fast and hassle-free. Built-in guides



make it easy to adjust or change the lens to a larger telephoto lens (up to 12 cm) or i-CS lens. The corridor format makes the camera ideal for monitoring corridors or tunnels, ensuring perfect adaptation to the monitored area, maximizing image quality and reducing demands on bandwidth and storage resources. With scene profiles, the camera can be automatically optimized for specific scenarios, so you can get the best possible video quality and reduce installation costs. The camera also has a video streaming indicator that makes it easy to see if the recording is working. The following are the minimum requirements for a BULLET fixed camera:

- Image sensor: CMOS
- Image sensor size: 1/2.8
- Technology to capture full-resolution color images with little blurring of objects in motion even in near total darkness, thanks to noise removal and enhanced photosensitivity.
- Wide dynamic range Forensic WDR imaging technology

- using a set of advanced algorithms that reduce noise and enhance the image signal to display every detail of the scene in the best possible way, switching seamlessly between WDR function and low-light mode.
- Minimum illumination/light sensitivity (color image): 0.07 lux
- Minimum illumination/light sensitivity (black and white image): 0.01 lux
- Remote focus
- Built-in infrared illuminator
- Built-in infrared lighting
- Local resource (memory card slot)
- Min. operating temperature range -30 to 50 °C
- For outdoor use
- Vandalism resistance class IK10
- IP class min. IP66
- Minimum video resolution: 1920x1080
- Min. number of frames per second 50
- Day/night operation mode
- Min. lens focal length range: 10.9 - 29 or 3- 9 mm
- Min. horizontal field of view range: 29-11 ° or 114-37 °
- Min. vertical field of view range: 17.9-6.5° or 58-21 °
- Min. optical zoom: 3
- Min. digital zoom : 12
- Compression: H.264 Baseline, High, Main, H.265, MJPEG
- A technology that reduces bit bandwidth and memory requirements, using intelligent algorithms so that information such as faces, tattoos, license plates and others suitable for investigation were identified, recorded and transmitted in full resolution and time-lapse.
- PoE Class: 3
- Signature firmware

- **Outdoor fixed dome camera**

The AXIS P3265-LVE camera provides exceptional image quality and detail for investigations in 2 MP resolution at up to 60 fps. The camera is available in two variants and offers a choice of lenses. The 9mm lens provides a wide surveillance range, ideal for large, open spaces, while the 22mm lens is ideal for surveillance from a distance, generating the accurate images needed for advanced analysis. With Lightfinder 2.0 and Forensic WDR features, the camera

provides accurate color reproduction and great detail in low light or near darkness. In addition, the camera is equipped with OptimizedIR technology, which guarantees sharp and clear recordings in total darkness at distances of up to 40 m (130 feet) without the need for additional lighting. This easy-to-install dome camera is designed to fit into any



environment. It is equipped with a varifocal lens with remote zoom and focus, so it can be adjusted to provide general and close-up views without manual fine-tuning. Audio and I/O connectivity allows for the integration of peripherals such as a microphone, which greatly enhances the value of the overall system. What's more, this rugged, outdoor-rated IK10 camera is equipped with built-in cybersecurity features to prevent unauthorized access and protect the system. For example, Axis Edge Vault secures the Axis device ID and simplifies authentication of Axis devices on the network. The following are the minimum requirements for an outdoor fixed dome camera."

- Image sensor: CMOS
- Image sensor size: 1/2.8"
- Technology to capture full-resolution color images with little blurring of objects in motion even in near total darkness, thanks to noise removal and enhanced photosensitivity.
- Wide dynamic range Forensic WDR imaging technology
- using a set of advanced algorithms that reduce noise and enhance the image signal to display every detail of the scene in the best possible way, switching seamlessly between WDR function and low-light mode.
- Minimum illumination/light sensitivity (color image): 0.1 lux
- Minimum illumination/light sensitivity (black and white image): 0.02 lux, 0 lux with IR illuminator on
- Local resource (memory card slot)
- Min. operating temperature range 0 to 50 °C
- For outdoor use
- Vandalism resistance class IK10
- IP class min. IP66
- Minimum video resolution: 1920x1080
- Min. number of frames per second 25
- Day/night operation mode
- Min. lens focal length range: 3.4-8.9 mm
- Min. horizontal field of view range: 100-36 °
- Min. vertical field of view range: 53-20 °
- Compression: H.264, H.265 Baseline, High, Main, MJPEG
- A technology that reduces bit bandwidth and memory requirements, using intelligent algorithms so that information such as faces, tattoos, license plates and others suitable for investigation were identified, recorded and transmitted in full resolution and time-lapse.
- PoE Class: 4
- Signature firmware

- **Fixed dome camera**

AXIS P3265-LV provides exceptional image quality and forensic detail at 2 MP resolution. Equipped with a 9mm varifocal lens for wide area viewing, it offers a 100-36 degree field of view and up to 60 fps at full frame rate. The camera has Lightfinder 2.0 and Forensic WDR features to ensure accurate color reproduction and great detail in low light or near darkness. It is also equipped with



with OptimizedIR technology, which guarantees sharp and clear recordings in total darkness at distances of up to 40 m (130 ft) without the need for additional lighting. The camera also offers Axis Zipstream functionality with support for H.264 and H.265 compression, which significantly reduces bandwidth and storage requirements without compromising image quality. The easy-to-install dome camera is designed to fit into any environment. The camera has a varifocal lens with remote zoom and focus options, so it can deliver general and close-up views without manual fine-tuning. Audio connectivity and an input/output interface allow the integration of peripherals such as a microphone, greatly enhancing the overall system. The high-performance camera has many integrated cybersecurity features to prevent unauthorized access and protect the system. For example, Axis Edge Vault secures the Axis device ID and simplifies the authentication of Axis devices on the network. The following are the minimum requirements for a fixed dome camera."

- Image sensor: CMOS
- Image sensor size: 1/2.8"
- Technology to capture full-resolution color images with little blurring of objects in motion even in near total darkness, thanks to noise removal and enhanced photosensitivity.
- Wide dynamic range Forensic WDR imaging technology
- using a set of advanced algorithms that reduce noise and enhance the image signal to display every detail of the scene in the best possible way, switching seamlessly between WDR function and low-light mode.
- Minimum illumination/light sensitivity (color image): 0.1 lux
- Minimum illumination/light sensitivity (black and white image): 0.02 lux, 0 lux with IR illuminator on
- Local resource (memory card slot)
- Min. operating temperature range 0 to 50 °C
- For outdoor use
- Vandalism resistance class IK10
- IP class min. IP52
- Minimum video resolution: 1920x1080
- Min. number of frames per second 25
- Day/night operation mode

- Min. lens focal length range: 3.4-8.9 mm
- Min. horizontal field of view range: 100-36 °
- Min. vertical field of view range: 53-20 °
- Compression: H.264, H.265 Baseline, High, Main, MJPEG
- A technology that reduces bit bandwidth and memory requirements, using intelligent algorithms so that information such as faces, tattoos, license plates and others suitable for investigation were identified, recorded and transmitted in full resolution and time-lapse.
- PoE Class: 4
- Signature firmware

## • **Fixed camera with 360° panoramic view**

With its Forensic WDR function, AXIS M3068-P provides clear images with dark and bright areas in the scene and exceptional 360° panoramic views at up to 15 fps. In addition, the day/night function provides high-quality black and white video images with higher light sensitivity even in low light. In smaller venues, it is possible to monitor an entire area with just one camera. The camera not only provides a full and clear image general, but also allows you to



zoom in and analyze recorded footage or live footage. Whether the event took place in the middle or in a corner, the camera provides a distortion-free view of the area thanks to its distortion correction function. AXIS M3068-P can provide a variety of distorted views, and multiple individually configured video streams can be taken simultaneously from the camera. The camera has its focus set at the factory, so it does not need to be adjusted. With the digital shift function, you can adjust the view rotation remotely and don't have to do it manually. In addition, the camera supports Axis Zipstream technology and compression with H.264 encoding and

H.265 significantly reducing bandwidth and storage resource requirements while maintaining image quality. The following are the minimum requirements for a fixed camera with 360° view:

- Image sensor: CMOS
- Image sensor size: 1/1.7"
- Wide dynamic range technology: Forensic WDR - imaging
- Minimum illumination/light sensitivity (color image): 0.32 lux
- Minimum illumination/light sensitivity (black and white image): 0.06 lux
- Min. operating temperature range: 0 to 40 °C
- Maximum video resolution: 2880x2880
- Min. number of frames per second: 25
- Min. lens focal length: 1.65 mm
- Horizontal field of view range: 185 °
- Vertical field of view range: 185 °
- Compression: H.264, H.265 Baseline ,High, Main MJPEG
- PoE Class: 2

- Signature firmware

- **High speed PTZ camera**

The AXIS Q6135-LE camera features OptimizedIR with automatically adjusting LED infrared illumination for surveillance in total darkness up to 250 m (820 ft) or more, depending on the scene. With the Sharpdome design, you can get a view 20° above the horizon with the same sharpness as below that. The camera has a 32x optical zoom, provides high-quality video images and clear details in 1080p HDTV resolution. The camera has a Lightfinder 2.0 function that allows it to capture sharp and saturated images of moving objects in low light.



The Speed Dry function, on the other hand, produces clear, sharp images in the rain and provides effective lens cleaning. With its processor, the AXIS Q6135-LE camera has many advanced security features to prevent unauthorized access and protect your system. Signed software and secure boot guarantee that the firmware has not been altered and that only authorized software is installed. The secure boot option guarantees that malware is absent when factory defaults are restored. Trusted Platform Module (TPM) with FIPS 140-2 Level 2 certification provides additional security. This module enables the secure storage of all cryptographic keys and certificates even in the event of a security breach. The following are the minimum requirements for a PTZ speed camera:

- Image sensor CMOS
- Image sensor size 1/2.8
- Lightfinder Technology Lightfinder 2.0
- Wide Dynamic Range Forensic WDR
- Minimum illumination/light sensitivity (color image) 0.06 lux
- Minimum illumination/light sensitivity (black and white image) 0.008 lux
- Built-in infrared lighting
- Optimized infrared module
- Memory card slot
- Operating temperature -50 to 50 °C
- Vandalism resistance class IK08
- IP class IP66
- Autotracking version Autotracking 2
- Day/night operation mode
- Electronic image stabilization
- Focal length 4.3 - 137.6mm
- Horizontal field of view 58.3-2.4 °
- Vertical field of view 34.9-1.3 °
- Tilt range +20 to -90
- Optical zoom 32
- Digital zoom 12
- High PoE Class
- Compression technology zpstream, H.264 Baseline, High, Main, H.265, MJPEG

- **Operator unit**

Minimum requirements for a VSS system operator unit:

|                            |                                                  |
|----------------------------|--------------------------------------------------|
| Hardware requirements      |                                                  |
| • Processor z card graphic | Intel® Core™ i7-11700K<br>Intel UHD Graphics 750 |
| • Cooling                  | SilentiumPC Fera3 HE1224                         |
| • Motherboard              | Gigabyte B560M DS3H                              |
| • Hard drive               | GOODRAM CX400 256 GB SSD                         |
| • Memory                   | GOODRAM 8GB 2666MHz DDR4                         |
| Program requirements       |                                                  |
| • Operating system         | Microsoft Windows Pro 10 64 bit                  |

- **Server**

**Minimum requirements for video surveillance system servers: 3**

**virtual machines per ARCHIVER role each equipped with:**

- 10 Intel Xeon 2nd Generation Cores with a minimum clock frequency of 2.8Ghz
- 24GB RAM
- 120GB of SSD RAID Class IOPS disk space
- 80TB of storage space for RAID video recording
- Network card with a minimum bandwidth of 1Gbit/sec.
- Windows Server 2019 or better

**1 virtual machine per DIRECTORY role:**

- 6 Intel Xeon 2nd generation cores with a minimum clock frequency of 2.8Ghz
- 32GB RAM
- 240GB of SSD RAID Class IOPS disk space
- Network card with a minimum bandwidth of 1Gbit/sec.
- Windows Server 2019 or better

## 13.5 Burglary and Robbery Alarm System

- **Control panel**

In addition to alarm functions, the advanced INTEGRA control panels also offer the possibility of implementing home automation and access control systems, making them ideal for implementation from small systems to extensive installations. In combination with additional modules - GSM and TCP/IP, they guarantee great communication capabilities. A big advantage of this system is the support of two SIM cards. The use of a second card allows a significant increase in performance and reliability of operation. To minimize the risk, it is recommended to use cards from different operators, thus avoiding possible problems from the provider. The control panel also allows you to monitor the funds on the card and informs you when they are close to running out. INTEGRA series control panels allow the use of the so-called prefix before the password. Such a solution allows you to extend the password to max. 16 characters, by adding from one to eight additional digits before the password. This feature allows to significantly reduce the risk of hacking into the system and at the same time increases the level of security of the control panel. In addition, the control panel can recognize whether the user is trying to disarm the system or is typing the password under duress, as the appropriate prefix is used. Such a solution is dedicated to places that require the highest standards of security, such as banking facilities, government institutions. The following are the minimum requirements for the control panel:

- Full compliance with EN50131 series standards for min. Grade 2
- built-in advanced 2 A+1.5 A power supply with extensive diagnostics
- expansion to min. 64 inputs with parametric resistance programming and 3EOL line support
- USB port for programming via PC
- The ability to divide the system into min. 32 zones and min. 8 partitions
- Expansion to min. 64 programmable outputs
- communication buses for connecting keypads and expansion modules
- built-in telephone communicator with monitoring, voice notification and remote control functions
- system operation with LCD keypads, partition keypads, keyfobs and proximity cards, and remotely with a computer or cell phone
- min. 64 independent timers for automatic control
- memory min. 5,631 events with print function
- support min. 192+8 users
- The ability to update the software via a computer.