Honeywell

# Intelliguard

# 5800/5900/5924

# Application Guide

*"C" Version and "DSCC" Version Update*
*January 1997*

**HOME & BUILDING CONTROL**
**Security Monitoring**

# Introduction

# Introduction

## What this guide is intended to provide

This guide is a supplement to the Intelliguard 5800/5900/5924 Application Guide (form #56-5016) from October 1993. Only changes to the original product information are presented here. If a particular feature or module is not addressed it infers that there have been no changes and the original information is still relevant. Therefore this guide cannot standalone and requires that you have read or reviewed the original Application Guide for a complete understanding of the product.

## Who should use this guide

This guide is written for anyone involved in delivering the Intelliguard 5800/5900/5924 to our customers. This guide is aimed at a diverse audience of both operations and sales people. This is the primary reference for sales people for learning the operation and application of the products. Operations personnel should use this as an introductory guide in conjunction with the Intelliguard 5900 Operation and Installation Manuals (Radionics #74-07629-000) and the Intelliguard 5900 Program Entry Guide (Radionics #74-07624-000).

If you have further questions about Intelliguard, contact your Radionics Area Representative at 800/538-5807 or Bruce Addleman, Product Marketing at 612/951-3668.

## The Market

Intelliguard Entry Control has many benefits, chief among them is that it can reduce false alarms due to user's who are unfamiliar with the operation of the security control panel, since entry control is designed to disarm the appropriate portions of the security system as well as allow access. Other benefits include many of the same associated with more traditional access control systems including reducing the cost of re-keying locks and accountability.

Intelliguard Entry Control also addresses the lower end of the access control market we don't participate in very well due to the high initial cost threshold associated with standalone access control systems. Because the platform for the fire and security system is also used for Entry Control the cost of the first door is roughly equivalent to the average cost per door of larger systems.

As has always been the case with access control, customers find many other ways to use access control once they have gained some experience. The simple integration and low cost of Intelliguard Entry Control will provide a progression to our traditional access control market. Every Entry Control customer will likely eventually become an access control customer as well.

The integration of products from Radionics and Westinghouse Security Electronics supports our strategy for partnering with a single vendor in these markets and to differentiate existing product for the benefit of our customers.

## Tailored Security

The concept of Tailored Security was first introduced along with the 5800/5900 in 1993. Your challenge, still, is to identify the features that your customer needs to assist them with their business situation. Your opportunities to Delight the Customer come from simple but elegant solutions. To that end you must strive to Tailor the Security system and to take advantage of the flexibility these products provide. While the concept has not changed, the fact that the new product features further the ability to provide Tailored Security suggests that, it is worth redefining here.

Tailored Security is really all about understanding customer requirements. When a customer describes their needs and concerns, they are doing so because they have an expectation that you can fulfill those needs and address their concerns. The Intelliguard 5800/5900 allows you to optimize the security system to work the way your customer operates their business. To do this you must fully understand your customers operation and expectations. Providing the customer with a system that works, the way they want, is the major feature of the 5800/5900. This guide will explain how.

## Exclusives

Below is a list of the exclusive features from the original product and any comments regarding their relationship to the Radionics product.

1. **Shared Areas** automatically turn on and off when other adjacent areas are armed and disarmed. That means to you easy access through common hallways or vestibules without creating false alarms. *Area types are now available in a number of products including the Radionics versions.*
2. **Master Areas** that cannot be armed until other critical areas are armed. This provides assurance that important areas such as a safe or vault are armed before the main system is armed. *Area types are now available in a number of products including the Radionics versions.*
3. **Passcode Access** means that a passcode must be entered before any command can be initiated. This means higher security because it prevents unauthorized or inadvertent use of your security system. *New versions of the Radionics products can be programmed to require a passcode to access the function menu.*
4. **Invisible Walk Test** that lets you test hold-up buttons or moneyclip traps before a store or bank opens for the day. What this means to you is assurance that your protection is working.
5. **Latest Closing Time** that limits how late a user can extend their closing time on systems with supervised closings. This ensures that employees will stay no later than the time you set.
6. **Changing Armed States** that lets you move from perimeter to master arm (or vice versa) without having to disarm. This makes it quick and easy to completely arm your system at night when you have been working with the perimeter protection on. *This feature is available now in the Radionics versions which include access control, however only from the card reader. A card can cause the area security to change to Perimeter from Master.*
7. **HSL Transmitter** that communicates alarms on closed window multiplex networks. That means to you the highest level of transmission security possible.

### New Exclusives

1. The ability to **execute a custom function from a credential reader** allows a customer access to complex commands without a lot of training. Custom functions might be used for environmental control such as turning on lights and ventilation controls or it might be used to establish a specific security routine.
2. **Westinghouse Security Electronics digital proximity reader** provides Honeywell customers with a industry leading access control technology and allows easy integration between access and security systems.

## Version Comparison

This chart shows the main differences in feature sets. Only new or changed features are shown. See the original application guide for other features. The new features are explained in detail in this guide.

| Feature | 5800DSCC | 5900DSCC | 5800C | 5900C/5924C |
|---|---|---|---|---|
| Annunciation | 48 points (8 on-board and 40 off-board | 134 points (8 on-board and 126 off-board) | 74 points (8 on-board and 66 off-board | 245 points (8 on-board and 237 off-board) |
| Passcode Capacity *assumes 5800 programmed in PS6 as a 5900 | 76 (PS6=25*) | 99 (PS6=70) | 100 (PS6=70*) | 250 (PS6=70) |
| Maximum number of D9210 Access modules | 0 | 0 | 4 | 8 |
| Credential Users includes sub-users | 0 | 0 | 400 | 1000 |
| Scheduled events | 17 | 17 | 64 scheduled events 40 if Windows enabled | 64 scheduled events 40 if Windows enabled |
| Event logger | 500 events | 500 events | 800 events | 800 events |
| Printers | 1 | 3 | 1 | 3 |

# Section One
# System Architecture

# Section One - System Architecture

## Basic Components

### Control/Communicator

#### "C" Version

The enhanced Intelliguard 5800, 5900 and 5924 are implemented on a new hardware platform that provides additional memory required to support the enhanced feature set. This new platform looks the same and provides the same terminations and connectors as it's predecessor. The 5800, 5900 and 5924 still differ only in their configuration of features and capacity. The product that supports the increased Capacity and enhanced features, specifically Intelliguard Entry Control, is identified as the "C" version.

#### "DSCC" Version

This same platform is being used for the 5800DSCC and 5900DSCC. This software variation was created to interface with the Honeywell Security Link transmission device known as DSCC (DSAS to SDI Communication Card). The DSCC was previously available only with the Intelliguard 5700 which ceased production in 1995. The 5800DSCC and 5900DSCC do not provide the enhanced features of the "C" version. They retain the features and capacity of the original version (B1). This variation, while not ideal, was created so that the "C" version would not be delayed by further development and so that we could have a current platform to support DSCC. This trade-off recognizes the diminishing role of HSL but also provides an opportunity to update the thousands of loyal HSL customers if required by competitive pressures.

The comparison chart in the introduction section provides the details of each of these new offerings. The only way to tell them apart is by their label. Review the original application guide (56-5016) for details about the capabilities and capacities associated with the DSCC version.

#### Packages

The configured packages that match the Business Alarm Price Book and the National Purchasing Manual shipped after introduction will be the "C" version. Previous version control/communicators will be available only as individual replacement components. If your branch has been ordering components instead of the configured packages, ensure that your orders reflect the appropriate control/communicator in lieu of the B1.

These same packages are available as the "DSCC" version by using a -DSCC suffix when ordering.

### Control Centers

The existing control centers work with all versions of the Intelliguard 5800/5900/5924.

## Expansion Modules

Expansion modules are used to increase the capacity of the control unit. They are generally mounted inside the control unit enclosure, which has room for 6 modules. Additional Expansion modules can be put in a separate enclosure, usually next to the control unit. Use the Power Requirements Chart in Section Five to determine if you must add additional power to accommodate the Expansion modules.

### Point Terminal (D9127)

This is an updated version of the POPIT (Point of Protection Interface Terminal). The D9127 provides increased addressing capability to support the new point capacity of the 5800 and 5900 "C" versions. D9127s can be used on all earlier systems supporting POPITs except the 5700/7112. Installations may include both the D9127 and the original D8127 POPIT, even on the same backbone (D8125 POPEX Module).

## OctoPOPIT Module (D8128C)

The OctoPOPIT module has also been updated to coincide with the increased point capacity of the 5900C. Like the POPIT, it may be used on all earlier systems supporting POPITs.

## Access Control Module (D9210)

The D9210 Access control module is the interface between the control/communicator and one reader controlled door. It is connected to the control/communicator via the SDI (keypad wire) like a control center. It may be placed within the same control/communicator enclosure like most other expansion modules. It may also be located anywhere within the protected premise in a remote enclosure, however it must be located within 2000' (wire distance) of the control/communicator when used with 22 AWG wire. The module is supervised so that a loss of communication between the module and the control/communicator will be annunciated. The D9210 can receive 12 vdc power via the SDI, which may be appropriate for smaller systems however, like a control center, it can also be powered from a standalone 12 vdc power supply.

The D9210 supports standard 5-wire, 26 bit Wiegand protocol data communications from the reader. The reader may be any technology as long as it communicates using a Wiegand protocol. Reader wire is limited to 300'. It is possible, depending on the current draw of the reader, to parallel two readers on the same door used for in/out control. Both readers will operate as one. There will be no control or indication of the direction the person was going. The D9210 also interfaces the other devices associated with the reader controlled door including;

- the electric locking device - a SPDT, dry contact, plug-in relay (D136) rated 2A @ 24 vdc
- the door contact - a supervised input with a 1000 ohm end of line resistor like an on-board point
- a request to exit and a request to enter device - normally open input, close to activate
- a 12 vdc voltage output for a buzzer - active on access granted and door left open

*Note:* The electric locking device at the door should be powered from a standalone power supply (either 12 or 24 vdc). It may be possible to power the D9210 and provide minimal 12 vdc lock power for a small system with a single access control module. You must use the Power Requirements Chart to determine if there is enough auxiliary power available from the control/communicator and to assess the impact on battery standby time.

## D9210 Configurations

The D9210 is available in several configurations providing options regarding mounting locations and power requirements.

- D9210BLCH - the module only, intended to be mounted within another enclosure like the control/communicator. (**B** = B version, **LC** = less can, **H** = Honeywell)
- D9210BH - the module mounted in a small (wiring room only) enclosure, ideally located at or near the controlled door to minimize the wiring between the door and the control/communicator.
- D9210BCH - a single module mounted on a skirt with a 1 amp 12/24 vdc power supply with plug-in transformer (battery(s) not supplied), mounted in another 5591(not the control) enclosure, also ideally located at or near the controlled door. The skirt has room for a second D9210BLCH and additional D9210BLCH modules can be mounted to the sides of the enclosure for a centrally wired and powered, multiple door system.

## WSE 4205W (Wiegand) Credential Readers

The reader recommended and fully supported is the WSE 4205 Wiegand digital proximity reader, available in indoor, indoor glass mounting and outdoor versions. The NexKey (card) and KeyMate (keychain token) are the same used in all WSE digital systems. These readers are currently exclusive to Honeywell and represents a significant commitment on the part of Radionics and WSE to our partnership which enables you to offer your customers an integration of premier products.

The D9210 will support most standard 26 bit Wiegand protocol readers. Readers are available from Radionics in a variety of technologies including ReadyKey, (which is proximity) Dorado magnetic stripe, Sensor Engineering Wiegand , Essex BFSK weatherproof keypad and HID proximity.

## Accessory Modules

### Dual Phone Line Module (D928)

The D928 replaced the D128 shortly after initial introduction in 1994. The D928 has the same features as the D128. It resolved issues with the D128 supervisory switching being heard during the customers telephone conversations.

### Printer Interface (D9131A)

The firmware of the printer interface has been updated to support the new messages of the "C" version panels. Existing D9131s can be upgraded by contacting Radionics Order Processing and requesting the D9131A Update Kit. An example of access messages can be found in section 2, Features.

### Power Supply/Battery Charger Module (D9142)

This 4 amp power supply is UL listed both as a supplemental power supply to provide added standby battery capacity, like the D8132, and as a standalone power supply.

## Communications Modules

### Honeywell Security Link (HSL) Transmitter Module (DSCC)

The DSCC module is only compatible with the 5800DSCC, 5900DSCC and 5924DSCC. It is not compatible with the "C" version panels which means that it will not work with systems which require the expanded capacity or entry control features. The chart in the introduction of this guide shows the capacity and features of the DSCC control/communicator models. The DSCC module is also not compatible with earlier versions of the 5800/5900/5924.

HSL provides Grade AA line security over a closed window multiplex network. Closed window networks provide an isolated path of communication to prevent interference from other transmitters on the same network and to find network problems quicker to reduce downtime.

The HSL transmitter module (DSCC) will transmit the same information as the digital communicator over Honeywell's existing HSL networks. The customers voice telephone line will serve as a backup transmission method in the event of an HSL failure and as access for remote programming of the control unit. The HSL transmitter module requires 2 module mounting locations in the control unit. It also requires a HSL dedicated line in addition to the normal telephone line.

### Cellular Transmission

#### C801

The C801 Cellular Transmitter module is mounted within and connects directly to the control/communicator. It provides an alternative signal path utilizing the cellular telephone network. This module provides many of the same features of the Telguard Cellular Alarm Transmission System (CATS). In fact the module is actually manufactured by Telular for Radionics. The main benefits are that the integration of the module within the control/communicator reduces installation time, costs, wall space requirements and the module is supported by Radionics Customer Support.

When used as a backup, the C801 will switch to cellular if the digital dialer fails to reach the Customer Service Center after a preset number of attempts. It also monitors the cellular radio link and will trip a point on the Intelliguard when there is an interruption in the cellular service.

Because the cellular module simply provides an alternate path, for the digital communicator, to reach the Customer Service Center, there is no difference in the signals received. The C801, in combination with an Intelliguard package for UL Mercantile service (LP), provides Grade A service for a burglary system and may be used as the second phone line in fire alarm applications.

The C801 is powered by it's own AC transformer and uses the panel battery for backup. Two batteries are required for systems using the C801.

## Telguard

The Telguard product may still be used in situations where added features are required.

## AirTouch Agreement

Cellular service is now available to your customers at a very affordable price. Air Touch Cellular provides cellular service to Honeywell for corporate and employee use. This service is limited to use for backup alarm signaling only and is not to be used with cellular hardware which provides additional features like priority phone. This service is available nationwide and should be used with either the C801 or the Telguard models. See the separate bulletin announcing the details of this program.

# Section Two
# Features

# Section Two - Features

## Intelliguard Entry Control

One of the significant features of the "C" version is the addition of entry control of the burglar alarm. This section describes the differences between entry control and traditional access control and also defines the elements and application of entry control of the burglar alarm.

### Before Entry Control

The typical Intelliguard system controls one or more areas of a building. Each area includes the security devices (points) and a control center. The control center is usually located near the entry/exit door for the area and is used for arming and disarming. The control center provides detailed information about the status of the security in the area and, in some cases, other areas. The scope of the control center determines what areas can be seen. The user's authority level determines what commands they can give in each area.

In most cases, the system is armed using the ALL ON/OFF key. This means that all areas will be armed that are within the scope of the control center and the user's authority level. The user leaves the building through the designated door during the exit delay.

The ALL ON/OFF key is also used most often to disarm. The user unlocks the door with a key to enter. The control center warns the user that the system must be disarmed. By using the ALL ON/OFF key, the user disarms all areas that are within the scope of the control center and the user's authority level. Of course the user has the option of changing the area status to one of the Perimeter Armed states using other control center commands.

### Simple Entry Control

Intelliguard entry control changes this typical scenario by adding a credential reader outside of the area to replace the mechanical key used to unlock the door. In it's simplest form, entry control unlocks the door for authorized user's and disarms the appropriate areas just as though the user had pressed the ALL ON/OFF key at the control center. There are several options to this sequence but like the ALL ON/OFF key it is the one that will be used most often. The addition of entry control impacts the disarm portion of the above scenario only. The control center is still required to provide the detailed system status information during the arming sequence and to issue commands.

### Why it's Called Entry Control

There are some important differences between entry control and our traditional access control offerings. The list below are customer requirements that are better served by an access control system.

1. **Very specific control of a persons access - The front door from 8-5, the lunch room from 11-2, the records vault on Wednesdays.** Entry control uses authority levels to determine access. Doors are assigned to an area. A user's authority level for the area determines whether they have access to all doors within the area or no access at all in that area. Time control is accomplished using SKEDs which will disable access for an entire authority level. SKEDs are difficult for most customers to manage effectively.
2. **Detailed historical reporting - Where did this person use their card yesterday?** This is indicative of the need for a computer controlled reporting system. The "C" version is similar to an access control system that uses a dumb terminal/printer for the user interface. Activity can be printed in real time or in chronological order from the log but no query function is available.
3. **Multiple panel requirements - "The ninth door."** A traditional access control system will provide an option for multiple panels to be interconnected or to be managed by a computer system. Entry control is limited to a single system. A customer with multiple sites, each with entry control requirements within the bounds of a single system, must manage each system independently and on-site.
4. **Large number of users**. Most entry level access control systems are able to manage thousands of users. Intelliguard is limited by memory and practicality to 250 unique users.

5. **Completely customer managed system.** Because this is an attachment to the security system, the level of opening/closing supervision the customer requires may restrict the customers ability to make user changes on-site.
6. **Anti-passback control.** Entry control can be used for both In and Out control of a door but no restrictions are placed on the sequential use of a card.

## Hardware

The 5800C will support 4 doors with entry control, the 5900C/5924C will support 8 doors. Each door requires a D9210 Access Control module, a reader, and the associated electric locking device. Most doors will also require a door contact. and a device (button or motion detector) to provide Request to Exit operation. The 12 or 24 vdc power for the locking device will likely be provided by an auxiliary power supply.

## Configuration

A new programming handler called ACCESS is used to configure the doors connected to the D9210s. 9210s (doors) are assigned a door # which coincides with the address set on the module (1-8). Doors are assigned to an area like any other point. The area assignment is important because it determines which areas alarm status is looked at to determine if access should be granted. Doors are also assigned to a control center to determine the "scope" of their impact on the system. This is most often the address of the control center located immediately inside the door. One reason to use a different control center address would be if the customer wanted only the local area (area scope) impacted by entry control yet wanted the option of all areas (panelwide scope) from the control center. This would require referencing a control center, which could be virtual, assigned to the same area with area scope. The final assignment is the point number for the door contact. The point can be assigned any valid number including that of an on-board point.

*Note:* Point numbers must not be duplicated. If the door contact is assigned the number of an on-board point (1-8) then that point cannot be used and the resistor must be removed. If the door contact is assigned an off-board point this means that a POPIT or a point on an OctoPOPIT module cannot be used.

## Standard Door Parameters

There are a number of other programmable parameters that are typical for the door of an access control system. The parameters, which are fully programmable for each door, include unlock time, buzzer output time and shunt time of up to 4 minutes. There is also an extended shunt time of up to 30 seconds which begins, when the original shunt timer runs out, if the door is still open. The extended shunt time will provide an additional buzzer output and create a "CLOSE DOOR #" warning message for the control center. Three other items are specific to how the lock works. Deactivate On Open provides for the lock to be relocked as soon as the door is opened. Some electromagnetic devices with built in door sensors require this option to be turned off. RTE (Request To Enter) Shunt Only and REX (Request to Exit) Shunt Only allow you to define whether or not the door will be unlocked or just shunted. Most often you will want to unlock the door for RTE and shunt only for REX, unless an electromagnetic lock is employed.

## Integrated Entry control Parameters

The fact that Intelliguard has integrated entry control into the alarm system provides several other options that would not ordinarily be found in a standalone access control system. The parameters described below are programmable for each entry controlled door in the system.

### Disarm On Open

This entry control specific parameter determines at what point in the sequence of events the alarm system will change armed states. The default (YES) indicates that the alarm will change state only after the door has been physically opened. This means that the system won't change states if a user is granted access but changes their mind and doesn't enter the area. If the parameter is set to NO the system changes state immediately when access is granted.

The user's authority level determines what changes, if any, will take place. For example, some users may only disarm the interior and those who follow will not change the system further.

### Auto Door

One standard access control function that changes with entry control is the automatic (or timed) unlocking of a door. The typical access control system may unlock the front door during scheduled business hours. Most systems can accommodate day of the week and holiday variations but they cannot anticipate changes to the schedule caused by weather or business conditions. This means that there may be days when the door is unlocked even though no one is around. This would also be true if Intelliguard managed the door using SKEDs.

The Auto Door parameter links the unlocking of the door to the status of the area security system. If the alarm is OFF then the door will be unlocked. When the area security is armed (any armed state) then the door is locked.

### Fire Unlock

Fire alarm systems are frequently interconnected with access control systems so that a fire alarm condition will cause fire exit doors (with electromagnetic locks) to unlock. In most jurisdictions this must be done mechanically so that the unlocking of the doors is not dependent upon another system processor outside of the fire alarm system, meaning that you interrupt power to the locking devices with a relay supervised by the fire alarm system.

Because Intelliguard integrates both the fire alarm control and the entry control doors it may be acceptable to the local authority to use the Fire Unlock parameter to send an unlock signal to the access control module (D9210) in the event of a fire alarm. It is most likely however, that the local authority will view the D9210 as another system processor and require the more traditional mechanical method.

Fire Unlock will activate upon a fire alarm from any area of the system. Fire Unlock will not unlock doors in a master armed area. Once unlocked the doors must be manually returned to normal operation using the Door Control command. They do not automatically return to normal operation when the fire alarm is RESET.

### Interlock Point

An interlock point is a point located anywhere in the system that, when faulted, will cause the access control module to deny access to anyone. This feature is most often used in a “man trap” situation where the first door must be closed before the second door is allowed to open. It might also be used to prevent someone from entering an area where there may be a hazardous condition.

### Custom Function

Entry controlled execution of a custom function is an exclusive feature of the Intelliguard system. A custom function may be assigned to a door so that it will execute at the control center assigned to the access control module. This feature will likely be used in an area where the user would have executed a custom function from the control center upon entering the area. Whether or not a custom function will execute is determined by the user’s authority level and the area’s status. Options for user’s whose authority level allows custom function execution at a door include; when the area is disarmed, any armed state, always and never. Because it is controlled by the user’s authority level, it may be available to a very limited number of user’s under very specific conditions. It is possible, for example, to use an access control module (D9210) and a credential reader only for the purpose of executing a custom function and not for access control.

## Interface to Standalone Access Systems

Earlier in this section there was a list of customer requirements that would cause you to provide your customer with an access control system rather than Intelliguard entry control. You may also find an opportunity for Intelliguard with a customer that has an existing access control system. In either case there are two possible methods to interface the access system to Intelliguard to provide some of the benefits of entry control.

### Using a Reader from the Access System

With some access control systems it may be possible to install a card reader from the access control system on the Intelliguard system. This would likely be done at doors leading into security areas.

| **Pros** | **Cons** |
|---|---|

- Access to an area may be controlled by the arm status of the area.
- Area security status is changed based on the user's authority level.
- Ability to execute a custom function.
- Auto Door function may be employed rather than relying on a schedule.
- User ID allows use with supervised systems.
- Lose control of the door from the standalone access system.
- Door not included in access system real time or historical reporting.
- Limited number of users.
- Customer must manage users in two different systems.

This method is dependent on the access system having a reader that is compatible with the D9210 access control module and the credentials being used in the existing access system. This means that there must be a reader available that conforms to the Wiegand, 5 wire, 26 bit data format, communications protocol. This does not necessarily mean that the access system must use Wiegand card readers, only that a Wiegand protocol reader is available that would be compatible with the access system credentials and the D9210 access control module.

For example, the Honeywell 4100 access controller from WSE uses a digital proximity card reader, that features a WSE proprietary RS-485 protocol, like the 4205. The 4205 is not directly compatible with the D9210 access control module because it does not use the Wiegand format communications protocol. However, WSE offers the **4205W** which is both compatible with the digital credentials of the 4100 access controller and the D9210 because it uses the Wiegand communications protocol.

### Relay Interface (Easikey Point Type)

An alternative to obtaining a direct reader interface is to interconnect an access system relay so that it acts as a disarming keyswitch to the area security system.

#### Pros

- Simple, inexpensive interface.
- Customer maintains control of door from standalone access system.

#### Cons

- Full disarm is only option.
- Access control not based on area security status.
- No user ID, can't be used with supervised systems.

This method requires getting a momentary relay from the access control system that will be activated when access is granted. The relay connects to a point on the Intelliguard system. The point is assigned to the appropriate area and given the point type of Easikey. This point type differs from a keyswitch in that in only allows disarming.

## Managing Users

In previous versions of Intelliguard there were only two elements to a user, their passcode and an authority level. The "C" version introduces a third element, the credential (card or token). As a result, the names of commands which manage these three elements have been changed from Passcode to User, for example, Add Passcode has been changed to Add User. The number of users for each panel is shown in the chart in the introduction. Earlier generations of central station automation systems may reduce the number of users that can be managed for supervised systems.

## Sub-Users

To meet the access control needs of larger facilities with many people, the "C" version employs sub-users. Three sub-users may be assigned to each user. A sub-user is issued their own credential, but they have the same authority level as the master user. Sub-users also share the user's assigned passcode (if you tell them what it is) and user name. Sub-users are designated in the system by the master user ID and the sub-user number (1-3). The third sub-user assigned to user 123 would be 123-3. The master user would be 123-0. Events generated by sub-users (log or printer) will display the master user name. For this reason it is recommended that the user name be a department name or number.

It is recommended that you only employ sub-users with users who need access but not disarming or custom function rights. The user and sub-users should not be issued a passcode. Using this method it would be possible, for example, to have a 5800C with 25 users that have access and disarm authority and the remaining 75 users, each with 3 sub-users (for a total of 300), could have access privileges only.

***Caution**:* Supervised systems must not allow sub-users to arm and disarm.

## Authority Level

The authority level has also been changed to include three new items, which define a user's authority when using their credential. Like the commands within an authority level, if the item is blank it is not part of the authority level. Unlike commands, the new items provide options that go beyond simply being enabled as you will see below.

As in previous versions of Intelliguard, a user may be assigned different authority levels in each area of the system to match their responsibilities. If a user is not assigned an authority level in an area then they are not authorized to issue commands at control centers in that area. Similarly, they are also not authorized to use the reader controlled doors assigned to that area. When a user is assigned an authority level in an area the three entry control related elements described below will determine; when they will gain entry (Access Level), what their entry will do to the security system (Disarm Level), and when a custom function will be executed (Function Level). When a user's authority level in an area includes access authority then the user has access to all doors within the same area. It is not possible to limit a user's access to something other than all doors in an area.

### Access Level

Access level defines when a user will be allowed access to an area. The determining factor for "when" is the status of the security system in the area being entered rather than a time of day like most access control systems. Options for the access level define the maximum security level at which a user can gain access. The options are;
**M** = access will always be allowed, when the area is **M**aster armed, Perimeter armed or disarmed.
**P** = access will be allowed if the area is **P**erimeter armed or disarmed. Access will be denied if the area is master armed.
**D** = access will only be allowed if the area is **d**isarmed.
**blank** = no access

### Disarm Level

Disarm level determines what will happen to the area security system when the user is granted access. Without entry control the user would ordinarily come through the entry door and use the control center to disarm the area (or areas) or possibly perimeter arm (because of Intelliguard's exclusive feature of being able to change armed states without disarming). The disarm level will do the same thing automatically each time access is granted. The options are:
**I** = disarm the local area's **I**nterior points only (Perimeter Instant), if the area was master armed. This has no effect if the local area is already Perimeter armed or disarmed.
**D** = disarm all, from either master armed or perimeter armed. This is the same as using the Disarm All command at the control center. All areas within the scope of the control center address, assigned to the D9210 access control module, and within the user's authority level will be disarmed.
**blank** = no change to the area security system, simply shunt the door contact for entry.

### Function Level

The D9210 access control module may be assigned a custom function. Most user's would not be given authority to do this at the control center nor should they be allowed to execute it from the reader. Only selected user's with the appropriate authority level would cause this extra command to execute upon their entry into the area. The options for function level determine when the custom function will execute for user's with this authority level. The options are;
**M** = custom function will execute if the area security system is armed (Master or Perimeter).
**D** = custom function will execute only if the entry area is disarmed.

**C** = custom function will execute every time access is granted to a user with this authority level.
**blank** = not authorized

*Note:* Users who will be executing a custom function must also have a passcode assigned.

## Standard Authority Levels

The four standard authority levels have been modified to include entry control functionality and a new level has been added as standard. The Service authority level (level 15) has not been changed. The accompanying chart shows the changes described below. Changes within the chart are indicated with **Bold** type style.

**Authority Level 1** is for the individual who manages the security system. In addition to arming and disarming, this person can make temporary changes (like bypassing a point) and permanent changes (like delete user). When entry control is employed this level will; always grant entry to user's (Access Level **M**), disarm all areas within the scope of the control center assigned to the access control module (Disarm Level **D**), will initiate the custom function assigned to the access control module when the system is disarmed (Function Level **D**).

**Authority Level 2** is for individuals who are responsible for the day-to-day operation of the system. This level allows arming and disarming and can make temporary changes (like bypassing a point). For entry control systems this level will always grant entry to user's (Access Level **M**) and disarm all areas within the scope of the control center assigned to the access control module (Disarm Level **D**).

**Authority Level 3** permits individuals to arm and disarm only and can make no changes to the system. Users with this authority level who use a credential will always be granted entry to the area (Access Level **M**) and disarm the interior of the local area (Disarm Level **I**).

**Authority Level 4** permits individuals to only arm the system and can make no changes to the system. Provide this user with a credential and they will be allowed to enter the area if it is not master armed.

**Authority Level 5** is for users who do not interface with the security system and require access only when the area security system is disarmed. Users with this authority level do not require a passcode.

Honeywell Standard Authority Levels

| # | Control Center Functions | Authority | Authority | Authority | Authority | Authority | Authority |
|---|---|---|---|---|---|---|---|
| 1 | Disarm | YES | YES | YES | | | |
| 2 | Master Arm | YES | YES | YES | YES | | |
| 3 | Master Arm Instant | YES | YES | | | | |
| 4 | Perimeter Arm Instant | YES | YES | YES | | | |
| 5 | Perimeter Arm Delay | YES | YES | YES | | | |
| 6 | Watch Mode | YES | YES | YES | | | |
| 7 | Perimeter Partial | YES | YES | | | | |
| 8 | View Area Status | YES | YES | | | | YES |
| 9 | View Event Memory | YES | YES | YES | | | YES |
| 10 | View Point Status | YES | YES | YES | | | YES |
| 11 | Walk Test | YES | YES | | | | YES |
| 12 | Fire Test | YES | YES | | | | YES |
| 13 | Send Report | | | | | | YES |
| 14 | **Door Control** | **YES** | **YES** | | | | **YES** |
| | **Cycle Door** | **YES** | **YES** | | | | **YES** |
| | **Unlock Door** | **YES** | **YES** | | | | **YES** |
| | **Secure Door** | **YES** | **YES** | | | | **YES** |
| 15 | Change Display | YES | **YES** | | | | YES |
| 16 | Change Time/Date | YES | **YES** | | | | YES |
| 17 | Change Passcode | | | | | | YES |
| 18 | **Add/Change User** | | | | | | YES |
| 19 | **Delete User** | YES | | | | | YES |
| 20 | Extend Closing | | | | | | |
| 21 | View Log | YES | **YES** | | | | YES |
| 22 | Print Log | YES | **YES** | | | | YES |
| 25 | Bypass a Point | YES | YES | | | | YES |
| 26 | Unbypass a Point | YES | YES | | | | YES |
| 27 | Reset Sensors | YES | YES | YES | YES | | YES |
| 28 | Change Relays | YES | YES | | | | YES |
| 29 | Remote Program | YES | **YES** | **YES** | | | YES |
| 30 | Move to Area | YES | YES | | | | YES |
| 32 | Display Revision # | YES | | | | | YES |
| 33 | Service Walk Test | | | | | | YES |
| 34 | Default Text | | | | | | YES |
| 35 | Change SKEDs | YES | | | | | YES |
| 36 | Invisible Test | YES | YES | | | | YES |
| 37 | **Access Level Control** | **YES** | | | | | **YES** |
| | Custom Functions 128-**143** | YES | | | | | |
| **Access Levels** | | | | | | | |
| **Access Level** | | **M** | **M** | **M** | **P** | **D** | |
| **Disarm Level** | | **D** | **D** | **I** | | | |
| **Function Level** | | **D** | | | | | |

## Adding/Changing Users

Adding a user to a system which employs entry control can be a three step process if they require a passcode, card (or token) and an authority level. It is always required for the user to have an authority level. Passcodes or cards may be issued independently. Like passcodes, cards may be changed by simply overwriting the existing card.

### On premise

At installation, users can be added from the programmer, however it is best to add the card from a credential reader. This not only assigns the card to the appropriate user, it also tests the card before it is issued. With the service passcode, access the ADD/CHANGE USER command. Enter the user number. You now have three options for a new user; ADD PASSCODE, ADD CARD, ADD LEVEL (authority level). If you are assigning a card to an existing user the options would be; CHANGE PASSCODE, ADD CARD, CHANGE LEVEL. If you needed to change the card assigned to a user the options would be; CHANGE PASSCODE, CHANGE CARD, CHANGE LEVEL. In either case when you access the option for CARD you will be instructed to PRESENT CARD. During the programming of the system, you were required to assign a door to the control center (in the control center assignment section). This is the door (reader) where you should PRESENT (the) CARD. The control center will respond to a valid card with CARD ADDED. The display CARD EXISTS means that the card has already been issued to another user. User names can only be added from one of the programming tools (D5200/D5400).

*Note:* If your branch currently has a policy that does not allow customers to add or change passcodes, then your customers will not be able to add or change cards from the control center.

### From the CSC

As during installation, users may be entered using the programmer (RAM III). Cards (or tokens) used with Intelliguard are not site specific. Therefore it is possible to take the next batch of cards from the shelf to meet your customers needs. It is strongly recommended that cards be added on premise to ensure that they are assigned to the appropriate user and that they are functional before issue.

## Deleting

The DELETE USER command removes all three elements of the user. It is not possible to delete a passcode or card independently. If a card (or token) is lost, using the ADD/CHANGE USER command to CHANGE CARD which will replace the lost card with a new card rendering the lost card invalid.

## Reporting

Each door can be programmed to generate events for several different conditions described below. When an event is enabled it can be routed to the log, the printer and/or the central station. Access Granted and Entry Denied events can also be enabled/disabled using a SKED. Customers, with large systems and many users, who wish to record all events should be encouraged to use the D9131 printer interface.

*Note:* Access events should not be reported to the central station at this time.

## Access Granted

Enabling Access Granted events will create a log event when;

- a user gains entry with their card (or token)
- the door is opened with the Door Control command
- the door is opened by a SKED
- their is an entry request or exit request (if enabled)

The log for access with a card will be a three line message as follows;
**12/21/96 4:28 PM**
**3 101 AXS GRANTD**
-the area number in which the event occurred (e.g., 3 = area 3).
-a 3-digit number identifying the point (door contact) involved in the event.
**123-0 USERS NAME**
-the user number (including sub-user number).
-the first ten characters of the user's name (default text for this example would be USER 123).

The printer report for the same event would be;

| Date | Time | Event | Acct | Area | ID | Pt # | Point Text |
|---|---|---|---|---|---|---|---|
| 12/21 | 4:28PM | Access Granted | 0999 | 3 | 1230 | 101 | Employee Door<br>Joanne Smith<br>(or USER 123 if not programmed) |

## Entry Denied

Enabling Entry Denied events will create a log event when a card or token is denied access for one of the following reasons.

- **LEVEL**, the user does not have an authority level in this area or it does not include access rights or the user's access level was not high enough for the area's armed state.
- **SECURED**, the door has been SECURED (disabled for everyone) by a command or SKED.
- **INTERLOCK**, the interlock point was faulted when the card was presented.
- **UNKNOWN**, the card presented is not valid for this system.

The log for denied entry will be a three line message as follows;
**12/21/96 4:28 PM**
**3 101 NO ENTRY**
-the area number in which the event occurred (e.g., 3 = area 3).
-a 3-digit number identifying the point (door contact) involved in the event.
**123-0 LEVEL**
-the user number (including sub-user number).
-the reason entry was denied

The printer report for the same event would be;

| Date | Time | Event | Acct | Area | ID | Pt # | Point Text |
|---|---|---|---|---|---|---|---|
| 12/21 | 4:28PM | No Entry - Level | 0999 | 3 | 1230 | 101 | Employee Door<br>Joanne Smith<br>(or USER 123 if not programmed) |

## Door Requests (Entry/Exit)

Use of the RTE and REX inputs can also generate events. Granted and Denied requests are also controlled by the Access Granted and Entry Denied parameters. Denied events would be caused by a "Secure" door.

*Note:* You would not ordinarily enable the Door Requests as they will quickly fill the event log, use a lot of printer paper and provide very little useful information since they cannot record who took the action.

## SKED Control

Four new SKEDs allow the Access Granted and Entry Denied event recording to be enabled/disabled by time/day. It is recommended that you always record Entry Denied events to aid in troubleshooting. Access Granted events also tend to fill the event log very quickly. SKED control of the Access Granted events is highly recommended.

## Access Level Control Command

This command allows an authorized user to disable/enable the access portion of an authority level. This means that all user's assigned this authority level in any area will be denied access. The restrictions remain in effect until the access level is enabled again, either by using this command or through a SKED.

## Door Control Command

The Door command provides manual control of the electric locking device associated with each of the controlled doors. This is a multiple option command which provides a way for a user (like a security guard) to momentarily open a door (s), unlock it until relocked and to secure a door, which locks the door and denies access to everyone. New SKED functions have been provided to unlock, secure and return the door to normal operation.

## Complete Entry Control

In the beginning of this section there was a description of system operation before entry control and how simply entry control can be incorporated into an Intelliguard system. What follows is a more in depth description of Intelliguard Entry Control in a typical retail application.

In a typical mall department store Intelliguard is frequently employed to independently control several areas of the store including the employee entrance, the receiving dock, the interior motion detection system, the cash and administrative offices and the customer doors. Most often the areas are controlled from a common control center located near the employee entrance. Using Intelliguard Entry Control to control the employee entrance provides several benefits to the customer.

Usually there is an early crew that arrives to do custodial work. A supervisor will open the employee door and disarm the interior motion system using the control center. Frequently they will re-arm the employee door. With a credential reader at the door. The supervisor's entry would cause the motion detection system to turn off (disarm Level I) leaving the employee door Perimeter armed. The crew who were denied access when the area was master armed are now able to enter and begin their shift (access level P). Employees who arrive later will use their credential to gain entry rather than cause the supervisor to disarm, let them in and rearm the door.

The custodial crew is restricted to the sales floor area until a security supervisor arrives, whose entry causes the receiving dock system, the offices and employee entrance to disarm (disarm level D).

Finally a credential reader next to the control center can be used to execute a custom function only when the employee entrance and motion system is disarmed (function level D). This custom function would disarm the customer doors and might be used to establish additional daytime operating standards over and above the simple disarming of the area security system, for example, turning on lights and bypassing the contact on the trash compactor.

This scenario might not match the operating characteristics of any particular customer but it does point out the flexibility and the possibilities of Intelliguard Entry Control.

# Points

## Off-board

Off-board points may come from POPITs, OctoPOPITs or the door contact point of the D9210. With the exception of the D9210 door contact, the point number of these points is determined by a hardware address. The D9210 door contact point number is defined in programming and may be assigned any valid point number.

The 5800 supports one point interface module (D8125) for a total of 74 points. The 5900C/5924C support two modules for a total of 245 points (126 with one POPEX module).

*Note:* Automation constraints require that Point #9 not be used. This will eliminate any confusion with low battery reporting which reports as Zone #9.

## *PS6 Automation Constraints*

*The customer sees points in the display of the control center and the system reports points to Honeywell's PS6 automation system. Alarms by point can be viewed in the Event Log or on the dispatch printer.. Customer Service Center (CSC) operators can display points for dispatching service and when discussing alarms with customers. For the purpose of dispatching authorities, alarms in the PS6 CSC automation system are grouped into zones. Zones in the CSC automation system will be referred to as CSC zones.*

*The new point capacity of each control/communicator changes the CSC zone reporting. For 5800C systems with greater than 48 points to report properly they will be treated like a 5900 by the automation system. The spread of off-board points across the CSC zones is shown in the chart.*

*The 5800C will spread the off-board points across the CSC zones as shown below.*

| Point number on control center | Point # on CSC 6500 | CSC Reporting | Total # of Points, On-board + Off-board |
|---|---|---|---|
| 1, 10-24 | 100, 102-116 | CSC zone 1 | 16 |
| 2, 25-40 | 200-216 | CSC zone 2 | 17 |
| 3, 41-56 | 300-316 | CSC zone 3 | 17 |
| 4, 57-72 | 400-416 | CSC zone 4 | 17 |
| 5, 73-75 | 500-503 | CSC zone 5 | 4 |
| 6 | 600 | CSC zone 6 | 1 |
| 7 | 700 | CSC zone 7 | 1 |
| 8 | 800 | CSC zone 8 | 1 |

*The 5900C/5924C will spread the off-board points across the CSC zones as shown below.*

| Point # on control center with 1-POPEX (D8125) | Point # on CSC 6500 | Point # on control center with 2nd POPEX | Point # on CSC 6500 | CSC Reporting | Total # of Points, On-board + Off-board |
|---|---|---|---|---|---|
| 1, 10-24 | 100, 102-116 | 137-152 | 117-132 | CSC zone 1 | 32 |
| 2, 25-40 | 200-216 | 153-168 | 217-232 | CSC zone 2 | 33 |
| 3, 41-56 | 300-316 | 169-184 | 317-332 | CSC zone 3 | 33 |
| 4, 57-72 | 400-416 | 185-200 | 417-432 | CSC zone 4 | 33 |
| 5, 73-88 | 500-516 | 201-216 | 517-532 | CSC zone 5 | 33 |
| 6, 89-104 | 600-616 | 217-232 | 617-632 | CSC zone 6 | 33 |
| 7, 105-120 | 700-716 | 233-247 | 717-731 | CSC zone 7 | 32 |
| 8, 121-127 | 800-807 | 129-136 | 809-816 | CSC zone 8 | 16 |

*To assure that no one CSC zone, for dispatching, is assigned more than the appropriate number of points, the Business Security Planner has a Security Survey Worksheet that calculates the number of CSC zones.* ***There must be no more than eight CSC zones per account.***

## Point Index

The 5800/5900 can be programmed so that you can provide a variety of services to customers. These are services such as burglary, fire, hold up and critical equipment monitoring. Each point is assigned to an area and programmed with a point index which defines the response of the area to that point. Within an area, some points will use the same point index (be programmed to work in the same manner) i.e.; all smoke detectors will be fire points and ring the fire horn.

Within each point index, there are several parameter choices which will be made by the installer based on the customer requirements conveyed by the sales representative. Point parameters are listed on the Program Record Sheet (Radionics # 74-07631-000). The following is a brief explanation of the new point parameters.

### Point Type

The table below describes two new point types.

| Point Type | Description |
|---|---|
| EasiKey | This point type provides an interface to external systems to allow disarming only. It will disarm the area assigned to the point. This point type is not used for D9210 points. |
| No Alarm, Relay Follows Point | This point type does not cause an alarm at the control center nor does it report. It simply causes the assigned relay to activate. |

### Point Response

Determines what type of electrical contact is used (normally open or closed) and what conditions warrant an alarm, supervisory, trouble, delay or no response.

There are several new choices of point response. Choosing the appropriate point response allows you to match devices to the application. For example, the proper point response for a sprinkler supervisory control valve requires that a supervisory signal is generated, when the supervisory switch on the valve stem senses the valve being closed, but indicate trouble if the wires to the switch are broken. Supervisory is a point response that is available for either fire or non-fire points.

The DS motion detectors with an integrated POPIT require a new point response. That is because the devices are sending alarm, trouble and diagnostic data directly as opposed to open, short, normal conditions like other devices.

### Point Parameters

### Annunciation

**Relay Follows Point** has been modified. This parameter now features an alternative to the original operation which triggers a relay whenever the point is in alarm (except invisible points). The relay remains activated until the point is cleared from the control center display. The alternative parameter activates the relay any time while the point is faulted. The difference being that the point doesn't have to be in alarm.

**Buzz on Fault** now features a silenceable option. This parameter causes the control center to sound a trouble tone. You now can choose if the tone can be silenced using the CLEAR key.

The **Display as Device** parameter adds the display CHECK DEVICE to the faulted points list when this point is off normal.

### Bypass/Force Arm

The **Returnable** parameter which determines if a bypass/force arm is temporary or maintained has been separated into two parameters, BP (Bypass) Returnable and FA (Force Arm) Returnable. If Returnable is set to NO then bypasses will be maintained until the unbypass command is used. If set to YES then bypasses will be cleared at disarming. If a force armed point is Returnable it will become part of the protection again if it becomes normal during the disarmed period.

## Relays

### Panelwide

Two relay conditions were deleted and two were added. The relay conditions that responded to keypad and printer failures were deleted and summary relays were added for supervisory fire and supervisory non-fire conditions.

## Commands

### Tailored Security

As stated earlier, your challenge with Tailored Security is to identify the features that your customer needs to assist them with their business situation. One of the best places to accomplish this is at the control center with the command list you create. If the command a customer needs most frequently is the first thing to appear in the command list, you have gone a long way towards Delighting Your Customer. Customers still fear long lists of commands they don't understand. You should scrutinize the command choices to ensure that they are necessary and in the proper order. Pick commands grudgingly. If commands are necessary for only one person then disable them in other access levels so that they are not in the way.

*Installation & Service Note:* It is not necessary to put commands in the list just so that they will be available to Installation or Service. Commands can be accessed directly from the control center as long as there is at least one command in the command list (by default, Remote Program). After accessing the command list with your service passcode, use the keypad to enter the number of the command you wish to access and press ENTER (numbers can be found on the Program Record Sheet, User Interface). For example, to access SERVICE WALK TEST press 33 ENTER. You will be within the command just as if you had chosen it from the command list. All commands within the Service Passcode authority level can be accessed this way. Don't clutter up the customer's command list unnecessarily.

### New/Modified commands

The authority level chart, earlier in this section, shows the new or modified commands associated with the "C" version. Review the operation of these commands in the Intelliguard User's Guide for the "C" version.

### Master Arm, Master Arm Instant and Disarm

These commands have been modified so that you can select several areas without the need to re-enter a passcode. If for example you are arming areas and press ENTER in response to ARM AREA 1?, the display will return with the next area available to be armed instead of returning to date and time.

### Add/Change User

The ADD/CHANGE USER command is used to manage the three elements of a user; their passcode, their credential (card or token), and their authority level. This commands operation correlates with the user's status. If you are entering a new user the commands will be ADD PASSCODE, ADD CARD and ADD LEVEL (authority level). If one or more of the elements of the user have been assigned then they will be displayed as CHANGE PASSCODE or CHANGE CARD or CHANGE LEVEL.

In either case when you choose the option for CARD you will be instructed to PRESENT CARD. Installation programming assigns a door to a control center (in the control center assignment section). This is the door (reader) where you would PRESENT (the) CARD. The door will not be available for card entry while using this part of the command. The control center will respond to a valid card with CARD ADDED. If this was an existing user who lost their card the new card presented would replace the lost card. The display CARD EXISTS means that the card has already been issued to another user.

*Note:* The 16 character user names can only be added/changed from one of the programming tools, the D5200 local programmer or the D5400 (RAM III) remote account manager.

### Delete User

This command differs from DELETE PASSCODE only in that it allows you to scroll through the users until you find the one you want to delete. This is usually only helpful if you have programmed user names.

### Access Level Control

Access control privileges are part of the user's authority level. The access privileges determine when an employee can gain access and what action will be taken with the security system. This command is a toggle which will disable or enable the access control privileges portion of the authority level only.

*NOTE:* If you disable the Access Level for authority level 1, you have disabled the access privileges for all users who have authority level 1 assigned in any area of the system.

### Door Control

Directly control the status of access controlled doors with this command. This is a multi-option command that provides for three different conditions at an access control door.

- CYCLE DOOR is used to momentarily unlock the door to allow someone to enter or exit without a credential. The door will operate just as it would for a valid card.
- UNLOCK DOOR will toggle the door unlocked for free access to anyone.
- SECURE DOOR locks the door and denies access to everyone. Use again to return the door to normal operation.

The three commands are sub-commands to Door Control. Each can be separately enabled/disabled as part of an authority level. Door Control is the command placed in the function list for a control center. Users will only see commands enabled in their authority level.

Each sub-command presents a dynamic display that shows the status of the doors within the scope of the control center. Selecting the door number and pressing enter will change the door to the new status.

An UNLOCKED door will be returned to normal operation because; another UNLOCK command was issued (acts as a toggle), a SECURE command was issued or the area was armed.

A SECURED door is returned to normal operation by another SECURE command.

### Custom functions

The 5900C and 5924C now allow access to two more custom functions. Also, the new operation of the arming and disarming commands means that it is possible to maintain user identification for supervised systems. Only complex custom functions will still require an embedded passcode.

## SKEDs

SKEDs (scheduled events) have been rearranged within the panel to allow maximum flexibility. User access windows and opening/closing windows are actually SKEDs. They are not frequently used and the "C" version now allows you to recover them for use as a SKEDs. If a system does not require them then there are a total of 64 SKEDs, otherwise there are 40.

New SKED functions are associated with entry control applications. They include;

- access level on/off, disables the access portion of an authority level.
- door control commands including UNLOCK, SECURE and LOCK to return the door to normal.
- access granted and entry denied events on/off.

## Other New Programmable Features

### Routing

Routing has been redesigned and now offers more flexibility for sending specific events to alternate locations. The previous version of the panel grouped similar events, such as any fire events, for reporting purposes. If fire events were enabled then all fire events were sent. Custom programming allows for the selection of individual events within the fire events group to meet specific requirements.

There are four different routes (or profiles) available. Each route defines what reports will be sent and which of the possible 4 phone numbers is the primary destination and which is the backup. Alternate location reporting is accomplished using a second route also with it's own primary and backup destinations.

## Access Reports

At this time, the Customer Service Center cannot support the reporting of Intelliguard entry control events such as Access Granted and Entry Denied. It is possible that some multi-location customers will want these new events to be sent to a proprietary 6500 receiver for remote reporting.

# Section Three
# Control Centers

# Section Three - Control Centers

## Scope

Each Control Center address is assigned a scope. Scope determines if the Control Center is capable of controlling areas other than the one to which the control center is assigned. There were three options to scope, Panelwide, Account and Area.

### Custom

Custom programming allows you to select the specific areas to participate in a control centers scope. This makes it possible to cross account boundaries without having to choose panelwide and to view a sub-set of all areas within the same account.

## ALL ON/OFF Key

The ALL ON/OFF key is a dynamic function key that when pressed makes some decisions about what the user wants to do based on the status of the local area. For example, if the local area is perimeter armed then this function will master arm all areas within the scope of the control center that are also within the user's authority level. This would be the proper response when someone was leaving for the night, but not if the person were coming into the area. This decision making process has been enhanced with the following logic to make the function more intuitive.

- if there is an active alarm, entry or exit delay in the area then the ALL ON/OFF key will disarm. This was done for two reasons. First, if the key is used during exit delay it is likely that the user forgot something or didn't want to arm. Second, if an entry delay is running, the user is most likely attempting to disarm. This resolves the problem of a Perimeter Delay armed area which would attempt to Master Arm when ALL ON/OFF was used during an entry delay or alarm.

- if the area is disarmed and there is a 24 hour alarm (fire or non-fire) or a trouble then the ALL ON/OFF key will silence the alarm/trouble (not arm). People are creatures of habit. If they most often interact with the control center by using the ALL ON/OFF key then that is what they will most likely do when the occasional alarm or trouble occurs (I've done it myself and you probably have too).

| Current Area Status | Delay or Alarm | New Area Status after ALL ON/OFF |
|---|---|---|
| Disarmed | None | Master Arm |
| Disarmed | ALARM/Trouble | *Disarmed (ALARM SILENCED) |
| Perimeter | None | Master Arm |
| Perimeter | Delay (entry or exit) | *Disarm |
| Perimeter | ALARM | *Disarm |
| Master Armed | | Disarm (always) |

*new result

### Follows Scope

There is a new option associated with the ALL ON/OFF key which will allow you to further tailor the operation of a control center to meet your customers needs. The "C" version allows you to program the ALL ON/OFF key so that it only impacts the local area, even if it is a panelwide control center. Customer requirements frequently cause us to put a panelwide control center in the office so that the entire system can be viewed from one location. However, for arming/disarming purposes, daily operation requires the control center operate only the local area. This has caused customers to use the command menu rather than take advantage of the simple operation of the ALL ON/OFF key. By programming ALL ON/OFF Follows Scope as NO, your customers can have their cake and eat it too.

## Master Arm & Disarm Commands

These commands have been modified slightly again to make them easier to use. Since the ALL ON/OFF key will arm or disarm ALL areas within the scope of the control center and the user's authority level, these commands are most often used to arm or disarm some areas rather than all. The commands have been modified such that after arming or disarming a single area, the user is asked if they want to arm or disarm the next available area so that they may continue without needing to enter their passcode a second (or third, or fourth) time.

This simple change may make creating custom functions, specifically for supervised systems, easier. For arming and disarming it will no longer be necessary to embed a passcode within the custom function thereby losing user identification. Make the arm or disarm command the first commands to execute and then embed a virtual passcode to initiate other commands whose results are not reported to the CSC.

## Closing Time Warning

The display PLEASE CLOSE NOW has been changed to ARM AREA NOW for two reasons. First, many customers do not understand CLOSE to mean ARM and second, CLOSE is used in the CLOSE DOOR # message from an entry controlled door to indicate that the door has been held open. ARM AREA NOW is generated by using a Closing Window.

## 550 LED Control Center

Two new parameters within the Control Center assignment section of the program were developed to enable a simple form of door control using an inexpensive 550 LED Control Center. These are possible because the ENTER key is not used to access menus. They can be assigned to either an area control center to control an interior door or to a control center used only for this purpose (virtual area). The two parameters are mutually exclusive, only one can be used at a control center.

*Note:* Do not use these parameters with a 540 Control Center. They will disable the command menu and provide inconsistent operation.

### Enter Key Relay

This parameter allows the ENTER key (after a valid passcode of course) to activate a relay for 10 seconds. The relay can be any one of the on-board or off-board relays. For example, assuming you are not using the alternate alarm output relay (relay B), this relay could provide 12 VDC (up to 2 amps) to a common door strike. If you were using an electromagnetic lock, and had enough power available, you might use the C relay (switched aux. power) instead.

### Enter Key Open Door

The ENTER key can be assigned to activate the lock associated with an access control module (D9210). The door will function just as though a credential was used to gain access.

# Section Four
# Fire Applications

# Section Four - Fire Applications

## Supervisory Signals

The “C” version supports a new point response for devices used for fire supervisory purposes. This means that a “Supervisory” signal is transmitted to the CSC when a device listed as a supervisory device, such as sprinkler control valves or room temperature devices is “off normal”. These point types can also send “Trouble” signals to indicate a problem with the wiring.

Check with your CSC to determine if they can support this new point response.

# Section Five
# Power Requirements

## Section Five - Power Requirements

# Standby Battery and Current Rating Chart

use with D5800/D5900/D5924 (12VDC)
All currents are in milliamperes (1 ampere = 1000 milliamperes).

| Model Number | Qty | AC Power On Normal Current Current Each Unit | Total | AC Power Off Minimum Current Current Each Unit | Total | In Alarm Maximum Current Current Each Unit | Total |
|---|---|---|---|---|---|---|---|
| D5800/D5900 | 1 | 500 x 1 = | 500 | 250 x 1 = | 250 | 500 x 1 = | 500 |
| D125B | | 20 x Qty = | | 19 x Qty = | | 123 x Qty = | |
| D127 | | 13 x Qty = | | 13 x Qty = | | 45 x Qty = | |
| D928 | | 14 x Qty = | | 14 x Qty = | | 45 x Qty = | |
| D129 | | 25 x Qty = | | 25 x Qty = | | 26 x Qty = | |
| D192C | | 15 x Qty = | | 26 x Qty = | | 50 x Qty = | |
| D540 | | 104 x Qty = | | 106 x Qty = | | 206 x Qty = | |
| D541 | | 104 x Qty = | | 106 x Qty = | | 206 x Qty = | |
| D542 | | 104 x Qty = | | 106 x Qty = | | 206 x Qty = | |
| D550 | | 20 x Qty = | | 20 x Qty = | | 75 x Qty = | |
| D811 | | 20 x Qty = | | 20 x Qty = | | 45 x Qty = | |
| D8125 | | 48 x Qty = | | 47 x Qty = | | 48 x Qty = | |
| D8126/8127 | | 3 x Qty = | | 3 x Qty = | | 4 x Qty = | |
| D8128C | | 50 x Qty = | | 50 x Qty = | | 50 x Qty = | |
| D8129 | | 20 x Qty = | | 20 x Qty = | | 20 x Qty + 25 x #relays = | |
| D8130 | | 5 x Qty = | | 5 x Qty = | | 54 x Qty = | |
| D9131A | | 24 x Qty = | | 22 x Qty = | | 36 x Qty = | |
| D9210B | | 100 x Qty = | | 100 x Qty = | | 120 x Qty = | |
| WSE 4205W | | 80 x Qty = | | 80 x Qty = | | 80 x Qty = | |
| C801 | | 0 x Qty = | | 50 x Qty = | | 1000 x Qty = | |
| InfraRed | | 20 x Qty = | | 20 x Qty = | | 20 x Qty = | |
| Shatterbox | | 14 x Qty = | | 14 x Qty = | | 19 x Qty = | |
| 2w Smoke | | .001 x Qty = | | .001 x Qty = | | 25 x Qty = | |
| Siren | | 0 x Qty = | | 0 x Qty = | | 500 x Qty = | |
| UL Bell | | 0 x Qty = | | 0 x Qty = | | 600 x Qty = | |
| *Ratings of other devices in the system which are not shown above:* | | | | | | | |
| | | x Qty = | | x Qty = | | x Qty = | |
| | | x Qty = | | x Qty = | | x Qty = | |
| | | x Qty = | | x Qty = | | x Qty = | |
| | | x Qty = | | x Qty = | | x Qty = | |
| | | **Total A =** | | **Total B =** | | **Total C =** | |

*Note:* The 24 volt section for 5924 does not change. Use the chart from the original application guide.

# Section Six
# Approval Agency Requirements

## Section Six - Approval Agency Requirements

### Entry Control OK on UL Burglary and Fire Systems

The D9210 is a UL listed component of the burglar alarm system. The WSE 4205W credential readers are UL listed access control devices (UL294).

### FM, CSFM, NYC-MEA

The “C” version has been submitted to each of these approval agencies. The process is a paperwork change to the existing listings and will be complete within 30 days.

# Section Seven
# Installation & Service

# Section Seven - Installation & Service

## Programming

### RAM III

The "C" version requires the new D5400 (RAM III) Remote Account Manager software. RAM III will eventually become the software for a laptop version of RAM along with an interface device. RAM II will continue to be used for earlier panels.

### D5200 Programmer

#### Reset Pin

In the original version of the 5800/5900 it was recommended that you lock the reset pin to speed up programming. The new platform (both "C" and "DSCC") requires the reset pin to be locked.

#### Handlers

#### ìDSCCî Version

The "DSCC" version uses the 5800B or 5900B handlers (version 1.30). Use the Irvine update system to retrieve this version.

#### ìCî Version

The "C" version panels require a completely new set of programming handlers. Handlers for the "B1" version will not function and will indicate this with the response "Incompatible Panel" when you attempt to read or write a program.

The set of handlers is required because of the larger memory of the new platform. With the exception of ACCESS, the handlers are just separated elements of handlers you are already familiar with.

#### 5800MAIN/5900MAIN

This handler provides parameter programming prompts for;

- Panel-wide
- Area-wide
- Control Center
- User Interface
- Function List
- Relay

#### POINTS

This handler covers Point Index and Point Assignment.

#### SKEDS

This handler covers SKEDs and Windows.

#### USERS1

Programming for User numbers 0-124. Including sub-users.

#### USERS2

Users 125 through 250 and sub-users.

#### ACCESS

This new handler has three elements for programming the parameters of the D9210 Access Control module.

- **Door Profile** - defines the area assignment, control center scope to emulate, point assignment for the door contact, the interlock point (if any), auto door operation (based on area arming status), unlock during a fire condition and when the disarm actions will occur (immediately or after the door opens).
- **Strike Profile** - defines the unlock and shunt times as well as whether the RTE/REX devices will unlock or only shunt the door contact.
- **Event Profile** - defines what events will be generated for each door.

### Handler Distribution

Initial distribution of the handlers will be provided by the Radionics technical trainers via a "flash card". This card will act as the "B" drive of your programmer. It will allow you to either copy the handlers to your programmer's "A" drive if you have room or use them from the "B" drive. Most programmers will not have sufficient room for the entire set. Additional 'flash cards" may be ordered from Radionics as needed.

### Irvine Handler Update System (HUSys)

The HUSys in Irvine has been updated to include the new handlers. It is recommended that you update your programmers using the "flash card" as this will take much less time. Except for version 1.30 of 5800B and 5900B.

## Retrofit

There are a number of issues to be considered before upgrading an existing system Each of the following should be reviewed to understand the impact to the customer and on the process.

### POPITs and point numbering

If you were to simply replace a 5900B1 (with two POPEX modules) the numbering of the points would change. For most customers this would cause some confusion if they refer to the points by number. If however they only know the points by name, then only the CSC must be updated. Remember, point numbers 73 through 127 and 193 through 247, must be D9127 POPITs. For example, to keep point 73 reporting as point 73 you must change the POPIT to a D9127 and connect it to the data backbone of the first D8125 POPEX module.

### OctoPOPITs

OctoPOPITs face the same numbering issue as POPITs but since they are typically mounted in or near the control enclosure they shouldn't pose much of a problem.

### Upgrade 5505 or 5700

The D8125 module for either of these controls will need to be replaced, unless recently added to the 5505. OctoPOPITs will also require replacement.

## Tech Support for Readers

Radionics technical support organization is prepared to support the WSE 4205W credential reader. Readers purchased from Radionics must be returned to Radionics for warranty repair.

## C801 Cellular Interface

### Memory Recall Dialing

The C801 will need one item programmed using a handset or lineman's test set. This item is known as memory recall dialing. Memory recall dialing provides the phone number the C801 will call instead of the number coming from the control/communicator. This is required because most systems will be required to make a long distance call, even if it is a local number, as a result of being a "roaming" cellular phone. Using this feature, as opposed to programming a long distance number as one of the four phone numbers in the control/communicator, will minimize the amount of time before a valid number can be dialed. Memory recall dialing should be used anytime the area code of the cellular phone number assigned to the C801 does not match the local area code. This item cannot be programmed remotely.

### Separate Transformer

The C801 requires a separate transformer for AC power. This is due to the significant amount of current required during transmission.

### Cellular Activation

Look for a separate bulletin relating to the activation process for cellular service.

# Section Eight
# Customer Service Center

## Section Eight - CSC

Details regarding CSC support for the “C” and “DSCC” versions have been sent separately as a bulletin.

# Section Nine
# Sales

## Section Nine - Sales

### Reporting Systems with Entry Control

The current codes of **58** for 5800, **59** for 5900 and **60** for 5924 should continue to be used. Entry control systems should also indicate the number of 9210s sold in the New Products Required This Sale Section using the code **61**. Product codes for other products mentioned in this guide;

- 46 = HSL Transmitter (DSCC)
- 47 = Cellular Transmitter (C801 or Telguard)
- 48 = Long Range Radio Transmitter (any)
- 56 = Intelliguard 5600
- 58 = Intelliguard 5800
- 59 = Intelliguard 5900
- 60 = Intelliguard 5924
- 61 = D9210 Access Module

.

# Section Ten
# Competition

## Section Ten - Competition

This section will look at competitive products in the integrated access control market. This includes the Silent Knight 4821 and the Access 2000. The information is based on current understanding of these products. It is subject to change as updated information is received.

## Radionics

Many of you compete against local alarm companies that use Radionics products. Radionics will market both an integrated access control product and the standard Burg/Fire product without access control. We made the decision to make all of our panels, moving forward, entry control capable.

The Intelliguard 5900C is a customized version of the Radionics 9412. It has all of the same features of the 9412 plus the reliability that is traditional with Radionics products. In addition, the 5900C has the exclusive features not offered in the Radionics product. Radionics will continue to market the 9112, with the new capacity and operating enhancements but without access control.

The Intelliguard 5800C is our custom version of the 7412. In addition to the exclusive features, mentioned in the introduction, the 5800C will support 4 doors of entry control, the 7412 is limited to 2 doors. The 7212, the basic burg/fire panel, will also feature the new capacity and operating enhancements.

## Silent Knight

Silent Knight offers two products that compete with Intelliguard Entry Control systems. The following information was obtained from their WEB page.

### Access 2000

- 16 zones
- 8 doors
- 500 users
- Wiegand or Prox

### Census 4821

- 400 points
- 8 areas
- 24 doors
- 1800 users
- global/local anti-passback
- 50 scheduled events
- local or remote management software

# Section Eleven
# Support Materials

## Section Eleven - Support Materials

### Updated Brochure

The Intelliguard brochure (56-5008) has been updated to include reference to entry control.

### Updated Data Sheet

The Intelliguard 5800/5900 Security System Data Sheet (56-5013) has also been updated with reference to entry control and specification data.

### Demo Upgrade

One of your D8620 demo cases should be upgraded during the technical training provided by Radionics. Any other demo cases should also be upgraded as follow-up to the training process. The upgrade includes a new control, D9210 access control module and a tethered WSE 4205W reader. The reader can be placed out of site behind the faceplate during demonstrations that don't include entry control.

# Section Twelve
# Guide Specifications




Form No. 56- 4140 1/97