www.innerrange.com

inner range

Intelligent Security Solutions

A Beginners Guide to Inner Range Systems

Inner Range manufactures a range of integrated Intrusion Detection and Access Control systems to cover sites of any size, while sharing a common configuration layout. Before configuring one of these systems, it is important to first establish the fundamentals of Inner Range's Intrusion Detection and Access Control systems.

Intrusion Detection

The intrusion detection system is made up of three parts; Inputs, Areas and Process Groups. These are all required for the identification and processing of an intrusion event. For intrusion detection to work correctly, an input is programmed into an area and assigned a process group.

Inputs (Zones)

An input can be any switch, button or detector that is physically wired to a controller or one of its expansion modules. The controller monitors these inputs for state changes such as alarm (also known as unsealed), tamper or seal. An input communicates changes to its current state by changing the resistance in the circuit. The set of resistors are called End of Line resistors.

There are also logical inputs called system inputs, these inputs monitor a particular condition such as AC Fail, Cabinet Tamper and many others. System inputs are also programmed into an area and assigned a process group.

Wireless inputs can also be used, including motion detectors, door contacts and smoke detectors. These work in the same way as hard wired inputs, with the addition of reporting when their battery is low.

Inputs can be programmed into one or more areas, however, it is common that an input only serves a single purpose.

Areas

An area is a collection of inputs that are grouped in some way. An area commonly represents a physical location, such as all the inputs in a board room. Alternatively, it could also represent all duress buttons in a building. When an area is armed (turned on), the controller will process the state changes of inputs, this processing is based on the process group assigned to an input within the area.

A site can be represented by a single area covering the whole building, or can be broken up into numerous smaller areas if more granular control is required.

An area can be programmed with an entry or exit delay to allow it to be armed or disarmed (turned on or off) without generating an alarm. The area is programmed with the siren and strobe outputs it can control and can be configured to auto-arm to ensure the inputs are being monitored.

Process Groups

For an input to be monitored by the system, the input needs to be programmed into an area and be assigned a process group. The process group defines how the controller responds based on the input's state changes and determines if any sirens need to be activated (including which tone to play) and if any communication with a monitoring station is required.

In normal operation, most process groups will only react if the area the input is assigned to is armed. However if, for example, a detector input is tampered with then the process group will react regardless of the area's arm state.

An input can be isolated to temporarily disable the monitoring of state changes, this is commonly used when a detector is faulty or an input is in alarm whilst an area is being armed.

Access Control

The access control system combines access control modules, doors and card readers to restrict users from accessing certain areas within a building.

Doors

An access control door is any electronically controlled obstruction such as a door, auto door, roller door or boom gate that restricts a person or vehicle from entering a particular area. When a door is wired to the controller or other modules, the lock state of the door is determined by the controller. In some cases, the door may be configured to automatically unlock during normal working hours and relock after hours. Users can also unlock doors by providing a credential such as a card or a PIN number at a reader. Access to a door also requires that the user has the appropriate permissions to enter/exit the door.

The controller is capable of monitoring the status of door inputs such as a door reed or tongue sense to determine if a door is open or closed, or if the lock is functioning correctly. This allows the controller to know if the door has been forced open or has been held open too long.

Readers

The card reader is an access point that a user interacts with to unlock a door. Depending on the door there may be a reader on either side or on both sides of the door. A door with only a single reader is restricting access from only one side of the door and usually, can be exited by using the door handle or a Request to Exit (REX) button. Doors with readers on both sides are generally used when knowledge of a user's location is important or both the inside and the outside of the door are restricted, such as airlocks in a hospital or in car parks. The access control system supports a range of reader technologies such as Inner Range SIFER, Wiegand and keypad readers.

DOTL

DOTL or Door Open Too Long (also known as Door Held) is a state where a door has been unlocked and opened, then not securely closed within a particular period of time. DOTL is used to ensure that users close the door properly after use. Prior to entering the DOTL state, a local audible warning tone can be generated to draw a persons attention to the open door, allowing them some time to close the door securely. If the warning time expires and the DOTL state occurs, it will result in a DOTL input going into alarm. This can be reported to a monitoring station to ensure someone knows the door has not been shut properly, or that there is a fault with the door or the lock.

Door Forced

The Door Forced state occurs when a door is locked and secured, but is then opened. The controller uses the door reed switch and/or the tongue sense to determine if a door has been opened/unsecured. If this occurs when the door should be locked, the controller sets a Door Forced input into the alarm state which can be reported to the monitoring station. This behaviour means the door forced state can be monitored directly, without needing to temporarily isolate (also known as shunt or bypass) the door inputs for standard day to day activity.

Integrated Systems

The controller combines the Intrusion and Access Control systems in a number of ways.

Door Follows Area State

The “door follows area state” functionality allows an access controlled door to lock and unlock based on an area being armed or disarmed. Door programming provides options to specify the area located on the inside and the outside of the door. Once linked to an area, the door can be configured to follow that area’s state. This could be either the area on the inside or outside of the door.

The door follows area state functionality can combine with Free Access Time Periods, which are periods of time that can be configured to automatically unlock and relock a door. This combination allows free access through the door between fixed hours, but only after someone has disarmed the area.

Area Disarm on Entry

When a user presents their access card at a reader to enter a door that has an armed area on the other side, if the user has permissions to access the door AND to disarm the area, then the area can be programmed to automatically disarm. This is used to reduce the number of steps needed to enter a door as the user does not need to disarm the area from a keypad after entry.

Restricting User Access

When a user presents their access card at a reader to enter a door that has an armed area on the other side, if the user only has permission to access the door and NOT to disarm the area then user will be denied access to the door. This is commonly used when certain people, such as a supervisor, needs to enter the area before others. The supervisor will be the only user provided the permission to disarm the area. Once the inside area is disarmed, any user with permission to access the door can present their access card at the reader and unlock it.

3-Badge Area Arming

Three badge arming allows the user to arm an area by presenting a card at a reader three times within a short period of time. The area that is armed by 3-badge arming can be either the area on the other side of the door or all areas within the system.

Users and Permissions

The user and permission programming determines who can interact with the system and how much control they have for items such as doors, areas or outputs.

Users

A user is any person that will interact with the Intruder Detection and Access Control system via a keypad, access control reader or the web interface. Every user will have one or more credentials and some permissions.

Credentials

To identify which user is interacting with the system each user requires unique credentials. Credentials include a security PIN for interacting with an LCD terminal, cards for accessing doors and may include a username and password for access to the web interface or software.

Permissions

A user with a credential may be able to interact with the system. However, without the appropriate permission, they will not be able to control areas, doors or outputs. Permissions are assigned to users, with a “What and When” structure. The What field allows for the assignment of a door, area or output, describing what the permission lets the user control. The When field is used to conditionally qualify when the user is allowed to control the What item. This offers the flexibility to provide a user access to a door only during working hours, for example.

Area Permissions

In addition to the flexibility of the What and When fields for permissions, the area can provide specific control options to allow the user to only arm or disarm the area. The arm only control of an area can be provided to users to ensure that if they were the last person onsite, they could arm the entire building.

Door Permissions

Assigning a user permission to access a door will mean that if they present a credential at a reader, the door will unlock for a short period of time.

Permission Groups

A permission group is a collection of permissions that can be assigned to one or more users. Many organisations have an internal structure where users share similar roles, for example, warehouse staff. It is easier to assign a single permission group to all the warehouse staff, instead of adding individual areas, doors or outputs on a per user basis. This means any changes can be made directly to the permission group, instead of manually making the change to each user. Users can have a number of permission groups assigned to them, in addition to individual items offering complete flexibility.

A permission group can contain items such as doors, areas, outputs and even other permission groups. The combination of permission groups makes complex site permissions much easier to maintain.

Glossary

Access Control - The selective restriction of access to a place or other resource.

Alarm - The state of an input when it is in an abnormal condition (not sealed).

Area - A grouping of inputs that can be armed or disarmed.

Armed - An area that is turned on and is monitoring the state of its inputs.

Closed - A door state that indicates the door is not open, the closed state is determined by the door reed and/or tongue sense.

Controller - The electronic component that provides the smarts for the Intrusion Detection and Access Control system. This is the central part of the system that processes and responds to the information received from all devices in the system.

Credentials - A unique identification that a user provides to interact with the system. This can be a security PIN, card or username and password.

Detector - A device that identifies a stimulus and communicates its alarm, sealed and tamper states to the controller via a change in End of Line resistance.

Disarmed - An area that is turned off and is not monitoring the state change of its inputs. A disarmed area will still monitor for the tamper state.

Door - An access point in a system that can be programmed to provide and restrict access to users as required, and monitored for abnormal conditions.

Door Forced - A system input for each door to indicate when a door is locked and has been opened without a valid unlock command.

Door Reed - A magnetic field detector that is used to detect the status of a door/window etc.

DOTL - Door Open Too Long (also known as Door Held). A system input for each door to indicate when a door is held open for too long.

End of Line - A pair of resistors that are wired to a detector that are used by the controller to identify the state of the detector.

Entry Delay - The duration of time that a user has to enter an area and disarm it without generating an intruder alarm.

Glossary

Exit Delay - The duration of time that a user has to exit an area after arming it without generating an intruder alarm.

Input - An input is either a switch, button or detector that is physically wired to a controller or one of its modules or a logical (non-physical) system process to be monitored.

Isolate - Inputs can be placed in the isolated state, where all state changes are ignored. Isolation can be temporary with the input automatically de-isolating when the area linked to it is disarmed, or persisted, requiring a user to manually de-isolate it. Persisted isolation is commonly used for faulty detectors or those undergoing maintenance, while temporary isolation can allow an area with unsealed inputs to arm successfully.

Open - A door state that indicates the door is not closed, the open state is determined by the door reed or tongue sense.

OSDP - Open Supervised Device Protocol – An alternative protocol to Wiegand, offering better security and easier installation over a bus interface, allowing multiple readers to be attached to the same cable.

Permissions - Authorisation granted to a user to interact with the system.

Process Groups - Options that define how input state changes will be processed.

Reader - A control point to access doors.

Reed Switch - An electronic switch operated by a magnetic field. Often used to determine if a door is open or closed

Seal - The state of an input when it is in a normal condition (not in alarm).

SIFER - An Inner Range multi-drop RS-485 and OSDP based reader that uses smart cards.

Tamper - The state of an input that has been tampered with.

Tongue Sense - A switch found in the electronic lock assembly of a door that is used to determine if the door is closed securely.

Wiegand - A data protocol used in proximity and smart card readers.

For more information, visit www.innerrange.com

Australia

Inner Range Pty Ltd
1 Millennium Court Knoxfield, Victoria, 3180, Australia
Tel: +61 3 9780 4300
Fax: +61 3 9753 3499
email: admin@innerrange.com

Europe

Inner Range (Europe) Ltd
Units 10 & 11 Theale Lakes Business Park Moulden Way,
Sulhampstead Reading, Berkshire, RG7 4GB United Kingdom
Tel: +44 (0)845 470 5000
Fax: +44 (0)845 470 5001
email: ireurope@innerrange.co.uk

SIFER is a registered trademark of Inner Range Pty Ltd.
This document is intended for background information on Inner Range systems only, and is not a replacement for training and certifications. Whilst every effort has been made to ensure the accuracy of this manual, Inner Range Pty Ltd assumes no responsibility or liability for any errors or omissions. Due to ongoing development the contents of this manual are subject to change without notice.
Part Number: 630000 February 2016