INTEGRATED SECURITY MANAGEMENT SYSTEM

Today’s ever-demanding security challenges faced by the different stakeholders of various diverse industries cannot be simply addressed with the standard off-the-shelf surveillance cameras and intruder detection systems. There arises the need for an integrated platform to provide seamless convergence of multiple technologies of video surveillance, card access, intruder detection, guard tour, under vehicle scanners, delay systems and visitor management. SecurNet in its 7th product development iteration is designed specifically for this purpose.

SecurNet is deployed in various key installations namely government buildings, healthcare institutions, military complexes, commercial establishment, transportation hubs, corrective and education institutions. Used extensively around the world, SecurNet provides total security protection for key installations, critical infrastructures and strategic assets on an integrated command and control platform.

With its powerful kernel and database management capability, SecurNet offers a features rich integrated security management system for personnel access, alarm reporting/notification, graphical information display, and situational event control.

INTUITIVE USER INTERFACE

- The IEI is the high level interface to third party systems such as CCTV, fire alarm, facilities booking, intercom etc.

CONFORMS TO INTERNATIONAL SECURITY STANDARD

- Supports Singapore Standard for Smart Card IDentification (SSID-SS529). This standard is based on International Civil Aviation Organisation (ICAO) standard for e-passports and specifies the data structure, security and access conditions for a smart card that includes personal identification data. The standard is widely adopted by various Singapore government agencies and private organisations.
- High secured database partition ensuring that data segment is only accessed by authorised users.
- Adoption of industry-leading level of encryption of up to 256 bit AES symmetric encryption and RSA-1024 bit authentication.

DATA PROTECTION

- Fast report generation engine that offers a series of standard and customisable report templates, exporting in .PDF, .XLS and .DOC format.
- Offers multi-monitors display on a single PC workstation to enhance the operational efficiency of the user by up to 50%.
- Network-wide Peer to Peer (P2P) communication between controllers facilitates system flexibility and supports enhanced controls such as global anti-passback.
- The needs for an integrated platform to provide seamless convergence of multiple technologies of video surveillance, card access, intruder detection, guard tour, under vehicle scanners, delay systems and visitor management. SecurNet in its 7th product development iteration is designed specifically for this purpose.

OUTSTANDING COMMAND & CONTROL FEATURES

ROBUST ARCHITECTURE

- Built upon industry-leading MS-SQL 2016 and .NET platform with Windows 7/8.1 OS environment while ensuring backward compatibility with WinXP, Vista and SQL 2005/2008/2012.
- Allows top-down system-wide automatic and remote update on firmware packages without the need for physical access to each individual devices/sites.
- Network-wide Peer to Peer (P2P) communication between controllers facilitates system flexibility and supports enhanced controls such as global anti-passback.

CONNECTIVITY

- Supports database mirroring and automatic failed-over to achieve higher database redundancy in the event of system down. It also supports 3rd party high availability (HA) data protection solutions.

RELIABILITY

- SecurNet supports database mirroring and automatic failed-over to achieve higher database redundancy in the event of system down. It also supports 3rd party high availability (HA) data protection solutions.

ADVANCED BIOMETRICS

- Supports multiple fingerprint scanning technologies inclusive of optional ‘Live’ fingerprint recognition.
- Traditional smart card (with or without PIN code) is considered inadequate for personal verification and the push for Biometric Technology to enhance the level of security. Our ID Verification System (IDVS) is designed for this purpose.
- The IDVS is best used for physical access control to protect Key Installation such as seaport, airport, custom checkpoint and military bases. In addition, it can also be used for ID card solution that requires biometric verification to enhance the application security level.
- Compliance with local SSID SS529 and International Standard (ICAO) for smart card identification.
- Flexible, scalable and customization to meet specific application needs.
- Highly secure that support Multi-Factor Authentication (Card + Biometrics +PIN etc).

SCALABILITY

- SecurNet can be configured from a single server platform and expanded to a multi-server/client network across the globe for remote sites centralized command and control.

Critical Infrastructure

Transport Hub

Homeland Assets

High Security Sites

Optional Live Fingerprint Recognition
SOFTWARE FEATURES

DATABASE MANAGEMENT
The database is the core of SecurNet system as it contains the essential system configuration parameters, card holder information, confidential building layout, floor maps etc.
The central database includes but is not limited to the following:
• Integration configuration
• Database configuration
• Floor plan setting
• Detailed transaction log
• Alarm log
• System audit log
The SecurNet database server provides database mirroring and automatic fail over features for large scale system deployment that requires higher DB redundancy. It also supports third party high availability (HA) solutions such as Marathon HA for extra high availability.

DATA PARTITION
SecurNet allows users to perform database partitioning based on either physical locations (floor level or zone) or organisational structure.
Database partition enables multiple departments to share a single centralised database while maintaining the security and confidentiality of individual department’s data.
In each partitioned data block, users can specify the specific information they would like to share, e.g. privilege, building layout, floor maps etc.

MESSAGE NOTIFICATION
SecurNet provides a seamless message and email notification function to deliver system messages via SMS, email or broadcast based on user access privileges.
Short Messaging Services (SMS) or emails can be triggered based on alarm priority, message type, or device/device group definitions. Notifications can be sent to multiple parties at the same time, and if the first recipient is not reachable, the system will automatically direct the message to a standby user. Content in the SMS or email body is configurable to include information such as device point name, location, status, description of the event and date/time stamp.
Time Zones can also be applied to the message notification to deliver messages within the scheduled period.

REPORT GENERATOR
The system provides a fast report generation engine to query information available in the database and present it in a formatted report. Standard report templates are provided, while customised report templates can be easily added into the system. Each report (of any type) comes with a date and time stamp. Reports can be viewed online or be easily exported out into .PDF, .XLS or .DOC format.
Users are able to schedule the report generation of a specified date and time. This option allows the report generation task to be executed after peak hours to avoid slowing down the system performance.

EVENT MANAGEMENT
The SecurNet integrated event and alarm management feature allows users to view, search and process all access control transactions, alarm, system responses and operator actions.
Users can directly launch relevant objects like video tours, live camera views or cardholder particulars for any event. With permitted authorisation, users can also manipulate data fields, change views, and perform quick searches and queries either in real-time or from historical databases.

TIME ZONE & TIME ACCESS
SecurNet offers a time zone and time access function that can be applied to all system activities including door access, message notification, system events response, and system administration etc. Every system activity can be assigned with time zone and time access definition.
The time zone is specified by a start and a stop time. There are 24 sets of start-stop times for each day. The time zone assigned to the cardholder for a given day for door access will be determined by his assigned access privilege.
Access time allows different sets of time zones to be grouped together in a seven-day per week period plus any number of special days. These groups can be used to configure the access privileges of cardholders for each access door reader.

TIME ATTENDANCE
The SecurNet Time Attendance function allows users to compute an employee’s daily clock-in and clock-out time automatically.
By pressing a function key on the card reader, followed by the card authentication, the system is able to capture the IN/OUT time data and process the data based on work shift definitions in the system.
A comprehensive time attendance report can be generated every month to list employees’ working hours details. The report is generated in .PDF format by default, and it can be exported directly to .XLS or .DOC format for Human Resource administration.

VISITOR MANAGEMENT
SecurNet offers optional client/server based and web-based visitor management and facility booking applications.
Users can input the visitor’s particulars, visit schedules and room allocation through the visitor management application. Upon visitor’s arrival, the security or reception personnel will verify the identity and issue a pass according to the specific assigned access rights.
The facility booking application is fully integrated with the access control system to grant access only to designated meeting rooms or other locations in the facility based on booking arrangements.

CARD PERSONALISATION
The card personalisation function allows the system administrator to input the card holder’s information, encode and print cards for individual card holders.
SecurNet provides a user-friendly interface for administrator to capture or import photos, biometrics data (fingerprints) and sign-atures and automatically process the cardholder information for ICAO and ISO standards conformance. It supports BMP, GIF, JPG and JPEG2000 photo formats.
A flexible and easy-to-use badge designer application is provided for the user to create customised card layouts. As the badge design is integrated to the same database of the SecurNet, each cardholder’s particulars can be directly retrieved from the central database or imported from a HR or SAP system.
Batch production is supported; the administrator can programme the number of cards to be produced and allow the software to complete the job.
SECURENET v7 ARCHITECTURE

**Database Server (DS)**
- Stores system and cardholder configuration data, message & event logs
- Supports distributed database architecture
- Provides hot standby redundancy
- Continuous operation

**Quad Door Controller Unit (QDCU)**
- Connects field devices
- Supports multiple card technologies
- Contact or contactless
- Pin or biometrics
- External power driven (Max 1200m)

**Card Access Unit (CAU)**
- Card readers
- Supports multiple card technologies
- Contact or contactless
- Pin or biometrics

**Integrated Surveillance Management**
- Interface 3rd party system
- CCTVs, fire alarm, facilities bookings
- Command & control from single PC
- Hot-standby mode

**Remote Sites**
- Interface to administer
- Remote access to SecurNet
- 10 Concurrent authorized users
- Standard browser

**Supervisory Console (SC)**
- Monitors and control
- Window-based design
- Comprehensive graphical interface
- System configuration
- System monitoring
- Report generation

**Supervised Console (SC)**
- Monitors and control
- Window-based design
- Comprehensive graphical interface
- System configuration
- System monitoring
- Report generation

**Card Personalization Management**
- Advanced Multi-Factor Authentication (MFA) integrated with biometrics identification
- Robust system compliance to Singapore standard for Smart Card ID, SSD (53329)
- Reliable and scalable expansion
- Database with information stored securely on the smartcard

**CCTV Systems**
- Secured Key Management Systems
- Customer Specified Systems
- Fire Alarm Systems

**Optional**
- Database Server (DS)
- Quad Door Controller Unit (QDCU)
- Card Access Unit (CAU)
- ID Verification System (IVS)

**Primary Database Server**
- TCP/IP
- RS422
- RS485

**Secondary Database Server**
- External power driven (Max 1200m)

**Integration System**
- STAR Configuration
- Multi-Drop Configuration
- Add-On Modules
- Bio-Readers

**Remote Sites**
- Monitoring & Control

**Supervisory Console (SC)**
- Monitors and control
- Window-based design
- Comprehensive graphical interface
- System configuration
- System monitoring
- Report generation
ADVANCED CONTROLLER TECHNOLOGY

QUAD DOOR CONTROLLER UNIT
SecurNet Quad Door Controller Unit (QDCU) is a high capacity intelligent LAN-based door access controller with an intrusion alarm monitoring function.

This intelligent controller is powered by a 32-Bits Atmel ARM 9 Thumb-based microcontroller that supports DSP Instruction Extensions and Jazella® Technology for Java® Acceleration.

It incorporates 10/100Mbps Ethernet port for direct network connection and communicates downstream through RS422 to other optional modules or readers.

FEATURES
- Reset and shutdown functions
- Battery backup registers
- Clock generator and power management
- Advanced interrupt controller and debug unit
- Periodic interval timer, watchdog timer and double real-time timer
- Encrypted peer to peer communication using IPsec protocol

A complete standalone QDCU is equipped with a ARM9 central processing unit and 2x Dual Door Module (DDM) unit.

In its basic configuration, a QDCU can support a maximum of 8x access card readers and 7x optional modules as expansion.

An add-on module, SIO (Serial I/O module) with a QDCU can cater up to 224 alarm points and 56 digital output points through a daisy chain configuration.

This makes it an excellent field controller for intrusion alarm monitoring or any distributed security management applications.

INTELLIGENT POWER MANAGEMENT
QDCU offers a battery charging module (BCM) that:
- Provides continuous charging to the backup battery
- Monitors the power supply and alert on battery low-voltage
- Provides power status feedback to the central software

SYSTEM SPECIFICATIONS

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Doors Supported</td>
<td>Up to 4 doors or 8 readers using STAR topology</td>
</tr>
<tr>
<td>Up to 16 doors or 32 readers using Multi-Drop topology</td>
<td></td>
</tr>
<tr>
<td>Reader Operation Mode</td>
<td>Card, Card+PIN, Card+Biometric, Supervised Access, Dual-Badge Mode</td>
</tr>
<tr>
<td>Number of Input/Output Points Supported</td>
<td>224 Digital Inputs (DI) and 56 Digital Outputs (DO) at maximum 7x SIO modules per controller. Each SIO provides 32 Di and 8 DO</td>
</tr>
<tr>
<td>Peer to Peer Communication</td>
<td>With IP secured encrypted communication and without higher level applications</td>
</tr>
<tr>
<td>Standalone Mode</td>
<td>All functions are able to perform without disruption</td>
</tr>
<tr>
<td>Anti-passback</td>
<td>All events and data are stored in controller’s buffer</td>
</tr>
<tr>
<td>Self Diagnostic</td>
<td>In-built self diagnostic feature for quick trouble-shooting</td>
</tr>
<tr>
<td>Card Holder Capacity</td>
<td>Up to 200,000 holders using STAR topology</td>
</tr>
<tr>
<td>Up to 100,000 holders per door using Multi-Drop topology</td>
<td></td>
</tr>
<tr>
<td>Event Buffer Size</td>
<td>Up to 200,000 events can be buffered and stored offline</td>
</tr>
<tr>
<td>Number of Blacklist</td>
<td>Up to 100,000 blacklist holders</td>
</tr>
<tr>
<td>Number of Access Grouping</td>
<td>Maximum 1024 access groups</td>
</tr>
<tr>
<td>Holiday Definitions</td>
<td>In as many that can be defined in a calendar period</td>
</tr>
<tr>
<td>Time or Event Response Programs</td>
<td>Maximum 256 schedules, with up to 255 cascaded command sequence. Each command sequence consisting up to 24 actions steps</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Maximum 255 time zones, with each consist of 4 configurable start/stop time set</td>
</tr>
</tbody>
</table>

OPERATIONAL SPECIFICATIONS

- Star config. up to 8x readers per trunk (Max. 50m)

- Multi-drop up to 16x readers per trunk (Max. 1200m)

- Expand up to 7x add-on module (Max. 1200m)

- BCM, SIO/LAM, CAU, DDM

ELECTRICAL SPECIFICATIONS

- AC input: 90-260 VAC, 50/60 Hz (auto switching)
- Power Consumption: Max. 40VA
- Backup Battery: 12VDC, 7AH, Lead Acid Maintenance
- Built-in Charger: Charging Voltage: 13.8V, Full Charge Time: 4 hours

MECHANICAL PARAMETERS

- Standard Package: Housed in a lockable enclosure panel, each QDCU comes with 2x dual door modules, power supply and back-up battery included
- Dimension: 600 (H) x 400 (W) x 200 (D) mm
- Weight: 18 lbs (7kg)

OPERATING ENVIRONMENT

- Temperature: Storage: -25°C to 70°C, Operating: 10°C to 60°C
- Humidity: 5% to 95% non-condensing
CARD READER SPECIFICATION

SecurNet ST8100 series of in-house designed and built access card readers are unobstrusive in appearance and comes in variety of aesthetically pleasant housing. Featuring the latest card technologies, encryption algorithms, fast processing speed and high capacity it is meant to met user's requirement in the highest security environment.

OPTICAL ADD-ON MODULE

SERIAL I/O MODULE (SIO) FOR SERIAL I/O TERMINATION

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microcontroller</td>
<td>32 bits ARM7 Chips</td>
</tr>
<tr>
<td>Communication Ports</td>
<td>RS422 Connection (4 wire), Maximum distance 1200m</td>
</tr>
<tr>
<td>Onboard I/O</td>
<td>32x Line Supervised Digital Input, 32x Digital Output Relay</td>
</tr>
<tr>
<td>Onboard Display</td>
<td>7 segment LED for status indication</td>
</tr>
<tr>
<td>Dip Switch ID</td>
<td>4 Bits address</td>
</tr>
<tr>
<td>Onboard Power</td>
<td>12V DC / 1A</td>
</tr>
</tbody>
</table>

LIFT ACCESS MODULE (LAM) FOR LIFT ACCESS OPERATION

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microcontroller</td>
<td>32 bits ARM7 Chips</td>
</tr>
<tr>
<td>Communication Ports</td>
<td>RS422 Connection (4 wire), Maximum distance 1200m</td>
</tr>
<tr>
<td>Onboard I/O</td>
<td>32x Digital Input, 32x Digital Output Relay</td>
</tr>
<tr>
<td>Onboard Display</td>
<td>7 segment LED for status indication</td>
</tr>
<tr>
<td>Dip Switch ID</td>
<td>4 Bits address</td>
</tr>
<tr>
<td>Onboard Power</td>
<td>12V DC / 1A</td>
</tr>
</tbody>
</table>

Common Serial I/O Points

- Key Access
- EM Lock
- Break Glass
- Door Sensor
- Motion Detector
- Press to Exit

Lift Reader (Multi-Drop Configuration)

- Door #1
- 32x DORs
- 32x DORs
- 32x DORs
- 32x DORs

Max 4x LAMs supported

Power Supply

- 12V-DC, 180-280mA (Typical)

Operating Environment

- 0-70°C (Operating), -20-70°C (Storage), 10-90% Relative Humidity, non-condensing IP65