VANDERBILT

# Integrated Security Systems

# SPC53xx Application & Engineering Specification

For large systems with up to 128 inputs / outputs and 16 doors

A6V10334451
11.05.2015

Vanderbilt International

~~Confidential~~

# Copyright

Technical specifications and availability subject to change without notice.



Edition: 11.05.2015

# Table of contents

# 1 General Intent

The following document is designed to specify the minimum criteria for the Design, Supply, Installation, and Commissioning & Maintenance of an Intrusion System or Integrated Security System. It is written using industry standard formatting and language and is intended for use by architects, consultants, and specifying engineers, who are preparing bid specifications for Intruder / Access security systems.

The text within this document may be copied into the appropriate sections of a bid specification by using the “cut and paste” method.

# 2 General Tender Requirements

**a** The tenderer shall include the design, cost, supply and commissioning of a complete intrusion/access control and alarm point monitoring system, compliant with the technical and performance criteria set out in this document.

**b** The tenderer shall supply a complete and functionally working system that includes all control equipment, hardware and software, cabling and ancillary services. The tenderer will be familiar with all matters related to the system, its requirements and installation.

**c** If the tenderer does not understand any requirement then clarification should be asked for by contacting:
<insert a contact name and telephone number>.

**d** After the tender has been awarded there shall be no price variation without prior agreement.

**e** A complete clause-by-clause compliance response is required.

**f** Any equipment tendered shall be from a manufacturer who has an established presence within the EC market place. The equipment manufacturer shall be accredited with EN ISO 9001.

g All technical and operational documentation for the intrusion/access control system should be supplied in Adobe Acrobat PDF format on a CD at the time of purchase.

h The tenderer shall submit their tender at <insert where tender shall be sent or handed to> by <insert time and date of closing>.

# 3 Document Scope

The scope of this document will be aimed at the main components of an Integrated Security System.

The Integrated Security Systems shall comprise of the following items:

- Intrusion Detection / Access control system
- Wireless devices
- Bus Input Expanders
- Bus Output Expanders
- Bus PSU Expanders
- Bus Access Control
- Bus Keypads
- Communications

# 4 System Usage

The Integrated Intrusion / Access security System as outlined in the tender document shall be used to secure the facility using intrusion detection methods pertaining to the country of operation’s standards. The system shall also be able to control the flow of authorized personnel and where specified vehicular traffic through the secured access area of the facility.

# 5 Abbreviations

| | | |
|---|---|---|
| **BUS** | | Data bus for system expansion allowing a distributed system |
| **I/O** | | **I**nput/**O**utput |
| **AS** | | **A**pplication **S**oftware |
| **OS** | | **O**perating **S**ystem |
| **ARC/CMS** | | **A**larm **R**eceiving **C**entre/**C**entral **M**onitoring **S**tation |
| **SMS** | | **S**hort **M**essage **S**ervice - Text notification |
| **PSTN** | | **P**ublic **S**witched **T**elephone **N**etwork - Phone line connection |
| **GSM** | | **G**lobal **S**ystem for **M**obile Communications - Cellular Connection |
| **GPRS** | | **G**eneral **P**acket **R**adio **S**ervice – Mobile data communication standard |
| **EOL** | | **E**nd **O**f **L**ine – Resistors added at the end of the detection circuit to allow monitoring of that circuit for a range of conditions. |
| **GUI** | | **G**raphical **U**ser **I**nterface |

*Abbreviations*

# 6 Definitions

| | | |
|---|---|---|
| **Hybrid Alarm System** | | System that supports hardwired detection and wireless detection. |
| **Wireless Access Point** | | A wireless access point is an interface that allows wireless devices to be added to the system and the system can process the signals from the wireless devices the same as they were wired devices. |
| **Tri-Colour** | | Tri-Colour LEDs can display Red / Green or Amber depending upon the programming. |
| **Standards / Approval** | | The product has been tested by an independent notified body to the specified standards. |

# 7 Quality

## 7.1 Manufacturer

Manufacturer: Minimum ten years' experience in manufacturing and maintaining similar systems. Alarm manufacturer shall be certified compliant with ISO 9001.

# 8 Intruder Systems – General

The Controller shall be capable of storing 10000 Intruder Events in its internal log, these events shall be accessible via the web server.
The controller shall support 64 calendars with a minimum of 3 different week types; each week type has 4 different on & off periods per day. The calendar can be used to enable/disable users, keypads, outputs, doors.
It shall be possible to create specific function with Cause & Effects programming via triggers and mapping gates. Status changes of areas, users, outputs, doors, etc. can be used as trigger. Several triggers can be combined in a mapping gate to be activated when all trigger conditions become true.
The system shall cope with daylight saving times automatically.
All system field expanders can be automatically addressed by the controller to prevent double addresses occurring on the system or manually set. The system software must detect double addresses if they occur.
It shall be possible to locally or remotely upgrade the firmware of controller and expanders.
The intruder inputs on the controller and any field expanders connected to the controller shall have the ability to analyse the input for gross attack and pulse count. The system shall also be able to vary the pulse count and gross attack settings on an input-by-input basis.
A wide variety of input types shall be available and for each input type a number of attributes should be configurable. Such as Chime, 24HR, Log, Inhibit, Normally open etc.
A general input type will be provided which can be used to monitor external equipment without intrusion functionality. This general type will support reporting and audible indications. It shall be possible to assign reporting codes to report specific events representing the equipment being monitored, water alarms, pressure alarms etc….

Alarm Relay Outputs shall be rated at 30V DC and 1A (resistive switching current), electronic outputs shall be rated at 12V DC and 400mA (resistive switching current)
The Controller and external Power Supplies shall be able to self-test the batteries to ensure that they are healthy on a regular basis.
Self-test for the detection of faults on the system shall occur when an Engineer exits from configuration mode.
The Controller shall support multiple languages a minimum of 4 different languages should be supported. When a language is selected, it shall change the language of all system keypads and all engineering and user menus on the system keypads and associated engineering tools (Web Servers etc.) to the language selected.
Engineering tools shall have the ability to read/configure the panel in one language whilst the panel and its system keypads are in a different language.

The controller shall support pluggable modules that allow additional communication paths in addition to the on-board IP facility if required. The system shall be configurable so that the most appropriate communication path can be determined as the primary communication path and then additional communication options used as secondary and tertiary paths.
Additional Pluggable PSTN modem(s) shall support V23/V90, Central station protocols (Contact ID, SIA, and Fast Format). PSTN modem must be capable of taking control of the PSTN line in an alarm situation and monitor the line for faults in Set / Unset operation. The modem shall support a minimum 56K speeds.
Additional pluggable GSM modem(s) shall support SMS for Event notification, SMS control and Central station protocols (Contact ID, SIA, Fast Format) and IP transmission over GPRS.
The controller should be able to send all alarms to the ARC/CMS via IP, PSTN or GSM modems. It must also be possible for the controller to send its alarms to multiple monitoring stations.
It must also be possible for the controller to send its alarms to multiple End users via SMS for Text notification.
The system will offer the ability to change event codes to individual receivers. The system will support the selection of events to be sent to individual receivers.

# 8.1Controller

The Controller shall have a minimum of 8 on board wired Inputs and 6 fully programmable outputs. The system shall be expandable up to 128 wired inputs and 128 outputs by the use field expansion devices, Combination of wired / wireless inputs shall be possible.
The controller shall employ a high-speed expansion bus (BUS) that can be configured as in Loop and Spur topology. When the expansion bus is configured as a Loop topology a single or dual cable fault between the same two-expansion devices (short or open of data bus) shall allow all the system to remain fully operational with no loss of functionality (with cable faults reported). If additional cable faults were to occur then only the field expansion devices that do not have a connection to the controller shall be lost.
The controller shall provide an integrated Ethernet port to allow more than 10 parallel IP communications with connected applications such as Programming Software, Alarm Receiving Centres (CMS / ARC), Web Browsers, Danger Management Systems (DMS), 3rd party products, etc.
The controller shall provide an integrated Web server for system programming and operation. The Web server shall be accessible from any remote computer system running a web browser that can gain access to the panel through a LAN or WAN, serial, USB or modem. To allow access remotely, the communication shall be using a Secure Socket Layer (SLL), providing the user with the ability to login in using the same credentials (or separate web authentication credentials) and user rights for operation as if they were standing at the panel.

## 8.2Hybrid systems

The System shall be expandable with several wireless access points to become a true hybrid alarm system. Therefore a combination of wired / wireless inputs (120 wireless inputs maximum) shall be possible. The wireless devices shall be addressed in the controller to allow multi-path reception from several wireless access points. The wireless access points shall use the European standard wireless frequency 868MHz, to providing greater security from interference and jamming.

## 8.3Grading

The system grade required is determined by the risk analysis of the site to be protected and all the equipment must meet the minimum grade for that risk. If the risk is determined to be a Grade 2 system then all components of the system must be Grade 2 or above.
The enclosures of panel and external power supplies shall have sufficient space to house the standby battery with sufficient capacity to support the controller, plug in modules and the connected field devices (system keypads / field expanders etc.) for the required hold-up time as defined by the standard.

The system shall enable the engineer, configuring the system, to easily choose the required grade from a list of templates already pre-configured and conforming to the relevant grade.

## Controller Technical Requirements

| | | |
|---|---|---|
| Programmable areas | | 16 |
| Number of user codes | | 500 |
| Event memory | | 10'000 intrusion events, 10'000 access events |
| Max. number of hardwired zones | | 128 |
| Max. number of wireless zones | | 120 (take away wired zones) |
| EOL resistor | | Dual 4k7 (default), other resistor combinations configurable |
| Number of on-board relays | | 1 strobe (30 VDC / 1 A resistive switching current) |
| Number of on-board open coll. | | 2 internal / external bell, 3 freely programmable (each max. 400 mA resistive switching current, supplied via auxiliary output) |
| Door Capacity | | Max. 16 entry doors Reader in only or 8 entry/exit doors or a combination of doors Reader in Reader in/out not exceeding 16 readers. |
| Time function | | 64 calendars (53 weeks, multiple on/off switching patterns for users, areas, inputs, outputs, keypads, doors) |
| Macro language | | Cause & Effect programming (1024 triggers / 512 mapping gates) |
| Number of field devices | | Max. 128 (32 keypads, 32 door-expanders, 64 input/output expanders) |
| Interfaces | | 2 X-BUS (2 spurs or 1 loop),<br>2 RS232 (for X-10 or external communication),<br>1 USB (PC connection),<br>1 SPC Fast Programmer,<br>1 Ethernet (RJ45) |
| Field bus | | X-BUS on RS-485 (307 kb/s) High Speed |
| Tamper contact | | Front spring tamper, 2 auxiliary tamper contact inputs |
| Output voltage | | 11-14 VDC in normal conditions (mains powered and fully charged battery) |
| Auxiliary power (nominal) | | Max. 1500 mA at 12 VDC (750 mA per output) |
| Operating temperature | | 0 ~ +40 °C |
| Standards / approval compliance | | EN50131-1, Grade 3, class II<br>SE: SFF1014, Larmklass 2<br>NL: REQ, Grade 3, class 2<br>HU: MABISZ<br>CZ: TESTALARM, TREZORTEST,NBU INCERT<br>NF: a2p |

Note for EN compliance the current supplied by the PSU to ancillary equipment needs to be supported by the battery for the required standby time.

# 8.4BUS Configurations (Installation)

## Loop Configuration

The Loop (or ring), cabling method offers the highest security by providing fault tolerant communications on the BUS. All system Keypads and field expanders are supervised and in case of a cable fault or break, the system continues to operate and all input circuits are monitored.

## Spur Configuration

The spur (or chain or open loop) cabling method offers a high level of fault tolerance and may be more convenient on certain installations. The controller shall support two spurs. In the case of a cable fault or break, all Expanders and detectors up to the fault will continue to be supervised

## Cables, distances and shielding

For normal installations a range of different common industry cables shall be able to be used (standard 4/6 core alarm cable (non shielded) / cat 5 / Belden etc.). Shielded cables should be used for sites with high electric field interference, e.g. Belden 9829, IYSTY 2 x 2 x 0.6 (min).

The system shall be able to support a minimum of 200m between each field expander irrespective of the cable type used. The system shall be able to extend this distance up to 400m between field expanders when Cat 5 / Belden 9829 / IYSTY 2 x 2 x 0.6 (min) cable is used in Loop and Spur cabling configuration.

# 8.5System Keypads

The system Keypad(s) shall be remote from the controller and the system shall be capable of allowing up to 32 Keypads on each controller. The Keypad shall be configurable per User & per Area/Multiple Areas, allowing each User to see only the menu options or events that apply to that User/Area.

A range of systems keypads shall be available with options for optional display and control features.

The standard keypad range shall support the following features;

- LCD display with 2 x lines of 16 characters to show all alert and warning messages with alphanumeric Keys to allow for both text and numeric data entry.
- Soft function keys that can change function depending upon the menu selected.
- The user shall be able to (Depending on user rights) System Set – Unset, Part A/B Set –Unset, Area Set –Unset.
- The illumination shall be programmable to allow one of three states (Always on, always off or by Key press).
- When multiple Keypads are used, the option to be able to silence the on board buzzer for quiet environments shall be capable of being deployed.
- Integral EM proximity reader for keypad logon resp. setting / unsetting (PACE)
- Local Wireless Access Point to support local wireless devices.

The enhanced keypad range shall have the following features;

- Graphical LCD display with 128 x 64 dots providing space for alert and warning messages with alphanumeric Keys to allow for both text and numeric data entry.
- Soft function keys (minimum of four) that can change function depending upon the mode of the system.
- The user shall be able to (Depending on user rights) System Set – Unset, Part A/B Set –Unset, Area Set –Unset.
- The illumination shall be programmable to allow one of three states (Always on, always off or by Keypress).
- When multiple Keypads are used, the option to be able to silence the on board buzzer for quiet environments shall be capable of being deployed.
- Integral EM proximity reader for keypad logon resp. setting / unsetting
- Integral speaker to provide voice annunciation
- Capable of displaying the installers logo
- Capable of showing the status of four Areas / Partitions at any one time.
- Support for locally attached key-switch and indication modules

The status of each Keypad on the system shall be viewable and this shall include;

- Tamper status
- Firmware Version
- Input Voltage
- Address ID
- Capability to disable keypads based on various conditions

# 8.6Keypad Technical Requirements

## Standard Keypad

| | | |
|---|---|---|
| LCD-display | | 2 x 16 characters |
| Special keys | | 2 soft keys, 1 multi-dimensional navigation key |
| LED indicators | | 3 status LEDs |
| Card reader | | Integrated (125kHz, EM 4102) |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front / back spring tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | 5 ~ +40 °C |
| Standards / approval compliance | | EN50131-1, Grade 3, class II<br>SE: SFF1014, Larmklass 2<br>HU: MABISZ<br>CZ: TESTALARM, TREZORTEST,NBU |

### Compact Keypad Table

### Enhanced keypad:

| | | |
|---|---|---|
| LCD-display | | 128 x 64 pixels (approx. 6 x 20 characters) |
| Special keys | | 4 soft keys, 1 multi-dimensional navigation key |
| LED indicators | | 5 status LEDs |
| Card reader | | Integrated (125kHz, EM 4102) |
| Audio | | Supported via integrated speaker and microphone |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front / back tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | 5 ~ +40 °C |

### Compact keypad:

| | | |
|---|---|---|
| Depth | | 17.5mm |
| Keys | | Touch key technology |
| LCD-display | | 128 x 64 pixels (approx. 6 x 20 characters) |
| Special keys | | 4 soft keys, 1 multi-dimensional navigation key |
| LED indicators | | 5 status LEDs |
| Card reader | | Integrated (125kHz, EM 4102), Mifare |
| Audio | | Supported via integrated speaker and microphone |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front / back tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | 5 ~ +40 °C |
| Wireless | | Receiver option available |

# 8.7System Indicator module

The system indicator module(s) shall be remote from the controller and shall be individually configurable including LEDs and buttons

The indicator module shall have the following features;

- 16 Tri-Colour LED(s) that are fully programmable to represent system events. The LEDs shall be programmable for different flash rates (Slow / Medium / Fast) or constant.
- 4 function keys should be fully programmable to activate outputs, set areas etc.
- Can be operated in a “linked” mode with a keypad so that the LEDs and switches are automatically assigned to system areas / Partitions. In a linked mode each function key corresponds to an area i.e. Set / Unset and the LEDs will then reflect the status of the area (Alarm / Fault / Status (Set / Unset / Partset) / Info.
- Internal Buzzer as audible notification
- Installed on the system expansion bus (BUS)
- Support a hardwired input that is fully programmable as any other system input
- EM Proximity reader to enable / disable the Input switches

# 8.8Indicator module Technical Requirements

| | | |
|---|---|---|
| Number of on-board zones | | 1 |
| EOL resistor | | Dual 4k7 (default), other resistor combinations configurable |
| Special keys | | 4 function keys, freely programmable |
| LED indicators | | 16 tri-colour LEDs |
| Card reader | | Integrated (125kHz, EM 4102) |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front / back tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | -10 ~ +50 °C |

# 8.9System key-switch module

The system key switch module(s) shall be remote from the controller and the system shall be configurable.

The key switch module shall have the following features;

- 2 Tri-colour LED(s) that are fully programmable to system / key switch events. The LEDs shall also be programmed for flash rate (Slow / Medium / Fast) or constant.
- Key switch that can have three positions with key only removable in one position
- Can be simply linked to a keypad to minimise programming.
- Internal Buzzer as audible notification
- Installed on the system expansion bus (BUS)
- System Output in the form of a Volt Free output rated at 30V 1A (resistive switching current)

# 8.10 Key-switch module Technical Requirements

| | | |
|---|---|---|
| Programmable key input | | 3 key positions (2-0-1 in 90° steps, cylinder type KABA1008C) |
| Number of on-board relays | | 1 (single-pole changeover, 30 VDC / max. 1 A resistive switching current) |
| LED indicators | | 2 tri-colour LEDs |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front / back tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | -10 ~ +50 °C |

# 8.11 Input / Output Expansion

The I/O Expander shall enable 8 additional Alarm Inputs and 2 relay outputs (30V / 1A) to be added onto the BUS. The input types and the outputs shall be fully programmable. The PCB shall have an on-board buzzer, status LED; tamper switch and thermal fuse to protect auxiliary devices. Power to the I/O Expander shall be provided via the BUS cable from the controller or by locally based intelligent power supply units.
The PCB shall be housed in a robust plastic enclosure.
The Alarm Inputs shall be capable of supporting a range of EOL resistor values to be able to take into account 3rd party legacy systems.
The Expanders may also be installed in the controller enclosure. This enclosure shall accommodate the standby battery, controller and I/O Expander(s).

# 8.12 Input / Output Expander Technical Requirements

| | | |
|---|---|---|
| Number of on-board zones | | 8 |
| EOL resistor | | Dual 4k7 (default), other resistor combinations configurable |
| Number of on-board relays | | 2 (single-pole changeover, 30 VDC / max. 1 A resistive switching current) |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front spring tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | -10 ~ +50 °C |
| Standards / approval | | EN50131-1, Grade 3, class II |

# 8.13Output Expansion

The Output Expander shall enable 8 additional relay Outputs (30V / 1A) to be added onto the BUS. The outputs shall be fully programmable. The PCB shall have an on-board buzzer, status LED; tamper switch and thermal fuse to protect auxiliary devices. Power to the Output Expander shall be provided via the BUS cable from the controller or by locally based intelligent power supply units. The PCB shall be housed in a robust plastic enclosure.The Expanders may also be installed in the controller enclosure. This enclosure shall accommodate the standby battery, controller and Output Expander(s).

# 8.14Output Expander Technical Requirements

| | | |
|---|---|---|
| Number of on-board relays | | 8 (single-pole changeover, 30 VDC / max. 1 A resistive switching current) |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front spring tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | -10 ~ +50 °C |
| Standards / approval | | EN50131-1, Grade 3, class II<br>HU: MABISZ<br>CZ: TESTALARM, TREZORTEST,NBU |

# 8.15Wireless Expansion

The Wireless Expander shall enable additional wireless devices to be added onto the BUS. The Wireless Expander acts as wireless access point and provides range extension and the possibility of multipath reception for wireless devices. The PCB shall have an on-board buzzer, status LED and tamper switch and thermal fuse to protect auxiliary devices. Power to the Wireless Expander shall be provided via the BUS cable from the controller or by locally based intelligent power supply units. The PCB shall be housed in a robust plastic enclosure.

NOTE: Wireless expanders should not be mounted in any controller or Smart PSU enclosures due to signal strength issues.

# 8.16Wireless Expander Technical Requirements

| | | |
|---|---|---|
| Radio module | | Integrated SiWay RF receiver (868 MHz) |

| | | |
|---|---|---|
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front spring tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Radio module | | -10 ~ +50 °C |

# 8.17PSU Expander

The BUS PSU Expander shall be able to supply battery backed 12V supply as well as supporting 8 additional Alarm Inputs and 2 relay outputs (30V / 1A) to be added onto the BUS. The power supply shall have independently and fused power outputs with a total of 2.6 A for auxiliary devices, battery management and built in Input/Output Expander. The input types and the outputs shall be fully programmable. The PCB shall have an on-board buzzer, status LED, tamper switch and thermal fuse to protect auxiliary devices. The BUS PSU Expander shall monitor all its conditions and report these back across the BUS to the attached controller. The PSU Expander housing shall be capable of adding additional Expanders (up to 4 in total) as well as a 17A/H battery.

# 8.18 BUS PSU Expander Technical Requirements

| | | |
|---|---|---|
| Number of on-board zones | | 8 |
| EOL resistor | | Dual 4k7 (default), other resistor combinations configurable |
| Number of on-board relays | | 2 (single-pole changeover, 30 VDC / max. 1 A resistive switching current) |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front spring tamper, back tamper |
| Output voltage | | 11-14 VDC in normal conditions (mains powered and fully charged battery) |
| Auxiliary power (nominal) | | Max. 1500 mA at 12 VDC (750 mA per output) |
| Operating temperature | | 0 ~ +40 °C |
| Standards / approval | | EN50131-1, Grade 3, class II<br>SE: SFF1014, Larmklass 2<br>HU: MABISZ<br>CZ: TESTALARM, TREZORTEST,NBU |

Note for EN compliance the current supplied by the PSU to ancillary equipment needs to be supported by the battery for the required standby time.

# 9 System Control

## 9.1 Area control advanced

System will provide ability to control interlock areas and to control areas based on the input from logical states of various elements, such as

System shall provide the ability to rearm an area after a given period.
System shall provide ability to delay the disarming of an area for a given period.
System shall provide ability to block arming/disarm based on a schedule.
System shall provide ability to a two stage arming process.
System shall provide ability to require two separate pins in order to arm/disarm area.
System shall provide an additional conditional acknowledge of safe disarm from user when system is disarmed, should this condition not be meet the system shall raise an alert condition.
System shall provide ability to block setting from keypad devices.
System shall provide ability to define an exit route for doors in the event of a fire condition.

# 10 User Control

## 10.1 Users via Keypad

Users shall be able to control the system via any system keypad that they have been programmed to have access to.

## 10.2 Users via Web Browser

It should also be possible to control the system via a standard web browser, hence providing the user with a GUI that can be accessed over IP from a computer running any operating system or from a mobile device supporting web access.
The events that the User can see / control shall be configurable are shown below;

- Area status with setting options
- Zone status with bypass options
- Door status with control options
- System alerts and restore options
- Create / delete and modify users
- View Verification data
- Log files for Intruder events
- Log files for Access events
- Test outputs
- SMS settings for this user
- View image from cameras
- Control of auto arming

## 10.3User Control

The system shall be able to be tailored for each user (User rights). This allows the system to be personalised based upon the system requirements rather than each user being fixed to a pre-configured profile that can give some users too much rights and insufficient rights for others. When User rights are set they shall be universally applied irrespective of how the user is interacting with the system. User rights will be defined using a profile system which can be applied to multiple users. User's rights will be configurable so that users may different rights across system based on location and/or time.

The User rights that shall be configurable are shown below;

- Unset of areas
- Partset A of areas
- Partset B of areas
- Fullset of areas
- Force set of areas
- Delay Auto set
- Restore alarms
- Inhibit zones
- Isolate zones
- View log file
- Enable / Disable Chime
- Edit calendars configuration
- Grant Engineer Access
- Grant manufacturer Access
- Change own code
- Configure SMS messages
- Set date Set
- Bell test
- Walk test
- Configure other users
- Activate / deactivate X-10 devices
- Lock / unlock doors
- Web Access to panel web server
- Edit Door configuration

## 10.4Users Accessibility

The system shall support users being able to be added for a specific period i.e. contractors working on a premise where their user codes will only work between pre-determined dates. The system shall also support calendar functionality where a user can only access the system on the days and time period that has been pre-set during tailoring the system to the site needs. The calendar shall provide a minimum of three different week types and these shall be able to be allocated to each user as appropriate.

## 10.5Users Reporting - SMS

The system shall support users being able to be informed of the status of the system by SMS. Each user shall be allowed up to 5 Mobile Numbers for the SMS messages to be sent, the messages sent to each mobile shall be independently tailored for that mobile user.

The SMS messages that could be sent to the User shall be configurable are shown below:

- Alarms
- Alarm Restore
- Confirmed Alarms
- Faults
- Fault Restore
- Setting of Areas
- Inhibits
- Doors
- Others

## 10.6Users Control - SMS

The system shall support users being able to control the system by SMS. Each mobile user shall be capable of controlling the system if authorised (the system shall only allow SMS control from mobile numbers already programmed within the system), the control each user has to remotely control the system by SMS shall be independently tailored for each mobile user.

The SMS control options available should include;

- Full Set areas
- Unset areas
- Partset A areas
- Partset B areas
- Clear Alerts
- Request System Status
- Request Event Log
- Allow Engineer Access
- Allow Manufacturer Access
- Control Outputs

# 11 Access Control

The system shall incorporate the necessary hardware, software, and firmware to collect, transmit, and process alarms, tamper and trouble conditions, access requests, and advisories in accordance with the security procedures configured. The system shall control the flow of authorised personnel traffic through the secured areas of a facility.
The system shall be modular in nature, and shall permit expansion of both capacity and functionality through the addition of Access Expanders and associated hardware. The system shall have the capability to handle up to 16 doors and 500 card holders. The system shall incorporate the necessary hardware, software, and firmware to collect, transmit, and

process alarms, tamper and trouble conditions, access requests, and advisories in accordance with the security procedures configured. The system shall control the flow of authorised personnel traffic through the secured areas of a facility.

# 11.1Access Expansion

The Access Expander shall support 2 reader ports, 4 Inputs, 2 relay outputs (30V / 1A) to be added onto the BUS. The input types and the outputs shall be fully programmable The PCB shall have an on-board buzzer, status LED and tamper switch. Power to the Access Expander shall be provided via the BUS cable from the controller or by locally based intelligent power supply units.

The Access Expanders may also be installed in the BUS PSU enclosure, replacing the standard I/O expander.

# 11.2Access Expander Technical Requirements

| | | |
|---|---|---|
| Memory | | Standalone capacity for up to 512 priority card holders. |
| Number of on-board zones | | 4, for door release switch (DRS) and door position switch (DPS), or freely programmable |
| EOL resistor | | Dual 4k7 (default), other resistor combinations configurable |
| Number of on-board relays | | 2, for door locks or freely programmable (single-pole changeover, 30 VDC / max. 1 A resistive switching current) |
| LED indicators | | 4 outputs (1 void and 1 valid per reader) |
| Number of card reader | | 2 |
| Card readers protocols accepted | | Wiegand 26 bit (standard), Wiegand 36 bit (proprietary), Cotag,<br>Wiegand 37 bit<br>IClass Mifare<br>IClass Desfire<br>EM4102<br>Clock&Data (proprietary) |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front spring tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | -10 ~ +50 °C |

# 11.3Access Configuration

The system's Access Door functionality shall have the capability to be configured via the system keypad / PC configuration program or a web browser.

The system shall monitor all doors for door open and closed states and also for when the door has been forced open without a valid card read.

An operator shall be able to perform the following actions on a door from the keypad or the web server and these actions must be logged:

- Unlock
- Lock
- Momentary (same as operating the Push to Exist switch)
- Normal Operation

The system shall allow the configuration of the doors on the Access Control System such that;

Each door shall open with the use of a proximity card or fob and it shall also be possible to configure the door so that a PIN code has to be used in conjunction with the card. The option to configure an exit door with either an egress switch or Pinpad where a PIN code is required to exit. PIN code and length shall be the same as used for the intrusion keypad.

Each door shall be able to be configured to go in to "Door locked" or "Door unlocked" based on the doors calendar schedule.

Where visitors are allowed on site it shall be possible to configure door(s) so that they have to be escorted through the door to gain entry.

Where a facility uses a custodian it shall be possible to configure door(s) such that the custodian card holder is the first one to gain entry and cannot leave the building via the exit door until all other card holders have left the building. This shall also be able to be configured for a room or section of building.

It shall be possible for each door to have its own door timings in respect to the following values:

- Door unlock time after a valid read
- Additional time added to unlock time after a valid read for individual card holders (e.g. for disabled people)
- Reader denied time after an invalid read
- How long a door can be open before a "Door Held Open" message is displayed

# 11.4Card Profiles

It shall be possible to have cards in a valid or void state; it must also be possible to define cards with a start and expiry date. It shall be possible that a card/fob will be able to be designated with one or more of the following types:

### Card void:

- Select to temporarily disable this card.

### Extended time:

- Select to extend door timers when this card is presented.

### PIN bypass:

- this card can access the door without pin entry for a door configured with a pin pad

### Priority:

- Priority cards will give access when doors are offline.

### Escort:

- Card set with this attribute may allow other cards through doors requiring Escort.

### Custodian:

- The custodian shall be the first person to enter the area and the last person to leave.

# 11.5Door Attributes

Each door on the system shall be able to have the following attributes assigned:

- Card and PIN

  Select if both card and PIN is required to gain entry. If this is disabled, cardholders can open the door with PIN only.
- PIN Only

  Select if only a PIN code is required. No card will be accepted.
- PIN to Exit:

  Select if a PIN is required on Exit reader. A door with entry and exit reader is needed.
- PIN to Set/Unset:

  Select if a PIN code is required to Unset / Fullset.
- Unset Outside:

  Panel/Area will UNSET when card, PIN, or PIN and Card, depending on the configuration, is presented at entry reader.
- Unset Inside:

  Panel/Area will UNSET when card, PIN, or PIN and Card, depending on the configuration, is presented at exit reader.
- Fullset Outside:

  Panel/Area will FULLSET when card, PIN, or PIN and Card, depending on the configuration, is presented twice at entry reader.
- Fullset Inside:

  Panel/Area will FULLSET when card, PIN, or PIN and Card, depending on the configuration, is presented twice at exit reader
- Emergency:

  Select if door lock should open within the area if a fire alarm is detected.
- Emergency Any:

  Select if door lock should open within any area if a fire alarm is detected.
- Escort:

  The escort feature enforces privileged card-holders to escort other card-holders through specific doors. If this feature is enabled on a door then a card with escort privilege must be granted access before other cards will be allowed access. Each door has a configurable timer that defines the time period where after other cards will be granted access.

  Note: You cannot assign both Escort and Custodian simultaneously on a Door Group as both the escort and custodian card-holders must be last to exit. If this was possible, neither would be able exit the door group.
- Custodian:

  The custodian feature enforces a cardholder with custodian privilege to always be inside a door group when other cardholders are inside. A door with two card readers for Entry/Exit is needed for this option. The custodian must be the first to enter. No other cards will be granted access until the custodian has entered. Custodian will not be allowed to exit until all non-custodian cards have exited. Escort and Custodian cannot be both assigned simultaneously on a Door Group as both the escort and custodian cardholders must be last to exit. If you do this neither cardholder would be able to exit the door group.

  It shall also be possible to configure two different types of anti-passback as follows:

- Interlock
- Only one door in a door group with 'Interlock' will be allowed to be open at a time. These doors shall have the ability to be grouped. Setting Prefix

  The system shall support the ability to activate a setting mode, which if not enable shall prevent accidental arming of the system
- Anti-Passback:
  - Prevent Passback:

    A door with two card readers for Entry/Exit is needed for this option. The door must also be assigned to a door group, the cardholder is only allowed to present the card / fob at the entry reader once. The cardholder is not allowed to present the same card again on the entry reader until the card /fob is presented to the exit reader first. This then allows the cardholder to present the card at the entry reader.
  - Soft Passback:

    If Anti-passback violations shall only be logged but not prevented. A door with two card readers is needed for this option and the door must be assigned to a door group.

## 11.6Intrusion & Access Control Interoperability

Intrusion system will override Access Settings and prevent access if the Card holder does not have the Intrusion rights to unset the system if it is set. The system shall provide the means to indicate temporarily the intrusion Area/System has been set by means of a warning device being triggered for a period of time – visual warning is switched on for a determined period. The Card/Fob shall be EM4102 standard to both the Intrusion and the Access Control systems – the user need only carry one credential. Logging of events – Door Alarms should be recorded in both the Intrusion Log and Access Control Log.

# 12 Access Control Integrated System

The integrated controller in conjunction with Access Expander(s) distributed on the system BUS will process and manage the Entry / Exit transactions through each of the access controlled points, which may be doors (with electromagnetic locks) or other forms of pedestrian / vehicle barriers. The Controller and Access Expanders will make all the access control decisions without the involvement of a host computer. The Controller shall be capable of storing 10000 Access Control Events in its internal log; these events shall be accessible via the web server. Each Access Expander shall support 2 access card readers providing either 2 doors of access control each with a request to exit switch or a single door with access card readers on both sides (read in / read out). Each Access Expander shall have the capability to operate in a standalone capacity if communication fails the integrated controller. In a standalone capacity, all card holders with the priority attribute shall still have access through all doors on the system. Each Access Expander shall have the capability to support the following Access card formats per user.

- Wiegand 26 Bit
- Wiegand 36 Bit
- HID Corporate 1000
- HID37F
- HID ICLASS DESFIRE
- EM4102
- Cotag
- HID 37
- HID ICLASS MIFARE

## 12.1 Access Expansion

The Access Expander shall support 2 reader ports, 4 Inputs, 2 relay outputs (30V / 1A) to be added onto the BUS. The input types and the outputs shall be fully programmable The PCB shall have an on-board buzzer, status LED and tamper switch. Power to the Access Expander shall be provided via the BUS cable from the controller or by locally based intelligent power supply units. The Access Expanders may also be installed in the BUS PSU enclosure, replacing the standard I/O expander.

## 12.2 Access Expander Technical Requirements

| | |
|---|---|
| Memory | Standalone capacity for up to 512 priority card holders. |

Issued by
**Vanderbilt International GmbH**
Borsigstraße 34
65205 Wiesbaden-Nordenstadt
Germany

| | |
|---|---|
| Number of on-board zones | 4, for door release switch (DRS) and door position switch (DPS), or freely programmable |
| EOL resistor | Dual 4k7 (default), other resistor combinations configurable |
| Number of on-board relays | 2, for door locks or freely programmable (single-pole changeover, 30 VDC / max. 1 A resistive switching current) |
| LED indicators | 4 outputs (1 void and 1 valid per reader) |
| Number of card reader | 2 |
| Card readers protocols accepted | Wiegand 26 bit (standard), Wiegand 36 bit (proprietary), Clock&Data (proprietary) |
| Field bus | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | Front spring tamper |
| Operating voltage | 9.5 ~ 14 VDC |
| Operating temperature | -10 ~ +50 °C |

## 12.3Access Configuration

The system's Access Door functionality shall have the capability to be configured via the system keypad / PC configuration program or a web browser.

The system shall monitor all doors for door open and closed states and also for when the door has been forced open without a valid card read.

An operator shall be able to perform the following actions on a door from the keypad or the web server and these actions must be logged:

- Unlock
- Lock
- Momentary (same as operating the Push to Exist switch)
- Normal Operation

The system shall allow the configuration of the doors on the Access Control System such that;

Each door shall open with the use of a proximity card or fob and it shall also be possible to configure the door so that a PIN code has to be used in conjunction with the card. The option to configure an exit door with either an egress switch or Pin pad where a PIN code is required to exit. PIN code and length shall be the same as used for the intrusion keypad.

Each door shall be able to be configured to go in to "Door locked" or "Door unlocked" based on the doors calendar schedule.

Where visitors are allowed on site it shall be possible to configure door(s) so that they have to be escorted through the door to gain entry.
Where a facility uses a custodian it shall be possible to configure door(s) such that the custodian card holder is the first one to gain entry and cannot leave the building via the exit door until all other card holders have left the building. This shall also be able to be configured for a room or section of building.

It shall be possible for each door to have its own door timings in respect to the following values:

- Door unlock time after a valid read
- Additional time added to unlock time after a valid read for individual card holders (e.g. for disabled people)
- Reader denied time after an invalid read
- How long a door can be open before a “Door Held Open” message is displayed

## 12.4Card Profiles

It shall be possible to have cards in a valid or void state; it must also be possible to define cards with a start and expiry date. It shall be possible that a card/fob will be able to be designated with one or more of the following types:

### Card void:

- Select to temporarily disable this card.

### Extended time:

- Select to extend door timers when this card is presented.

### PIN bypass:

- This card can access the door without pin entry for a door configured with a pin pad

### Priority:

- Priority cards will give access when doors are offline.

### Escort:

- Card set with this attribute may allow other cards through doors requiring Escort.

Issued by
**Vanderbilt International GmbH**
Borsigstraße 34
65205 Wiesbaden-Nordenstadt
Germany

### Custodian:

- The custodian shall be the first person to enter the area and the last person to leave.

## 12.5Door Attributes

Each door on the system shall be able to have the following attributes assigned:

- Card and PIN

  Select if both card and PIN is required to gain entry. If this is disabled, cardholders can open the door with PIN only.
- PIN Only

  Select if only a PIN code is required. No card will be accepted.
- PIN to Exit:

  Select if a PIN is required on Exit reader. A door with entry and exit reader is needed.
- PIN to Set/Unset:

  Select if a PIN code is required to Unset / Fullset.
- Unset Outside:

  Panel/Area will UNSET when card, PIN, or PIN and Card, depending on the configuration, is presented at entry reader.
- Unset Inside:

  Panel/Area will UNSET when card, PIN, or PIN and Card, depending on the configuration, is presented at exit reader.
- Fullset Outside:

  Panel/Area will FULLSET when card, PIN, or PIN and Card, depending on the configuration, is presented twice at entry reader.
- Fullset Inside:

  Panel/Area will FULLSET when card, PIN, or PIN and Card, depending on the configuration, is presented twice at exit reader
- Emergency:

  Select if door lock should open within the area if a fire alarm is detected.
- Emergency Any:

  Select if door lock should open within any area if a fire alarm is detected.
- Escort:

  The escort feature enforces privileged card-holders to escort other card-holders through specific doors. If this feature is enabled on a door then a card with escort privilege must be granted access before other cards will be allowed access. Each door has a configurable timer that defines the time period where after other cards will be granted access.

  Note: You cannot assign both Escort and Custodian simultaneously on a Door Group as both the escort and custodian card-holders must be last to exit. If this was possible, neither would be able exit the door group.
- Custodian:

  The custodian feature enforces a cardholder with custodian privilege to always be inside a door group when other cardholders are inside. A door with two card

readers for Entry/Exit is needed for this option. The custodian must be the first to enter. No other cards will be granted access until the custodian has entered. Custodian will not be allowed to exit until all non-custodian cards have exited. Escort and Custodian cannot be both assigned simultaneously on a Door Group as both the escort and custodian cardholders must be last to exit. If you do this neither cardholder would be able to exit the door group.

It shall also be possible to configure two different types of anti-passback as follows:

- Interlock
- Only one door in a door group with 'Interlock' will be allowed to be open at a time. These doors shall have the ability to be grouped. Setting Prefix

  The system shall support the ability to activate a setting mode, which if not enable shall prevent accidental arming of the system
- Anti-Passback:
  - Prevent Passback:

    A door with two card readers for Entry/Exit is needed for this option. The door must also be assigned to a door group, the cardholder is only allowed to present the card / fob at the entry reader once. The cardholder is not allowed to present the same card again on the entry reader until the card /fob is presented to the exit reader first. This then allows the cardholder to present the card at the entry reader.
  - Soft Passback:

    If Anti-passback violations shall only be logged but not prevented. A door with two card readers is needed for this option and the door must be assigned to a door group.

## 12.6Intrusion & Access Control Interoperability

Intrusion system will override Access Settings and prevent access if the Card holder does not have the Intrusion rights to unset the system if it is set. The system shall provide the means to indicate temporarily the intrusion Area/System has been set by means of a warning device being triggered for a period of time – visual warning is switched on for a determined period. The Card/Fob shall be EM4102 standard to both the Intrusion and the Access Control systems – the user need only carry one credential. Logging of events – Door Alarms should be recorded in both the Intrusion Log and Access Control Log.

Issued by
**Vanderbilt International GmbH**
Borsigstraße 34
65205 Wiesbaden-Nordenstadt
Germany

# 13 Verification Control System

## 13.1General

The integrated controller in conjunction with verification products(s) distributed on the system BUS/IP will process and manage the verification. The system shall allow for audio and/or video verification.

## 13.2Audio Expansion

The system shall support Audio devices which directly connect to the systems expansion bus and are addressable and configurable via software tool, locally or remotely.

The system shall support at least 16 independent zones of audio detection; each audio zone shall be capable of supporting at least 4 satellite audio expansion devices.

Power for the audio expander should be from the system's battery backed up power supply(s) such that in the event of a power failure the system continues to function for the specified period depending on the grade of the system.

The Audio Expander shall support (in addition to the audio speaker and microphone) at least 4 inputs and 1 open collector output to allow connection of conventional security devices meeting the approval standards as well as being able to control local equipment (sounders, beacons etc.)

## 13.3Audio Expander Technical Requirements

| | | |
|---|---|---|
| Number of on-board zones | | 4 |
| EOL resistor | | Dual 4k7 (default), other resistor combinations configurable |
| Number of Outputs | | 1 |
| Field bus | | X-BUS on RS-485 (307 kb/s) |
| Tamper contact | | Front spring tamper |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | -10 ~ +50 °C |

## 13.4Audio Configuration

The device shall be fully configurable and audible (via software) to be able to cope with different environments, sensitivity, gain, recording duration should be covered as a minimum. The configuration of the system shall be stored in a software tool so that in the event of the need to reprogrammed existing/new system the settings can be immediately restored.

The system shall be configurable with a „privacy feature“ which prevents a remote operator from listening into the system if no alarm on that site has occurred.

The audio alarm events shall be delivered to a dedicated IP based receiver, the receiver should be compatible with „off the shelf“ alarm management software packages.

The system’s audio expander functionality shall have the capability to be configured via the system keypad / PC configuration program or a web browser.

## 13.5Operation

The system shall store the files associated with the last alarm event as well as storing to 8 historic alarm events for retrieval if required. The retention of the historic audio alarm event log will work on a FIFO basis

The system shall store pre and post alarm audio events as per the configuration such that in the event of an alarm and the system shall either automatically or upon request deliver the event recording off-site to a remote operator.

In the event of an alarm the audio alarm events shall be retrievable from the site without the need for the remote operator to have to search for the relevant event.

It shall be possible (after an alarm) for the operator to manually select which audio zone they wish to listen to listen into the site live and manually select an audio zone to

Issued by
**Vanderbilt International GmbH**
Borsigstraße 34
65205 Wiesbaden-Nordenstadt
Germany

## 13.6Video Expansion

The system shall support Video devices which connect to the system using local network and IP connectivity, configurable via software tool, locally or remotely.

The system shall support at least 4 independent video devices.

Power for the video devices should be from the system's battery backed up power supply(s) such that in the event of a power failure the system continues to function for the specified period depending on the grade of the system.

## 13.7Video Technical Requirements

| | | |
|---|---|---|
| | | Spec for video devices required |
| | | Spec for video devices required |
| | | Spec for video devices required |
| | | Spec for video devices required |
| | | Spec for video devices required |
| Operating voltage | | 9.5 ~ 14 VDC |
| Operating temperature | | -10 ~ +50 °C |

## 13.8Video Device Configuration

The device shall be fully configurable and audible (via software) to be able to cope with different environments, sensitivity, gain, recording duration should be covered as a minimum. The configuration of the system shall be stored in a software tool so that in the event of the need to reprogrammed existing/new system the settings can be immediately restored.

The system shall be configurable with a „privacy feature“ which prevents a remote operator from listening into the system if no alarm on that site has occurred.

The audio alarm events shall be delivered to a dedicated IP based receiver, the receiver should be compatible with „off the shelf“alarm management software packages.

The system's audio expander functionality shall have the capability to be configured via the system keypad / PC configuration program or a web browser.

## 13.9Operation

The audio expander shall store the files associated with the last alarm event as well as storing to 8 historic alarm events for retrieval if required. The retention of the historic audio alarm event log will work on a FIFO basis

The system shall store pre and post alarm audio events as per the configuration such that in the event of an alarm and the system shall either automatically or upon request deliver the event recording off-site to a remote operator.

In the event of an alarm the audio alarm events shall be retrievable from the site without the need for the remote operator to have to search for the relevant event.

It shall be possible (after an alarm) for the operator to manually select which audio zone they wish to listen to listen into the site live and manually select an audio zone to

# 14 Control System interfaces

## 14.1General

The integration control system shall provide the ability to interface to automation software and BMS systems. The system shall provide interface specifications for third party developers. This interface shall allow for control of system areas, zones, doors and alerts.

The manufacturer will provide an API (under NDA) in order to allow for external system integration.

Issued by
**Vanderbilt International GmbH**
Borsigstraße 34
65205 Wiesbaden-Nordenstadt
Germany

## 14.2Software

The system shall provide the following software options designed to simply implementation and reduce ongoing maintenance tasks.

## 14.3User management

The integration control system shall provide the AS to allow for the control and configuration of users across multiple sites or a single site. The user management application software will allow for the adding, editing and deleting of users and user profiles and calendars.

It shall be possible to administer user credentials (both Intrusion & Access) across multiple sites with minimum of effort which means not having to contact sites on an individual basis to effect any changes.

The user management AS shall be an on-line system which automatically stores system data in a central location using an SQL database. A library of basic reports should be available as well as the ability to create “custom reports”

## 14.4Configuration file management

The integration control system shall provide the AS to allow for the remote backup of site configuration files. The file management software will allow for viewing of back up files and the downloading of files to the integration control system.

The system shall support a suite of software tools designed to speed up and simplify programming, store system configurations and diagnose technical problems remotely.

It shall be possible to perform tasks on-site or remotely, remote connectivity to the system shall support encrypted communication to AES256 standards as well as having additional security levels to prevent remote abuse.

The system’s configuration file shall be stored in such a way that it can be edited on-line or off-line and centrally stored in the software tool.

On connecting with the system if there is any differences between the data stored in the system to that held in the centralised database the operator should be immediately informed and given the choice of synchronising/overwriting data.

During the process of up/downloading the system shall advise the operator of progress and a successful data transfer.

The option to configure the centralised software to automatically check the remote systems configuration and compare with the configuration files. Should any difference be detected the system shall save the latest configuration and at the same time archive the older configuration. The remote systems older configuration file shall be archived and retrievable so in the event of needing to “roll back“ to a known point this can be easily achieved.

## 14.5Remote site maintenance

The integration control system shall provide the AS to allow for the remote maintenance management of sites. This system shall allow for the review of reports and provide reports on a scheduled basis.

The system shall support automated remote servicing where a routine service can be performed in terms of collecting technical data from the remote system without having send personnel onto site. It shall be possible to schedule automated services on a pre-defined frequency.

It shall be possible to perform the remote maintenance whist the system is Set/ARMED without effecting the security of the site.

The Remote Maintenance function shall have the capability to detect and identify on a report the absolute status of the system to the point where if any of the features are shunted or disabled the system will show this.

The system shall provide 2 levels of report identifying the results of a Remote Maintenance visit –

Level 1 Report - shall be a “top level report” which gives a graphical summary on either

pass/fail of the main areas tested.

Level 2 Report - shall expand on Level 1 report and provide a detailed electrical and system status report covering all aspects of a remote service as detailed by local standards.

## 14.6Remote monitoring and web access

The integration control system shall provide the AS to allow for the remote access to the embedded web server through a secure cloud interface. This system will also allow for email notification to an individual or group.

A user with the appropriate privileges shall be able to connect to the system through a secure cloud service from any machine using standard browser technology. It shall be possible for the user to use any PC/Tablet/Phone to connect to the system without having to install any software.

Once connected the user can navigate the system, investigate /control/reprogram the system depending on his/her level authority (defined by their own unique user profile).

It shall also be possible for the service provider to investigate and program the system using the web interface.

All activity of the users who connect to the system shall be logged in the memory of the system; this can be viewed/is retrievable in the normal manner.

In the event of an alarm the system shall be capable of delivering an email which determines the root cause, time and date of the alarm and provides a link for the user to connect via a secure portal service.

With connecting to the system via the secure cloud the user shall be presented on the first screen full details of the event/associated events with the option to restore the system.

# 15 Warranties

## 1.1 General

The Intrusion control equipment, including door controllers and readers, shall be warranted by the manufacturer against electronic failure for at least x years. It is accepted that the security system will require preventative maintenance. After the successful completion of required testing, the owner's representative shall certify the System as substantially complete which shall signify the start of the system's one (1) year warranty/maintenance period included as part of this contract. The system shall be warranted in its entirety to be free of mechanical or electrical defects for a period of one (1) year after the date of substantial completion. Any sign of mechanical, electrical, electronic, programming, or software malfunction shall be corrected, replaced, or repaired promptly by the contractor at no expense to the owner. Included as part of the maintenance service, the contractor shall provide, at no cost to the owner, firmware updates. These shall be available free of charge for the lifetime of the product. Software updates that include "bug fixes" shall be available on a free of charge basis during the Warranty/Maintenance period. The contractor shall verify proper operation of the system after incorporation of each update. Software updates shall be fully documented.

Issued by
**Vanderbilt International GmbH**
Borsigstraße 34
65205 Wiesbaden-Nordenstadt
Germany

# 16 Commissioning and Training

## 16.1General

The system shall be programmed with the information supplied. The system must be fully working with all system parameters. It is the tenderer’s responsibility to ensure that all the necessary information is obtained before commissioning the system.

The tenderer shall supply detailed “as installed” drawings of the entire system.