Saflec Systems
48 Richard Road
Industria North
1709

Tell: +27 (11) 477-4760
Fax: +27 (11) 477-5789

RE: Saflec Systems Architecture

Introduction:
Saflec is a South African company and all hardware & software development is done at our offices in Johannesburg. We have designed our system with the installers and end user in mind, always thinking of ways to make the system more user-friendly and easier to use while keeping it simple to design and install. Saflec has to date a large list of satisfied clients that are using our system in all industries, including corporate, mining and government.

1. Detailed Specification

1.1. System Architecture

1.1.1. General

The Access Control system shall use a Client Server architecture based around a modular PC network, utilizing industry standard operating systems, networks and protocols

The system shall allow the distribution of system functions such as monitoring and control and graphical user interface etc. across the network to allow maximum flexibility and performance. The architecture shall include support of various Wide Area Networks using standard hardware and software to link door controllers into a single integrated system. The network protocol used shall be industry standard TCP/IP.

1.1.2. Communications Redundancy

The system must be capable of supporting fully duplicated communications links to Operator Workstations and field devices that support this type of connection

1.1.3. Network

The Server Computer and Operator Workstation hardware shall be capable of interfacing to an IEEE 802.3 Standard Local Area Network (LAN), and also capable to operate using IEEE 802.11 Wireless Local Area Network (WLAN).

1.2. Computer Hardware

1.2.1. Server Computer

The system server computer shall comprise of the following minimum requirements:

- Server / VMWARE
- Intel Core i5 330UM 1.20GHz
- 4GB of RAM
- Graphics card capable of 1280x1024 pixel resolution and 65K colors
- 12 function-key keyboard
- Mouse pointing device
- 80 GB Hard disk drive
- DVD ROM drive
- TCP/IP adaptor
- UL Listed server computer platform shall be used when UL compliant system is required.
- Tenderer to include as an option, the utilization of Virtual machines (eg. VMWare) if supported by the solution.

1.2.2. Operator Workstation

The system shall be capable of supporting simultaneous Operator Workstation connections using a TCP/IP Local Area Network (LAN). The Network connection must allow a limitless number of casual users access to the 80 connections on a first-come-first-served basis.

The Operator Workstation shall comprise the following minimum hardware:

- Intel Core i5 U540 1.20GHz2GB of RAM
- Graphics card capable of 1280x1024 pixel resolution and 65K colors
- A 50 GB Hard disk drive
- A 12 function-key keyboard

- A mouse pointing device
- TCP/IP adaptor

1.2.3. Printers

Printers shall be available for printing either reports or online alarms. Report printers shall be any Windows compatible printer such as a laser printer. Alarm printers shall be 132 column printers to allow real time alarms to be printed as they occur.

1.2.4. Access Card Printers

Access card printers shall be available to print

- Temporary access cards
- Employee access cards
- Contractor access cards
- Replacement access cards

1.3. Communications

The ACCESS CONTROL system shall provide communications over a variety of physical media topologies as follows:

- Ethernet
- Proprietary Networks

The system shall be capable of supporting separate communications links to networks of control devices. Each connection shall operate independently of the others and facilities shall be provided by system displays to individually place these links in service or out of service.

Given the sufficient level of system privilege, it shall be possible to view, manipulate and analyze all data in the system from any Operator Workstation on the network, including those operating remotely.

Once a control device is configured and placed in service, the system shall automatically begin background diagnostic scanning of the device to ensure that communications are monitored independently of any monitoring scanning.

The system shall perform checks on data integrity of all data acquired from the

device. If an invalid or time out response is received, the data shall be ignored and the system will record the transaction as an error. Statistics shall be kept and displayed by the system on errors encountered in communication by means of a communications barometer. The barometer shall increment for every failed call and decrement for each successful call. In addition, the system shall alarm separate *marginal* and *failure* conditions based on user-defined limits to advise the operator of the device and link that has failed. Communications statistics shall be displayed as standard on the system and shall also be available as part of the reporting system or custom displays.

1.4. System Software

The ACCESS CONTROL system server shall be based around the Microsoft Windows 64 bit multi- tasking environment (Windows Server).

Standard services supported by the server computer operating system will include the following:

- Multi-tasking Multi-user support
- Real Time and relational databases to integrate connected systems into unified presentation layer
- ACCESS CONTROL Application software

Software at the Operator Workstation shall comprise of:

- Windows Server
- ACCESS CONTROL Client Application software
- TCP/IP Networking

The networking software shall use the industry standard TCP/IP LAN protocol. The server computer or an alternative network connected computer shall be capable of acting as a File Server for graphic displays and cardholder photo images. All LAN connected Operator Workstations shall be able to view custom displays and photo images from the server computer.

All system peripherals shall be capable of being connected to the server computer via the LAN.

1.5. System support for Virtualization

The ACCESS CONTROL system shall be qualified and supported on VMware. This support shall include operations of the ACCESS CONTROL server software, and also related communications gateways and storage devices.

Completed test plans demonstrating the offered ACCESS CONTROL solutions support for Virtual Machine platforms shall be available. Also characterizations of performance results and required Virtual Machine settings shall be available.

1.6. Operator Interface

1.6.1. General

The operator interface provided by the system shall allow for efficient communication of operational data and abnormal conditions. It shall provide a consistent framework for viewing of information. The ACCESS CONTROL shall also have an unlimited number of custom (facility specific) displays created to meet the needs of the specific facility.

The operator interface software shall be capable of running in the Windows server platform. The operator interface shall be interactive and totally graphics and/or icon based. Graphics shall be capable of supporting at least 65,000 colors at a minimum 1280 x 1024 pixel resolution. The operator interface shall also be compatible with Windows Terminal Services allowing remote PDA devices to be used as mobile operator interfaces.

The operator interface shall employ standard Windowing conventions so as to reduce required Operator training. In particular, standard tool bar icons and drop-down menus shall be available on all standard and custom displays to allow easy access to common functions. The tool bar and pull down menus shall be fully configurable. Similarly, such functions shall also be available via a standard set of Function-Key based pushbuttons without requiring configuration.

1.6.2. Operator Input Devices

The operator interface shall be capable of being mouse driven and simultaneously support keyboard data input. Both fixed menus and configurable function keys shall be supported to aid novice and experienced operator respectively. The

interface shall also be capable of supporting a touch-screen for pointing and command input.

The operator interface shall use a Tool Bar for common operator commands. The operator shall be able to request display of commonly used displays and activate system functions via Drop-Down menus

All operator interface input shall be possible using only the pointing device and QWERTY section of the keyboard. Fast access to common functions shall be possible using predefined function keys on the keyboard. A Keyboard overlay shall be available to assist operators with using these function keys.

1.6.3. Operator Functions

The following functions shall be performed through the operator interface:

- Display and control of field equipment
- Initiate printing of reports
- Archive and retrieve event logs
- View ActiveX documents
- Use ActiveX controls
- Change own password
- Monitoring of data communications channels
- Configure system parameters

1.6.4. Operator Security and Sign-On

If necessary, each operator can be assigned a user profile that defines their permissions
All actions initiated by the operator shall be logged in the Event database by operator identifier. In addition, any control actions to a given point shall only be allowed if the control level configured in the operator's profile exceeds the level assigned to the controlled point.
Utilities shall be provided to allow administration of the operator passwords.

1.6.5. Sign-On/Sign-Off

The operator shall be permitted to sign on to the system if the correct Operator Identity and the Operator Password have been entered. This password shall be encrypted. It shall also be possible to have the system authentication integrated directly into Windows, Windows Group Accounts, or an LDAP Server such that the operator uses the pre-existing account details to sign on to the ACCESS CONTROL system. This ensures that operators only need to remember 1 set of credentials for both their workstation and the ACCESS CONTROL

During Operator Workstation lockout the other Windows functions of the computer running the Operator Workstation software shall not be affected.

It shall be possible to assign operators either single or multi-user accounts. Single user accounts enable the operator to sign-on to only a single Operator Workstation thus preventing simultaneous sign-on by the same operator from different workstations. Operators with the highest sign-on security level who may require simultaneous access to more than one Operator Workstation would typically use the multi-user password.

Each operator shall be assigned a password and a defined Scope of Responsibility which defines the locations in the facility that may be managed and controlled by the individual operator.

1.7.1. Reporting

The system shall support a flexible reporting package to allow easy generation of report data. The reports provided shall include pre-configured standard reports for common requirements.

1.7.2. Custom Reports

In addition to standard reports, configurable report generation facilities must be provided to allow custom reports to be produced. They shall be able to be configured at any time with the system online, and shall be able to access any database values. At least three methods of custom report generation shall be available, including the following:

1.7.3. Microsoft Excel Report

The ACCESS CONTROL shall provide the facility for the use of Microsoft Excel, CVS and PDF as a reporting tool – allowing calculations such as summations, maximal, minimal and standard deviations, and the production of graphs, charts and tables. Systems that do not provide support for Microsoft Excel in this respect shall not be acceptable.

Data accessible for Excel reporting shall include alarms, events, and point parameter values.

1.7.4. SQL Reporting Services Custom Report

Being based on SQL Server, the ACCESS CONTROL system shall support a simple custom report format using the SQL reporting services. This shall enable customer reports to be designed in either Reporting Services, or Visual Studio and shall enable access to all point data, cardholder data and alarm and event data. The design of the SQL Custom Reports solution shall be available from any of the LAN connected Operator Workstations. No addition license fees shall be required to utilize this standard custom reporting solution. To facilitate rapid development of simple custom reports the system shall be delivered with template reports.

1.8.1. Time Scheuldes

It shall be possible to specify time schedules for the control of all ACCESS CONTROL points. It shall be possible to control a range of a single point to a large number of points from a single schedule. A single time schedule shall define the control to any combination of day and time.

The ACCESS CONTROL scheduling management system must be more flexible than providing weekly schedules with a provision for a finite number of special occasions/holidays. The ACCESS CONTROL scheduling system shall allow schedules to be entered that recur on a non-weekly basis or only occur once on a given day in the future.

Examples:

- Schedules shall be capable of recurring on any multiple of weeks (every 1 week, every 2 weeks, every 7 weeks, etc.)
- It shall be possible to enter a schedule that only occurs once on any given day in the future

The ACCESS CONTROL time schedule must also provide the ability to override the normal schedule for holidays or special occasions. The user shall be able to create multiple different grouping of dates (Calendars) that can be assigned to individual points as applicable.

Examples:

- Daily or weekly recurring time schedules; capable of recurring until a specified date or without end (Mon-Fri 7:00 to 18:00, Thursday 7:00 to 22:00)
- Time schedules active for greater than 24 hours (Saturday-Sunday 9:00 to 14:00)
- Time schedules that occur on a specified group of Calendar Days (e.g. Holidays) Configuring time schedules must be done through a graphical user interface whereby the operator selects the appropriate time span from a calendar. Systems where times and days must be manually entered or managed by an external spreadsheet type form are not acceptable. The user interface must support the capability of navigating

to any future date to allow the user to enter a time schedule

1.9.1. Cardholder Management System

The ACCESS CONTROL shall store security related cardholder/passholder information in a relational database such as Microsoft SQL Server.

The cardholder database shall support at least 1,000,000 cardholders. The data specific to the requirements of different ACCESS CONTROL systems. It shall be possible to increase or decrease this number of user definable fields. Systems without the ability to increase the number of user definable fields shall not be accepted.

1.9.2. Cardholder Database

It shall be possible to define labels and field types for each of the user definable fields. It shall be possible to define lists of choices for certain user fields to avoid unnecessary typing, for example, defining a list of department names. It shall also be possible to modify the layout of cardholder fields on the display screen to alter the look to particular user's requirements. It shall also be possible to create more complicated calculations between user fields. For example, creating the value of one user field based on the value of two others. It shall be possible to define default values for all user fields, which shall be applied when the cardholder is first added to the system.

1.9.3. Searching and Sorting

It shall be possible to define which user fields in the cardholder database are searchable fields. All searchable fields shall be able to be used to call up a list of cardholders who match a certain criteria. In addition, it shall be possible to search on multiple cardholder characteristics at one time, for example, all cardholders in department "X" who have a supervisor of "Y". A list of matching cardholders shall be displayed and an appropriate choice may be made.

1.9.4. Multi-Selection

It shall be possible for multiple cardholders to be selected and a single edit to be performed on all of these cardholders selected. For example, it shall be possible to select all cardholders in department "X" and change their address to "Z" in a single operation

1.9.5. Templates

The ACCESS CONTROL shall define templates in order to add groups of cardholders with predefined characteristics. A template shall contain all the relevant details for a particular group of cardholders such as all their user fields and access levels. When adding a new cardholder to this group using the template, the cardholder shall be added with the same characteristics as defined in the template.

1.9.6. Cardholders and Cards

Multiple cards assigned to a single cardholder shall be able to be in different states. For example, it shall be possible for a single cardholder to have both an "active" card assigned and an "inactive", "lost" or "stolen" card assigned.

The system is to have the capability to assign a temporary access card (eg to replace a misplaced card) for a defined period of time while suspending the original card.

It shall also be possible to support different technologies of access control cards in the one system. For example, a single cardholder may have a proximity card, a magnetic stripe card and a biometric template assigned to them.

Cards may be created and assigned to cardholders separately. It shall be possible to "return" a card when a cardholder no longer requires it, and then reassign it to another cardholder without having to delete and recreate the card.

When cardholders or cards are deleted or expired, or when a card is returned from use by a cardholder, the system shall automatically download this to the field controllers so these cards no longer provide access.

1.10. Access Permissions, Time Periods and Zones

1.10.1 Time Periods

The ACCESS CONTROL shall support a minimum of 256 time periods.

The operator shall be able to access a summary display listing all time periods and their descriptions. From this display the operator shall, if the operator is configured for the time period's Organization code, be able to go to a time period detail display showing the time periods configurable parameters.
Once the changes have been saved the ACCESS CONTROL shall automatically download the new data before it is enabled in the Access Control System. This shall allow operators to make a number of changes but only be required to download once.

1.10.2. Zones

The operator shall be able to access a summary display listing all zones and their descriptions. From this display the operator shall, if the operator is configured for the zones assigned Organization, be able to go to a zone detail display showing the zone configurable parameters.
Zones shall be automatically created when card readers are configured in the system. Zones are defined by the card readers, which allow entry to the physical space, which the zone represents. One reader may only be defined as entering one zone. Each reader will indicate the zone it allows entry to and optionally the zone from which one has exited

1.10.3. Access Permissions

The operator shall be able to access a summary display listing all access permissions and their descriptions. From this display the operator shall, if the operator is configured for the access permission's Organization, be able to go to an access permission detail display showing the access permission's configurable parameters.
Once the changes have been saved the operator will be required to download the new data before it is enabled in the Access Control System. This shall allow operators to make a number of changes but only be required to download once.
Each access permission detail display containing changed data that has not been downloaded shall clearly indicate this to the operator via a flashing warning message. Download of this data shall cause the warning message to disappear.

1.10.4. Assigning Access to Cardholders

Cardholders may have any number of different access levels assigned to them. This shall not be limited by the FMSACCESS CONTROL system. Each of these access levels may define a separate set of readers and times that will allow the cardholder access. Operators shall be presented with a list of all access levels already assigned to the cardholder and all access levels that are currently unassigned.

1.10.5. Deleting Cardholders

Cardholders may be deleted but retained in the database for future reference if required. It shall then be possible to "undelete" the cardholder should this be required. It shall also be possible to permanently delete the cardholder record in order to prevent unnecessarily large databases from developing.

1.10.6. Card/Cardholder Expiry

Cardholder and card expiry dates may be defined down to a resolution of date and time in minutes.

It shall be possible to assign cardholders and cards separate expiry dates, enabling a card assigned to a cardholder to expire before the cardholder expires. However, it shall not be possible for the card expiry date to exceed the cardholder expiry date of the cardholder to which a card is assigned.

Expiry dates may be set up by default to be a particular given date, or a relative period from the time the cardholder was created (e.g. 1 year).

It shall be possible to assign a cardholder a commencement date and have their assigned cards automatically become active on this commencement date.

1.10.7. Cardholder Alarms

It shall be possible to specify that the cardholder generate an alarm when they use their card. This setting may override the alarm setting of the reader to which a cardholder may be presenting their card

1.10.8. Cardholder Events

All changes to cardholders in the system shall be logged in the event summary and shall list the new value of the cardholder field. Similarly, any time a cardholder

accesses a card reader; an event will be listed in the event summary. It shall be possible to automatically view all the events generated for a particular cardholder directly from the cardholder displays without having to run a separate report.

1.10.9. Uses Before Expiry

It shall be possible to define the number of times that a cardholder may use their cards. This number shall be decremented every time the cardholder uses their card at a reader until the number is 0, when the cardholder shall no longer have access.

1.10.10. Photo Identification Badges

It shall be possible to capture portraits and signatures for all cardholders and then create photo identification badges using these images.

Image capture and printing of photo identification badges must be fully integrated into the ACCESS CONTROL system and must use the same database. Any system, which uses a separate photo badging system or separate database, will not be acceptable.

Capture devices must include Video Capture cards, Digital Cameras, scanners and signature tablets and capture facilities must support the MCI or TWAIN standards for image capture. Devices may be connected directly via PC boards or through serial or USB ports. If using a Video Capture card for image capture, a live preview facility must be provided. Import and export facilities for images shall also be available.

The ACCESS CONTROL system must provide a tool for the creation of photo badging card layouts. This must allow the incorporation of standard display creation facilities such as image import, a variety of fonts and text effects, a variety of tools for drawing objects and a facility for linking to the cardholder database and any user fields within this. This tool shall be the same tool as used for the creation of custom graphics in the ACCESS CONTROL system as described in section 1.6.9 so as to reduce training and maintenance requirements for the system.

In addition, it shall also be possible to incorporate bar codes and automatic magnetic stripe encoding facilities into the photo badging system.

1.11. Biometric Support

The ACCESS CONTROL shall provide the ability to use biometric devices such as hand geometry readers for high security access control. These devices shall be fully integrated into the ACCESS CONTROL system allowing centralised template management of biometric templates. The ACCESS CONTROL system shall be the master database for all cardholder information including biometric templates. The ACCESS CONTROL shall allow for hand geometry changes over time by automatically uploading validated hand templates and downloading them automatically to those hand readers to which the user has access rights.

1.12. Visitor management

The ACCESS CONTROL shall optionally provide the ability to manage and track visitors to the facility. This shall include visitors who are given access control cards. It shall be possible to store information that defines who the visitor is, what company they represented and whom they were visiting in the facility. This information shall be displayed on a different display to that of a standard cardholder so that operators can enter visitor information easily and without the distraction of all the standard cardholder user fields.

The system shall be capable of doing the following:

Manage Incoming visitors : Record their data, assign a badge and print a pass
Manage outgoing visitors : Retrieve their badge and store the visit data
Pre-Registering Visitors
Temporary Badge assignment

The visitor management system shall have the ability to capture a visitor's picture, and store data of ID documents such as a passport when used with the appropriate document capture tools like a scanner.
All information about when a visitor arrived and when a visitor departed shall be recorded in the standard ACCESS CONTROL event summary. For visitors who are assigned access control cards, it shall support the automatic expiry of their cards

1.13. Elevator Control

The ACCESS CONTROL shall be capable of controlling access to different floors of a building

1.14. Software Functions

1.14.1. Event Initiated Programs

Physical and software outputs or groups of outputs shall be assignable through configurable algorithms to an input point. When an input changes state the outputs assigned shall be activated as specified by their physical or configured output modes.

When alarm events of individual or groups of points are suppressed by event initiated programs, any occurrence of such alarm events during the suppress mode shall not be enunciated, reported or journalized.

1.14.2. Event Management

Events shall consist of alarms, changes of state in a monitored status point, cardholder movements, and changes in system status and operator actions.

All journal events shall be recorded as necessary to include event description, condition, message, time of occurrence, operator responsible and any other information or tags.

1.14.3. Report Management

The system shall support a flexible reporting package to allow easy generation of report data. The reports provided shall include pre-configured standard reports for common requirements such as Alarm Event reports and custom report generation facilities that are configurable by the user.

1.15. Server Software Architecture:

Saflec offers three server software options for all sizes of installations:

1.15.1. Basic Edition software V3

- 8 doors can be configured
- Proximity readers only
- Can not be used with client software
- MS SQL as database platform
- Once-off license
- All standard functions included eg: reporting, anti-pass back and zone control
- Flexible user password control

1.15.2. Professional Edition software V3

- 12 doors can be configured
- Proximity and biometric readers (Morpho and Virdi)
- Can use client software for remote administration
- MS SQL as database platform
- Once-off license
- All standard functions included eg: reporting, anti-pass back and zone control
- Flexible user password control

1.15.3. Corporate Edition software V3

- Unlimited doors
- All existing integration included
- Can use client software for remote administration
- MS SQL as database platform
- Once-off license
- All standard functions included eg: reporting, anti-pass back and zone control
- Multiple companies support
- Flexible GUI interface
- Multiple site support
- Extremely flexible event-based action model.

- Configurable extra data fields with automatic lists, dropdown lists, photographs or notes fields
- Sequencing tasks (For example: enforcing T&A clockings before allowing the tag holder to leave)
- Extremely flexible event-based action model
- Flexible user password control
- Flexible plug-in modules for further integration to 3rd party applications

1.16. Client Software Architecture

Saflec offers two client software applications for remote administration on Professional and Corporate Additions:

1.16.1. Client addition software V3

- This has all the functions of the server software

1.16.2. Personnel Assistant V3 (PA)

- Built-in card designer for printing cards or labels at a reception area
- Visitor capturing with flexible options (For example: mandatory fields)
- Configurable wizard for information capture

1.17. Hardware Architecture (Controllers & Expansion boards):

Our hardware doesn't require any interface cards in the computers and our main communication is done on Ethernet connections. We have combined the typical topology of having a master controller and door controllers into one, by doing this we only have controllers that are intelligent and decision making is done on the door controller level. The access control information is downloaded to the controllers which makes the system more reliable as it is not dependant on external factors like operating systems, computers or networks.

Every controller can be linked on an RS-485 device network that can have up to 16 controllers. RS-485 is an easy and secure way of connecting multiple controllers and allows long cable runs.
An entire system can have many device networks which means that the system can essentially be as large as necessary, limited only by the server and network capabilities.
One of our larger systems to date consists of more than 200 device networks, 500 controllers and 4000 access points spread across the whole of South Africa, but centrally managed.

Saflec offers a variety of Ethernet controllers. The entry level 3 series controller and the new 6 series controllers

1.17.1. The SDC-320 Two Door Ethernet Controller offers the following features:

- Fully offline operation
- 1000 cardholders
- 100 000 transactions stored while in offline mode (No connectivity to the server)
- On-board time/date battery backup
- Micro SD memory.
- Supplied with secure enclosure with Power Supply and battery backup
- RS-485 reader network connection with a maximum of 4 readers.
- RS-485 readers or Wiegand readers
- Readers must be powered from the controller
- 4 digital inputs
- 1 Dedicated Fire input
- 1 Dedicated tamper input
- 2 x relay outputs
- No Events or Actions between controllers. Only Anti-Passback between controllers.

1.17.2. The SDC-325 Sallis Ethernet 8 Door Controller offers the following features:

- Fully offline operation
- 1000 cardholders
- 100 000 transactions stored while in offline mode (No connectivity to the server)
- On-board time/date battery backup
- Micro SD memory.
- Supplied with secure enclosure with Power Supply and battery backup
- RS-485 reader network connection with a maximum of.
- 1 x Sallis RS-485 router
- 8 x Sallis RS-485 nodes

1.17.3. The SDC-520 / 550 controllers have the following functionality. The 5 series were discontinued and replaced by the 6 series controllers.

- Fully offline operation
- 3200 cardholders on SDC-550 and 30000 cardholders on SDC-520 (And SDC-550 with SEB-700 expansion)
- 6000 transactions stored while in offline mode (No connectivity to the server)
- 40 000 transactions stored if the Ethernet devices is used.
- Supplied with secure enclosure with Power Supply and battery backup
- Expansion headers for future expansion (SDC-550 Only)
- Isolated RS-485 controller network connection
- Isolated RS-485 reader network connection (Isolated on SDC-52x Only)
- RS-232 connection (SDC-550) or USB connection (SDC-52x)
- 8 digital inputs & 5 relay outputs (SDC-550) and 4 digital inputs & 2 relay outputs (SDC-52x)
- Expandable to 8 doors by using remote I/O expansion units
- Events and Actions between controllers and device Networks.

1.17.4. The SDC-620 / 650 controllers have the following functionality:

- Fully offline operation
- 250 000 cardholders
- 6 500 000 transactions stored while in offline mode (No connectivity to the server)
- Supplied with secure enclosure with Power Supply and battery backup
- Expansion headers for future expansion (SDC-650 Only)
- Isolated RS-485 controller network connection
- Isolated RS-485 reader network connection (Isolated on SDC-52x Only)
- RS-232 connection (SDC-650) or USB connection (SDC-52x)
- 8 digital inputs & 5 relay outputs (SDC-550) and 4 digital inputs & 2 relay outputs (SDC-52x)
- Expandable to 8 doors by using remote I/O expansion units
- Events and Actions between controllers and device Networks.
- HID OSDP technology

1.17.5. The SDC-655 Sallis Ethernet 15 Door Controller offers the following features:

- Fully offline operation
- 250 000 cardholders
- 6 500 000 transactions stored while in offline mode (No connectivity to the server)
- On-board time/date battery backup
- Micro SD memory.
- Supplied with secure enclosure with Power Supply and battery backup
- RS-485 reader network connection with a maximum of.
- 1 x Sallis RS-485 router
- 15 x Sallis RS-485 nodes
-

Saflec manufactured remote I/O expansion units (SEB-710/721/722) to be used with the 5 series door controllers. These units are used to increase the amount of doors controlled by the controller to 8 doors and in cases where the doors are situated far apart.

1.17.6. The SEB-710 units can only connect to the SDC-550 / 650 controller by using the expansion header on the controller. The expansion units offer the following

- 8 x outputs (potential free or powered)
- 8 x digital/analogue inputs
- Additional 8 x digital/analogue or 8 x transistor outputs. (Must be used as an input or output.
- External power must be supplied for powered outputs.
- Only the pc board is powered from the controller
-

1.17.7. The SEB-721 has a built-in remote receiver to be used with most rolling-code (code hopping) remotes as a longer range option.

- 4 x digital inputs

- 2 x relay outputs
- Can be used with all 5 series controllers
- RS-485 host connection to controller
- Compatible with 1,2,3 & 4 button transmitters

1.17.8. The SEB-722 units have the following connections available:

- Enclosure, 5 Amp PSU and 7aH battery
- 4 x digital inputs
- 2 x relay outputs
- Can be used with all 5 series controllers
- RS-485 host connection to controller
- RS-485 slave reader network for 1-4 readers (SSR-201)
- 2 Wiegand ports for external devices.

1.18. Hardware Architecture (Readers & data converters)

We use RS-485 connections on our readers where possible as this makes installations easier and less cable needs to be used. One can have up to 16 devices connected directly to a controller (Up to 10 readers). This gives you the ability to control 5 doors with both In & Out readers, or up to 8 doors using other devices like the remote expansion board or Wiegand boards.

Our readers work on 125 KHz frequency and can read any EM4102, Hi-Tag 1 & 2 cards.
We manufacture the readers with the following connection options:

- SSR-201, RS-485 reader with addressing
- SSR-202, Wiegand reader (can be programmed to send out CLOCK & DATA output) for 3rd party applications
- SSR-250D, RS-485 display reader
- SSR-250DKP, RS-485 display with a keypad reader
- SSR-221, USB take-on reader (uses power from USB port and no drivers needed – emulates a USB keyboard)
- SSI-301W, RS485 to Wiegand converter. 12Vdc must be supplied to the RS-485 connector and Wiegand connector

Saflec recognizes that technology improves on a daily basis. The Wiegand converter board can convert any 16, 24, 32 or 40 bit codes to our RS-485 network so that any external readers can be used. This enables the end user to change between technologies without changing the complete system. We have current interfaces to Morpho, Virdi & Suprema biometric readers so that template management is done with our software and no 3rd party interfaces are needed. Any other readers can also be connected to our system as you can still run their software separately if needed.

We are willing to consider integrating other 3rd party devices into the software, but this will be handled on a case-by-case basis.

Our software is integrated to various CCTV platforms. For more details please contact our office or visit our webpage at www.saflecsystems.co.za

1.19. HID MultiClass SE Readers

HID Global's iCLASS SE® platform goes beyond the traditional smart card model to offer a secure, standards-based and flexible platform that has become the new benchmark for highly adaptable, interoperable and secure access control solutions. multiCLASS SE® readers simplify migration from legacy technologies with support to 125 kHz EM4102 tecgnology.
The Saflec controllers are also fully integrated to the new Secured communications offered by HID by using OSDP with Secure Channel Protocol. This includes the option to add their Mobile functionality to the iClass reader leveraging mobile devices to access doors, parking facilities and gates.

If you have any queries, please don't hesitate to contact us.

Regards

Saflec Systems (Pty) Ltd.