الهيئة الملكية لمدينة الرياض
ROYAL COMMISSION FOR RIYADH CITY

Document Number : M-ESD-700000-SCSS-ESP-000001-08

TECHNICAL SPECIFICATIONS – ACCESS CONTROL & INTRUSION DETECTION (AC/ID)

DESIGN AND CONSTRUCTION OF RIYADH METRO PROJECT – LINE 7

Document information

GENERAL INFORMATION

Document volume	Vol 2.3 WPS 1 – Transit System
Version	V8
Reference Number	M-ESD-700000-SCSS-ESP-000001-08

TABLE OF CONTENT

ACRONYMS AND ABBREVIATIONS....4

REFERENCE DOCUMENTS:....7

1 - INTRODUCTION....8

2 - SCOPE OF WORK....9

3 - ARCHITECTURE....10

4 - SYSTEM AND FUNCTIONAL REQUIREMENTS....12

4.1 - AC/ID System....13

4.2 - Perimeter protection system....14

5 - NETWORK MANAGEMENT SYSTEM (NMS)....15

5.1 - Operation related functionalities....15

5.2 - Maintenance related functionalities....16

5.3 - Provisioning related functionalities....16

5.4 - Administrative related functionalities....16

6 - INTERFACE REQUIREMENTS....17

7 - ANNEX A....18

TABLE OF FIGURES

Figure 1 : AC/ID network architecture with dedicated fiber rings....10
Figure 2 : AC/ID common network architecture....10

TABLE OVERVIEW

Table 1 : Standards....19

ACRONYMS AND ABBREVIATIONS

AC/ID	Access Control / Intrusion Detection
AFC	Automated Fare Collection
ATC	Automatic Train Control
ATO	Automatic Train Operation
ATP	Automatic Train Protection
ATR	Automatic Train Regulation
ATS	Automatic Train Supervision
BBRS	Broad band radio system
BRT	Bus Rapid Transit
BS	Base stations
CBTC	Communication Based Train Control
CCR	Central Control Room
CCS	Central Control System
CCTV	Closed Circuit TeleVision
CDR	Call Detail Records
COTS	Commercial Off The Shelf
CT	Call Type
CTN	Cable Transmission Network
DMZ	Demilitarized Zone
DTMF	Dual-Tone Multi-Frequency
E&M	Electro & Mechanical
FDS	Fire Detection system
FN	Functional Number
GC	Group Call
GUI	Graphical User Interface
HMI	Human-Machine Interface
HDPE	High Density Polyethylene
HVAC	Heating, Ventilation and Air-Conditioning
I/O	Input / Output
IP	Internet Protocol
ISMS	Information Security Management System [ISO 27000 Series] (including cybersecurity [ISO 27032])
IXL	Interlocking

KPI	Key-Performance-Indicator
LAN	Local Area Network
MCS	Master Clock System
MIS	Management Information System
MMI	Man Machine Interface
MMIS	Maintenance Management Information System
MOI	Ministry of Interior
MOS	Mean Opinion Score
OCC	Operation Control Center
ODF	Optical distribution frame
O&M	Operations and Maintenance
PAS	Public Address System
PIS	Passenger Information System
PLC	Programmable Logic Controller
PRCS	Power Remote Control System
PSD	Platform Screen Doors
PSIM	Physical Security Information Management
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SIL	Safety Integrity Level
SMR	Station Master Room
SMS	Short Message Service
SOC	Security Operation Center
STI-PA	Speech Transmission Index - Public Address
TBS	TETRA Base Station
TCC	Transportation Control Center
TCP	Transmission Control Protocol
TETRA	Terrestrial Trunked Radio
TTM	Traffic Traction Management
UPS	Uninterruptible Power Supply
UTO	Unattended Train Operation
VCP	Visual Control Panel

VDU	Video Display Unit
VLAN	Virtual Local Area Network
VMS	Video Management System
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Trademark ® no meaning

REFERENCE DOCUMENTS:

[Ref. 1] : Volume 2.3
[Ref. 2] : M-ESD-700000-SCDN-ESP-000001_CTN
[Ref. 3] : M-ESD-700000-SCTV-ESP-000001_CCTV
[Ref. 4] : M-ESD-700000-SCPA-ESP-000001_PAS
[Ref. 5] : M-ESD-700000-SCRA-ESP-000001_Radio_Transmission
[Ref. 6] : M-ESD-700000-SCPI-ESP-000001_PIS
[Ref. 7] : M-ESD-700000-SCTL-ESP-000001_Telephone and Intercom
Volume 2.2
[Ref. 8] : M-ESD-700000-0000-ESP-000002
[Ref. 9] : M-ESD-700000-0000-ESP-000003
[Ref. 10] : M-ESD-700000-CW00-RPT-000002

1 - INTRODUCTION

This document defines the contractor scope of work, technical and functional specifications and the main performances for the requested Access Control & Intrusion Detection (AC/ID) for Riyadh metro line 7.

The document shall be read in conjunction with the documents composing Volume 2.2, to reach the objectives set for the project.

Information about track alignment and stations can be found in: METRO LINE 7 PHASE 1 TRACK ALIGNMENT REPORT M-ESD-700000-CRAL-RPT-000001.

2 - SCOPE OF WORK

The following requirements are applicable for all telecommunication sub-systems, including AC/ID.

It is the responsibility of the contractor to ensure that design document approval is achieved before any installation starts, and the different pre-required tests have been passed with success (including time for submission, approval, resubmission and approval…). It is also the contractors responsibility to ensure that all possible interfaces and sub-systems are taken into account.

The contractor is responsible for the following topics:

- Complete detailed system architecture
- Preliminary and final design taking ISMS requirements (ISO 27000 Series) and National Cybersecurity Authority (nca.gov.sa) into account.
- Securing the interoperability of existing and interconnected (internal & external) systems.
- Bandwidth calculation (traffic / call profile) etc.
- Sub-system interconnection strategy / security, redundancy strategy
- Manufacturing drawings
- Procurement
- Equipment supplier shall be unified along the line.
- FAT and installation strategy
- Installation
- Exhaustive documentation including e.g., different coverage studies.
- Exhaustive QoS / KPI specifications, configuration etc.
- Test (measurement and functional end to end tests) and commissioning.
- Technical support
- Maintenance of operating equipment
- Final system approval
- Training and system hand over

To assure the project timeline and to validate all system criteria's the following milestones applicable to each of the telecommunication sub-system shall be respected. The Engineer's approval shall be obtained for each of the acceptance documents/certifications/procedures required by acceptance stages (a - e) prior to the formal execution of the associated acceptance test. Delivery times shall be agreed upon.

a) All relevant certifications and documentation shall be delivered.
b) Successfully executed factory acceptance tests.
c) Installation – acceptance procedure with independent third party.
d) Functional acceptance – acceptance procedure after system integration is completed.
    - For example, QoS / radio coverage measurements, video coverage study, PAS quality etc. – acceptance procedure with independent third party.
e) End to end functional tests – acceptance procedure at Test platform and on live network.

3 - ARCHITECTURE

All stations, depot and all technical and operational facilities shall be equipped with an Access Control & Intrusion Detection (AC/ID) system.
For the AC/ID network architecture two solutions are possible:

1) All centralized master unit's AC/ID at stations, depot technical facilities etc. shall be directly interconnected via dedicated optical fiber cables in a ring structure with the OCC and TCC. Starting from the centralized master unit AC/ID e.g., at stations the different units shall be directly interconnected. Dedicated transmission nodes are not required in this case. See figure 1. The SMR is not shown.

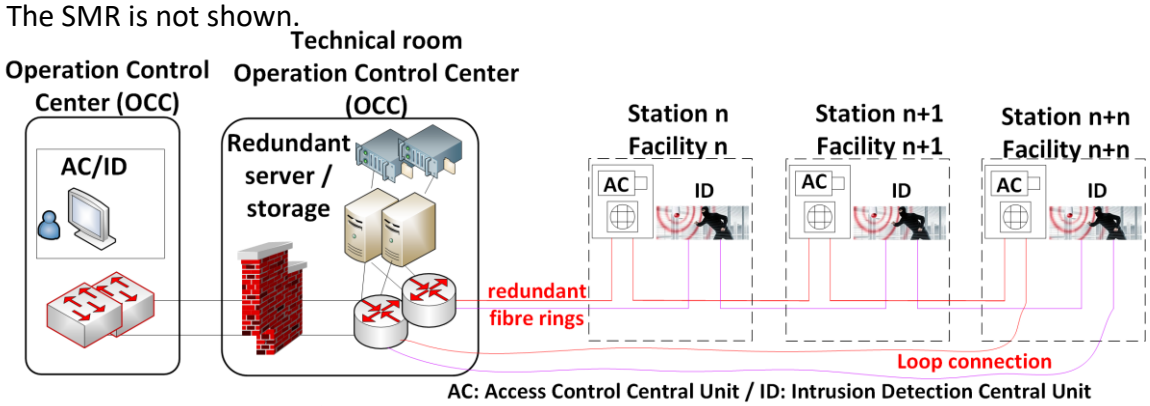

Figure 1 : AC/ID network architecture with dedicated fiber rings

2) A dedicated CTN shall be provided for the AC/ID system. Redundant transmission nodes with dedicated fibers shall be used. As far as possible an end-to-end optical fiber system solution shall be provided.

- Each station, depot and facility shall be equipped with centralized redundant transmission access nodes. These transmission nodes shall be interconnected in a redundant ring structure with the OCC and TCC. The centralized AC/ID master units shall be connected to the local redundant transmission access nodes. See figure 2. The SMR is not shown.
- In case of a CTN solution the following sub-systems shall use the same infrastructure:
  - AC/ID
  - PAS
  - PIS
  - Telephone and intercom system

  Each sub-system shall use a dedicated VPN.

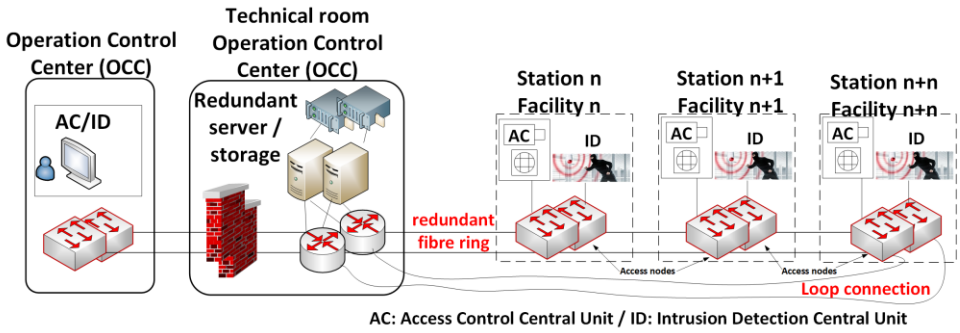

Figure 2 : AC/ID common network architecture

- In both cases the AC/ID network shall be protected via fire walls (level EAL4+). The centralized redundant fire walls AC/ID server and storages shall be located in the OCC. A geo-redundant AC/ID management system shall be located in the OCC.
- In case a station is isolated from the OCC the local AC/ID central units shall work in a standalone mode and shall be monitored via the SMR.
- An interconnection to the SCADA shall be established via the fire walls for alarm monitoring purpose. The AC/ID system shall be interconnected via fire walls with the fire alarm system.

The system shall be protected by an uninterruptible power supply (UPS).

The provided system shall be able to protect itself and recover from “Intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation” deduced from EN 62443 Security Level -4 (SL 1 – 4). For more details, please see [Ref. 2].

4 - SYSTEM AND FUNCTIONAL REQUIREMENTS

The AC/ID system consists mainly of:

- AC/ID System
- Perimeter protection system

To optimize the AC/ID system an interconnection to the CCTV system, intercom, SCADA and fire alarm system shall be established. All activities shall be logged and synchronized with the interconnected subsystems.

Employer and visitor access shall be manageable. The used technology for the access control card reader shall be the same as for the AFC to facilitate the interoperability.

The provided systems shall be ONVIF interoperable.

The provided equipment shall withstand dust, rain, vibration, shock, impact and temperature fluctuations. The ingress protection and impact protection rating shall be adapted to the environment (underground vs elevated) and agreed with the client.

The provided system shall be synchronized via the master clock system.

The most effective and technically feasible solution shall be provided with the objective to avoid false alarm.

On power supply restoration, recovery from shutdown shall be automatic such that all system functions are fully available to the operators and users within a time period of < 5 minutes.

The provided equipment shall be COTS and extendable without replacing existing equipment. Sustainability is required for the purchases, procurements, operational processes and the production of the "new assets". Local sustainability goals shall be fulfilled.

The supplier shall provide an energy saving and CO2 emission reduction concept. Objective is the CO2 neutrality.

Each equipment installed in the railway environment shall be EN 50121-4, EN 50125 and EN 61373 compliant or equivalent.

MTTR shall be 3h after failure detection/confirmation and spare parts available. After installation of the telephone and intercom systems, any maintenance operation shall be executable with less or equal to 2 maintenance staff members.

The telephone and intercom systems shall be properly fixed with the necessary clearance to avoid that it can be moved or accidentally damaged by the users. The steel parts and structures shall be designed considering atmospheric corrosion class C4 according to EN ISO9223.

The provided system shall be synchronized via the master clock system. The telephone and intercom internal clock shall enable free running in the event of a master clock signals loss without drifting a single second for a period of at least one week. The PIS shall manage the transition into and out of daylight-saving time properly without compromising the system. Network Time Protocol (NTP) shall be used as the protocol for the standardized time synchronization.

4.1 - AC/ID System

All technical and operational facilities along the metro line, stations, SMR, depot OCC and TCC shall be protected via an AC/ID system. The access shall be controlled via access cards (smart cards), fingerprint scanning, or face recognition technologies linked to CCTV and shall be controlled and monitored from the active OCC. All buildings shall be equipped with a local slave access control system. In case the connection to the centralized geo-redundant access control system fails the access to the buildings are not blocked. Each main door, tunnel access, electrical sub-stations, building entrances, technical facilities etc. shall be equipped with an intercom system with an embedded camera. The intercom system shall be used for example by someone having problems with the fingerprint reader or with the ID card. The embedded camera shall be used by the security team for identifying the person and to activate after positive identification the remote-controlled electric door strike to open the door.

The centralized access control system shall be connected to the CCTV, intercom and fire alarm system. As soon as someone tries to enter a building the CCTV shall start recording. In case the doors are kept open for too long an alarm shall be triggered locally (SMR) and at the active OCC. The door status open/closed shall continuously be monitored. Break-glass units shall be installed on predefined locations.

The access control system shall be interfaced with the fire alarm system in order to open / close doors in case of fire and to assure staff evacuation. The electrical locks shall be configurable as either “fail open” or “fail close” in accordance with safety regulation.

In case of unauthorized access (intrusion) an alarm shall be triggered via for example door / window dry contacts and the image of the best positioned camera shall be automatically displayed to a predefined monitor at the SMR, active OCC and TCC, with indication of the exact position of the intrusion and the telephone number of the nearest security staff. Operational related manholes (cover) shall be surveyed.

All events such as door opened, closed, forced opened, valid card, invalid card etc. shall be reported with time and date to the OCC and TCC and the SMR. For each event a detailed log file (time, date, location, CCTV picture etc.) shall be generated.

4.2 - Perimeter protection system

The sensitive property of the metro operator along the metro line, depot, shunting yards etc. above ground shall be protected with a centralized monitored wire fencing. To detect intruder the fence shall be equipped for example with optical fiber detectors. Based on a special algorithm in the centralized control and processing unit an intrusion can be identified based on the movement of the wire fence. In cases where an optical fiber detection system is not appropriate, infrared, motion detectors, vibration detection, ultrasonic or a combination of different systems are acceptable. The system shall be controlled and monitored from the active OCC and TCC.

The fence protection system shall be connected to the CCTV system. In case an intrusion is detected the nearest camera shall automatically point to this area and the image shall be displayed on a predefined monitor at the OCC. The monitor shall indicate at the same time the coordinates of the intrusion and the telephone number of the local security team responsible for this area.

5 - NETWORK MANAGEMENT SYSTEM (NMS)

A fully geo-redundant network management system (NMS) shall be provided.
Through the NMS a system network engineer manages the AC/ID network components inside the whole network and is able to perform all key functions related to:

- Operation
- Maintenance
- Provisioning
- Administration

from a centralized position. English and Arabic language shall be supported.

The NMS shall be able to share preselected information with the MMS and SCADA.

5.1 - Operation related functionalities

The following operational related functionalities shall be supported in real time:

- Monitor of system hardware (equipment)
  - Status health information of all network nodes and links
  - System access information about the last physical system access
  - Detailed firmware and software release information including date of latest update of each single equipment.
  - Detailed history (date, time, error reason, alarms, message) of each single equipment outage down to card level
  - Every alarm, action shall be captured in a log file. Search functionalities based on timestamp, events, locations shall be supported.
- KPI performance,
- Availability (RAM),
- Bandwidth monitoring and internet links monitoring in case of web-based applications,
- Error tracking and handling, filtering
- Alarm monitoring, all events shall be stored and time-stamped with an accuracy of 1 second.
- Free audible alarm configuration for each system component (enable / disable / inhibit)
- System status information including statistic reports to keep it optimized for efficient usage.
- Alarm and system related help functionalities (offline) shall be provided.
- Alarm thresholds and triggers shall be configurable and adjustable.
- Operator / Maintenance specified help functionalities shall be supported. Help functionalities shall be changeable based on user profile.
- Manual / automatic / semi-automatic report generation shall be supported including all previous indicated information. The report shall be configurable.
- Alarms, performance and availability statistics / reports shall be sent automatically to predefined destinations for example MMS.
- Periodic self- test capabilities including automatic alarm reporting.

5.2 - Maintenance related functionalities

The following maintenance related functionalities shall be supported:

- Network monitoring and error handling. Alarm information provided shall enable quick identification of the fault and its source.
- Adding new equipment to the system. Easily add, delete and modify nodes, configuration of new circuits from end to end shall be supported.
- Removing equipment from the system
- Modifying system configuration (single equipment and bulk provisioning; automated scripts shall be supported based on day and time)
- Inhibit equipment and functions, bulk or single equipment, and support related temporary or fixed alarms configurations.
- The Inhibit function shall allow an operator and maintenance to add a comment in text format for one or multiple system elements to indicate why the element is “inhibit”. During activation the information shall be sent to the TCC / indicated at the NMS.
- Redundant backup database with all network elements / configuration shall be provided. In case of an important outage the system configuration can be reestablished.

5.3 - Provisioning related functionalities

The following provisioning related functionalities shall be supported:

- Spare parts repair and return
- Adding new functionalities / capabilities
- Provide information for any circuit or group of elements in printed and soft copy shall be supported.
- The interrogation and modification of any network configuration shall be supported.

5.4 - Administrative related functionalities

The following administrative related functionalities shall be supported:

- System access control (password rules see ISMS) including multiple user profiles and access rights,
- Each user shall get the detailed information of his user profile; access rights; assigned and available functionalities.
- System planning
- Resource allocation and optimization
- Coordination of network resources,
- System analytics and security,
- Management of related accounting functions

  The following functionalities shall be provided:

  - Log-off functions through a single sign-off.
  - Workstation / client locking
  - In order to unlock a workstation, the operator shall enter his password.

The Transmission System shall continue to function even if the whole NMS is out of service.

6 - INTERFACE REQUIREMENTS

The AC/ID system shall be interconnected with:

- Transmission network (CTN)
- AC/ID related clients/workstations
- OCC and TCC
- Maintenance management system
- Clock system
- SCADA / ICS (PSIM)
- Energy/Low Voltage/UPS

All external and internal interconnections (interfaces) shall comply with ISMS politique (IEC 27000-series or equivalent).

The AC/ID system shall support where necessary:

- Power over Ethernet (PoE) in accordance with IEEE 802.3af or equivalent.
- PoE+ in accordance with IEEE 802.3at or equivalent.
- PoE++ in accordance with IEEE 802.3bt or equivalent.
- 4pPOE in accordance with IEEE 802.3bt or equivalent.

PoE, PoE++, 4pPOE shall be supported and validated based on IEC60512-99-002.

IPv4 and IPv6 shall be supported in compliancy with RFC 791 and RFC 2330 or equivalent.

HTTPS, SNMP V3, TLS shall be supported.

Used protocols shall be in line with ISMS requirements (ISO 27000 Series) and National Cybersecurity Authority (nca.gov.sa) and shall be validated.

7 - ANNEX A

The following table provides an extraction of applicable standards. The latest standards shall apply unless if older version of a standard is used for a technical reason, which shall be agreed upfront.

Standard	Description
ANSI/ BHMA A156.31, GRADE 2	AMERICAN NATIONAL STANDARD FOR ELECTRIC STRIKES AND FRAME MOUNTED ACTUATORS
BS 5979	Remote centers receiving signals from fire and security systems. Code of practice
EN 1125	Building hardware. Panic exit devices operated by a horizontal bar, for use on escape routes. Requirements and test methods
EN 14846	Building hardware - Electromechanically operated locks and striking plates
EN 5013	European Standards for Intruder Alarm Systems
EN 50130-4	Alarm systems:Part 4 electromagnetic compatibility immunity requirements for components.
EN 50131	Alarm systems: intrusion & hold-up systems
EN 50133	Alarm systems
EN 50164-3	Lightning Protection Components (LPC) - Part 3: Requirements for isolating spark gaps
EN 60529	International Protection (Ingress Protection)
EN 61643-11	Low-voltage surge protective devices - Part 11: Surge protective devices connected to low-voltage power systems - Requirements and tests methods
EN 61643-21	Low voltage surge protective devices - Part 21: Surge protective devices connected to telecommunications and signaling networks – Performance requirements and test methods
EN 62305-1	Protection against lightning - Part 1: General principles
EN 62305-2	Protection against lightning - Part 2: Risk management
EN 62305-3	Protection against lightning - Part 3: Physical damage to structures and life hazard
EN 62305-4	Protection against lightning - Part 4: Electrical and electronic systems within structures
IEEE 802.3af	Power Over Ethernet
IEEE 802.3at	Power Over Ethernet Plus
ISO/IEC 14443A, B2	Four-part international standard for proximity and contactless smart cards
ISO/IEC 15693	Standard for cards which can be read from a greater distance as compared with proximity cards
ISO/IEC 19784-1	Framework and Biometric Service Provider for iris identification engine
ISO/IEC 19785-1	Common Biometric Exchange Formats Framework
ISO/IEC 19794-5	Information technology - Biometric data interchange formats - Face image data
ISO/IEC 19794-6	Biometric Data Interchange Formats - Iris Image Data
ISO/IEC 19794-8	Information technology - Biometric data interchange formats -- Part 8: Finger pattern skeletal data
ISO/IEC 27037	Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence
ISO/IEC 60950-1	Information technology equipment - Safety - Part 1: General requirements
ISO/IEC 7810	Physical characteristics for identification cards
NFPA 780	Standard for the Installation of Lightning Protection Systems
OASIS / CAP	Common Alerting Protocol

Standard	Description
ONVIF Profile A	Broader access control configuration
ONVIF Profile C	IP-based basic Access Control
OPC Foundation	Open Platform Communications standards and specifications for industrial telecommunication data exchange
PSIA	Physical Security Interoperability Alliance standards
SIA AC-011996.10	Access Control Standard Protocol for the 26-bit Wiegand TM Reader Interface
UL 1076	Standard for Proprietary Burglar Alarm Units and Systems
UL 1981	Standard for Central-Station Automation Systems
UL 294	Standard for Access Control System Units

TABLE 1 : STANDARDS