Contents

1 Subject of specification 2
2 Scope of validity 2
2.1 Deviations 2
2.2 Exclusions 2
3 Definitions 2
3.1 Basic terms 2
3.2 Ambient Conditions 3
3.3 Electrical data 3
4 Description 3
4.1 Operation Principle 3
4.2 System Requirements 4
4.3 Main control panel 6
4.4 System components 7
4.5 Signal wiring 9
4.6 Electrical Supply 10
4.7 Painting 10
4.8 Labelling 10
4.9 Services 10
4.10 Cables, Conductors, Secondary Items 11
4.11 Documentation 11
5 Relevant documents 12
6 Norms and standards 12
6.1 Regulations 12
6.2 Polish standards 13
7 Enclosures 13
8 Record of changes 14

This document is the property of Grupa LOTOS SA.. Coping and giving it to other are forbidden without express written authority by Grupa LOTOS SA

1 Subject of specification

This specification used in conjunction with other technical specifications of LOTOS Group S.A. (GL S.A.) establishes the minimum requirements for the design and manufacture Burglar Alarm System.

2 Scope of validity

This specification applies to the preparation of tender documents, inquiries and contracts concerning new investments and modernization projects planned by LOTOS Group S.A.
It shall also be a basis for preparing both detailed specifications and inquiries for individual or package unit supplies.

2.1 Deviations

Any deviations from this specification and relevant specifications, standards and documents, including the bidder's proposals indicating a more economic design or solution, shall be submitted in writing for checking and approval by LOTOS Group S.A. No deviation or modification shall be permitted unless confirmed in writing by LOTOS Group S.A.

The bidder shall present in written form any ambiguity in this standard or any other LOTOS Group S.A standards as well as conflict with referenced documents/standards, and shall receive LOTOS Group's written explanation.

2.2 Exclusions

The specification does not include:

- Requirements for low voltage power distribution system
- Requirements for cable parameters
- Requirements for cable routing and laying.

Above-mentioned exclusions are scope of separate specifications

3 Definitions

3.1 Basic terms

Flash memory - the memory, where the control panel basic program is stored. It is cleared electrically, and its contents may be changed with the use of computer.

Object - group of partitions being an independent alarm system.

Partition - group of zones supervising separated part of object. Arming and disarming is carried out simultaneously for the group.

Zone - pair of contacts at the control panel main board or module board (connected to the control panel by means of bus), to which the detectors are connected. The control panel monitors detector statuses via the zone.

Zone violation - Change of zones status when the detector is activated (for example: zone contact opening or shortening, change of detector parametric resistance).

Output - pair of contacts at the control panel main board or expander module boards, where the voltage is controlled by the control panel.

Relay output - Electromagnetic switch located at the expander board, controlled (switched over) by the control panel.

Bus - The group of wires, to which the modules operating with control panel main board are connected. In a control panel usually one bus is used for connecting LCD keypads, and the others buses – for connecting expanders.

Expander - electronic device which extends control panel features. There are expanders to increase number of control panel zones or (and) outputs.

Tamper protection – function uses in control panels, expanders, alarm devices and detectors. It protects against opening and/or tearing off from the base.

Antimasking - function uses in motion detectors. It signalises objects moving close in front of the detector, thus preventing any attempts to cover it.

3.2 Ambient Conditions

Ambient temperature:

- design maximum 35ºC
- design minimum –25ºC

Humidity min average monthly	70%
Humidity max average monthly	90%
Plant design elevation above sea level	1m
Design wind speed	25m/s
Design snow fall	290mm

3.3 Electrical data

Available power supply on site:

Frequency	50 Hz
Low voltage	230 VAC TN-S

4 Description

4.1 Operation Principle

4.1.1 Basic principles

The Burglar Alarm System shall be designed to ensure security of area defined in general contractual conditions by means of technical measures. The system shall be design according to requirements for Class SA3 included in standard PN-93/E-08390. The class of system can be modified and adopted for special well-grounded applications after detail risk analyse.

4.1.2 Architecture

Burglar Alarm System should have stand-alone dissipation structure consisting of:

- main control unit
- zone expanders
- outputs expanders (if necessary)
- LCD keypads
- partition keypads
- detectors
- visual and audible alarm devices

Main control unit, expanders and keypads shall be connected via communication buses. The bus functionality shall be checked automatically. Motion detectors, magnetic contacts, glass break detectors should be connected directly with control unit or zone expanders. At least two alarm devices shall be foreseen for single object. Whole system should be based on digital fully programmable control units. GL S.A. recommends addressable systems for special well-rounded applications after functional analyse of the system.

Main control unit should enable connections of required interfaces for co-operation with:

- CCTV System
- Access Control System

The main control unit shall interface with control centre in guardhouse using communication link or telephone line. The interface shall enable access to all information coming from the system components.

Objects shall be divided into partitions. Size of partitions shall be agreed upon with security service from Grupa LOTOS SA. Each partition shall have it's own partition keypad, which could be also used for controlling other partitions when needed. Partitions may be controlled by users, timers, control inputs or their status may depend on the state of other partitions.

4.2 System Requirements

4.2.1 General

The proposed equipment shall be designed in order to minimize the consequences due to the failure of

the system itself or equipment connected to the system. Supplier shall state all necessary information to qualify the reliability of the system in his proposed configuration. Identification and location of fault in the system shall be as far as possible automatic. Additionally it must be possible to send alarm to an external device. All control methods, operating and maintenance procedures shall be designed to allow easy maintenance and operation.

The proposed system shall be designed in order to keep the spare parts number to a minimum.

As far as redundant configuration exists, it shall be possible to replace system modules without interruptions the system operation.

System shall enable controlling main control panel by LCD keypad and PC computer (via RS-232 port, telephone line or computer network). The system shall allow editing the names of users, partitions, zones, outputs and modules in order to facilitate control and supervision of the system.

The system shall enable permanent recording of all burglary attempts to controlled zone. An event log shall consist of following features:

- storage capacity up to 1000 events,
- recorded events: arming (disarming, alarms, clearing alarms, bypassing), un-bypassing zones, failures, application of user functions, starting the service mode , etc.
- registering events related to access control
- date and time of the event occurrence
- function of event printout with optional event selection, names of zones, modules and users as defined in the system.

If the system is supported with CCTV and zone is intruded, an alarm shall be triggered and the relevant camera shall be pointed at the violated zone. At the same time recording of pictures from the camera shall be automatically started.

4.2.2 Requirements for transmission

Classes of transmission systems (transmission delay, delay of monitored information, viability) shall be in accordance with requirements for Class SA3 given in following standards PN-93/E-08390/51, 52, 54, 55 i 56 referring to transmission of alarms. Transmission via a specialised tracks shall be according to class 2, transmission via digital communication system shall be according to class 1, transmission via caustic communication system shall be according to class 1.

4.2.3 Requirements for building protection

The system shall base on digital dual motion detectors and glass break detectors. Magnetic contacts shall be mounted in all widows and doors, which may enable enter to the protected area. It should be possible to synchronize the detectors against each other and adjust their sensitivity to prevent false alarms.

As far as possible, all installation components and cables related to Burglar Alarm System shall be located inside partitions. Communication buses, which run outside protected area shall be hidden and protected against disconnection. Installation work shall be done in accordance with manufacture instruction.

4.2.4 Requirements for perimeter protection

The system shall base on:

- active infrared barriers
- passive infrared detectors
- sensor cables

suitable for outdoor application and manufactured as weather-proof.

The barriers shall be arranged along the inner side of the fence to create a tight protection ring. The barriers shall be arranged so that their coverage areas do not overlap. The barriers shall be installed at a suitable distance from the fence so that the intruder cannot jump straight from the fence top over their coverage area. The recommended spacing between the barrier beams and the fence is 2 –2,5 metres.

Fence sensors shall be applied in places where barriers can not be used due to obstacles effects effective line of sight between transmitter and receiver.

The barrier beam or fence sensors, which cover the entry area, shall be interlocked with the access control system, which controls the gates to disable automatically the protection of the relevant sector when an authorized vehicle or person enters the site. The details should be adapted according to a security procedures of protected area and GL S.A. disposition.

All sensors and contacts shall be connected as separate lines to the control unit, so eventual further changes and reconfigurations will be fast, easy and comfortable. That way of connection will also allow controlling state of each zone with high precision.

Monitoring of the state of all zones shall be possible in software connected to main control unit.

All detectors shall be connected in parametric connection mode, so besides the state of the sensor, state of the cables shall be monitored as well. Every set barrier beam shall be connected as separate line, so location of intruder will be known precisely.

4.3 Main control panel

The device shall enable monitoring of detector presence and performance using different configuration options and reaction types to choose from. The control panel capacity regarding numbers of expanders and keypads shall be adapted to system requirements.

Control panel program shall be stored in non-volatile flush memory to keep the control panel settings even in deenergized state.

The firmware shall by updated with no need for dismounting of the control panel.

Programming control panel settings shall be possible:

- locally by means of LCD keypad
- locally by means of computer connected to RS-232 port
- remotely by means of computer connecting to the control panel through a modem

Control panel shall enable setting up to 240 user codes, up to 8 master codes (1 code for each object) and 1 service code. Additionally the coding shall enable:

- several types of user codes with an option to define additional authority levels for the system access
- keypad function menu depending on the user authority and code type
- defining the access to keypads, code locks and proximity card readers
- periodical change of access codes by means of prefixes

Better protection against unauthorized access to the facility shall be ensure at least by defining partitions protected with two passwords.

Control panel shall create event log feathers with following:

- storage capacity up to 1000 events
- recorded events: arming/disarming, alarms, clearing alarms, bypassing/un-bypassing zones, failures, application of user functions, starting the service mode , etc.
- registering events related to access control
- date and time of the event occurrence.

Additionally control panel shall equipped with:

- communication buses for system expansion
- automatic diagnostics of system components
- real-time clock with calendar and battery backup
- visual status signalling for outputs

- battery charging circuit
- telephone dialler
- electric protection of all zones, outputs and communication buses

4.4 System components

4.4.1 Zone expanders

Expander shall be used as a device designed to work together with main control panel. It shall allow extension of the alarm system by min. eight zones having identical features as the zones of the control panel main board. NO and NC type detectors may be connected to the expander. The zones can be configured to work with a single parameter (EOL) and with a double parameter (2EOL). Each of the zones should be individually programmed and assigned one of a few types of response to violation.

4.4.2 Active infrared barrier

Every barrier shall consist of one transmitter and receiver. The transmitter shall emit an invisible infrared light in direction of the receiver. When a person interrupts either the beam range between transmitter and receiver an alarm shall be released.

The single barrier shall be moulded type and consist of 2 double parabolic mirrors, which form 4-chanel auto synchronized IR-barrier.

The distance between the single beams has to be less than 20 cm. Barriers can be multiplied to arranged IR-curtain.

The alarm evaluation mode and alarm response sensibility shall be adjustable. The alarm response sensibility of each of the barrier shall be adjusted individually.

In case when visibility conditions between transmitter and receiver changes as result of strong developing of fog, snowfall or when the optic gets dirty and the sight distance communication could be interrupted then an alarm shall be set in. It shall become active when the sight distance communication during a defined period of time (5 - 30 sec.) is sinking below the level adjusted.

For each device a separate lens heater should be installed. The heater shall be supplied with DC voltage.

There shall be also tamper switch used for each transmitter and receiver, so any trial of damaging the cable or barrier enclosure shall result in alarm. Technical alarm shall be activated when an error occurs in the data processing device or it fails due to external disturbances. Briers shall be enclosed at least in an IP54 enclosure.

4.4.3 Fence sensor cable

The fence sensor cable shall utilise signals generated by the minute flexing of a microphonic sensor cable. The cable shall detect an intruder cutting through, climbing on or lifting the fence fabric. The cable insulation shall be UV-resistant and resistant against harsh wetter conditions. The system shall eliminate alarms caused by natural or environmental events.

Specific characteristic intrusion signatures shall be analysed by a digital signal processor. A terminator at the end of the cable shall permit the signal processor to supervise the integrity of each zone. In cases when the intruder is detected or cable continuity fails an alarm shall be activated. The processors shall communicate with main control unit by either relay contact or on a data link. The processor shall be enclosed in an IP66 enclosure on the safe side of the fence.

4.4.4 Dual motion detector

Digital dual motion detectors shall combine photoelectric infrared sensor (a dual pyro-electric element) and microwave sensor, which provide high efficiency and maximum immunity to interference. The detector shall be fitted out additionally with UV and visible light filter.

The detector shall based on digital signal processing, having digital temperature compensation, sensitivity adjustment, antimasking and tampering protection. Supply voltage supervision is required and low power consumption shall be considered. Digital signal processing shall alarm only when both sensors detect motion.

Interchangeable Fresnel lenses shall feature wide angle and range of vertical detection curtain adjusted to protected area. Adjustable holder for easy mounting on wall or on ceiling shall be provided with the detector.

4.4.5 Break glass detector

Glass break detection method shall cover different glass types (also laminated and armoured glass).

It shall be possible to set sensitivity level. Supply voltage supervision is required and low power consumption shall be provided. The detector shall be equipped with tamper protection.

Supplier can applied other types of detectors then listed above if it is necessary.

4.4.6 Magnetic contact

The magnetic contacts shall be used wherever required for controlling the status of doors, gates windows and/or other movable elements used for protection or monitoring of access to particular partitions.

Magnetic contact types may differ in their mounting configuration and housing depending on material and technology used for windows and doors manufacturing. It is preferred to apply magnetic contact for flush mounting. If magnetic contact has been designed for surface mounting then it shall be equipped with tamper protection. Each of the magnetic contact elements shall be placed in a watertight enclosure.

4.4.7 Alarm device

Self activating outdoor siren with flash shall be initiated with control panel. The siren shall feature

- acoustic signal - magnetodynamic horn
- optical signal - xenon strobe tube
- 4 different sounds available
- 2 controlling inputs
- highly resistant polycarbonate housing
- tamper protection against opening and against pull-off
- galvanized steel inner cover
- impregnated electronic circuits
- optional hermetic magnetic contact
- individual power supply - 12V 1,3 Ah battery
- ingress protection min. IP34

Indoor acoustic siren shall feature:

- acoustic signal - piezo buzzer
- min. 3 different sounds available
- durable ABS housing
- tamper protection against opening
- impregnated electronic circuits
- ingress protection IP32

4.4.8 LCD keypad

LCD keypad shall enable programming of main control panel. The keypad shall feature:

- large, well-readable with min. 2x16 characters display with permanent or temporary display backlighting activated on pressing a key or by any control panel zone.
- 16-key keyboard with backlighting controlled in the same way as the display backlighting.
- 2 zones with properties identical to main panel zones.
- Microswitch to detect keypad tampering.
- RS-232 port allowing the alarm system to be operated by means of computer uses supervisory and user program.

4.4.9 Partition keypad

Partition keypad shall be a device designed to work with main control panel. It shall be used for arming and disarming a single partition and provided with the access control feature, as well as it controls the operation of electromagnetic door lock and monitors whether the door is open or locked. The partition keypad shall allow changing the user code and calling the functions for control external devices.

Partition keypad shall be provided with 12 keys with temporary backlit (operating automatically), and LEDs described as follows:

- ALARM (red) – continuous light shall indicate an alarm triggered in the partition operated with this partition keypad, and LED flashing shall indicate that alarm occurred in this partition previously.
- ARMED (green) - continuous light shall inform that the partition assigned to this partition keypad is armed. The LED shall blink when the delay time is counted down.
- TROUBLE (yellow) – the LED shall blink when technical problem has been detected in the system.

There shall be letters printed on keys together with digits in order to identify code numbers with passwords. If an erratic code (not recognized by the control panel) is typed three times, the alarm shall be activated.

4.5 Signal wiring

Signal wiring shall interconnect the main control unit and the other electronic security system devices. In addition to the relevant user signals being carried over regular signal wiring, the monitoring signal should be sent over the anti-sabotage line to detect any disconnection of those devices. Any wire break should be detected and logged. This requirement applies to all components of the electronic security system.

4.6 Electrical Supply

GL S.A. will provide to the Supplier power supply limited to feed the Burglar Alarm System according to power requirements defined by the Supplier.

The Supplier has to provide all the equipment necessary to generate the different power supplies needed internally by the Burglar Alarm System.

If not other wise stated the power and distribution system of the Burglar Alarm System need not be redundant. An output signal shall be provided to indicate an electrical failure in the power supply unit and in the power distribution system.Burglar Alarm System shall be powered from stand-by gas-proof battery providing 24 hours support in case of main power failure.

Supplier shall provide over voltage protection. The protection shall ensure safety of control units as well as field mounted equipment in case of electromagnetic impulse discharge.

4.7 Painting

Painting of outdoor equipment is to be carried out in accordance with the requirements imposed by an industrial, chemical and sea atmosphere. Care is to be taken than all structural components are properly painted. Devices colour may be according to manufacturer standard.

4.8 Labelling

Burglar Alarm System shall be labelled with the manufacturer's name and logotype to assure the integrity of the complete system. Every equipment shall be provided with a tag showing an equipment specific number in accordance with documentation and related equipment numbering procedure.

The tag shall be marked by means of an imprint on the nameplates. Nameplates shall be stainless steel, non-corrosive alloy or rigid plastic, which shall be durably fixed to a non-removable part of the frame of equipment. The Supplier shall submit a tag proposal for GL S.A. approval in prior to manufacturing.

4.9 Services

Services, which shall be provided by the Supplier:

- detail design
- system programming
- factory acceptance test and inspection
- packing and shipment
- assembling on site
- system test operation lasting form 7 till 28 days
- training of personnel (including system users, administrators and service staff) designated by GL SA
- preparation of operating manual, maintenance instruction and procedure describing reaction in case of different alarms
- maintenance during warranty period

Supplier shall posses a concession of Polish Ministry of Interior and Administration in the field of services related to technical protection measures of premises in accordance with art. 15 o the Act of August 22, 1997 on protection of persons and premises.

The system designer should be qualified as a security worker in field of technical protection. GL SA reserves the right for acceptance of any subcontractor.

4.10 Cables, Conductors, Secondary Items

All cables, conductors, plugs, fixtures and mechanical protection devices shall be included in the Supplier's scope of supply. The cabling of the Burglar Alarm system shall include all links required to equipment provided by Supplier. All cables and terminal blocks shall be labelled at each end with a labelling system in accordance with GL SA procedure.

All outdoor equipment shall be delivered with cable glands. Supplier shall do selection of cable glands in accordance with cable nominal diameters given by cable manufacture.

4.11 Documentation

Sets of documentation shall be delivered with the system by the Supplier for system acceptance and takeover:

1. Technical description including:
   - Subject of design
   - Law basis for preparation of the system design
   - Description of protected premises containing its architecture and construction
   - Partition into zones
   - Design preconditions and list of relevant projects (including agreements with GL SA done in writing, plans for rooms' arrangement, electrical installation layouts etc.)
   - Hazard analysis
   - Regulations and standards selected as basis for determination of protection methods
   - Description of system organization
   - System description including details of used equipment
   - Description of system installation including data of cables and mounting elements, cable arrangement details and installation hints.
   - Information about power supply for control panels and peripheral devices
   - Calculation of system power balance in respect to emergency power supply including list of norms and settlements taken for determination of time of emergency operation.
   - Equipment list
   - Information related to principles of operation, maintenance and services
   - Remarks related to installation works
   - Operating, installation and maintenance instructions
   - List of relevant standards and other documents
2. Material Take-off
3. Cable List

4. Drawings
   - description of graphical symbols
   - block diagrams
   - layout drawing showing equipment arrangement inside zones
   - layout drawing showing equipment arrangement in guardroom
   - connection (wiring) diagrams
   - power supply single line diagrams
   - panels arrangement drawings
   - mounting examples
5. As built documentation including revised drawings to reflect changes with equipment and wiring system
6. Start up check lists
7. Acceptance report

In prior to detail design the Supplier shall agree requirements for the system (i.e. system functionality, equipment locations, cable arrangement, interfaces with existing facilities) with representatives of GL SA. The agreements shall be in written.

5 Relevant documents

- 3720 Telecommunication installations
- 3730 Telecommunication cabling
- 3760 Telecommunication cables
- 3770 Numbering scheme for objects and telecommunication cables

6 Norms and standards

6.1 Regulations

Act of August 22, 1997 on protection of persons and premises (OJL of 1997, No. 114, item 740)

Minister of Economy, Labour and Social Policy order of March 12, 2003 on basic requirements for electric equipment (Journal of Laws No 49 pos. 414).

Minister of Infrastructure order of April 2, 2003 on evaluation of equipment conformity with basic requirements concerning electromagnetic compatibility, and method of its labelling (Journal of Laws No 90, pos. 848).

Minister of Economy, Labour and Social Policy order of July 28, 2003 on basic requirements for protective equipment and systems intended for use in explosion endangered zones (Journal of Laws No 143, pos. 1393).

Council of Ministers order of September 10th 2002, on conditions and mode of conducting compliance assessment of terminal telecommunication equipment intended for connecting to public networks terminals and radio equipment with basic requirements, and method of marking them. (Journal of Laws No 176, pos. 1442).

6.2 Polish standards

PN-E-08390-1:1996 Alarm systems. Terminology

PN-E-08390-3:1998 Alarm systems. Intrusion alarm systems. Requirements and tests of control and indicating equipment

PN-E-08390-5:2000 Alarm systems. Intrusion alarm systems. Requirements and test for warning devices

PN-93/E-08390.13 Alarm systems. General requirements. Environmental conditions.

PN-93/E-08390.14 Alarm systems. General requirements. Code of practice

PN-93/E-08390.22 Alarm systems. Requirements for intruder alarm systems. Requirements for detectors.

PN-93/E-08390.23 Alarm systems. Requirements for intruder alarm systems. Requirements for infrared-beam interruption detectors in buildings

PN-93/E-08390.24 Alarm systems. Requirements for intruder alarm systems. Ultrasonic Doppler detectors for use in buildings

PN-93/E-08390.25 Alarm systems. Requirements for intruder alarm systems. Microwave Doppler detectors for use in buildings

PN-93/E-08390.26 Alarm systems. Requirements for intruder alarm systems. Passive infra-red detectors for use in buildings

PN-93/E-08390.51 Alarm systems. Alarm transmission system. General system requirements.

PN-93/E-08390.52 Alarm systems. Alarm transmission system. Equipment general requirements.

PN-93/E-08390.54 Alarm systems. Alarm transmission system applying dedicated transmission lines.

PN-93/E-08390.55 Alarm systems. Alarm transmission system. Digital communication systems applying public telephone and computer network..

PN-93/E-08390.56 Alarm systems. Alarm transmission system. Acoustic communication systems applying public telephone and computer network..

7 Enclosures

- Attachment No. 1 Block diagram. Burglar Alarm System.

8 Record of changes

No.	Date	Description	Introduced by
1	30-11-2013 (rev. 2)	Review, update, standardize and changes to the Standard within scope of order No. OK/990/2012	Editorial board coordinated by T.Wróbel
-	31-08-2015	Page layout corrections, no contents changes.	T. Wróbel