Security System Usage Scenarios

- Employees enter/exit a zone by swiping their ID card through the card readers located near the doors. In this case the building is treated as an entire zone. Cards carry a personal ID that must be matched to permission within the system.
    1. An employee swipes their ID card through the employee card reader located near the door
    2. The entry/exit sensor in the employee card reader scans the employee's personal ID from the ID card
    3. The system checks that the employee's appearance in the security camera monitoring the door matches the photo ID scanned from the ID card, that the card's ID number is active and registered in the employee database, and that the security level coded on the card matches that assigned to the zone
    4. If all the ID information checks out, the system deactivates the door lock
    5. The employee opens the door to enter or exit the security zone.
    6. The system records the name and ID info the the employee pulled from the ID card and the name/number of the zone that the employee entered/exited, along with the time of entry/exit

- Security guards on patrol swipe their ID cards through the checkpoint card readers placed along their routes
    1. A security guard on patrol swipes their ID card through a security card reader at one of the checkpoints along their patrol route.
    2. The security card reader scans the guard's ID card
    3. The system logs the time at which the guard swiped their ID card

- Security personnel use the control center to trigger an emergency evacuation upon detection of a fire
    1. A fire is detected by the sensors of the Security System
    2. The Personnel in the Control Center are alerted of the emergency.
    3. The Personnel in the Control Center trigger an emergency evacuation.
    4. Alarms are raised in the emergency areas notifying anyone in the area to evacuate
    5. All doors in the emergency area allow unrestricted exit but deny entrance.
    6. Once the emergency is resolved, the alarms are deactivated and all doors in the emergency area return to their normal state

- Security personal use the system to resolve Violations/Alarms/Events via keyboard and mouse
    1. The security personnel in the control center use the keyboard and mouse connected to (one of) the computer screen(s) in the control center to access the system
    2. The system displays a list of unresolved security violations/alarms

3. The security personnel access the information about a violation/alarm that was logged into the violation/alarm database by clicking on the type of the violation/event's name in the list
4. Once the information about the violation/event is accessed, a message is displayed under the information saying "This security violation/event is currently unresolved. Resolve it?", along with a choice to click Yes or No
5. The security personnel click Yes
6. Any emergency/lockdown override of the system caused by the violation/alarm that has been resolved is deactivated
7. The list of unresolved violations/alarms displayed on (one of) the computer screen(s) is decremented by one
8. The information about the violation/alarm prints a new message "This Violation/alarm has been resolved"
9. If all violations/alarms logged into the database are resolved, the system deactivates the alarm in the control center

- Security personnel in the Control Center retrieve the location history of security personnel or employees by entering a name or ID card information.

1. The security personnel in the control center enter an employee's name or the information on their ID card
2. The system displays the records of the zones that the employee has entered and/or exited, along with the times of those entries/exits

- Security personnel in the control center print the information of unresolved violations/alarms as they happen using the printer in the control center

1. Personnel accesses the security interface via a control center'(s) computer.
2. Personnel accesses interface for security violations/alarms (list of them)
3. Personnel accesses the information about a violation/alarm by clicking on its classification, i.e. break-in, fire/smoke detected, etc.
4. Personnel accesses the printer interface
5. The printer interface is displayed.
6. Personnel clicks the print button in the printer interface,
7. The information about the security violation/alarm is printed on paper

- The security personnel in the control center set/upgrade/downgrade security levels based on zone

  Set

  1. Personnel accesses the security interface via a control center'(s) computer.
  2. Personnel accesses interface for security zones (list of them, current security levels)
  3. If a security zone has no security level set for it, a message is displayed

next to the name/number of the zone saying “Universal Access”

4. The security personnel click on the message next to the zone ID
5. The system opens a page containing a scrollable list of all available security levels
6. The security personnel scroll to one of the security levels in the list and clicks it
7. A pop-up is opened that contains the message “Set Security Level?”, along with a Yes or No button choice
8. The security personnel click the Yes button,
9. The zone is assigned a security level

Upgrade/downgrade

1. Personnel accesses the security interface via a control center’(s) computer.
2. Personnel accesses interface for security zones (list of them, current security levels)
3. The security personnel click on the security level of a zone
4. The system opens a page containing a scrollable list of all available security levels, with the current security level of the zone being highlighted
5. The security personnel scroll to another security level to another and clicks it
6. A pop-up is opened that contains the message “Change Security Level?”, along with a Yes or No button choice
7. The security personnel click the Yes button
8. The zone’s security level is changed, which relaxes or tightens access restrictions to the zone based on the security permission on employee ID cards

- The security personnel in the control center issue, reissue, and terminate ID cards

Issue Card

1. The security personnel in the control center access the security system interface via the keyboard and mouse connected to (one of) the computer screen(s) in the control center
2. The security personnel in the control center enter the name, photo ID, and required security permission for a new employee into the system
3. The employee’s ID information is entered into the employee database
4. The system processes the ID information and assigns the employee a unique ID number
5. The system prints a physical ID card for the employee.

Terminate Card

1. The security personnel in the control center access the security system interface via the keyboard and mouse connected to (one of) the computer screen(s) in the control center
2. The security personnel access the interface for employee ID cards (list

of them)

3. The system displays a list of employee names and the ID numbers of their ID cards
4. The security personnel select the employee name and ID number of the ID card to be terminated
5. The system opens a page containing the ID information on the employee's ID card. This includes the employee's name, photo ID, and current security permission for accessing security zones, along with a button to deactivate the card
6. The security personnel press the button to deactivate the employee ID card
7. The security personnel access the employee database and remove the employee ID information

Reissue

1. The security personnel in the control center access the security system interface via (one of) the computer screen(s) in the control center
2. The security personnel access the interface for employee ID cards (list of them)
3. The system displays a list of employee names and the ID numbers of their ID cards
4. The security personnel select the employee name and ID number of the employee ID card to be terminated
5. The information on the employee's ID card is displayed on (one of) the computer screen(s) in the control center. This includes the employee's name, photo ID, and current security permission for accessing security zones, along with a button to deactivate the card
6. The security personnel press the button to deactivate the employee ID card
7. The security personnel access the employee database and remove the employee ID information
8. The security personnel in the control center enter new employee ID information into the Security System
9. The new employee ID information is entered into the employee database
10. The system processes the information and assigns the employee a new ID number
11. The system prints a new ID card for the employee

- Security personnel in the control center add, change, or remove security zones

    Adding zone:

    1. Personnel accesses the security interface via (one of) the computer screen(s) in the control center

2. Personnel accesses interface for security zones (list of them, current security levels)
3. The interface displays a list of options for adding, changing, updating, and removing security zones.
4. Personnel selects the option to add a zone.
5. The interface provides the personnel with a form listing the elements required to add a zone. (Note: Elements include area, initial security level, associated control center)
6. Request for additional information is sent to the Head of Security.
7. Once sufficient information is provided, and if the request is granted, a zone is added to the system.

Changing zone:

1. Personnel accesses the security interface via (one of) the computer screen(s) in the control center
2. Personnel accesses interface for security zones (list of them, current security levels)
3. The interface displays a list of options for adding, changing, updating, and removing security zones.
4. Personnel selects the interface option of changing a zone.
5. Interface provides personnel with a form containing the elements required for a zone change. (Note: Elements include area and the optional choice of changing the zone's control center)
6. The change request is sent to the Head of Security.
7. Once sufficient information is provided, and if the request is granted, the system changes the zone.

Removing zone:

1. Personnel accesses the security interface via (one of) the computer screen(s) in the control center
2. Personnel accesses interface for security zones (list of them, current security levels)
3. The interface displays a list of options for adding, changing, updating, and removing security zones.
4. Personnel selects the interface option of removing a zone.
5. Interface provides personnel a form with a button for removal.
6. Request for removal is sent to the Head of Security.
7. Once sufficient information and reasons are provided, and if the request is granted, the system removes the zone.

- Security personnel in the control center trigger a lockdown event override of the system that allows expansion and contraction of the lockdown to prevent the escape of perpetrators
    1. The Security Personnel initiate a security lockdown of the system after a major violation of security.

2. Based on parameters of the event, the system locks down all doors and windows in the violated zone, or an enclosing zone determined by the Security personnel
3. After the violation has been resolved, the Security Personnel resolve the lockdown from the Control Center, returning all of the doors and windows to their original state before the lockdown.

- Security personnel in the control center trigger an emergency event override of the system that allows evacuation from the affected zone(s).
    1. A fire or other emergency is detected by the sensors of the Security System
    2. The Personnel in the Control Center are alerted of the emergency.
    3. The Personnel in the Control Center trigger an emergency evacuation.
    4. Alarms are raised in the emergency areas notifying anyone in the area to evacuate
    5. All doors in the emergency area allow unrestricted exit but deny entrance.

- Security personnel in the control center deactivate an emergency or lockdown event override using a password
    1. After an emergency is resolved, the Personnel in the Control Center enter the override password in the system with the keyboard.
    2. System verifies the override password.
    3. The Security Personnel deactivate the emergency event override.
    4. Alarms are deactivated and the system resets to a monitoring state

- Security personnel in the control center pause active patrols to prevent activation of a security violation/alarm if one or more security guards on patrol report an anomaly via radio
    1. A security guard notices an anomaly and reports it to the control center.
    2. The security personnel in the control center pause the patrol of the guard who reported the anomaly. This prevents a security violation or alarm from being activated if the guard is late to their next checkpoint after investigating the anomaly.

- Unauthorized user triggers a break-in event, either by triggering a Window Sensor or Door Sensor Alarm
    1. Unauthorized User forces or breaks open a window or door that is monitored by the security system
    2. The window/door sensor detects the break-in and raises the appropriate alarm.
    3. The system notifies the security personnel in the control center and logs the event to the database