DOC NUMBER: 569-DB07-AIC-184-002	CLIENT NUMBER: PRD-AIC-TSP-003

CLIENT:

TAKEDA/BAXALTA

PROJECT

BURITI EPCMV PROJECT

SECURITY ACCESS CONTROL SYSTEM

TECHNICAL SPECIFICATION

1	22NOV2021	ISSUE FOR CONSTRUCTION CONSIDERING COMMENTS	MAV	MAF	RSP
0	13OCT2021	ISSUE FOR CONSTRUCTION	MAV	MAF	RSP
E	24SEP2021	90% DD ISSUE	MAV	MAF	RSP
D	08FEB2021	30% DD ISSUE	MAV	MAF	MAJ
C	16OCT2020	FINAL BD ISSUE	MAV	MAF	MSS
B	28AUG2020	90% BD ISSUE	MAV	MAF	MSS
A	09JUL2020	50% BD ISSUE	MAV	MAF	MSS
REV	DATE	DESCRIPTION	EXEC	CHECK	APPROV.

INDEX

1. REVISION HISTORY

Rev.	Reason for change
A	50% BD ISSUE
B	90% BD ISSUE
C	FINAL BD ISSUE
D	• Included DOC NUMBER and rename CLIENT NUMBER (Former PRD-AIC-TS-003). • New numbers of drawings for Riser Diagrams of ACS, item 6.3. • Adding document for Bill of Materials – ACS, item 6.4. • Adding “to be confirmed” the integration ACS and CCTV system at Hemobrás site, item 7.3.1.10. • Fixed item 7.3.1.21 according to comments from manufacturer. • Updated item 7.3.5.2. • Updated item 7.4.1.1.2 • Deleted sub-item 7.4.2.1-f according to comments from manufacturer and updated supplier. • Updated item 7.4.4.4 according to comments from manufacturer. • Updated item 7.4.5.1 according to comments from manufacturer. • Traffic Control Barriers out of scope, item 7.4.10 • Revised PC Requirements for LiNC-NXG SYS, item 7.4.11.4 • Added PRK736 Reader w/ Keypad, item 7.4.6.4. • Updated item 7.4.9.5 • Deleted item 7.4.10 (out of scope)
E	• Deleted text double strikethrough • Updated item 3.1 • Updated item 6.4 • Updated item 7.2, 7.3.5.2, 7.4.5.2l • Added item 7.3.1.25
0	• Rewritten items 7.3.1.10, 7.3.5.2, 7.3.5.3 • Renumbered item 8 • Added items 9, 10, 11, 12, 13, 14, 15
1	• Added items 16 and 17

2. PROJECT DESCRIPTION

2.1 Takeda has re-negotiated a licensing and tech transfer agreement (LTTA) with the Brazilian state- owned company Hemobrás (HB) to transfer the technology of Takeda's recombinant FVIII (rFVIII) product ADVATE from Takeda to Hemobrás. Hemobrás is planning to construct a vertically integrated facility for manufacturing of rFVIII at the Hemobrás owned site at Goiana, Pernambuco (PE), Brazil (Project Buriti).

2.2 The scope of Project Buriti is to design, build and qualify a new vertically integrated rFVIII Manufacturing facility, and includes implementation of all needed support buildings and Systems (Warehouse, QC Lab, Administration, Cafeteria and Utilities) on an existing brownfield site. It is expected that the new facility is completely self-contained, and the existing Goiana site provides only basic utility supply (city water, gas, power) and logistics (access road, site security). The project also must account for operation's waste management (specifically process waste). The site's capacity layout for ADVATE manufacturing shall be based on three 2500L chemostat bioreactors, even though only equipment for a two bioreactor operation should be implemented at first.

2.3 To guarantee an optimal integration with current facility operations, a complete functional telecommunications systems connection between the new building and the existing Hemobrás buildings will be designed.

3. SCOPE.

3.1 This document has been prepared to define the specifications and minimum requirements for the supply of the Access Control System to be installed on the facilities of buildings B07A-Drug Product, B07B-Drug Substance, B07C-Boilers and B07F-Emergency Generators.

3.2 A system compatible with the existing system on site is required.

4. ACRONYMS.

ACS	Access Control System
CR	Card Reader
CRk	Card Reader to be provided with keypad
DC	Door Controller
DPS	Door position switch
ES	Electric strike
FTS	Full-height turnstile
ML	Magnetic lock
OWS	Sign-up station
TS	Turnstile

5. REGULATIONS AND STANDARDS.

5.1 Systems design, equipment, materials, and procedures, considered in this project, have to fulfill the next regulations and standards:

Alarm and electronic security systems Part 11-1: Electronic access control systems - System and components requirements	IEC 60839-11-1:2013
Degrees of protection provided by enclosures (IP Code)	NBR IEC 60529:2017
Degrees of protection provided by enclosures for electrical equipment against external mechanical impacts (IK code)	NBR IEC 62262:2015
Alarm systems — Intrusion and hold-up systems Part 1: System requirements	NBR IEC 62642-1:2019
Alarm systems - Intrusion and hold-up systems Part 6: Power supplies	NBR IEC 62642-6:2019
Environmental testing - Part 1: General and guidance	IEC 60068-1 Ed. 7.0 EN-FR
Alarm systems - Part 1: Environmental test methods	IEC 62599-1 Ed. 1.0 b
Alarm systems - Part 2: Electromagnetic compatibility - Immunity requirements for components of fire and security alarm systems	IEC 62599-2 Ed. 1.0 b
Low Voltage Electrical Installations (Instalações Elétricas de Baixa Tensão)	NBR 5410
Regulatory Standards of the Brazilian Labor Department (Normas Regulamentadoras do Ministério do Trabalho)	NR
Electronic Industries Association	EIA
International Standards Organization	ISO

6. PROJECT DELIVERABLES.

6.1 Drawings and documents for basic design, that follow Hemobrás's requirements and standards.

6.2 Drawings will be issued in AutoCAD and Documents will be issued in Microsoft Office.

6.3 Reference drawings:

7A-I-0-7-06	Riser Diagram	Drug Product	Security ACS
7B-I-0-7-06	Riser Diagram	Drug Substance	Security ACS
7A-I-1-3-12	Ground floor	Drug Product	Access Control
7B-I-1-3-12	Ground floor	Drug Substance	Access Control
7A-I-2-3-22	First floor	Drug Product	Access Control
7B-I-2-3-22	First floor	Drug Substance	Access Control
7A-I-0-3-02	Walkable ceiling	Drug Product	Access Control
7B-I-0-3-02	Walkable ceiling	Drug Substance	Access Control
7A-I-3-3-32	Second floor	Drug Product	Access Control

7B-I-3-3-32	Second floor	Drug Substance	Access Control
7C-I-1-3-12	Ground floor	Boiler	Access Control
7F-I-1-3-12	Ground floor	Emergency generators	Access Control

6.4 Reference documents:

PRD-AIC-TSP-003	Security Access Control System Technical Specification
PRD-AIC-TSP-015	Security Access Control System Design Basis
PRD-AIC-LIS-022	ACS Equipment Devices Schedule
PRD-AIC-LIS-040	Bill of materials - ACS

7. ENGINEERING INFORMATION.

7.1 General definitions

7.1.1 Access control has an important role to play in identifying and controlling a given area, people, vehicles, assets, etc. All identification parameters, permissions and filters are defined through a dedicated system that can be called a security and access control platform.

7.1.2 The project shall fully comply with ABNT standards, and in the absence or omission thereof, the internationally recognized standards mentioned above shall be observed.

7.1.3 All electronic equipment must meet the requirements of regulations on radio frequency electromagnetic interference.

7.2 Subject Areas Covered

7.2.1 The new Access Control System shall be installed in the following buildings described below belonging to the Buriti project,

BUILDING TAG	DESCRIPTION
B07A	DRUG PRODUCT (FDP)
B07B	SUBSTANCE PRODUCT (BDS)
B07C	BOILERS
B07F	EMERGENCY GENERATORS

7.3 Access Control System and Door Interlock

7.3.1 System Description

7.3.1.1 The Access Control System allows to track what or who was present in the controlled area.

7.3.1.2 The Access Control System shall be installed utilizing proximity card reader type devices.

7.3.1.3 The Access Control System will be composed of equipment and applications dedicated to management and access control of people, vehicles, and materials in the places where they will be installed in the buildings.

7.3.1.4 The Access Control System will have as main objective to act in the restriction and access control of unauthorized persons and vehicles, to the places controlled.

7.3.1.5 All access and access attempts, authorized or unauthorized, must be duly registered, and this information should be shared with the CCTV Security System, both in real time as in the form of a database in places that have cameras.

7.3.1.6 The Access Control System will consist of a set of connectivity products employed from according to specific engineering rules, whose main characteristics are:

a) Open architecture.

b) Standardized protocols of transmission and physical arrangement.

c) Compliance with international standards.

d) Customized design and installation.

e) Provide a minimum of 20% reserve for possible extensions.

f) Fully compatible with the system existing on the Hemobrás website.

7.3.1.7 The network infrastructure of the access control system will include all interlocking systems of doors and entrance and exit monitoring to be used inside all buildings (offices, laboratories, conference rooms, production, and support areas, etc.).

7.3.1.8 The set of specifications will ensure a modular implementation with expansion capability programmed. The products used must ensure maximum connectivity to the devices and prepare for the infrastructure for future technologies. The topology employed should facilitate diagnostics and maintenance.

7.3.1.9 The system in its entirety will be composed of equipment platforms, devices and software that enables its migration and continuous updating from the same platform without major impacts on operation and maintenance of the entire system, considering the state of the art in the entire control system of access.

7.3.1.10 The Access Control System in conjunction with the CCTV Security System, will form the Integrated Safety System of Takeda/Baxalta´s new buildings located at Hemobrás site and Hemobrás existent buildings, whose main monitoring should be in a Monitoring Room/CCTV to be allocated in the Hemobrás Guardhouse.

7.3.1.11 As the basis of any package system, i.e., cameras, etc., the library should be provided SDK (Software Development Kit) and must be integrable to the existent system.

7.3.1.12 This integration will enable the CCTV Security System to be alerted whenever a unauthorized access attempt, generating an alarm and consequently record of the occurrence in both systems and action of Hemobrás's Security people.

7.3.1.13 The system shall perform the management, recognition and access control of people and vehicles through an identification technology and with the aid of physical blockages such as: Full-height turnstile, turnstiles, door controllers and gates. The identification can be done by a single technology or by combined technologies.

7.3.1.14 The system also aims to keep a record of people who pass through the environment controlled, allowing or not its access through pre-determined criteria and permissions and registering its movement for reporting purposes and access history.

7.3.1.15 To do this, the system must communicate with the access control equipment in real-time mode, sending and receiving constantly a series of information that enables the management. In addition to the real-time operation, the system should allow the control equipment to operate in stand-alone mode in case of absence of the access control system server, in an eventual interruption in the data network.

7.3.1.16 Communication between the access control system server, the operator stations, and door controllers should be carried out over the Ethernet network with protocol TCP/IP. The operator stations must work in WEB environment and/or client/server software, while all system parameterizations should be done through client/server software.

7.3.1.17 Door controllers should allow identification of persons at the specified locations for the release of access by employees, contractors, and visitors. Card Readers must be installed for both entry and exit access.

7.3.1.18 Through a single terminal, the system administrator should obtain in a single interface the control absolute of the system, being able at any time to block an employee, determine its location, check date and time of access on site, issue reports with employee data such as name, identity, sector of the company in which they work, what are the times they usually use the access system and all the information about your access history. It should also be able to control people's access at certain times of the week, Saturdays, Sundays, or holidays, allowing, for example, the access can be allowed to an employee.

7.3.1.19 The access control system should provide for visitor identification. It will have screen for registration of data, photo capture and access profile assignment.

7.3.1.20 Visitors must be identified at the receptions (visitor registration module) or previously scheduled by those visited (visitor scheduling module). When the registration is made at receptions, operators must capture the image of the visitor and his/her respective document (front and back) to complement its registration information. No solutions that require double registration will be accepted.

7.3.1.21 The system should allow automatic recover of visitor data in the event of the return of same, regardless of where the equipment and devices are installed. You must process real-time and online information (including scanned images) to identify the employees, third parties and visitors.

7.3.1.22 The access control system should allow importing and exporting the information to the database necessary for the registration of employees, including the captured images, thus dispensing with the manual registration. It should also allow you to consult and control, in real time and online, the database information for any access request action, regardless of the location of installation of equipment and/or devices.

7.3.1.23 The system should automatically register and display on the screen of operator stations and management, messages containing all site access operations, alerts and alarms, all containing the description of the day, time, username, location of the equipment to which access was given requested, etc.

7.3.1.24 The doors of Automation Rooms, Electrical Rooms (Switchgears, MCC room, generator), will have card reader at the main entrance in addition to an electromagnetic lock, magnetic position sensor, unlock button and emergency. Double doors, used for equipment entry, will be equipped with mechanical locking devices, so that the opening is only released from the inside of the room, no allowing access from the outside and equipped with magnetic sensors on both sheets, to monitoring status open/close.

7.3.1.25 The access control system should be interfaced with the BMS to inform with a general alarm of an event that has occurred in the system. The operator must access the access control system to check where the event was.

7.3.2 Door Interlock System

7.3.2.1 Components and definitions

7.3.2.1.1 Door Position Sensor (S) - monitors door position (closed or open).

7.3.2.1.2 Proximity Card Reader (CR) - releases access for registered persons.

7.3.2.1.3 Magnetic lock (ML) - The magnetic lock will lock the door when energized or unlocked when de-energized. The magnetic lock will receive signals from the door control panel.

7.3.2.1.4 Motorized Port Touchless Sensor (PBT) - The PBT is a touchless sensor to open a motorized door. When activated on a block, PB will send a signal to the control panel to open the desired door. If all the doors inside the lock are in the closed position, the door opens automatically. But if any door is in the open position, the desired door will not open unless the Emergency is triggered or if there is a fire alarm condition.

7.3.2.1.5 Every Motorized Door should have a PBT (Touchless Sensor).

7.3.2.1.6 Emergency Switch / "Anti-Panic" (RE) - The Emergency Switch will be of the type glass breaker, located on all sides of the door, inside the interlock, including the inside the Clean Room. An Emergency button will not be installed next to a reader of access card readers since it represents the breach of security. The Emergency button will de-energize all magnetic locks within the Interlock when activated.

7.3.2.1.7 The Emergency button should only be activated in cases of emergency or failure of the system.

7.3.2.1.8 Signaling LEDs - lock (red) and release (green).

7.3.2.2 System Description

7.3.2.2.1 In places where airflow and contamination insulation are considered critical will be equipped with a door control and sequencing system. The objective is preventing the opening of more than one door to an airlock at any time. The exact opening sequence of the doors will be, as indicated on the control panels and signage. Door interlocking systems shall be equipped with emergency for local emergency release and an interface to the building fire for automatic release after an alarm is activated.

7.3.2.2.2 When a door is in the open position the next door will be blocked and not can be opened until the first one is closed. The locking system will have a range of configurable time between the opening of the first door and the opening of the second that will be with based on recovery time. This will be done through the door control system.

7.3.2.2.3 The Door Interlock System should be dedicated and not centralized to a Central PLC.

7.3.2.2.4 Because it is a system used in pharmaceutical environment, the project and subsequently the manufacturing procedures should be framed in the standards and procedures of GMP applicable to this type of industry and those of the FDA and ANVISA.

7.3.2.2.5 Door interlock has the function of not allowing the opening of two or more doors simultaneously. When the system is triggered from one of them, the other doors are locked while the first door remains open.

7.3.2.2.6 The door is cleared for opening when the Green LED is lit; the open a door the system locks the interlocked one(s) by igniting the Red LED of the locked doors.

7.3.3 Access Control System Network

7.3.3.1 Communication between the access control system server, the operating stations, and the door controllers should be carried out over the Ethernet network with protocol TCP/IP. The operation stations must work in WEB environment and/or client/server software, while all system parameterizations should be done through client/server software.

7.3.3.2 The structured cabling system will integrate the various means of transmission (metal cables, optical fiber, radio, etc.) supporting multiple applications including the access control system.

7.3.3.3 The entire communication network of electrical (UTP) and fiber optic cables must be certified.

7.3.4 Basic System Requirements

7.3.4.1 Identify individually each employee, service provider, visitor and other persons who may have access to the buildings, thus preventing unknown people from having access to areas that are not authorized.

7.3.4.2 Within the same area, in the case of Classified/Controlled Areas there will be the need to identify and allow the employee to enter or not to enter certain rooms.

7.3.4.3 Printing access cards (badges), using information from the Access Control System Database.

7.3.4.4 Support all card reader and card market technologies such as Proximity, Barcodes, Magnetic band among others.

7.3.4.5 Allow access control with proximity card readers, keyboard and biometrics (printing digital).

7.3.4.6 Based on digital communication technology, using Convergent Network (Ethernet TCP/IP) for communicate between the access control system, and the Door Controllers Units, Turnstiles IP, and Gates IP.

7.3.4.7 The implementation of the Access Control system will offer the following basic features:

a) People Access Control (General).

b) Access Control within GMP areas.

c) Access Control of vehicles into the buildings.

d) Access card printing (badge)

e) Emergency action (door release and other types of unlocks in cases of fire alarm)

f) Communication with Hemobrás Security Monitoring Room (Guardhouse).

g) Fully compatible with the system existing on the Hemobrás website.

7.3.4.8 The system shall consist of at least the following equipment:

a) Management and visualization workstation.

b) Sign-up stations with image capture of people and documents.

c) the Central Sign-up Station, for sign-up and printing of employee cards and service providers (TBD, can be used existent Hemobrás station).

d) the Database Server located in the Automation Room.

e) the Application Server located in the Automation Room.

7.3.5 Access Control Architecture

7.3.5.1 The architecture of the access control and door interlock system should be scalable, decentralized and provide for redundancy mechanisms.

7.3.5.2 See reference drawings in item 6.3.

7.3.5.3 Regardless of whether sites have different and distant addresses, the architecture of the access control and identification should consider at least 03 (three) functional levels and one level of contingency:

7.3.5.3.1 **First level**: This level must consist of server and workstations (microcomputers). It must be responsible for the administration and control of the whole system.

a) Server: Equipment responsible for providing all functions and services concerning the network, including the database.

b) Workstations: Responsible for the implementation of information, registration, management as well as for the control and monitoring of all access events that occur in the blocks. This equipment, regardless of the address of installation, must be interconnected and in communication with the server.

7.3.5.3.2 **Second level:** This level should consist of the concentrator(s), and should be the responsible for intercommunication between levels, management, interpretation, and implementation of information regarding access events. This level, when controlling a safety-critical environment (requires rules such as: re-entry denied, re-entry denied by time, maximum room capacity, invalid date and time, suspended person, etc.), should be able to manage the business rules autonomously, even if communication with the (the) server(s), necessarily using concentrator(s). In case of location without high level of security, validation should be done at the third level through the validation list.

7.3.5.3.3 **Third level:** This level should consist of the Door local controller(s), card readers, turnstiles, doors, etc. should be responsible for collecting the information of identification, human interface devices and execution of physical blocking of access. This level must load at least one validation list to maintain user access, if lose communication with the central controllers or concentrators.

a) Door Position Sensor (S) - monitors door position (closed or open). This level should consist of local servers, which should assume operation automatically until communication with the central server is re-established. The local server should have full autonomy to manage access permissions and other functions, as well as report all information to the central server when returning the communication, being this application used only in critical locations.

8. EQUIPMENT SPECIFICATIONS

8.1.1 The Access Control System and Door Interlocks shall consist of at least the following equipment:

8.1.1.1 Sign-up station (OWS)

8.1.1.1.1 01 (one) OWS will be supplied and installed to capture and scan documents of employees and visitors to the buildings.

8.1.1.1.2 The following features must be fulfilled:

Workstation PC requirements Windows 8, 8.1, or 10 Professional, Microsoft SQL Server 2012, 2014, or 2016, Intel Core 2 Dual 2.8 GHz, 12 GB RAM or greater, 500 GB hard drive, DVD R or R/W, 100MB or 100/1000 MB NIC, monitor to support 1024x768 or greater, Mouse and keyboard.

a) Supplied with two color micro-cameras, USB type, one for the photo of the document, and another for the user's photo, in transparent acrylic pedestal, with automatic camera switching, the switching must be made without the activation of any electromechanical device.

Reference: Dell or technically equivalent.

8.1.2 Proximity cards

8.1.2.1 1,000 (one thousand) proximity cards should be provided with the following characteristics:

8.1.2.2 The cards to be supplied are PC-73 model or technically equivalent with the following characteristics:

a) Frequency @ 125 kHz

b) 37-bits

c) Supports photo customization.

d) Made of white PVC.

e) Access card and frequency control with 8.57 X 5.40 X 0.18 cm.

f) With alligator clamp centered on the narrowest edge (badge vertical) and the badge can also be used as a cord.

g) Customized through overlay also in PVC, in polychrome, with photo of the user in art to be defined by the CONTRACTOR.

Reference: PCSC.

8.1.3 Door Controller

8.1.3.1 The reference model is from the manufacturer PCSC, the IQ Series, model IQ-200, where the number of Reader Ports supported is 2.

8.1.3.2 General features:

a) Information storage of 100,000 cards

b) Stored history 60,000 transactions

c) Coding of 16 different zones

d) 4 authorization groups per card

e) 64 periods of time, with 7 sequences per period

f) 366 holidays

g) 1 year of battery safeguarding clock, calendar, and memory

h) Expandable

i) Firmware electronic update (Flash memory)

j) Automatic card deactivation by date

k) Real-time visual diagnostics (via indicator display)

l) External power supply: 220Vac UPS

m) Internal Power supply: 12Vdc

n) AC and DC failure indicator

o) Supported communication protocols:

- Ethernet (10/100 TCP/IP)

8.1.4 Card readers

8.1.4.1 The card readers, also of the PSCS reference brand to be installed have the following features output pattern, the Wiegand industry standard. Two types of card readers are considered:

8.1.4.2 Reader without keyboard, model PR-732:

a) Versatile mounting

b) Voltage/current: 5-12 VDC 50-80mA

c) Outputs: Wiegand and RS-232

d) Reading distance: 7.6-8.9 cm

e) Visual (LED) and audible notification

8.1.4.3 Parking reader, model PR-735:

a) Wall mounted

b) Voltage/current: 1.2A @ 5VDC to 0.4A @15VDC

c) Outputs: Wiegand and RS-232

d) Reading distance: 45.7-61.0 cm

e) Developed for both internal and external applications

f) Visual (LED) and audible notification

8.1.4.4 PRK-736 Reader w/ Keypad:

a) Versatile mounting

b) Voltage/current: 5-12 VDC 50-80mA

c) Outputs: Wiegand and RS-232

d) Reading distance: 7.6-8.9 cm

e) Visual (LED) and audible notification

8.1.5 Door position switch

8.1.5.1 A Door Position Switch is a switch and magnet mounted on the door and frame that monitors the door status. If door is held open beyond rearm time or if door is forced open, alarm will sound in the Access Control system. Will be supplied by the door's supplier.

8.1.6 Electric strike

8.1.6.1 An electric strike is an access control device used for door frames. It replaces the fixed strike faceplate often used with a latch (also known as a keeper). Like a fixed strike plate, it normally presents a ramped or beveled surface to the locking latch allowing the door to close and latch just like a fixed strike would. Will be supplied by the door's supplier.

8.1.7 Maglock strike

8.1.7.1 A magnetic lock, or mag lock, consists of a large magnet that is installed along the top of a door frame. A metal plate, or armature plate, is fastened to the door so it lines up with the magnet. When electrical power is supplied to the magnet, it creates a magnetic charge that keeps the magnet tightly pressed to the metal plate. This keeps the door securely locked until power is removed or interrupted.

8.1.7.2 With a magnetic lock, the door is always locked from both sides of the opening. This makes mag locks a very secure option for areas that require high levels of security. Users must activate the lock with a keycard or other device when leaving and when entering. A handle or latchset is used to operate the door, but typically has no locking function.

8.1.7.3 All magnetic locks will work only with DC current, 12 volts.

8.1.7.4 All magnetic locks are fail safe.

8.1.7.5 2 sets of 80Kgf pull magnetic locks work well in light duty installations such as electrical and automation rooms.

8.1.7.6 Will be supplied by the door's supplier.

8.1.8 Main features of access control software

8.1.8.1 The Reference System is the one developed by PCSC, LiNC-NXG, or technically equivalent.

8.1.8.2 It must be scalable in nature, new elements can be added, as well as the modification of its license, allowing an expansion of the system with low cost if compared to a new project.

8.1.8.3 The software must be a fully integrated and scalable access control and security management solution, developed for all types and sizes of applications in installations.

8.1.8.4 Main functionalities of the software:

a) Fault Tolerant Architecture
b) Legacy Support
c) 100% Distributed Intelligence
d) Peer-to-Peer Communications
e) Password / Level Control Functions
f) Password Controlled Data Segregation
g) Operator Audit
h) Active Directory
i) Lock Down
j) Password Controlled Administration
k) One Click Bulk Activation or Deactivation by Cardholder Affiliation
l) Supervisor Controlled Access
m) Visitor Controlled Access
n) Long Access / Handicapped Access
o) Network Time Protocol (NTP)
p) Access Actions by Cardholder or Group
q) Temporary Authorization Group
r) Photo Trace
s) Operator Solicited Open Door
t) Two Person Minimum Occupancy Rule (TPMOR)
u) Automatic System Shutdown Prior to Battery Failure
v) Automatic Door Opening by Time or Supervisor
w) Automatic Card Activation and Deactivation by Date and Time
x) Automatic User Scheduled Reports
y) Automatic Daylight Savings Control
z) User Defined Reports
aa) Intelligent Elevator Control
bb) Floor Destination Reporting
cc) 5 State Alarm Monitoring
dd) Occurred and Logged History Time Stamp (UTC Time Stamp)
ee) Regional Anti-Passback
ff) Strict / Lenient and Soft Anti-Passback
gg) 3 Levels of Entry / Exit
hh) Network Status with Firmware Verification

ii) User Selectable Alarm Type (Supervised or Dry Contact)

jj) Individual Alarm Latching Selection

kk) User Defined Input / Output Polarity

ll) Priority Alarm Processing

mm) Integrated Video Badging

nn) Integrated Alarm Graphics

oo) Integrated CCTV

pp) Supported OS: LiNC-NXG SYS - PC requirements Windows Server 2012 R2 or 2016 or Windows 8, 8.1, or 10 Professional Microsoft SQL Server 2012, 2014 or 2016 Intel Core 2 Dual 2.8 GHz or greater, 12 GB RAM or greater, 500GB SATA HD or greater, DVD-R or R/W, 100MB or 100/1000MB NIC, Monitor to support 1024x768 or greater, Mouse and keyboard

9. OPTICAL FIBER INSTALLATION

9.1 Before cabling optical fiber is Contractor’s liability to present FAT and SAT tests.

9.2 Optical fiber installation minimum requirements:

a) A 3-meter cable spare length must be considered in connection points.
b) Fasten optical fiber with plastic ties every 1.5 meters from entrance point to back, to liberate cable without jacket from mechanical stress.
c) Remove optical fiber jacket and cover and route each strand to their connection point considering 1 meter cable spare length in the interior.
d) Identify optical fiber cable pathways using fastened ID labels at every 20 meters of cable and in connection points. These IDs will help in installation, maintenance and relocation process.
e) Each strand must be identify placing one label not further than 5 cm away from strand jacked remove point. TX or RX legend and assigned pair must be on the label.
f) Optical fiber connectors must be LC.

9.3 Is Contractor’s liability to perform a technical evaluation to each optical fiber link to guarantee fulfillment of regulations and stablished parameters.

9.4 To guarantee fulfillment of regulations in optical fiber links, contractor must perform and present test methods for optical fiber links, these test methods must be performed from cable fabrication to the last operation test.

9.5 During installation two different kind of metering, with very different scopes must be identified:

a) Construction metering: Its scope is to verify received materials quality and condition and to verify quality of works through each phase of the project, if any work is not made with the stablished quality Contractor must fix it before moving to the next phase.

b) Final metering: More exhaustive metering, will be used when installation is finished, will be performed over a complete section of the project, and verifying results within stablished regulations.

9.6 Test methods for Optical Fiber engulfs fabrication method measuring concentricity, core, cover, attenuation, bandwidth, dispersion, and many others.

9.7 Contractor’s minimal optical fiber test:

9.7.1 On site cable drums: Verifies received materials with no transport damage. Tests:

a) Deficiency detection
b) Previous checkups

9.7.1.1 Physical cable inspection and optical fiber attenuation check through OTDR (Optical Time Domain Reflectometer). These tests are performed in site warehouse in the presence of TAKEDA/BAXALTA technical staff.

9.7.1.2 Cable drums condition is reviewed, and cabling is not allowed if any fault is detected.

9.7.1.3 Retro disperse signal test is performed to each cable drum for future reference. Test results must match manufacturer cable data sheet. Retro disperse attenuation check must be performed in each optical fiber strand. This test must be performed; manufacturers data sheet is not enough.

9.7.2 2. Laid cable: Verifies laid cable, reviewing applied tension to the cable to guarantee optimal cable conditions without any break or tearing. Tests:

a) Deficiency detection
b) Retro disperse attenuation

9.7.2.1 Physical cable inspection and retro disperse attenuation check through OTDR (Optical Time Domain Reflectometer). These tests are performed when cable is laid in the presence of TAKEDA/BAXALTA technical staff. Retro disperse attenuation check must be performed in each optical fiber strand and results must be compared to on site cable drum test results to review the loss of attenuation.

9.7.3 Final metering: When cable installation is finished, final metering must be performed

a) Deficiency detection
b) Retro disperse attenuation

c) Insertion losses attenuation

9.7.3.1 These tests must be performed to each optical fiber strand in operational wavelength with one OTDR (Optical Time Domain Reflectometer). This equipment reviews optical fiber condition and splices. OTDR sends an optical pulse and measures time since pulse was sent until pulse reflection is received. OTDR measures attenuation in each splice and fusion or mechanical connector to verify results against regulation data.

10. CABLE PATHWAYS

10.1 Cable pathways for Buriti project will provide Access Control services to project areas. Contractor must supply cable pathways with complete mechanical supports, accessories, and materials to deliver a complete and functional Access Control System. Two different kind of cable pathways will be used: Conduit and Cable tray.

10.1.1 Conduit

10.1.1.1 Inside the buildings cabling will be routed in galvanized steel cable tray type mesh and galvanized steel conduit thick wall outdoor and thin wall in indoor according to the different areas in the plant and proper accessories such as: connectors, monitors, curves, pull boxes, etc. in filling packing lines areas shall be used stainless steel 304/316 rigid metallic conduit (RMC) shall be considered accessories for grounding for the tray and/or conduit and the proper accessories according the classification of areas.

10.1.1.2 Conduit cable pathways installation highlights:

a) Complete conduit section must be used when distances allow it, using parts of conduit sections with connectors is not recommended this practice weakens pathways.
b) Conduit ends must be smooth and without any cutting edge.
c) Mechanical supports for conduits must be installed in distances not further than 2 meters from each other and separated 50 cm to a pull box in each conduit connected. Mechanical supports must be conduit manufacturer approved. No cable or wood made supports will be allowed.
d) Conduits will never be supported to existing pipping or other installations elements such as process pipping, HVAC ducts, dropped ceiling fixtures, etc.
e) Conduit hand tool bends, threads and lubricants are considered in conduit installation prices.
f) Non-proper hand tool bends are allowed.
g) Conduits must be clean in the inside to maintain these plastic lids must be installed.

10.1.1.3 Cable pathways must follow parallel or perpendicular routes to walls, columns, beams, pipe racks, etc. For conduits running in parallel routes mechanical supports will be installed every 2 meters when there is no pull box or register.

10.1.1.4 Conduit bend radius chart:

Conduit Diameter	Interior radius
21 mm Ø (3/4”)	160 mm
27 mm Ø (1”)	200 mm
41 mm Ø (1 1/2”)	300 mm
41 mm Ø (1 1/2”)	490 mm

10.1.1.5 Contractor must consider all rigid and intermediate metallic conduit installation’s works and must follow next directions:

10.1.1.6 Type: Rigid and Intermediate metallic conduit.

10.1.1.7 Diameters: 27 and 53 millimeters.

10.1.1.8 Threaded ends.

10.1.1.9 Contractor must consider all accessories, materials, and tools to perform conduit installation.

10.1.2 Cable Tray

10.1.2.1 Cable tray must be used as Access Control System cable pathway.

10.1.2.2 Cable tray will be galvanized steel mesh type, contractor must install factory made cable tray fittings. Handmade fittings are not allowed.

10.1.2.3 Contractor must consider all rigid and intermediate metallic conduit installation’s works and must follow next directions:

10.1.2.4 Type: galvanized steel mesh type.

10.1.2.5 100 millimeters width.

10.1.2.6 Factory made fittings.

11. TELECOMMUNICATION SYSTEMS ACCEPTANCE PROTOCOLS

11.1 The telecommunication’s contractor must provide the Factory Acceptance Test for Access Control system (FAT) 30 days before placing them for review, approval and monitoring during their development. Contractor will present the certificate of FAT tests.

11.2 Site Acceptance Tests (SAT) are contractor’s responsibility to verify the correct equipment operation and interconnection. Test protocol must be delivered 30 days before test to be reviewed and evaluated. The results will show correct equipment function with real field tests in accordance to specification document and manufacturers own specifications.

11.3 System test will be in accordance to equipment manufacturer statements and the results will be indicated in the test protocol.

11.4 Before performing any test, contractor will be sure that all components are complete, identified and properly connected prior to test the entire system.

11.5 All special tools, test equipment, parts and spare parts required to perform these tests will be provided by the contractor.

12. SYSTEM STARTUP

12.1 Once Access Control System is interconnected with Access Control Existing System, Contractor must perform and deliver Operational Site Acceptance Tests (OSAT) to corroborate operational features and functionality of equipment in accordance to this technical specification, equipment operation and maintenance manuals.

12.2 Any fault, damage or prejudice occurred during supply, installation or interconnection of cabling, tests and system startup must be solved by the Contractor in a time frame less than 15 natural days since proper TAKEDA/BAXALTA notification this solution will not be an expense for TAKEDA/BAXALTA.

12.3 If during cable, cable pathways, accessories or material installation Contractor wants to change original proposal in any mean, he must present a complete report with the explanation of the change to be evaluated and approved by TAKEDA/BAXALTA.

12.4 Installation and Startup of Access Control System must be performed in such way they don’t affect existing and operating systems in the TAKEDA/BAXALTA plant.

12.5 Is Contractor’s liability to perform startup and performance tests to Access Control System. Contractor must provide all materials, accessories and installation consumables for startup and final tests of Access Control System.

12.6 Is Contractor’s liability to perform integral performance tests to Telecommunications Systems, presenting operational procedures, equipment’s wiring diagrams, nominal signal levels, monitoring points and adjustment points to be verified and measure, indicating accurate expected values, delivering these results hardcopy and electronic document.

12.7 All infrastructure (FO cables, FO fusion terminations, UTP cables, connectors) shall be certified.

13. SPARE PARTS

13.1 Contractor must elaborate a spare part price chart for maintenance of the Access Control System basing this chart on system knowledge, provided equipment and level of expected repairs.

13.2 Listed spare parts must have manufacturer item number and description. Item number must match part number in the complete system. Spear part price chart must be validated and approved by TAKEDA/BAXALTA.

14. DOCUMENTATION

14.1 Technical documentation must be in English and Portuguese.

14.2 Contractor must deliver to TAKEDA/BAXALTA a work schedule program including: supply, reception, installation and startup of Voice and Data system's equipment and accessories including concept and location, including the next listed minimum documentation in the indicated phases:

14.3 Contractor must deliver next electronic documents within the technical proposal:

a) System Architecture Network Diagram
b) System Topology
c) System functional description
d) Software and hardware system elements data sheets
e) Detailed bill of materials
f) Startup and 2-year maintenance spare parts schedule

14.4 Contractor must deliver next electronic documents (PDF and Source file) for approval after the order is placed:

a) Hardware and Software data sheets
b) System Topology
c) Detailed bill of materials including all equipment, accessories and materials
d) Startup and 2-year maintenance spare parts schedule
e) Quality certification manufacturer issued
f) Acceptance tests protocols
g) Inspection arrangement and tests
h) Quality control arrangement

14.5 Contractor must deliver next electronic (PDF and Source file) and hard copy documents for final and reception:

a) Hardware and Software data sheets
b) Bill of materials
c) Installation details
d) Quality certification manufacturer issued
e) Acceptance tests protocols
f) Startup and 2 year maintenance spare parts schedule
g) Electrical calculations report
h) Wiring diagrams and equipment location drawings
i) Heat dissipation calculation report
j) Installation and maintenance manuals
k) Photographic report including installation, interconnection, tests and startup.
l) Equipment and documents inventory the certificate of FAT tests.
m) Installation, interconnection, tests, startup, and quality control procedures
n) Installation applied regulations
o) Guaranty procedure (telephone number and direction of technical support responsible)
p) Red lines drawings
q) As-built drawings

14.6 Contractor must deliver electronical documentation in the next software latest:

a) Auto CAD 2019
b) Microsoft Office Word and Excel 2019 or last version
c) PDF for manuals, catalogs, etc.
d) Revit 2019 or last version

15. WARRANTIES

15.1 Contractor must deliver operational and maintenance manuals, licenses, passwords, programming keys, warranties, assistance time frames, homologation certifications and manufacturer certified documents of all equipment, components, hardware, software, cables and third party equipment of the Access Control System. All documents hardcopy and electronical will be incorporated to Access Control System's project book one construction and reception phases are completed and approved by TAKEDA/BAXALTA.

15.2 Contractor must guarantee equipment is fault free in materials and workforce installation in accordance to type and quality mentioned in this technical specification.

15.3 Access Control System's equipment warranty time is no less than 18 months since startup and acceptance of Access Control System.

15.4 Any fault or malfunction of the Access Control System during warranty time is Contractor's liability. Is Contractor's obligation to repair, correct, change, or substitute elements, materials, or even complete equipment until achieving complete Access Control System functionality with no cost to TAKEDA/BAXALTA.

15.5 Contractor must present a comply warranty proposal considering fast response times.

16. TRAINING

16.1 Training courses for the personnel must be included, so they can achieve the correct and safe operation and management of the system.

16.2 The courses shall include didactic materials and the required reference manuals in Portuguese.

16.3 Courses for Operators, for Operation Engineers and for Maintenance Engineers must be implemented.

16.4 The courses shall cover the following areas:

a) Operation.
b) Maintenance.
c) Configuration.
d) Administration.

16.5 Contend and duration of the courses must be sent to the client for approval.

16.6 Place will be designated by the client, 10 persons per course must be at least considered.

17. VENDOR SERVICES

17.1 Vendor system shall present a proposal including installation, configuration, programming, testing, commissioning, repair and service to the entire system, and must also include training services for operation and maintenance personnel.

17.2 Any detail omitted in this document does not relieve the vendor of his obligation to provide a complete system operating satisfactorily.

17.3 The contractor is responsible to complete pending work.

18. MAINTENANCE REQUIREMENTS

18.1 Maintenance of the equipment and devices mentioned in the above topics will be an important procedure to increase their useful life. Planning the right time for maintenance can reduce the cost and avoid equipment downtime.

18.2 The Access Control System should be able to receive any type of maintenance that needs to be done, so that parts can be replaced in a modular way and quickly, requiring a team previously trained, with training in electronics and specific training for this type of service and product.

18.3 The system should also be easy to connect to measuring and testing devices to check and indicate defects instantly. All devices to be used must contain technical manuals easily found on the Databook and/or web site of the manufacturer.