IDCUBE

COMMAND AND CONTROL APPLICATION

www.idcubesystems.com

SECURITY VIEW

Access 360

SECURITY VIEW

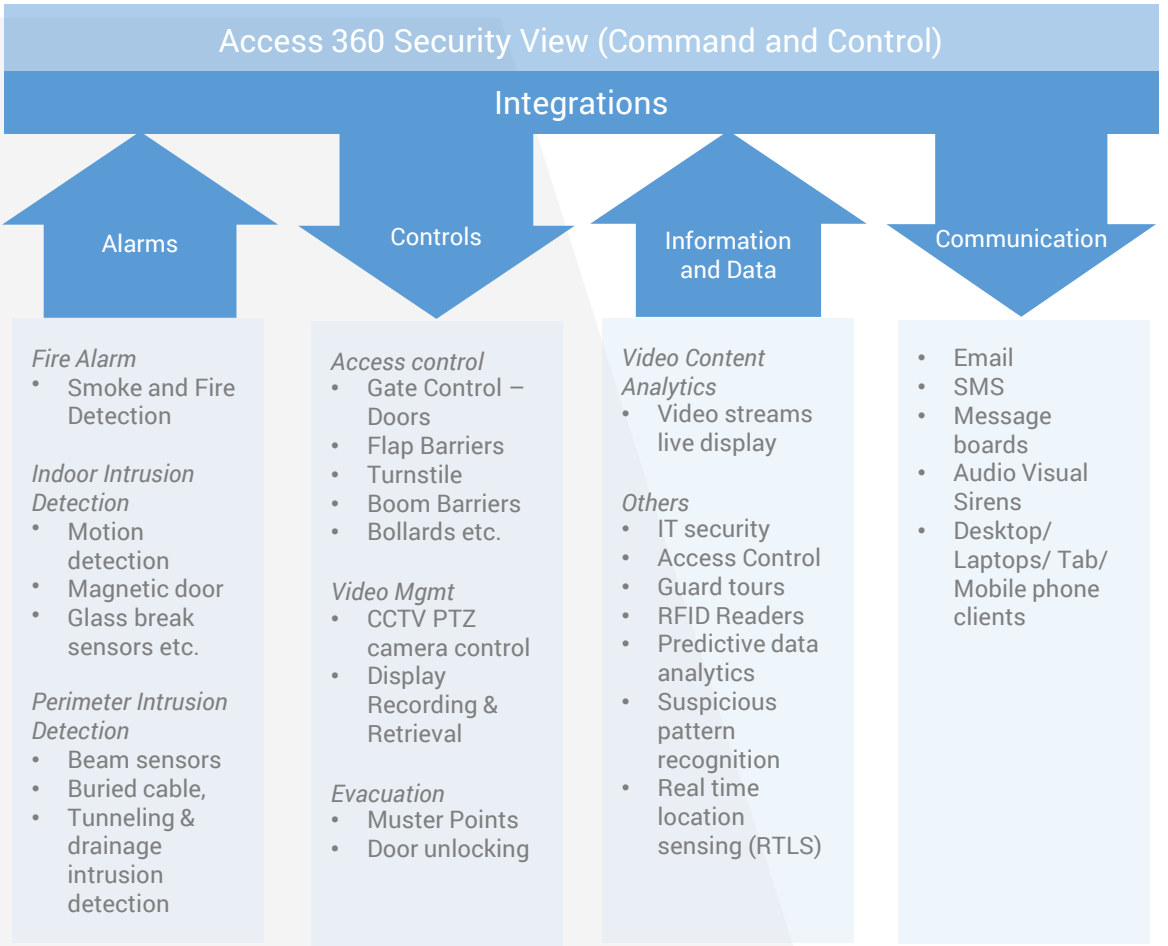
PRODUCT OVERVIEW

SecurityView is an open platform physical security command and control application, designed to deliver integrated and mission critical functionalities for use in varied organizations ranging from military infrastructures to commercial facilities. SecurityView has been developed based on the principles and norms of service oriented architecture (SOA). SecurityView utilizes variety of technologies to present information and guide response mechanism for an incident.

The application sits on top of best of breed security subsystems to correlate sensor inputs, video streams and access control events for reformative actions.

GUARD TOUR

Guard tour is an integral feature of SecurityView, using which the user can prescheduled guard trips. On each trip the guard is expected to cover checkpoints, located at particular distances. A reader is fixed at each of these checkpoints where the guard on duty must flash the allotted smart card.



The distance between these checkpoints must be covered within specific time, based on the actual physical distance between them.

For a guard tour, an administrator configures checkpoints to be covered, the sequence, guard credentials, the expected completion time between checkpoints and the time for the trip. If a guard does not complete a tour as defined then an alarm is raised in the real time. The system also provides the facility to generate guard tour reports.

ANTI-PASSBACK

Many organizations follow strict regulations to deal with tailgating. The anti pass back feature prevents misuse of access control system by preventing tailgating. The feature requires that for every use of the card at the “in“ reader, there is a corresponding use at the “out” reader and vice versa. The system supports all anti pass back scenarios such as global, local and timed. The anti-passback policy can be configured as either hard or soft.

DOOR SCHEDULING

The doors can be configured in 3 states - unlocked, locked and permanent-locked. In the unlocked state, the door remains open and the facility can be accessed by anyone. In the locked state, the doors can only be accessed by authorized users. Whereas, in the permanent locked state, even authorized users are not allowed to access the facility. Security view system allows the user to configure the door state schedule. For example, a banking facility may configure the door schedule for its main door as follows: During the public visiting hours (9am -2pm) the door is in unlocked state and remains open for public access. From 2 pm to 6pm, the door switches to locked state, wherein only the employees are allowed to access the facility. From 6 pm onwards the door switches to permanently locked state.

ARMING AND DISARMING OF ALARMS & SCHEDULING

The alarms and doors can be configured to switch the state from locked to unlocked to permanent locked or in any order, by entering a PIN. For example, a security guard shall disable the alarms by entering a PIN, when the vault is being opened and once the vault has been operated upon, the vibration/ motion sensor inside a vault shall be armed back by entering another PIN.

Schedules can be configured for the relays for applications such as light control, sensor activation and deactivation etc.

LOGICAL AREA CONTROL & HEAD COUNTS

The logical area control tool is used to divide the facility into logical zones based on access points such as offices of teams (operations, finance, R&D), server rooms, warehouses, security command centers etc. for easy determination of employees' location.

Forming logical zones help in identifying the head count specific to each zone. The feature is very helpful in identification of people during emergency evacuation. Each logical zone can be uniquely marked in graphical maps with different shapes and colors. The who's where report identifies the location of personnel based on logical zones.

MONITORING

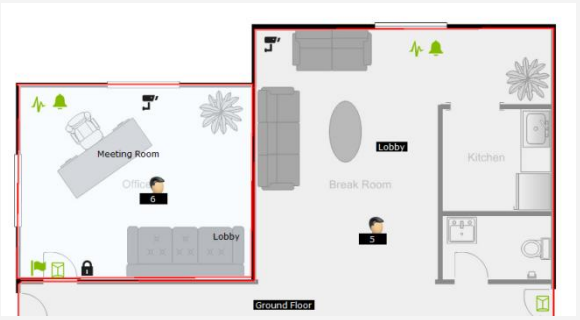
- **Devices Tab**: User monitors different IP based hardware devices such as controllers, readers etc., in real time using the SecurityView interface. The status and location of devices are tracked and offline devices are detected & indicated.
- **Doors Tab**: The user gets the current door status in real time, i.e., opened, closed, locked, unlocked, permanent locked, door forced, door held and tampered. The interface provides options to change the alarm status as well as the lock mode.
- **Input-Output (Sensor-Transducer) Tab**: The user monitors sensor inputs and corresponding outputs in real time. The system allows an administrator to configure automatic activation of certain transducers on state change of a sensor. The interface allows deactivation of certain transducers.
- **Events Tab**: An intuitive interface to view real time events, alarms and escalated alarms from a group of facilities. Detailed information on event type such as location of event occurrence, related branch/ facility, employees details, time of occurrence and acknowledgement (if required) are provided here.

  The interface allows the user to view alarms segregated into four categories, which are, Critical, Warning, Attention and Normal (as defined in the alarm management policy). By selecting a particular category (for e.g., Critical), all the alarms belonging to that category can be viewed.

  Color coding allows easy identification of these categories. The interface provides automatic pop ups for certain types of alarms or pop ups can be opened by clicking on an event. The pop ups allow a user to view associated videos at the

time of occurrence of an event along with the option to view live video streams from the same camera. The pop up also displays standard operating procedure (SOP actionable list) for the event. User may chose to acknowledge the event (if compulsory) and enter the remarks explaining the cause of the event as well as remedial actions. The pop up provides an option to deactivate an audio visual alarm associated with the event.
Overall alarm summary window summarizes the number of active alarms of different types. The interface also shows escalated alarms from other facilities for which it is configured as a parent branch.

- **Hawk Eye Tab**: It showcases detailed graphical representation of the entire physical security infrastructure, which includes facility drawings, logical zones, head counts, icons representing hardware equipments such as cameras, doors, locks, sensors and actuators. Each icon is a functional representation of the actual device, therefore provides real time status and operational capabilities.



MUSTERPOINT

Muster points are created to manage evacuation procedures during incidents such as fire, earthquake etc. Each card that is shown at the muster point is recorded. This in turn helps the security personnel or support staff in getting real time information on number of people who have safely evacuated and people still inside the facility.

ALARM MANAGEMENT

Alarm management allows the security administrators to define various alarm management policies . The policies are then mapped to various sources of alarms as per the level of criticality.

- **Alarm classification**: A new alarm policy is defined into the system and classified based on type (critical, warning, attention and normal). Other distinctive alarm features are added such as sound effect and duration.
- **Escalations and Notifications**: The alarm policy is further defined by appending escalation and notification policy. Various levels of escalation (1 to 5) ensure immediate action. Authority can be notified via emails, pop ups, SMS etc.
- **Alarm Response**: Here the alarm policy is appended by defining alarm response mechanism. For the policy, acknowledgement can be made

mandatory. In case an alarm is not acknowledged, the alarm gets escalated via email or SMS.

- **Policy Assignment/ Mappings**: The above defined policy is then mapped to various alarm sources as per the criticality.

INTEGRATIONS

- **CCTV Integration**: It provides integrated monitoring on occurrence of an event. It allows mapping of an access control event with corresponding video streams. For example, if deny access alarm is raised, the authority can directly access the corresponding video streams by a single click of the event.
- **Intrusion System Integrations/ Sensor Integration**: Advanced indoor and outdoor intrusion detection techniques involves sensors such as motion sensors, magnetic door sensors, glass break sensor, buried cable sensor, beam sensor etc. and actuators such as street lighting, audio visual strobes etc. Most of the sensors are meant to detect any unauthorized movements in a protected zone. Two types of sensor responses can be programmed into the system - *Soft Response* or *Hard Response*. In *Soft Response,* the SecurityView administrator is notified via pop up, email/SMS. The personnel may respond back by acknowledging the incident and entering the remedial actions performed.

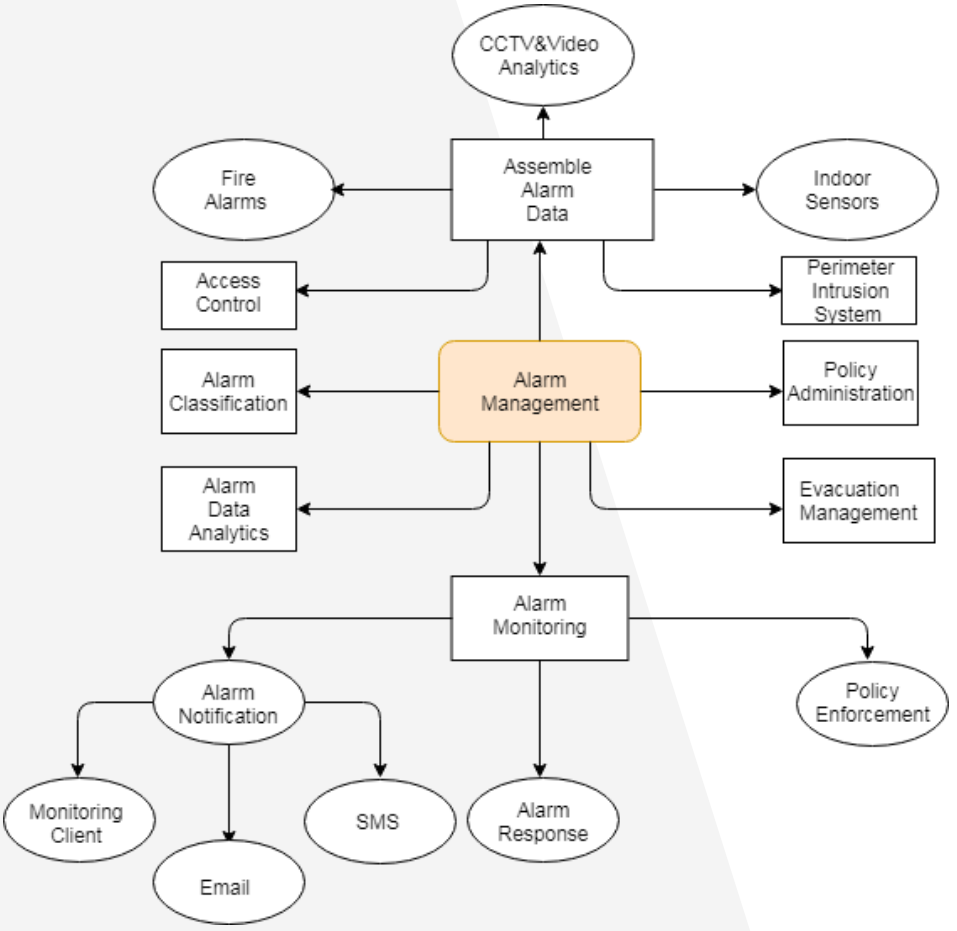
In *hard response* the actuator devices such as audio visual strobes are linked to the sensor inputs in the following ways

a. **Manual**: The strobes gets activated as soon as the sensor input is raised and can be deactivated only by the software. It ensures that the facility shall remain on alert till the security personnel confirms the safety.
b. **Timed Response**: The strobes remain activated for a specified interval of time on receiving the sensor input.
c. **Close on event close**: The strobe goes on as long as the sensor provides input to the system.
d. **Schedules:** The implementation of schedules along with I/O linking simplifies the management of even complex security scenarios. The security administrator may define a combination of actuator schedules as well as sensor input driven logic for its activation and deactivation. For example, the street lighting can be scheduled to automatically turn on during the night time and turn off during the daytime. Moreover the administrator can define the lighting to turn on whenever the light/ photo sensors detect darkness. The administrator further gets a single integrated interface for monitoring live status and to operate the devices.

- **Fire Alarm Integration**: SecurityView platform integrates with fire alarm system to meet the fire and safety procedures. Based on the requirements, there are two types of responses that can be programmed into the system - *Soft response & Hard Response*. In *soft-response*, a fire alarm is raised, the authority is notified via pop-ups, SMS/email. *Hard response* links doors to the system which is done in the following ways:

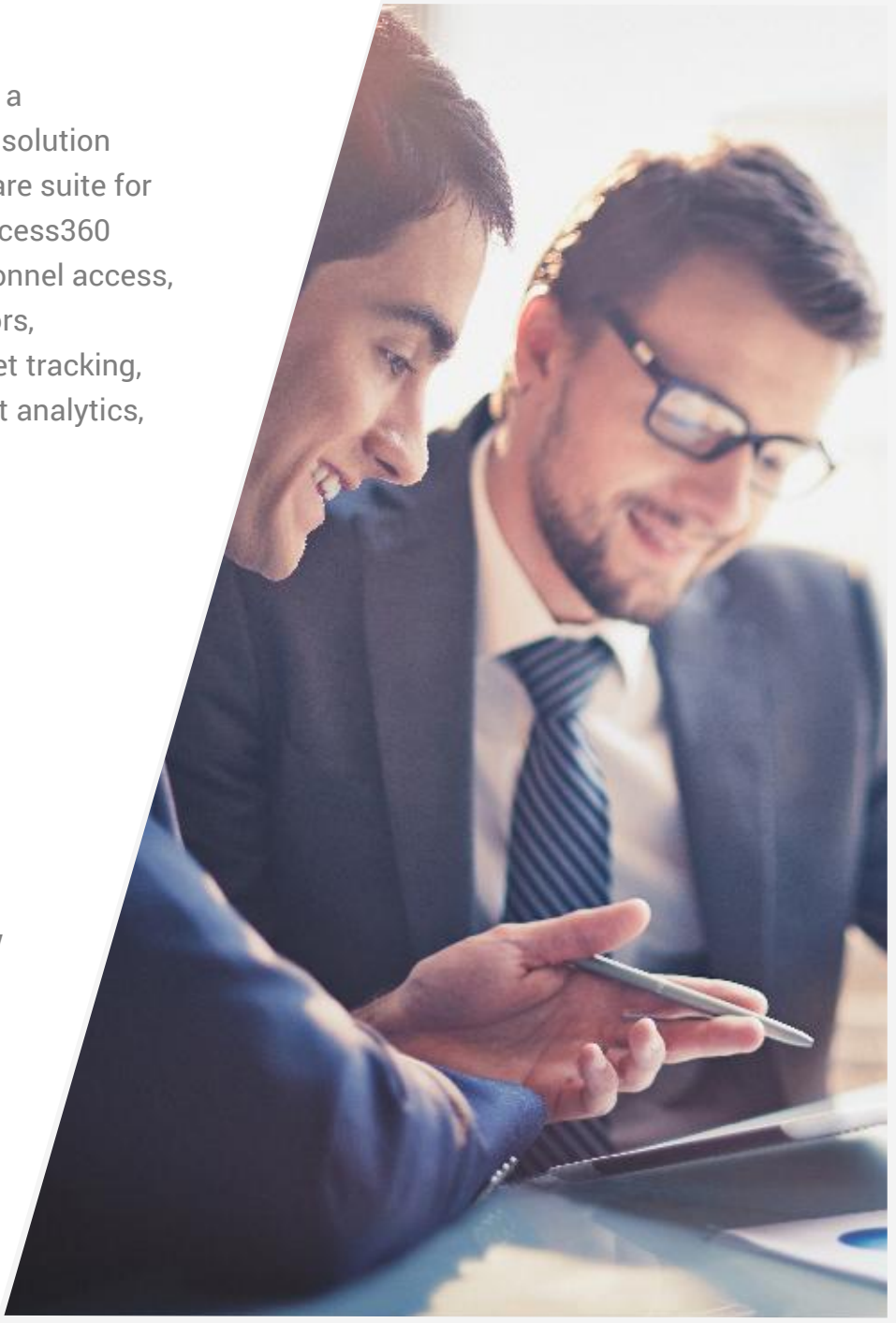
a. **Close on event close**: All the doors are opened when the fire alarm is raised and automatically closes as soon as the alarm is attended. The system is particularly useful in case of mock fire drills. In such scenarios, it is not necessary for the authorities to individually check each protected zone for anomalies. Hence, automatic closure of door is preferred.

b. **Manual close**: The doors open up as soon as the alarm is raised and are closed by the administrator through the software. It adds to the safety procedures, by ensuring that the doors are closed only after the facility is out of danger.



IDCUBE

IDCUBE is uniquely positioned as a comprehensive physical security solution provider via its Access360 software suite for organizations of all sizes. The Access360 platform helps in managing personnel access, vehicle access, attendance, visitors, contractors, cafeteria usage, asset tracking, video management, video content analytics, LPR/NPR and more



We are trusted by large businesses and SMEs across industries. We work with some of the most acclaimed global system integrators and solution providers. IDCUBE's distributor and channel partner network now has over 300 active businesses and this number is growing because of the opportunities our partners see in working with us.

INDIA

Corporate Office
B-19, Sector-2,
Noida- 201301
(U.P.) INDIA
Tel. : +91-120-4130715

Delhi
A-18, Kotla Village
Extension,
Delhi-110091
INDIA

Bengaluru
#20, 1st floor, 3rd Cross,
Malleshwaram,
Bangalore-560003,
Karnataka, INDIA
Tel.:+91-80-23564241/42

UAE

IDCUBE - FZE
Techno Hub 1 – Office G 042,
Dubai Silicon Oasis,
Dubai, UAE
Tel. : +971-555512541

Email: contact@idcubesystems.com | Website: www.idcubesystems.com