Contents

1 Subject of specification 2
2 Scope of validity 2
2.1 Deviations 2
2.2 Exclusions 2
3 Hierarchy of documents 2
4 Definitions 2
4.1 Basic terms 2
4.2 Abbreviations 3
4.3 Ambient Conditions 3
4.4 Electrical data 3
5 Description 3
5.1 Operation Principle 3
5.2 System Requirements 4
5.3 System components 5
5.4 Mechanical interlock equipment 8
5.5 Vehicle traffic recording terminals 8
5.6 Electronic key record system (KRS) 9
5.7 Signal wiring 10
5.8 Software 10
5.9 Electrical Supply 11
5.10 Labelling 11
5.11 Services 11
5.12 Cables, Conductors, Secondary Items 12
5.13 Documentation 12
6 Relevant documents 13
7 Regulations and standards 13
7.1 Regulations 13
7.2 Norms 13
8 Enclosures 13
9 Record of changes 14

1 Subject of specification

This specification used in conjunction with standard technical specifications of LOTOS Group S.A. (GLSA) establishes the minimum requirements for the design and manufacture of access control 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 deviation from this specification and the relevant specifications, standards and related documents including proposals, which the bidder claims to be economically and / or technically superior solutions, must be submitted in writing for review and approval by Grupa LOTOS SA. Non-approved exceptions are not acceptable by Grupa Lotos S.A.

The supplier must report in writing any ambiguity in this or any other specifications of Grupa LOTOS SA or non-compliance with the referred documents / standards and obtain a written explanation from Grupa Lotos SA.

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 scopes of separate specifications listed in item no. 5.

3 Hierarchy of documents

In case of conflicts existing between this specification and other documents, the following order of precedence shall govern:

- The current Polish legislation
- Terms of purchase order / contract and other requirements agreed in writing with GLSA
- Data Sheets approved by GLSA
- This specification
- Other Specifications
- Drawings and other documents
- Standards

4 Definitions

4.1 Basic terms

Fail-Safe - A lock that defaults to the “unlocked” position when power is removed. Requires power to go to a “locked” position.

Fail-Secure - A lock that defaults to the "locked" position when power is removed. Requires power to go to an "unlocked" position.

Interlock - A pair or group of separate doors equipped with a control system that prevent the simultaneous opening of more than one door at a time.

Proximity - In access control terms, proximity refers to presenting an access card within the reader's Radio Frequency (RF) field without having to make actual physical contact with the reader itself.

Wiegand - A communication protocol widely accepted as an industry standard in the manufacturing of access control equipment..

Tamper switch - switch uses in controllers, locks, strikes. It protects against opening and/or tearing off from the base.

4.2 Abbreviations

GLSA – Grupa Lotos S. A.

ACS – access control system

WTR - work time recording

KRS - electronic key record system

4.3 Ambient Conditions

▪ Ambient temperature (max/min)	+36°C/-25°C
▪ Average monthly humidity (min/max)	70%/90%
▪ Elevation above sea level	1m
▪ Wind speed	26 m/s
▪ Atmosphere	typical for refinery Grupa Lotos S. A. (marine, aggressive industrial, chemical and dusty)

4.4 Electrical data

Available power supply on site:

Frequency	50 Hz
Low voltage	230 VAC TN-S

5 Description

5.1 Operation Principle

5.1.1 Basic principles

The Access Control System shall be designed to ensure control of area defined in general contractual conditions by means of technical measures. Designed system shall fulfil requirements of B access class and 2nd or 3rd recognition class (final design to be agreed with GLSA Security Office), defined in attached standards.

5.1.2 Architecture

Access Control System shall have stand-alone dissipation structure consisting of:

- Main host computer
- Operator's stations
- Area controllers
- Door controllers
- Proximity cards and card readers
- Biometric readers (if required)
- Electric door strikers
- Electromagnetic locks
- Exit devices
- Evacuation push button station

The factory Access Control System includes local operator's stations, which are stands for issuing of passes, furnished with PC unit, display monitor and suitable printer capable of plastic cards handling (e.g. thermo-sublimation one) or of other type. Such stations are foreseen in receptions of main administrative buildings with entrances located outside the works, as well as on security service posts at gates.

Main host computer, area controllers and door controllers shall be connected via communication bus or computer network. The bus or computer network functionality shall be checked automatically.

Access control server shall meet requirements specified for automatics system computers, included in standard 3620.

Proximity card readers, electric door strikers, Electromagnetic locks and exit devices shall be connected directly with door controllers. Whole system shall be based on digital fully programmable controllers.

Area controller shall enable connection of required interfaces for co-operation with:

- CCTV System
- Burglar Alarm System
- Fire Alarm & Detection System

5.2 System Requirements

5.2.1 General

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

5.2.2 Functional requirements

To ensure maximum security and the safety of users the system shall record all of the following events:

- authorized entry into the security zone
- authorized exit from the security zone
- unauthorized entry attempt
- forced entry
- system equipment sabotaged
- system communication lost
- no powered supply available

The system shall control and record the movements of persons throughout the area by assigning individual permission to each passage, using time zones to protect the passage, and controlling the time of staying inside the zone.

Leaving the zone (opening the door from inside the zone) shall be performed by pressing the door handle or button. The controlled doors shall be equipped with automatic shutting devices. The system shall have a modular configuration and its ID card-based operation.

The system shall also enable possibility of data exchange for work time recording (WTR) module purposes, utilizing the readers as WTR readers. The user opening passage that is controlled on the grounds of set methodology (e.g. for the first and last time during twenty-four hours), generates signal that shall be used for work time recording purposes.

The new system, which is to be designed, shall use for data transmission separated LAN network. The network is dedicated for communication between existing in GLSA components of access control system.

5.3 System components

5.3.1 Area controller

The area controller shall link the host computer and a network of door controllers. The area controller shall poll the door controllers and check the data as it is entered, using internally stored tables to monitor and control access throughout a site. One area controller shall support all door controllers located in an object. The area controller shall have a built in UPS, which shall ensure 4 hour back-up. The connection to the host computer shall be done using RS232/485, Ethernet or Token Ring protocol.

The area controller shall feature:

- High performance processor
- Battery backed-up memory
- Two separate serial channels for high speed polling
- Radio time receiver support
- Monitor connection for system diagnostic

5.3.2 Door controller

Door controller shall supervise directly proximity card readers, strikers, locks and exit buttons accepting, analysing and transmitting the messages, which will enable access.

Every controller shall feature as minimum:

- 2 door lock outputs
- 4 LED outputs
- 2 alarm outputs
- 2 reader inputs
- 2 pin pads inputs
- 7 digital inputs
- 2 buzzer outputs

Door locks shall be controlled from a relay. They shall be wired to fail "closed" or "open". The internal 12VDC power supply shall be used to power the lock or alternatively, the relay may be used as a "volt- free" switch for use with an external door lock power supply. The standard 12VDC power supply shall provide enough current for 2 typical 250mA - 500mA locks.

The controller shall be closed in enclosure. Removal of the enclosure front cover shall immediately activate a tamper switch.

5.3.3 Intelligent door controller

The controller shall combine features of area and door controllers. Additional fittings shall enable the controller to collect stored tables and transaction data. Controller shall check and verify rights and receive orders from server and send to him expecting data. Intelligent door controller shall additionally supervise directly proximity card readers, electric door strikers, locks and exit buttons in rules specified and act in a pre-defined manner. The operation shall be possible without any communication between the door controller and server, allowing the controller to operate in autonomous manner.

Every controller shall feature as minimum:

- 2 door lock outputs
- 4 LED outputs
- 2 alarm outputs
- 2 reader inputs
- 2 pin pads inputs
- 7 digital inputs
- 2 buzzer outputs

Door locks shall be controlled from a relay. They shall be wired to fail "closed" or "open". The internal 12VDC power supply shall be used to power the lock or alternatively, the relay may be used as a "volt- free" switch for use with an external door lock power supply. The standard 12VDC power supply shall provide enough current for 2 typical 250mA - 500mA locks.

The controller shall be closed in enclosure. Removal of the enclosure front cover shall immediately activate a tamper switch.

5.3.4 Proximity card readers

Proximity card readers shall combine multiple configuration options and enable for both indoor and outdoor applications. The reader shall feature:

- a beeper and multicolour LED which can be host and/or locally controlled.
- Enables various beeper and LED configurations, depending on individual site requirements.

- Can read cards with formats up to 85 bits
- Designed for mounting directly onto metal with no change in read range performance.
- Available with Wiegand output.

An internal self-test routine shall check and verify the set-up configuration, determine the internal or external control of the LED and beeper, and initialize reader operation. An additional external loop-back test shall allow for the reader outputs and inputs to be verified without the use of additional test equipment.

Long-reach proximity sensors shall be used for vehicle traffic handling.

5.3.5 Biometric readers

After adjusting it with GLSA, the following biometric readers can be used for high risk level objects, or such that are occupied by organizational units of particular importance:

- fingerprint lines readers
- iris readers
- facial features readers

Biometric readers shall also enable use of proximity cards, thanks to proximity reader operating on Wiegand standard basis.

5.3.6 Electric door strikers

The striker shall be fail safe device. Electrically actuated shall lock strike jaw. The lock shall be equipped with monitoring signal switch. The lock shall be powered by 12VDC.

5.3.7 Electromagnetic locks

Electromagnetic lock shall be fail safe device that require constant power to remain locked. It shall comprise of a lock body, mounted to the door head jamb, and an armature plate, which is mounted on the door stile. The armature plate shall be a passive piece of steel that pivots on its mount, and when aligned with the lock body in its powered state, shall be magnetically drawn together. Minimum holding force shall be 250 kg. The lock shall be equipped with door position switch. The lock shall be powered by 12VDC.

5.3.8 Proximity card

The proximity card shall cooperate with card readers, which communicate with controllers by means of Wiegand protocol. The cards shall be easily customized with multicolored graphics by using thermo transfer image printers or by placing on card PVC label printed in the same technology. The cards shall be strong and flexible, resistant to breaking, and resistant over a broad range of temperature and humidity ranges.

5.3.9 Exit devices

Exit device shall be designed to allow immediate exiting at all times and shall not require lever or knob rotation. It shall be located on the perimeter doors of a building and always in the designated means of egress route.

4.3.10 Auxiliary equipment

Depending on requirements, the following equipment may be additionally used in access control system:

- keypads
- door opening sensors

- door opening modules activated by phone
- interphone equipment

5.4 Mechanical interlock equipment

5.4.1 Tripod turnstiles

The basis for unlocking mechanism actuation shall be reception of control pulse, after positive verification of proximity card user data. Internal lock shall unlock that gate for specified period only. Opening and closure state of the gate shall be signalled on the equipment enclosure. After unlocking of the mechanism and passing through the gate, automatic activation of push-in mechanism shall proceed, which assists passing through and locking of rotation until subsequent control pulse is obtained. Software of gate control processor shall enable bi-directional movements, and storing of signal coming from external devices with alternate unlocking of the lock.

The device shall also enable the mechanism unlocking by means of additional pushbutton installed at guard post.

In emergency (supply failure or evacuation of people), possibility of the mechanism unlocking shall be provided, by means of:

- safety catch releasing of arms movement interlock (the arms are moving freely in both directions)
- dismantling of gate arms (by means of main bolt unscrewing on gate rotor)

5.4.2 Swing gates

On reception of control signal, processing unit of the gate shall unlock the arm, which enables pushing it, and authorized person passing through. After passing through is done, the spring actuated mechanism shall restore arm closed position and bring about automatic locking of the gate. The moment of arm unlocking shall be confirmed by audible signal, in order to inform person passing through if authorization to get in or out has been granted to him/her. The gate shall feature possibility of arm remote locking (e.g. by means of switch installed in guard post).

In case when unauthorized person passing attempt is detected, the device shall activate alarm signal.

5.5 Vehicle traffic recording terminals

5.5.1 General requirements

Vehicle traffic recording terminal shall be installed at each GLSA area entrance gate. Each terminal shall be equipped with integrated proximity card reader, alphanumeric and functional keypad, as well as LCD display. The terminal shall communicate with access control server through LAN network. The terminal shall perform verification and registering functions. Function of physical entrance control shall be accomplished by entrance barriers or gates (depending on GLSA requirements), manually or automatically controlled by security staff. The terminals shall be operated by security staff only.

5.5.2 Entrance terminal – requirements

Recording device shall be adapted to outdoor applications. The device, equipped with network interface card shall enable connecting to managing informatics system through LAN network, and provide bi-directional data transfer.

The terminal shall fulfil at least following requirements:

- Stainless steel enclosure

- Alphanumeric keypad with functional menu description
- 6-row, 40 characters in each row, LCD display
- 256 kB RAM internal memory
- Two control outputs
- Connector for additional external reader
- Eight digital inputs
- Possibility of additional peripheral devices connection (scanners, scales, etc.)
- Integrated UPS
- Standard communication ports RS 232, RS 485, TCP/IP
- Protection class IP66

5.6 Electronic key record system (KRS)

5.6.1 Basic requirements

Access control design in selected, important objects indicated by GLSA, shall take into account use of electronic key record. The system shall use electronic – mechanical key dispensers for this purpose. The key dispenser shall enable electronic monitoring and mechanical protection of keys, as well as controlling of authorized persons access to adequate keys with simultaneous use of proximity cards employed in access control system.

5.6.2 Software

The system software shall enable granting of rights and recording of basic events connected with key drawing, i.e. time of key drawing and returning, as well as identification of authorized person according to following procedure:

- authentication of own rights in KRS system by means of card or/and biometric reader
- key dispenser opening
- physical releasing of mechanical protection panel
- recording of the event by KRS system
- drawing of key by authorized person
- key dispenser closing

Settings of rights shall be stored in non-volatile key dispenser memory.

KRS software shall be accessible from level of access control system server and shall enable viewing of current events as well as printing reports from operator's station of that system.

Key dispenser software shall also permit for grouping of nests in zones and creation of so-called time-windows, in order to limit access time to key dispenser for individual users.

5.6.3 Construction of key dispenser

The key dispenser shall be equipped with back-up power supply, enabling 72-hour operation of the device in case of basic supply failure. The key dispenser shall also give possibility of mechanical opening and unlocking of all keys deposited in it. LCD display and numerical keypad shall enable manual configuration of the dispenser.

The dispenser controller shall be furnished with relay outputs, for signalling of alarms related to the following events:

- the dispenser sabotage attempt
- taking a key out or putting it in without entering of proper code
- occurrence of so-called silent alarm
- exceeding of maximum drawer opening time, or after 3 incorrect card readouts
- lack of 230V voltage, or battery voltage too low
- burnout of one from lock fuses, or other lock failure
- error detection in non-volatile memory and loss of key dispenser settings.

5.7 Signal wiring

Signal wiring shall interconnect the host computer and the other electronic devices belonging to Access Control System. System shall enable to control communication lines continuity and detect disturbances which may affect proper system operation.

5.8 Software

Specialized software provides a graphics display allowing full remote control of the connected equipment. The software memorizes all data necessary for system control and enables creating and printing reports.

5.9 Electrical Supply

GLSA will provide to the Supplier power supply limited to feed the Access Control 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 Access Control 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. Door controllers shall be powered from stand-by gas-proof battery providing 4 hours support in case of main power failure.
Supplier shall provide over voltage protection. The protection shall ensure safety of controllers as well as other system components in case of electromagnetic impulse discharge.

5.10 Labelling

Access Control System shall be labelled with the manufacturer's name and logotype to assure the integrity of the complete system. Each of 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 GLSA approval in prior to manufacturing.

5.11 Services

Services which shall be provided by the Supplier:

- detail design
- system programming
- 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 shall be qualified as a security worker in field of technical protection. GL SA reserves the right for acceptance of any subcontractor.

5.12 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 access control 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 no. 6120.

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.

5.13 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 Security Office. The agreements shall be in written.

6 Relevant documents

Any "Technical Specification" issued by GRUPA LOTOS S.A. listed in Contract Files.

7 Regulations and standards

It is in each case understood that quoted standards, regulations, directives and orders are of their latest editions, along with amendments, annexes and supplements in force.

7.1 Regulations

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

Act of August 30 2002, on conformity system assessment (JOL of 2002, No.166, item 1360)

Regulation of the Minister of Economy of August 21, 2007, on basic requirements for electric equipment (JOL No 155 pos. 1089).

Act of August 30, 2002 on the system of the conformity assessment (JOL 2002 No 166 pos. 1360).

Act of August 29, 2003 on for amendment to the act about the system of the conformity assessment and about the amendment to some acts (JOL 2003 No 170 pos. 1652) as amended.

7.2 Norms

PN-EN 50133-1 - Alarm systems. Access control systems for use in security applications. Part 1: Systems requirements

PN-EN 50133-2-1 - Alarm systems. Access control systems for use in security applications. Part 2-1: General requirements for components

PN-EN 50133-7 - Alarm systems. Access control systems for use in security applications. Part 7: Application guidelines

8 Enclosures

- Attachment No. 1: Access Control System –block diagram.

9 Record of changes

No.	Date	Description	Introduced by
bb	5.12.2005	Change of requirements for LAN network in item 4.2.2 and in attachment no. 1. Replacement of standard no. 3770 by standard no. 6120.	Krzysztof Drabek
1	30-11-2013 (rev. 1)	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