Table of Contents

Product Description

1.1 General

The increasing complexity of technical building equipment demands a management system with superior performance, optimally combining the different technologies into a global security solution. This will protect persons and assets, while effectively utilizing manpower.

The management system must guarantee the strict regulation of security technologies, the highest level of reliability, and integrate new infrastructures such as the Internet.

Operators of buildings and facilities increasingly demand complete system solutions. A high capacity of integration and continuity of the system is a basic requirement for a management system.

Therefore the Building Management System shall provide bi-directional communication with monitoring and control of the following systems:

- Fire Detection Systems
- Intrusion Detection Systems
- Video Systems, such as DVR/NVR, matrix switches, encoders, decoders, storage devices, VCA and IP cameras
- Public Address and Voice Alarm systems (PA/VA) for evacuation and audio information
- Online and offline access control systems, visitor management systems, guard tour systems

Optionally, fully bi-directional communication with monitoring and control should also be available for the following systems:

- Perimeter fence control
- Emergency exit/escape route management
- People and asset tracking systems
- Intercom systems
- Building automation systems, such as DDC, heating/ventilation/air-conditioning (HVAC), elevators, escalators, light and energy management
- IP network and device surveillance (e.g. switches, routers)
- Mobile devices for security guards

1.1.1 Definition of Terms

ACS	Access Control System
BAS	Building Automation System
BMS	Building Management System
CCTV	Closed Circuit Television
DDC	Direct Digital Control (devices often used with BAS)
FAS	Fire Alarm System
HVAC	Heating, Ventilation, Air-Conditioning
IDS	Intrusion Detection System
LAN	Local Area Network
OLE	Object Linking and Embedding
OPC	OLE for Process Control
PA	Public Address
SMS	Security Management System
T&A	Time & Attendance
VA	Voice Alarm
VLAN	Virtual Local Network Area
WAN	Wide Area Network
WLAN	Wireless Local Area Network
…	

1.1.2 System Design and Functionality

The Building Management System (BMS) must be an open-architecture, PC-based system installed under Windows operating systems. It shall provide convenient control and information for security systems such as fire panels, intrusion detection systems, IP and analogue video systems and DVRs, access control systems, or public address / voice alarm systems, as well as for building automation systems such as lighting or blind control or HVAC.

The BMS shall run using the latest standard Microsoft SQL Server database for configuration and central event logging. It must be modularly designed, providing an individual system for specific requirements.

The system requires only a software license key on the central login server for system operation even for redundant server systems. No hardware dongle is needed. The feature licensing is done via an activation key created on a secure licensing server. The system's functionality can be extended by entering a new activation key. Hardware or software keys are not required at the client workstations.

1.1.3 Open Architecture

The BMS has an open architecture design. It supports industry standards for databases, networks, drawings, video cameras, and more, such as OPC, AutoCAD, HTML, ASPX, JScript and SQL. No customized or proprietary PC software or hardware is required to operate the system.

1.1.4 Server Structure and Workstations

Depending on the configuration or occurring load, the management system runs on one or more servers operating as one system. One or several of these servers are the central login servers for the operating level. The central login servers and optional connection servers run under one of the following operating systems:

- Windows Server 2008 R2 or Windows Server 2012 R2
- Windows 7, Windows 8.1 or Windows 10

Any standard PC hardware shall be usable. Multi-Core, Multi-CPU and high-end redundant hardware solutions are also supported.

The system operation uses networked workstations running under the following operating systems:

- Windows 7 or Windows 8.1 or Windows 10 (32 or 64 bit)

The BMS must provide a web server-based solution. Only Internet Explorer is required for a workstation to access the BMS login server.

The BMS server, the optional connection servers, and the workstations all connect using a standard IP network. It is also possible for wireless connection of mobile workstations (for example mobile phones or tablet PCs).

Workstations can connect using Intranet or Internet networks. Location maps and video images are delivered and adapted to the transmission conditions.

Communication between the central BMS server and the workstations must be secured with https protocol. The system displays the operating status of all servers and workstations/operators.

The BMS can access a remote database server by browsing remote SQL server instances or by manually entering the server name and database instance.

1.1.5 Subsystem Connections and Standard Interfacing

All subsystems, such as fire or intrusion panels, evacuation systems, or video devices are connected using the OPC interface standard. The BMS monitors these interfaces. The monitoring signals malfunctions and operational availability of the connection to each subsystem in the BMS user interface.

The OPC server supports the import of existing subsystem configurations for direct use inside the BMS configuration, avoiding double input of similar data.

It is possible to use OPC servers (software drivers) running on any PC inside the corporate network.

The BMS provides flexible expansion options for the hardware (interfaces, connection server). The connection of subsystems is possible on any connection server in the network. Redundant connections are available when supported by subsystems.

1.1.6 Workstations and User Interfaces

Client workstations are connected by standard IP network. Any computer in the corporate network is usable as a workstation. Mobile computers (notebooks) can access the system by wireless network connection (WLAN).

The system is expandable to support an unlimited number of integrated client workstations where up to 80 clients can operate concurrently per logon server.

The BMS user interface is browser based and provides a flexible and simple way (standard HTML/CSS format and JScript) to adapt to specific requirements, such as different operator groups. The adaptation must be possible with standard HTML editors such as Microsoft Share Point Designer.

The BMS supports up to four monitors per client workstation by using a corresponding graphics card. The user interface is easily adaptable to the number of monitors using standard HTML editors.

The BMS automatically adapts the screen resolution and number of client workstation monitors from where the operator logs in. It automatically provides the user interface and screen resolution assigned to that operator.

1.1.7 System Modularity

The BMS has a modular structure that provides specific project solutions. The system can be extended at any time. Common extensions are the number of operators, monitored detector points or camera channels.

Each module itself is also modular and extendable. The modules and their extensions, as well as all the common system features, must allow any combination, such as access control management with video or intrusion alarm management with video.

1.2 System Overview

The system can perform a wide variety of security management and administrative functions as part of a total integrated package. These functions include the following:

- Central alarm management and monitoring
- Distributed alarm management and monitoring
- Intrusion detection and security management
- Fire detection system and life safety management
- Video management and monitoring
- Access control management
- Public Address and Voice Alarm
- 3rd party system support, such as automation systems

1.2.1 Central Alarm Management and Monitoring

To support central or distributed alarm management and monitoring, the BMS must provide a wide range of display and control features. The user interface shall provide the same look and feel regardless of which alarm comes in.

Central Alarm Queue

The central alarm management and monitoring provides an alarm/event queue where all incoming events display on up to 3 different inboxes. At a minimum, the queue must provide the following information:

- Alarm date/time
- Alarm state
- Current alarm state
- Alarm location
- Operator who is working on the alarm/event when it was acknowledged

Up to 3 inboxes with different priorities can be configured. Each message will be automatically displayed in one of the 3 inboxes according to its priority. Messages can be manually moved from one inbox to another one.

Only authorized operators see the alarm. The display is controlled by the alarm/event priority. The alarm queue provides the acknowledging, deleting, and forwarding of entries. The system must handle up to 5000 alarms/events simultaneously for a short period.
A minimum of 500 events per second must be handled even on a long term.

Graphical Location Maps

The BMS must support the display of location maps in AutoCAD DWF format and other bitmap and vector graphics format. Drawings from AutoCAD versions up to 2016 must be supported.

The drawing format for the location maps must support a logical partitioning by defining sub-areas inside the drawing, by marking the area and giving a logical name.

The time-consuming conversion into a bitmap format and the splitting into sections should be avoided. In the case of structural changes inside the drawing (new walls, doors, and so on), no changes inside the BMS are necessary.

The BMS must provide a location tree to allow easy selection of locations and sub-locations, such as single floors or rooms. The location tree shall have no limits in the number of levels or sub-levels. Creating the location tree and the location names automatically by scanning the drawings for logical sub-areas shall be possible. A single click on the location/sub-location shall show the assigned graphics or sub-areas with all detector icons visible for that area.

The BMS must provide a zoom and pan feature for zooming into a location and move around inside the drawing, simply by using a standard mouse with click and draw operation. This allows operators to find a specific detector, door, or reader for fast control, such as open door manually, switch on/off lights, show camera live image, and so on.

The BMS must support multi-layered drawings and allow layers to be shown or hidden depending on the incoming event. For example, this allows the display of escape routes and fire extinguisher locations when there is a fire alarm. A manual layer control during normal operation must also be possible.

The BMS must provide an extensible library of standard icons for fire and intrusion detectors, doors, readers, cameras, PA amplifiers, loudspeakers, in 2D and 3D. You can place these icons directly onto the drawing. All assigned control commands are provided when clicking the icon.

When a detector point sends an alarm/event message, the assigned icon animates inside the drawing, displaying the corresponding event colour. The location and the relative size of an icon are definable inside the drawing and should be done by the architect or planner.

The BMS must provide a means of displaying icons corresponding to the current detector status, e.g.

- door	open - closed – blocked - …
- barrier:	open - closed – blocked - …
- camera:	motion alarm – recording - …

All icons are provided in a vector format, so that when the operator zooms in and out, the size scales automatically to the view.

Moving the mouse cursor over a detector icon provides a tool tip with detailed detector information, such as complete address, actual status, and detector type.

Alarm Documents/Plans

The BMS must support the display of individual alarm documents/plans depending on the alarm type. Individual documents display for:

- intrusion detection alarms
- fire alarms
- access control alarms
- video alarms
- maintenance and service alarms, such as pollution
- 3rd party events

The documents shall provide at least the following information:

- Alarm/event date and time
- Alarm/event state
- Alarm/event location
- Detector type and detailed address
- Detailed step-by-step instructions (Standard Operating Procedures)

To minimize the number of documents, they must support macros which are dynamically substituted by the real alarm/event data when displayed.

The documents must support the integration of bitmaps, live video, form elements (checkboxes, tables, and so on) as used in Microsoft Office to create specific forms, customizable control buttons to control subsystems directly, and any combination of these items.

The documents must be assignable to locations inside the location tree to display information when an alarm/event comes from a specific location.

The BMS must store an unchangeable snapshot of the alarm documents in the event log during alarm/event operation, providing seamless event reporting. The document’s format is based on open standards, allowing you to configure them using standard editors.

Device condition counter

The BMS must provide a means of basic status overview on all relevant system functions and subsystem devices. This display shall be freely customizable and placeable individually inside the BMS user interface. Possible content shall be

- Number of operators logged in
- Number of doors open
- Number of barriers open
- Number of windows open (magnetic contacts)
- Number of detectors in malfunction/technical alarm
- Number of fire detectors in fire alarm
- Number of fire detectors blocked
- Number of detectors in maintenance mode
- …

The content of that status overview or parts of it should be shown only to authorized operators.

A double-click on one of the entries shall provide a filtered list with all the individual detectors and devices corresponding to that status.

Schedules and Timers

The BMS must provide timer and schedule functions to support:

- time based display of information
- time based automatic controls into any subsystem
- time based access

The timer supports minimum 4 time frames per weekday, public holidays, and individual special days.

Operator Alarm

The BMS must support a manual alarm trigger by an operator to allow alarm operating caused, for example, by a bomb threat phone call.

The operator clicks on the relevant location inside the location tree and enters the specific alarm code. The alarm operating behind that trigger is identical to alarms/events from detectors, which means all assigned documents and drawings are displayed accordingly.

Message Processing and Escalation

The BMS analyzes all incoming events and messages. It provides a wide range of standard alarm/event states. There should be no limitation in creating additional customer specific states. For each event state, the following parameters are definable:

- State name
- Background/foreground color
- Alarm sound
- Priority

For alarm sounds, standard formats such as WAV, MP3 or WMA are supported. The priority directly controls the order how events are displayed. For example, if an operator is working on a malfunction event, and an intrusion alarm with higher priority comes in, this event is automatically placed in the foreground. The previous event is maintained in the background. The operator can toggle between all events he has acknowledged on his workstation. Assigned location maps and documentation toggle automatically as well.

The defined colors are used when animating a detector icon which has sent an event.

The BMS must support the definition of escalation scenarios if an operator does not react within a defined period of time. The BMS forwards the alarm/message automatically to the next defined and authorized operator group when the time period is exceeded. There is no limitation to the escalation levels. If no operator group acknowledges the alarm, the BMS supports a separate and automatic way of alarm notification as a final step.

The BMS provides a workflow feature to the operator that allows the forwarding of events to other operator groups which are also authorized to respond to such events.

Multi-client Capability and Partitioning

The BMS supports a multi-client capability that separates message distribution to dedicated operator or operator groups which are permitted to operate on those events. This shall allow at least:

- individual display of locations/location maps
- individual access to subsystems
- individual control into subsystems
- individual assignment of access hardware to tenants

Device Overview

The BMS must provide a real-time device overview of the entire system’s status. All connected subsystems are shown on a status tree, such as intrusion detection system (IDS), fire detection system (FDS), video systems, access control hardware, and individual detectors, as well as internal items, such as server or operator status. A direct control into subsystems is possible by clicking on panel/detector address.

The device overview supports state filtering/sorting to search for specific states, such as all detectors in malfunction or all doors in an open state.

The states inside the device overview are shown using the same colours as on the detector icon. This option can be blocked to certain operators.

1.2.2 Intrusion Detection and Security Management

The BMS shall provide the advanced and seamless connection, monitoring and control of OPC-compliant intrusion detection systems (IDS) and similar security systems, such as hold-up systems or perimeter fence control. It should support the standard detector types typically connected to those systems, such as:

- motion detectors
- glass break sensors
- seismic detectors
- hold up buttons
- magnetic contacts
- Light barriers
- RF barriers
- Electronic Radio Seals
- Input contacts (2- and 4-state mode)
- and so on

The BMS must provide the real-time overview on actual status of all connected detectors as well as the typical controls, such as reset, block, or activate single detector points. The BMS shows all possible states coming from a single detector, such as:

- alarm states, like intrusion or motion alarm
- malfunction states, like pollution or offline
- standby mode

The states are shown with corresponding event color/text and detailed detector group/address. If the detector is assigned to an individual location inside the location tree, the full location path is shown too, immediately identifying where the alarm is coming from.

The BMS must provide a library of detector icons, directly to be used in location maps, that support direct controlling of the detector by clicking an icon. The BMS configuration tool provides a simple way of assigning a detector type/icon to the detector addresses inside the subsystems by drag and drop or by auto assignment.

Arming and Disarming Zones/Areas

The BMS must allow authorized operators to arm or disarm existing areas/zones defined inside the IDS. The actual status of the areas/zones are shown real-time in the device overview.

Alarm Monitoring, Display, and Event Log

Any alarm/event coming from an IDS detector, the IDS itself, or from a similar system must be displayed real-time to all authorized operators on their dedicated workstations with all corresponding location maps, animated icons, and assigned alarm documents. At the same time alarms/events are stored in the BMS event log. All operator actions on such an event are also stored in the event log for seamless reporting.

Seamless Integration with Video Management

The BMS must be able to link directly to connected video systems. It displays live video from one or more dedicated cameras in the same user interface corresponding to the intrusion alarm/event highlighting the relation of the alarm with the alarm related video. The BMS also allows the automatic trigger of alarm archives in corresponding OPC compliant DVR systems. Links to such alarm archives are stored in the BMS event log, and allow direct access to the archive in later reporting.

1.2.3 Fire System and Life Safety Management

The BMS provides an advanced and seamless connection, monitoring and control of OPC compliant fire alarm systems. It supports the standard detector types typically connected to those systems, such as:

- smoke detectors
- flame detectors
- heat detectors
- fire push buttons, manual call points
- and so on

The BMS must provide a real-time overview of the actual status of all connected detectors, as well as typical control functions, such as reset, block, or activate single detector points, or switch them into maintenance mode. The BMS displays all possible states coming from a single detector, such as:

- alarm states, like pre-alarm or fire alarm
- malfunction states, like pollution or offline
- standby mode

The BMS displays all states using corresponding event color/text and detailed detector group/address. If the detector is assigned to an individual location inside the location tree, the full location path is displayed, providing immediate information about where the alarm is coming from.

The BMS must provide a library of detector icons, to be used directly in location maps, and which support direct controlling of individual detectors by clicking the icon. The BMS configuration tool provides a simple way of assigning a detector type/icon to the detector addresses inside the subsystems by drag and drop or auto assignment.

Fire Detector Maintenance Mode and Blocking

The BMS must allow to switch individual detectors or detector groups into maintenance mode, for operational testing on the fire system and the connected detectors. Activating a fire detector by using test gas or heat causes a maintenance alarm inside the BMS, and is handled according to the configuration.

The BMS must allow to deactivate/block individual fire detectors. This helps prevent false alarms if, for example, welding is taking place in the vicinity of a detector or detector group.

The actual status of the fire system, down to the individual detectors, must be visualized real-time in the device overview.

Alarm Monitoring, Display, and Event Log

Any alarm/event coming from a fire detector or the fire panel itself must be displayed real-time to all authorized operators, on their dedicated workstations, with all corresponding location maps, animated icons, and assigned alarm documents. At the same time, the BMS must store the alarms/events in the event log. All operator actions on an event must also be stored to the event log for seamless reporting.

Seamless Integration with Access Control Management

The BMS must allow to link directly to a connected access control hardware or an emergency door management system to open all doors along a dedicated escape route automatically.

Seamless Integration with PA or Evacuation Management

The BMS must allow to trigger automatically announcements in a public address/evacuation system. With the BMS timer functions, progressive evacuation scenarios must be definable. This allows, for example, the triggering of the same announcement with a defined delay for different floors. BMS must allow to integrate and monitor all critical PA/VA devices like network controllers, amplifiers, call stations, network bridges like CobraNet or Dante/OMNEO.

A seamless integration of PA/VA call management into the UI of the management system and display the current states of the audio zones in the AutoCAD maps must be possible.

Seamless Integration with Video Management

The BMS must allow to link directly to connected video systems. It can display live video from one or more dedicated cameras, in the same user interface for the surveillance of an escape route for example. At the same time, the BMS allows the automatic trigger of alarm archives in corresponding OPC compliant DVR systems. Links to such alarm archives must be stored in the BMS event log, and allow direct access to the archive when generating reports.

1.2.4 Video Management

The BMS must provide a fully integrated video management module for interaction with the following video systems:

- DVR and NVR systems
- IP video web server
- analogue matrix switches
- video encoder/decoder
- IP-based matrix switches based on encoders/decoders
- Network storage devices
- IP cameras

Any combination of the above systems must be possible to be able to mix existing video equipment with new devices.

The video management module must at least allow the display of live and archive images from these sources. The video streaming shall be IP based to allow flexible visualization on client workstations. Analogue video sources must be converted by an IP-based video web server or encoder.

Interfacing of Video Subsystems

Beside pure video streaming the BMS must provide a fully bi-directional interface to the video subsystems for monitoring and control. The BMS must provide the following features and commands:

- Show live image
- Show archive images
- Search/filter archives
- Status monitoring of digital inputs
- Control of digital relay outputs
- Switch camera to monitor (analogue and IP based-matrix switches)
- Auto dome controls
- Activating/deactivating video motion detection

The interfacing should be OPC compliant to provide direct import of existing video subsystem configuration, including all connected cameras and the camera type, inputs, outputs, available event states, and control commands. A second configuration of these devices inside the BMS should be minimized or avoided.

Video Display Features

The BMS video management module must provide additional display features for the visualization of live video or archive images inside the BMS user interface. The following visualizations must be possible:

- A matrix view with up to 16 camera sources per screen for manual camera selections
- An alarm matrix with up to 16 (4x4) camera sources for displaying alarm/event based live images
- Alarm documents with pre-defined video sources per alarm/event

The matrix view must provide a dynamic layout depending on the number of cameras selected simultaneously as well as a fixed layout where the operator can choose from 3:4 and 16:9 formats like 2x2, 3x3, 4x4 and asymmetric 1+5 and 1+7. When fixed layout is selected the operator must have the opportunity to display cameras in preferred fields/cameos, e.g. main entrance always in the middle.

The BMS must provide the possibility to simultaneously display different video sources/codecs. It must support at least the following video codecs:

- JPEG
- MPEG2
- MPEG4
- Wavelet
- H.264

The BMS must support an easy way for extending the system with other codecs.

Maximize and Zoom Feature

The video management module must allow operators to maximize single camera images, providing a better overview when something interesting happens inside the view. Additionally, a digital zoom feature must be provided for non-PTZ cameras.

Camera Selection

Cameras are selectable for visualization by clicking on a camera icon inside a location map, by click an address entry inside the BMS device overview, or automatically by defined alarm/event triggers. If chosen manually, the operator must have the possibility to select a live image or, if available, archive images from that camera. The mixed selection of live and archive images, and the simultaneous display in the same matrix view must be possible, to allow seamless reporting/replay of alarms/events, such as intrusion.

Playback of DVR Archives

An operator must be able to play DVR archives in the same way as selecting a live image display. The BMS video management module must allow the selection of an instant replay when clicking on a camera icon or device overview entry. A search, filtering by date and time, must be provided. This feature must be uniform for different DVR types in a mixed installation.

Camera and Matrix Favorites

The video management module must provide the storage of camera selections as favourites from the operator’s workstation. This should allow operators a fast and easy toggle between different camera selections, such as a day view and a night view, by simply selecting from the favourites list.

Auto Dome Control

Auto dome cameras that are detected during import of the video subsystem must be controllable using an onscreen keypad or, if supported by the subsystem, as an in-window PTZ control by using the mouse. The feature must be uniform for different auto dome types or video subsystems.

Analog Matrix Switch Control

The video management module must provide the control of analog matrix switches, including:

- switch camera to monitor control
- auto dome control
- monitoring alarm inputs

IP-Based Video Encoders/Decoders and Network Matrix

The video management module must provide the control of IP-based digital video encoders and decoders, allowing the setup of a network matrix switch distributed over the entire building or enterprise.

Video Content Analytics

The BMS must provide direct use of intelligent video analytics and alarming inside the central alarm management when supported by a camera or IP video device. It must be possible to trigger action on different recognized video scenarios, e.g. Idle Object, Crossing Line, Entering Field, Leaving Field, Crowd Detection and other

Video Motion Detection

The BMS must provide direct use of video motion detecting and alarming inside the central alarm management when supported by a camera or IP video device. All pre-defined alarm documents will be displayed and the camera’s icon shown in the location map is animated. The BMS must allow the operator to arm and disarm the video motion detection and alarming for an individual camera or globally for all video devices. This helps preventing false alarms during normal office hours, for example.

Privacy Zones

The BMS video management module must provide a means of defining privacy zones inside video live images to hide specific areas. This shall be independent from the video source. The hidden area inside a live image shall be dependent from the operator and his permission.

Other Video Alarms

Other video alarms, such as video loss or events on alarm inputs, are handled by the central BMS alarm management and monitoring. They are displayed in the alarm queue with all corresponding alarm documents and location maps.

Local Storage and Snapshots

In addition to DVR archives, the video management module must provide a local recording feature on an operator’s workstation. The recording must be captured in a standard format, such as AVI or DivX, so that the operator can replay the video using Windows Media Player or standard DVD player. Recording and replay has to be started with a single mouse click.
If the video source supports audio this should be recorded and replayed too.

The operator must also be able to capture snapshots of live images from individual cameras or the entire matrix. The snapshot must be captured in a standard graphical format, such as JPEG. The snapshot must include the following data:

- Date/time of snapshot
- Video source name(s)
- Workstation name where snapshot was captured

The snapshot must provide a print button for direct printing on a connected printer.

The BMS shall be able to access video files on iSCSI devices.

Reference Images

The video management module must provide the storage and retrieval of reference images per selected camera, to allow a simple detection of manipulation on a camera, e.g. viewing angle was changed.

Image freeze/unfreeze

The video management module must provide a means of freezing/unfreezing live images from any video source for enhanced analysis of critical situations.

Video Tour/Optical Guard Tour

The video management module must support a video tour from the selected cameras inside the matrix view, and also from a favourite camera list. After the video/camera sources are selected, the video tour starts with a single mouse click. The time for toggling must be definable by the operator.

Video Keyboard

The BMS video management shall provide an interface to a video keyboard which supports all features available on screen, such as:

- favorite selection
- maximize view
- create snapshot
- start video guard tour
- digital zoom in/out
- start/stop local recordings

The keyboard shall provide a joystick for auto dome control with moving and zooming and a jog-dial for quick search in the video archive. The control shall be uniform in a mixed installation of video subsystems.

The keyboard should be connectable by standard USB port to a BMS workstation, and is auto detected by the video management module.

Seamless Integration with IP video based Intercom

The BMS video management should provide a means of using the intercom functions of IP video devices supporting it, to set up a bi-directional communication to certain doors, for example, including the live streaming from the door’s camera. Together with the access control management complete door management solutions shall be provided.

Seamless Integration with Access Control Management

The BMS must provide a direct interaction with the access control management module, allowing the operator to display dedicated camera images when there is an access control alarm, such as

- duress alarm
- door open time exceeded
- card/cardholder not authorized
- card unknown
- tamper alarms

Together with the alarm document feature inside the BMS’ central alarm monitoring, the video management module shall provide a higher security level together with the video verification mode of the access control management.

Seamless Integration with Intrusion Management

The BMS must provide a direct interaction with the intrusion management module to allow the display of dedicated camera images when there is an intrusion alarm. The BMS must be able to trigger alarm recordings inside connected DVR systems. The

BMS must store those alarms in its event log that an operator can directly link from the alarm entry to the corresponding alarm archive of the DVR.

1.2.5 Access Control Management

The BMS must provide a fully integrated access control solution containing an access management module and the connected access controller, access readers, and input/output extensions.

The access management module shall provide a wide range of access control functions, for individual customizing of site, building, and floor access permissions, time profiles, schedules, and access alarm events.

All access control alarms, such as door open time exceeded, access denied, card unknown, and more, must be directly handled by the central BMS alarm management and monitoring. Access alarms/events must be visualized with all the common BMS display features like location maps, alarm documents/instructions, live video, and more.

Access Controller Hardware

The access controller must be a rail mountable device for use in specific enclosures as well as existing standard 19” racks.

In particular, the access controller connects to the host computer using common interfaces, such as Ethernet, RS-232, and RS-485 with open and encrypted protocol.

The controller shall have a modular design with downloadable software so that the application program can be easily updated without touching the controller itself.

The controller shall have a liquid crystal display and a button for selecting the display of all network parameters like IP address, DHCP, MAC address, and the state of all inputs and outputs.

The controller, input-output interfaces, and card readers shall work in off-line mode if there is a failure with the network/host connection.

The access controller must support up to four proximity readers with standard Wiegand interface or up to 8 serial readers using RS485 connectivity and an open and encrypted bus protocol like OSDP-SC or OSDP version2. The controller must provide a means of extending the number of Wiegand reader to a total of eight. The controller must support the following reader/card formats:

- Wiegand connection
  - Mifare Classic
  - Mifare DESFire EV1
  - LEGIC Prime
  - LEGIC Advant
  - Prox 26 Bit
  - EM 26 Bit
  - HID corporate 1000
  - HID iClass
  - HID and Suprema Biometric Reader
  - Balogh Long Range Readers
- Or serial connection
  - Legic Prime and Advant
  - Hitag 1 and 2
  - Mifare Classic and DESFire
  - Suprema fingerprint reader

With Wiegand readers the access control management must provide up to four different card formats to be used simultaneously.

The access controller shall provide eight inputs and eight outputs, expandable to 64, using I/O extensions connectable using standard RS-485. All inputs must be usable in 2- or 4-state mode. The configuration software must allow flexible definition of the resistors/terminators used in 4-state mode wiring.

Once extended, the basic access controller shall also show the states of the I/O extensions in its display. The I/O extensions must also be rail mountable.

The access controller should support standard CF flash memory for storing cardholder data and access events. The CF memory must be formatted with a standard FAT file system, to allow reading them using a standard card reader connected to a computer, if the access controller fails.

The access controller memory shall be expandable to store up to 200,000 cardholders.

The access controller, with the corresponding BMS access management module, must provide a simple way of configuring entrances in the form of pre-defined door templates. The administrator of the access system must be able to configure an entrance by selecting from a list of door models. The following door templates should be provided by the system:

- Door with entry and exit reader
- Door with entry reader and request to exit button
- Door with entry or exit reader
- Parking lot with barrier and traffic light control
- Elevator with floor control
- Mantrap
- Door with combined arm/disarm IDS feature
- Time and attendance door
- Combined car/truck entrance with double reader

Selecting a pre-defined door template automatically assigns the next free reader/input/output channel inside the controller to the chosen function. The access configuration shall provide a wiring table for the installer for printout.

A controller internal configuration tool allows the installer to set up associations to extend e.g. pre-defined door templates using spare inputs and/or outputs. This tool shall allow also the triggering of spare relay outputs based on standard access or door events, such as door open time exceeded turns a local buzzer on. The tool must allow the installer to define the period of time, pulsing, and pulse length. The defined associations must also run when the access controller is in offline mode.

The access controller is CE approved. A UL variant shall also be available.

Cardholder Enrollment

The access control management module must provide an easy way of entering cardholders to the internal database. In addition to basic data, such as first name, last name, badge number and access authorizations, the following information must be possible:

- PIN code
- Validity period
- Membership
- Status fields, such as employee, visitor, guard
- Address fields
- Personal data
- Individual fields editable by administrator

It is possible to enter the badge number manually or by enrolment readers connected to the operator’s/administrator’s workstations.
Up to 5 cards per cardholder shall be possible.

Central Cardholder Management

It shall be possible to enroll all cardholders and access authorizations on one central server and replicate this information to distributed access control databases on connected access control servers. This helps in distributed systems with several servers to maintain and synchronize cardholder information and access authorizations online on all connected servers.

Import/Export of Cardholder Master Records

The access control management must provide an import/export interface to import existing cardholder master records from a personal database or Time & Attendance system, or to export the master records for further use by another application.

The interface must support both comma-separated and fixed-field-length format files. An easy adaptation to that file format must be possible. Different import files with different formats are supported simultaneously.

The interface supports the definition of import/export rules, such as split an incoming name into first name and last name fields.

The interface supports the definition of schedules for automatic importing and exporting.

API for Master Data, Time Stamps and Commands

An application programming interface shall be available to integrate with 3rd party systems like visitor management, identity management via a C++ or C# interface.

Badge Design and Card Printing

The access control management must provide a tool for designing badges. The tool supports the input of bitmaps, text and all database fields, such as name or badge number. The tool supports standard badge printers that come with a Windows compliant printer driver. Printing on both card sides is also supported if the printer can do. It shall be possible to support at least HID / Fargo printers.

PIN Code and Duress Alarm

The access control management must support the input of a PIN code for each cardholder. The length of the PIN code is defined once in the system. The input of a validity period has to be supported.

The access control management must provide a duress code alarm feature that generates an alarm in the central BMS alarm monitoring and management when cardholders key in their PIN codes in another defined way.

Blocking Cardholders and Blacklist

The access control management must allow the blocking of cardholders, for example by validity period. An operator must also be able to add badges to a black list, for example when stolen or lost. If a black-listed card is used at a reader, an alarm has to be triggered in the central BMS alarm management and monitoring, displaying all defined and corresponding alarm documents.

Special Days, Day Models, and Time Models

The access control management must allow the creation of time models, containing day models/periods and the specific handling of special days, such as public holidays. The definition of time models provides a simple way of defining periodically recurring day models, which have a specific order. The time models can be combined with the access authorization at entrances/entrance groups.

Access Authorizations

The access control management must provide the grouping of entrances, which can consist of one or more readers. An entrance can be used in several groups. Access authorizations/entrance groups must be assignable directly to a cardholder, or be combinable with time models using area-time authorizations.

Area-Time Authorizations

The access control management must allow to combine access authorizations with time models. The assigned time model defines the time when an access authorization is active at an entrance/entrance group.

Access Profiles

The access control management must support the grouping of access authorizations or access-time authorizations, providing an easy way of assigning frequently used access profiles to employees and visitors.

Areas

The access control management must support the defining of areas. An operator must be able to create separate areas for persons and vehicles (parking lots). Areas have to be assignable to entrances, allowing the tracking of persons, area balancing, and mustering. Passing an entrance/reader assigned to a parking lot shall show the location of the person’s car, or the location of the people using other entrances/readers.

Area Balancing and Mustering

The access control management must allow area balancing. All doors to an area must have an entrance and exit reader, allowing an exact tracking and counting of people inside an area. In case of an emergency, the system must provide an area muster list.

It must be possible to use the area balancing to interact with other subsystems connected to the BMS. For example, it must be possible to switch on/off the lights inside an area, when the first person enters or last person leaves.

Route

The access control management must allow the definition of routes, which are special access authorizations that force the cardholder to pass readers in a fixed sequence. Route checking must start automatically when the first reader is passed, and ends after passing the last reader. Any violation by the cardholder should trigger an alarm in the central BMS alarm management and monitoring.

N-person Access

The access control management must provide the possibility to allow access to an entrance/door only when at least two authorized cardholders swipe their badges. The number of cardholders for that kind of access check in front of an entrance shall not be limited by the system.

Access Sequence Check

The access control management must provide an access sequence check, allowing an authorized cardholder to enter a door or group of doors belonging to an area only when he has already passed another dedicated door.

Guard Tour

The access control management must provide the possibility to use existing access reader hardware to perform guard tours. The system must allow the grouping of readers to a guard tour sequence. The delay time a guard needs between two readers (checkpoints) must be definable. All violations, such as wrong sequence or timeout, should trigger an alarm in the central BMS alarm management and monitoring.

Visitor Management

The access control management must allow the administration of visitors in the same database. Visitors are handled separately from employees.

The following additional information shall be assignable to a visitor:

- Identification number
- Address

- Photo and signature
- License Plate Number of Vehicle
- Person to visit
- Attendant necessary
- Expected arrival and departure date and time
- Actual arrival and departure date and time
- Reason for visit
- Access authorizations

The visitor management shall allow the printing of a visitor badge from this data. The printout of a visitor pass for acknowledgement shall also be possible.
It shall be possible to monitor the presence of a visitor in a virtual attendance tableau (soft tableau) and alert the security operator of an overstaying visitor

Video Verification

The access control management must allow video verification access, by combining access control with existing video devices via the BMS video management. The dedicated readers are configured for verification mode by a checkbox in the configuration.

Instead of opening the door directly when a card is presented, the reader/controller shall generate an event in the central BMS alarm management and monitoring. The reader is identified in a location map, and a corresponding alarm document displays the database image of the cardholder along with a live image from the corresponding door. The operator must determine if both images match, and can decide to open the door or to deny the access.

Elevator Control

The access control management shall allow the definition of floor authorizations, and can assign them to card holders. If a cardholder presents his card at an elevator reader, the system shall activate the elevator’s floor buttons the cardholder is authorized for.

Car Park Management

The access control management shall allow the administration and control of parking lots. This includes the administration of the access authorization and the control of barriers and traffic lights. The system must provide the possibility to limit the number of vehicles inside a parking lot so that a balancing is possible, and the traffic lights are controlled accordingly. An online overview of the occupancy status of parking lots must be available. It must be possible to recognize overstaying car parkers. For guests parkers an assignment of multiple entry tickets (vouchers) must be available.

Random Screening

The access control management must be able to perform an additional security check at the site/building exits. The readers at such exits are easily set to that mode by checking a checkbox and setting the frequency. Randomly the door will not open, and at the same time an event is triggered in the central BMS alarm management with all the corresponding location maps and alarm documents. The cardholder’s badge is now blocked in the entire system. The operator/guard must check the cardholder and his personal belongings. Afterwards, he opens the door manually by clicking on the door icon inside the location map and re-activates the badge. Optionally if no operator/guard is available the door will be unblocked after a configurable time.

Handling of VIP (Very Important Persons)

The access control management shall allow the identification of persons as VIPs, so that the administrator/operator has a simple way to exclude such persons from random screening, or to disable the PIN code check for them. Also unauthorized operators shall be prevented from changing VIPs’ access rights.

Time and Attendance Data

The access control management must support access control readers as time and attendance readers. The booking events are stored in the central event log. The event log supports the filtering for such events and the export into standard CSV format text files for use in other applications.

Access Control Management Alarm Events

The access control management must provide a wide range of standard alarm and event states. The following alarms/events must be supported:

- Card unknown
- Card not authorized
- Card outside time profile
- Card anti-pass back
- Access timeout
- Door open time exceeded
- Door opened unauthorized
- Door blocked
- Tamper alarm controller
- Tamper alarm reader
- PIN code error
- Duress alarm code
- Access denied
- Wrong card version
- Card blocked
- Card blacklisted
- Card out of route
- Guard tour alarms
- Random screening
- Other individual alarm extensions

All access control alarm/events must be handled by the central BMS alarm monitoring and management, so that corresponding location maps, alarm documents, and live video are shown in the configured way.

All events are logged in the central BMS event log together with all assigned alarm documents for a complete reporting.

Cardholder Images

The access control management must provide standard features for taking photos, scanning, or importing cardholder images for the cardholder database. Stored cardholder images must be displayed automatically in the video verification alarm document.

Operator Permissions

The access control management must allow the setting of individual operator permissions per single dialog screen. Permissions can be set to:

- read only
- read and write
- read, write, change
- read, write, change and delete

Audit trail for master record operations

The access control management must provide an audit trail for changes on cardholder master records as well as changes on access permissions. The audit trail must log at least the following operations

- create, delete a cardholder master record
- change cardholder master record content, e.g. name, address
- change cardholder access rights
- create, delete an access permission
- change access permission content, e.g. time profile

Workstation Profiles

The access control management must allow the setting of individual workstation profiles. This allows, for example, blocking/hiding of individual dialogs at dedicated workstations. This raises the security level.

Seamless Interaction with Video Management

The BMS access management must provide a seamless integration and interaction with the video management module, allowing video verification or surveillance of e.g. parking lots.

Seamless Interaction with Fire Management

The BMS access management must provide a seamless software integration and interaction with the fire management panel, allowing the automatic opening of dedicated doors along an escape or rescue route.

Seamless Interaction with Intrusion Management

The BMS access management must provide a seamless software integration and interaction with the intrusion management panel, allowing the automatic blocking of dedicated doors belonging to the intrusion area.

Seamless Interaction with Offline Doors

The BMS access management must provide a seamless integration and interaction with offline locks or door fittings on remote doors which do not have cables or online connection.

Seamless Interaction with Key and Asset Management Systems

The BMS access management must provide a seamless integration and interaction with key and asset management systems to manage and monitor access to brass keys and assets like mobile phones, weapons and documents.

Seamless Interaction with Automatic Number Plate Recognition System

The BMS access management must provide a seamless interaction with Automatic Number Plate Recognition systems as additional check from the access controller.

1.2.6 3rd Party System Support

The BMS must provide the connection of OPC-compliant 3rd party systems, integrating them into the entire security solution. The following systems should be supported as subsystems:

- Building automation systems
- Perimeter fence/wall control systems
- IP network and device monitoring
- Intercom systems
- Emergency exit management
- And so on

The BMS must be able to perform a selective import of the existing 3rd party subsystem configuration, such as detector addresses and corresponding event states.

The BMS must provide at least the possibility to monitor the status of such subsystems and their peripheral devices. If supported by the subsystem, control is also possible.

The BMS must provide the definition of the specific event states as an alarm event, which are handled in the central BMS alarm management and monitoring with all corresponding alarm documents and location maps.

Building Automation Systems

The BMS must allow the monitoring of defined items inside OPC-compliant building automation systems, such as DDC/PLC units, air conditioning, ventilation, and others. This allows alarms in case of malfunctions, such as the air conditioning of a computer centre, which might cause damage of computer equipment.

If provided by the subsystem’s controls, the BMS can, for example, control ventilation flaps if there is a fire alarm.

If the subsystem's OPC server provides raw (analog) values the BMS must be able to display them via configurable means on the client monitor.

Perimeter Fence/Wall Control System Monitoring

The BMS must allow the monitoring of perimeter fence/wall control systems. In case of an alarm at the fence/wall, the BMS must show the location inside the location map view, display live images from dedicated cameras, switch exterior lights on in that area at night, and trigger an archival image storage inside a connected DVR system.

IP Network and Device Monitoring

The BMS must allow the monitoring of vital IP network devices, such as servers, printers, routers, using standard SNMP traps and existing OPC-compliant drivers. In case of malfunctions, the defined procedures in the central alarm management and monitoring are activated, showing location map, animated detector/item, and alarm documents instructing the operator what procedure to follow.

Emergency Exit Management Systems

The BMS must support the connection of OPC-compliant emergency exit management systems, such as Dorma, allowing the automatic release of emergency/escape exits in case of a fire alarm.

Seamless Interaction with other BMS Modules

The BMS must provide a seamless integration and interaction between the 3rd party systems and the access control, intrusion, video and fire management modules.

1.2.7 Integration with Third Party Applications

Backend Interface

The BMS must provide a means of backend interface that allows to connect itself as a subsystem to other building management systems, such as

- Building automation systems
- SCADA systems (Supervisory Control and Data Acquisition)
- PSIM systems (Physical Security and Information Management)
- ERP systems systems (Supervisory Control (Enterprise Resource Planning)

Those systems can monitor and control all to the BMS connected subsystems, e.g. status of doors from the BMS access control management. Realization of this interface shall be configurable and shall not require any development of code.

Access Control SDK

The BMS must offer an SDK based on C++ or .NET languages to integrate third party applications with the BMS. It shall be possible to synchronize master data (i.e. cardholder data, authorizations) with, send access events with time stamps to and receive commands (i.e. door commands) from the third party application.

1.2.8 System Operation

Operators and Authorization Management

The BMS must allow the creation of individual authorizations per operator or operator group. This includes:

- selectable displaying, monitoring, and control of locations, such as individual floor, building, or site permissions
- selectable displaying, monitoring, and control of subsystems, such as intrusion, video, fire, or access control panels
- selectable displaying, monitoring, and control of detector points, such as readers, doors, cameras, or intrusion detectors

Especially when the BMS access control management is used, the system grants access control operators the following permissions on the master records and event data, per dialog:

- read only
- read and write
- read, write, and change
- read, write, change, and delete

Operators and Login

The BMS must provide a separate login as well as login via Windows authentication (single login). The behaviour must be customizable. A 2-men-rule login for certain operators and permissions must also be possible.

Data Security and User Account Control

The BMS must allow to associate an operator login to a dedicated workstation. The BMS must support a minimum 128-bit data encryption according to a certified algorithm for communication between the central server and all connected workstations. BMS must allow to change all necessary passwords regularly. Default passwords shall be complex and not hard-coded. Brute-Force-Attacks shall be made ineffective. It shall be possible to avoid storage of sensitive information like error logs on the server.

Central Configuration Tool

The BMS configuration must be simple and intuitive for the administrator. The system provides one central configuration platform/tool from where everything concerning subsystems, system behaviour, cardholder settings, display features, and authorizations is set up.

The BMS configuration must support the direct implementation of OPC-compliant subsystems. Existing subsystem configurations are imported by the BMS configuration to avoid entering data a second time.

The BMS configuration must support a network search/browse of network devices, such as DVR or video web server. Network settings of subsystems and the integration of 3rd party configuration must be possible.

Subsystem and Detector Programming

Subsystems and their peripheral devices must be easily and intuitively configurable in the BMS configuration tool. If supported by the subsystem, a direct import of its data must be provided by the BMS.

Customizing the User Interface

The user interface must be adaptable to the information requirement and the expertise of the operator, and to the configuration of the workstations (resolution and number of monitors).

The BMS application shall be a web server-based solution. On the operator workstations, no additional software must be installed locally. Only Internet Explorer (version 9, 10 or

11) is required to log into the BMS. The user interface shall be browser-based, using standard HTML format.

This allows easy customization using standard HTML editors. The BMS shall provide one default user interfaces which adapts to all 1-monitor standard resolutions and also for 2048x768, 2560x1024 (2-monitor operation).

The BMS administrator or installer can adapt these default interfaces to individual requirement using a standard editor. The following adaptations must be easily possible:

- Integration of corporate logo(s)
- Integration of corporate images as wallpaper
- Individual contents per operator or operator group
- Individual contents corresponding to the workstation

These settings are necessary only once. The BMS must automatically detect from where an operator is logging in, and supplies the right contents and resolution to him.

The BMS must provide a toolbox containing all specific controls for display features, such as location tree, alarm queue, toolbar, customizable action buttons, for individual use in HTML files.

To create customized workflows and user interfaces scripting shall be supported in HTML pages using JScript.

From any detector a predefined URL shall be available by a simple mouse click displaying additional information to the detectors / objects on demand.

Association Management for Display and Control

The BMS must provide an easy and intuitive way of defining/designing the system behavior in case of events/alarms. The system must allow the definition by easy IF/THEN or IF/THEN/ELSE conditions as well as AND and OR operations. The following triggers are possible for these conditions:

- Event/alarm from any single detector point
- Event/alarm from any group of detectors
- Event/alarm from any subsystem, such as common status
- Event/alarm from any subsystem interface
- Internal timers, such as timeout in alarm operating
- Status changes of alarms/events, such as deletion or forwarding by operator

The following outputs are possible when a condition/trigger is TRUE:

- Display message to authorized operators
- Display corresponding alarm documents and location maps
- Control automatically the triggering detector, such as reset
- Control automatically any other connected detector, such as displaying a dedicated camera
- Control automatically any group of detectors, such as switch all lights on a dedicated floor
-
- Start internal timer for creating time-dependant chains of events, such as PA evacuation announcements on different floors with 20 seconds delay
- Influence internal variable counters (count up/down) to count the number of specific events, such as generating a new event when 100 persons have passed a light barrier

Combined with the BMS timer/scheduler, time-dependant results must be possible, such as forwarding of alarms to dedicated operator groups depending of the day time.

Printer

The BMS must support any standard laser or inkjet printer that comes with a Windows-compliant printer driver for use as an alarm printer. The printers must be connectable directly to a workstation or to the network.

The BMS must allow the manual and automatic printing of all alarm documents, including location maps and instructions, and alarm details, such as location, detector address, and type.

The BMS access control management must support standard badge printers from the market that come with a Windows-compliant printer driver.

Event Log

All events, messages, controls, or alarms in the entire system, such as user login, fire/intrusion/access alarms, shall be seamlessly logged in the central BMS event log. The stored information must be secure from manipulation.

Individual filter functions shall be definable for outputting to screen or printer. Operators must have the ability to store their own individual filters. An export in a standard CSV format text file must be possible for additional processing in other applications.

Reporting Services

Report generation shall be available either from the event log page or directly from any detector in the device or location overview to display events from the event log database.
Reports shall be interactive allowing to zoom in with a mouse click for more detailed information
A set of minimum five pre-defined reports shall be offered.
Display, refresh, export and print functions shall be available for the reports.
Microsoft Report Builder 2.0 shall be used to create custom reports.
Ad hoc information of any detector shall be available on mouse click.