HONEYWELL SILENT KNIGHT

3 VIRTUAL TRAINING MANUAL

FED®

LEARNING CENTER

COMMUNICATION TECHNOLOGIES & FIRMWARE UPDATE PROCEDURE

Terminology

DACT
- Digital Alarm Communicator Transmitter

DACR
- Digital Alarm Communicator Receiver

RJ31X
- Phone Jack
- Required by FCC

POTS Line
- Plain Old Telephone System
- Copper Line

CID
- Contact Identification – Reporting format developed by Ademco Manufacturing

SIA
- Security Industrial Association – Reporting format developed as a standard for reporting to central stations

IP
- Internet Protocol - Language used by computers to communicate via the internet

Communicator Examples

Each FACP can do its own reporting
Each using different types of communications and formats

1 FACP can be designated as the communicator for all sites
Still using different types of communications

Phone Line Terminals

Tip and Ring Connections

TELCO Line 1 & 2
Panel uses TELCO to call out

DACT Reporting Formats

Both Formats Will Report by Zone or Point

Contact ID
No Panel ID reporting
- Each panel can report different zones or have its own account number

SIA
SIA 8 – 8 events per call
SIA 20 – 20 events per call
SIA 500 – 500 bytes per call
Panel ID reporting
- Each panel can have its own unique ID and share the same account number

Contact ID

Event Format = AAAAIIQEEEMMZZZK	
AAAA	Account number
II	Message type always 18
Q	Event qualifier 1 = New, 3 = Restore, 6 = Old
EEE	Event code - 3 digits (see manual)
MM	Used to report the module number the point is linked to. Zone reporting does not send module number but will 0 fill. Used to report partition # for Ademco Security.
ZZZ	Zone number reporting the Alarm (001-999) or Point ID (zero filled)
K	Message sum

Example 1:
Zone Reporting
Manual pull alarm on zone 15
Account number 1234
- 123418111500015C

Example 2:
Point Reporting
Heat detector alarm on point 8 module 2
Account number 1234
- 123418111002008C

Events are sent to the central station as a fixed string of 16 digits

CID Link Reporting Examples

Will Report Without Panel ID
Report by zone
Different zones for each FACP

| Panel 1 | Panel 2 | Panel 3 | Panel 4 |
| Zones 1-199 | Zones 200-399 | Zones 400-599 | Zones 600-999 |

SIA Without Panel ID

Example 1:
One event
- Fire alarm on zone 15
  – FA15

Example 2:
Two events
- Module 10 / fire alarm, point #5
  – pi10/FA5

Event Format = EEZZZZ	
EE	Event code (2 characters)
ZZZZ	Event parameter (zone or point) (up to four digits - not zero filled)

SIA With Panel ID

Example 1:
Zone
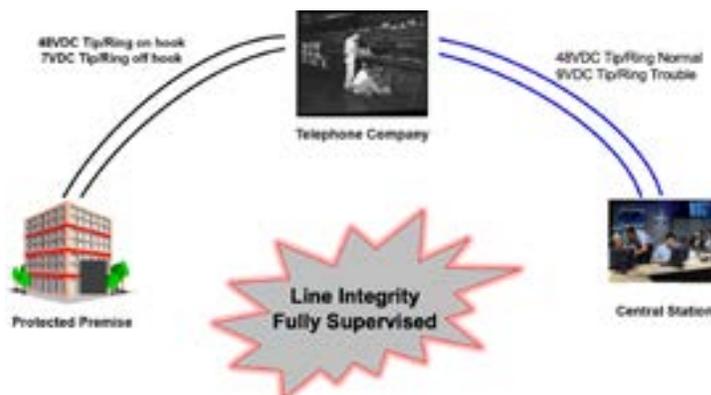- Fire alarm, panel 1, zone 15
  – FA01000015

Example 2:
Point
- Fire alarm, panel 1, module 97, point #5
  – FA01970005

Event Format = EEPPMMZZZZ	
EE	Event code (2 characters)
PP	Panel ID (2 digit - zero filled)
MM	Module address (2 digit - zero filled)
ZZZZ	Event parameter (zone or point) (up to four digits - not zero filled)

DACT Communications Path w/ POTS Lines

DACT Communications Path New Phone Lines
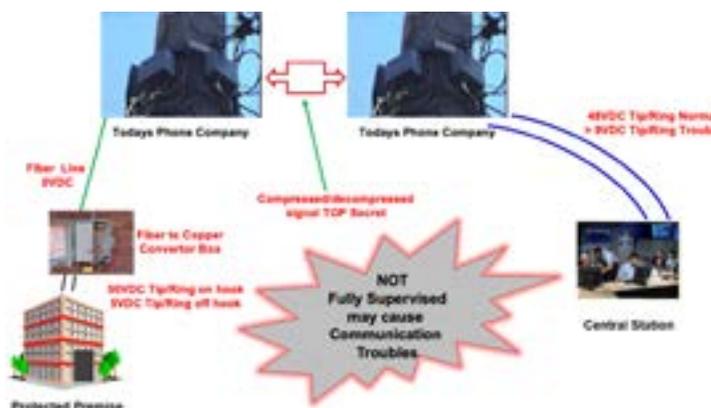
DACT Troubles

Phone Line 1 or 2 Trouble
- Less than approximately 3 VDC across tip and ring
- Up to a 2-minute delay

Comm (1 or 2) Trouble
- Failure to communicate to the receiver using phone line (1 or 2)
  - Remote supervising station phone line busy
  - Phone number programmed incorrectly
  - Incompatible reporting format
  - Defective or incompatible phone line

Receiver (1-4) Trouble
- Failure to communicate to the receiver phone number (1-4)
  - Remote supervising station phone line busy
  - Phone number programmed incorrectly
  - Incompatible reporting format
  - Defective or incompatible phone line

NFPA 72 References

The IP or Cellular Communicator meets all requirements for a Single Communication Path (no redundant communications required)

- – Under the following section: Other Communication Technologies
  (now Performance-Based Technology)
- 2002 edition of NFPA 72 section 8.5.4
- 2007 edition of NFPA 72 section 8.6.4
- 2010, 2013, and 2016 of NFPA72 section 26.6.3

Single Communications Path

Shall be permitted and the path shall be supervised at an interval of not more than 60 mins

- NFPA 72 2010 is 5 min
  - – 26.6.3.1.5 (NFPA72 2013)
  - – 26.6.3.3 (NFPA72 2016)

Multiple Communications Paths

NFPA 72 2013 26.6.3.1.6

- If multiple transmission paths are used, the following requirements shall be met:
- Each path shall be supervised within not more than 6 hours
- The failure of any path of a multipath system shall be annunciated at the supervising station within not more than 6 hours
- The failure to complete a signal transmission shall be annunciated at the protected premises in accordance with Section 10.15
  - – NFPA 72 2016 (26.6.3.4)
  - – NFPA 72 2010 (26.6.3.1.4.2 Supervision is 24 Hours)

6000 Series IP Built-In Communicator

- Integrated communicator
- Contact ID reporting
- Single path
  - – UL listed
- Utilizes AlarmNet

Benefits of IP Connectivity

- Eliminates phone line cost
- Built in connectivity
- Simple installation
- Secure connection - 256-bit AES encryption
  - Banks use for credit card transactions

IP Troubles
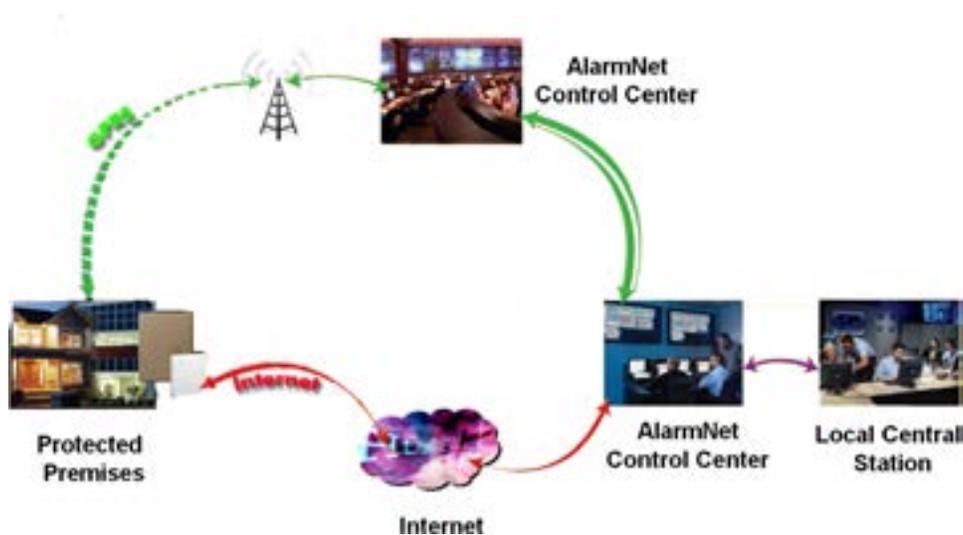
Ethernet Fault
- Can't establish a link with the local router
- Ethernet cable is not plugged in

AUTOTEST COMM ERROR Receiver # Ethernet
- Occurs when ethernet auto test fails
- No internet connection

IP/Cellular Communications Path

AlarmNet REGISTRATION Troubles

Registration Fail
- Received acknowledgment from the AlarmNet server that registration has failed for an unknown reason

Database Full
- Received acknowledgment from the AlarmNet server that the destination central station database is full and cannot accept new subscriber accounts

Subscriber ID Rejected
- Received acknowledgment from the AlarmNet server that the subscriber ID is rejected (generally an incorrect subscriber ID was entered)

Account Disabled
- Received acknowledgment from the AlarmNet server that the subscriber account has been disabled

PIN Required
- Received acknowledgment from the AlarmNet server that a PIN is required or a previous PIN that was used was bad.
  - This typically occurs because the FACP's MAC address has changed (FACP replaced). The user need to get a temporary PIN from AlarmNet website and enter it in the FACP to register the new MAC address with the existing subscriber account.

CLSS-Enabled 5G LTE-M Commercial Fire Alarm Communicator

The CLSS-Enabled 5G LTE-M Fire Alarm Communicator transmits alarm signals from the fire panel over the 5G/LTE-M networks to the designated monitoring station while leveraging connectivity with CLSS to enable powerful tools
  - AT&T (HW-TG7FS-A)
  - Verizon (HW-TG7FS-V)
- Compliant with 2019 and earlier editions of NFPA 72, the CLSS LTE Fire Communicator can serve as the sole communication path.
- For existing installations, all landlines dedicated to the master control unit can be replaced with a single CLSS 5G/LTE-M Fire Communicator because of its 5 or 60-minute supervision modes.

Transmits fire alarm signals through the Telguard Communication Center

Features & Benefits:

Dialer Capture Communicator Features
- Certified for use on AT&T 5G and Verizon 5G networks
- Sole, primary, or backup path communications
- 5- or 60-minute supervision modes
  - 180 seconds available in Canada
- Alarm panel 12/24V auxiliary output
- 2 supervisory outputs and 1 trip input available
- Supports most common alarm formats: Contact ID, SIA2, pulse (3x1, 4x2), modem lle, IIIa, and DMP
- Locking, red metal enclosure
- Includes plug-in AC adapter with backup battery (available accessory)
- Software features included (mobile app and browser)
- (NOTE: CLSS features only available when using contact ID reporting)
- CLSS site manager
  - Dealer view of all accounts and real-time information on event generation
- CLSS facility manager
  - End user view of asset information across multiple sites and event alerts mobile app

> **Transmits fire alarm signals through the Telguard Communication Center**

Internal IP Dialer Setup

Receiver Configuration
- Enter the installer code
  - Default code is 123456
- Select option 6. Network Prog
- Select option 6. Communicator Optns
- Select option 3. Receiver Config
  - Select panel
- ► to enter reporting format, using the up or down arrow select: Ethernet
- ► to add the city ID, central station ID, and subscriber ID
  - All ID information must be four digits
- Press the ◄ back to Communicator Optns

> **Only use when programming internal IP dialer**

Reporting Table Setup

In Communicator Options

- Go to the reporting table
  - Option 4
- Press the ✳ (asterisk) to add row
- ► to move, then ▲ to change reporting status to Y or N for alarms, supervisory, and troubles
- ► for primary receiver which should auto fill
- ► to test primary account
  - Select Y or N
- ◄ to exit and then ▲ or ▼ to save changes
- Once reporting table is setup you can manually register AlarmNet
- Select option 1. System Tests
- Select option 8. Register AlarmNet
- Press the ► for Yes

Only use when programming internal IP dialer

Updating Panel Firmware

6000 Series Firmware Updates

The Honeywell Silent Knight 6000 Series addressable fire alarm control panels were designed to accept panel firmware updates.

Updating the panel to the latest released firmware is highly recommended in order to fix known issues and add additional features and product support.

*Note: Honeywell Fire Software Suite (HFSS) is required in order to perform firmware upgrades.

Locating the Firmware Version

Two ways to locate the Firmware Version for the FACP

Annunciator
- Internal
- Remote
  - Go to: Main Menu/System Info

HFSS
- Go to: Computer Access Details

Updating the Firmware

Download, then extract the latest firmware file from the Silent Knight website
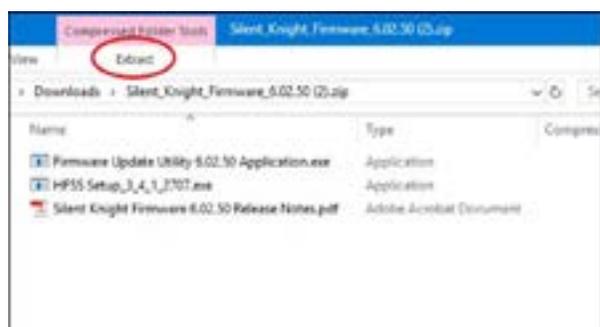
Read the Release Notes for information about the update

Open HFSS

Check the Status Bar
- Waiting on USB port
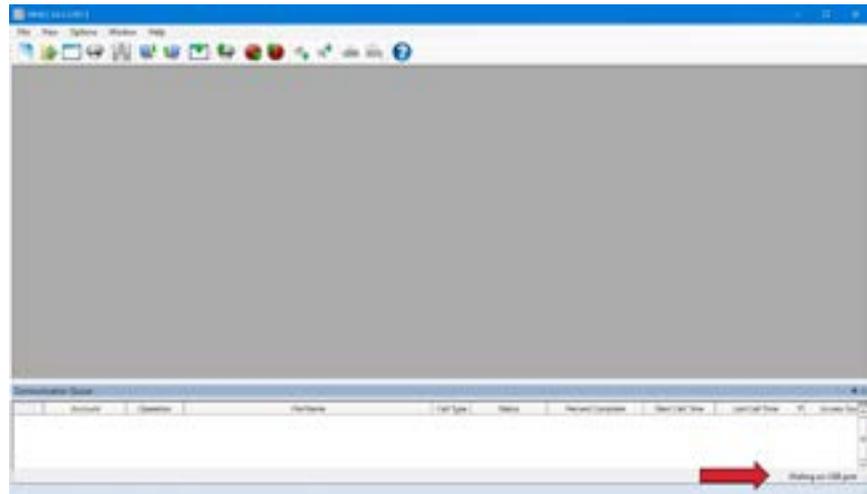
*Get Configuration – To create a backup of the program

Click on Firmware Update Utility icon

- Click: Run

Click Update
- Click Yes to Update
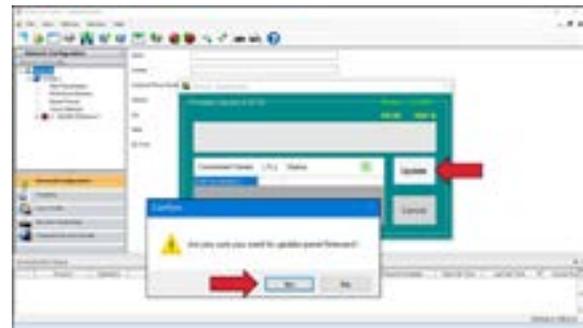
When Updating the Panel
- Erase data
- Update data to the panel
  - If you receive an error while updating data to the panel Do not reboot
- Completed successfully
  - Panel will restart
  - Once completed successfully you can disconnect your USB from the panel
- Panel may complete additional updates
  - SBUS
  - SLC
  - Do not power down panel until has completed internal updates
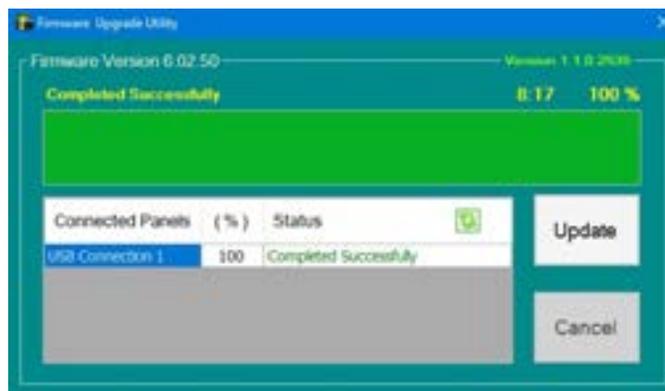
COMMON COMMUNICATION LINK

Common Communication Link

The 6000 Series panel can be networked to create a virtual system that is larger than 1,110 addressable points.

Must be in conduit 2' cable

External SK-NIC wiring option

Class B wiring

Class A wiring
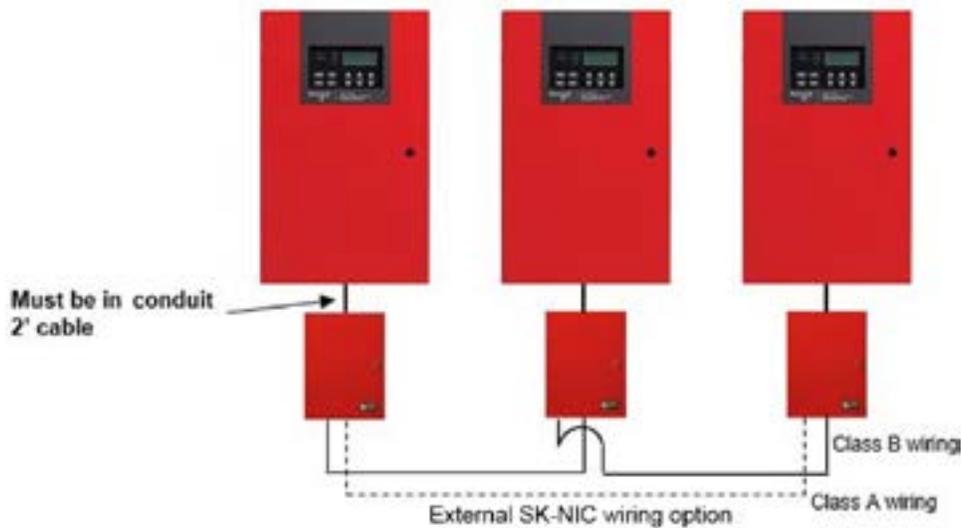
> **Example, a network of 17-6820/EVS panels provides a maximum addressable point capacity of 18,870 points (1,110 x 17 = 18,870 SK devices)**

Panels

6700   6808   6820   6820EVS

Panels can be linked together for common communications to the central station
Up to 17 panels can be linked
All panels need to have unique ID number
All panels need to be in their own site

> **An SK-6700, SK-6808, SK-6820, and SK-6820EVS can be linked together**

Site

A panel in a site is isolated from other linked panels
- Separate buildings
- Isolate panels within a building based on location needs

Events from one site are not shared with other sites

Prevents events such as an alarm, supervisory, or trouble from being remotely reset or silenced
- A multi-site annunciator can be added to view events from other sites

There can be up to 17 sites in a network

Can have one panel per site
- Site names can be customized
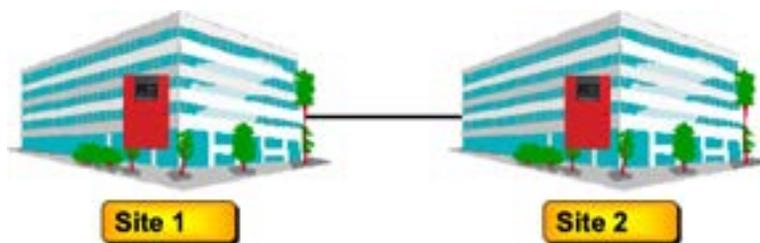
Multi-Site Annunciator

Multi-Site Annunciators are unique as they can display the status and event history of all sites they are assigned to.
- Useful in guard shacks or security centers
- A multi-site display is indicated by the words "Multi-Site Display" at the top of the idle screen
- SK-6700, SK-6808, SK-6820, and SK-6820EVS menu system is disabled on a multi-site annunciator
    - Pressing ENTER or the Right Arrow brings you directly into View Event History and allows you to view the Event History from every panel in each of the sites that the multi-site display is assigned to
- To access the menu system
    - A multi-site user password must be entered and then a site must be selected from the site selection menu to gain access to the selected site. The annunciator will then temporarily act as a single-site annunciator

The ACK, DRILL, RESET and F-Macro keys are disabled until a multi-site user access code has been entered and a specific site has been selected
Multi-Site Annunciator silencing rules:
- If any of the assigned sites are silenced, the silenced LED will be lit
    - This is called being locally silenced
    - A locally silenced multi-site annunciator will display a blinking silenced LED
- If any new troubles, supervisory, pre-alarms, or alarms are triggered in any assigned sites, locally silenced annunciator will resound
- If a multi-site annunciator is locally silenced for 4 or 24 hours depending on the System Auto-Unsilence time set in the Panel Parameters, the locally silenced annunciator will resound

A multi-site annunciator will sound the highest priority tone from the sites it is assigned to

A multi-site display is created in Module Programming in the edit properties menu for an annunciator
- An annunciator cannot be programmed as a multi-site display when it is associated with an EVS-VCM or EVS-RVM in a EVS system

Network System Hardware Features

SK-NIC
Uses unshielded, twisted-pair wiring or fiber optic cable

Same footprint of a 6815/5815XL
- Each SK-NIC will monitor for earth ground faults on the twisted pairs connected to port 1 of its terminal block TB2.
- Earth fault detection for any wiring at port 2 of TB2 is done at the next/previous SK-NIC

*Each Linked FACP on the network MUST have a SK-NIC

SK-NIC Card

Mounting
Can be installed in the FACP
- Except with 6700
- Same footprint of a 6815/5815XL

Can be mounted outside of panel using SK-NIC-KIT

SK-NIC-KIT Mounting Kit
- Available accessory kit that includes
  - SK-NIC
  - Small cabinet with door
  - Extended cable & mounting hardware
  - The accessory kit is required to install the SK-NIC outside of the SK-6700 cabinet
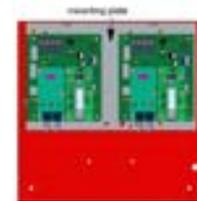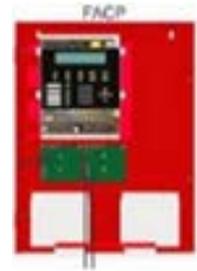
*Up to two SK-NIC cards can fit inside the 5815RMK

Networking Hardware

SK-NIC Connections

Copper Wire
- 16 to 18 AWG twisted-pair, unshielded
  - 3 twists per foot
- Up to 3000 feet of separation between each node

Fiber Optic Single Mode
- Optimized for 9/125 micrometer cable @ 1310 nm

Fiber Optic Multi-Mode
- Up to 200 microns optimized for 62.5/125 microns
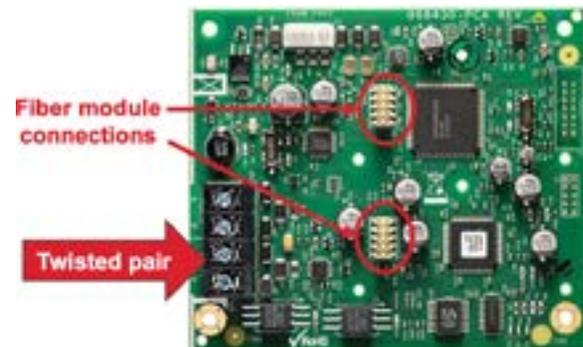
Has 625K baud ARCNET Repeater

Fiber Loop Modules

Two types of fiber optic modules are used as one channel to transmit or receive communications

SK-FSL (Fiber-Optic Single-Mode)
- Connection: LC style 9/125 micrometer
- Up to 30dB loss between nodes

SK-FML (Fiber-Optic Multi-Mode)
- Connection: ST style 62.5/125 micrometers
- Up to 8dB loss between nodes

SK-FSL

SK-FML

*Up to two fiber cards can be added to the SK-NIC Both cards may be combined in the same configuration

Network System Hardware Features

1 3000 ft — Unshielded Twisted Pair

2 30 dB — Single-Mode Fiber

3 8 dB — Multi-Mode Fiber

All 3 methods of panel connectivity can be used within the same networked system

Networking Hardware

Connecting 2 SK-NICs
- Edit SBUS module to define ports used
  - UTP copper
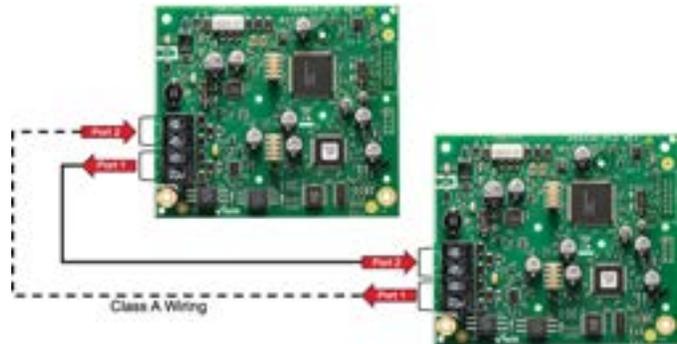
*Must connect from the out of Port 1 (NIC #1) to the in on Port 2 (NIC #2)

Connecting 2 SK-NICs
- Edit SBUS module to define ports used
  - Single or multi-mode fiber
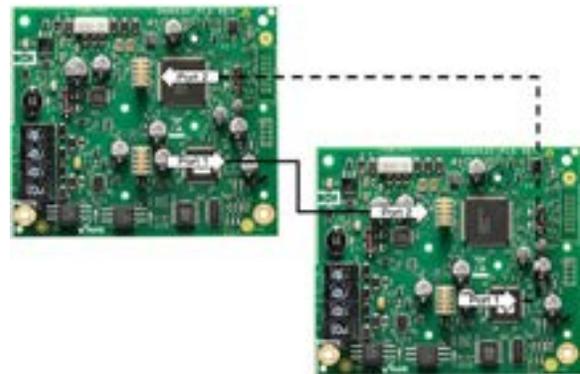
*Must connect from the out of Port 1 (NIC #1) to the in on Port 2 (NIC #2)

SK-NIC Connection to Panel
6-pin cable connects SK-NIC to panel
labeled Data Network
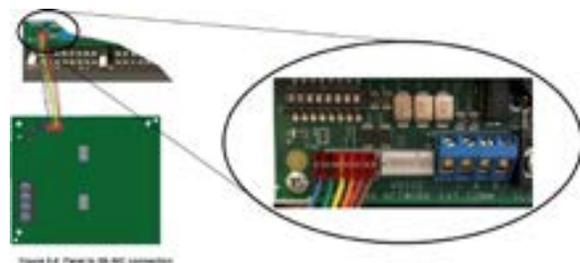
*Do Not bridge the Date Network and Voice Network pins

Setting Network Panel ID

Set using DIP switch positions 1 - 17
Valid range of network ID's is 1-17
- Dipswitches 6, 7, and 8
    - Not utilized

NOTE: It is important that much thought is given when choosing the panel IDs for each panel. It can be difficult to change the IDs once panel programming has begun.

> You MUST default the panel when changing the panel ID
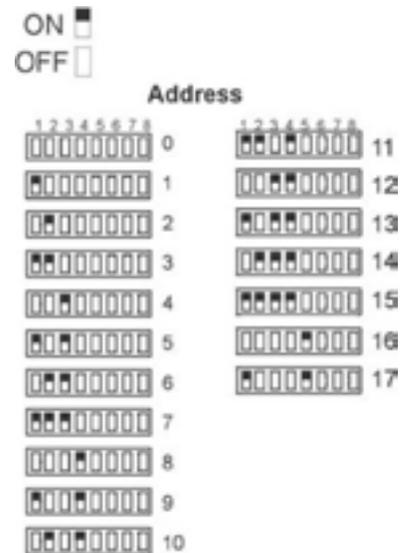
Linked Panels in HFSS

The first time you get configuration after learning the network in HFSS, you will notice all panels are assigned to Site 1.

Using HFSS you will must re-assign the panels to their own site.

> Panel ID must match Site ID for complete Mapping
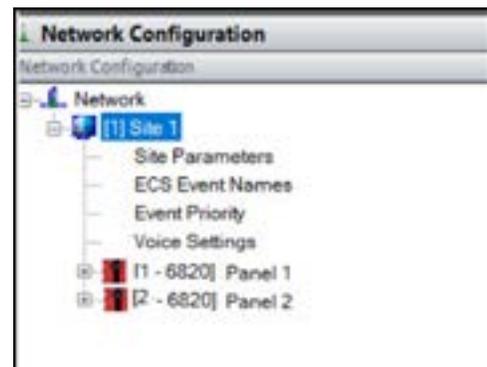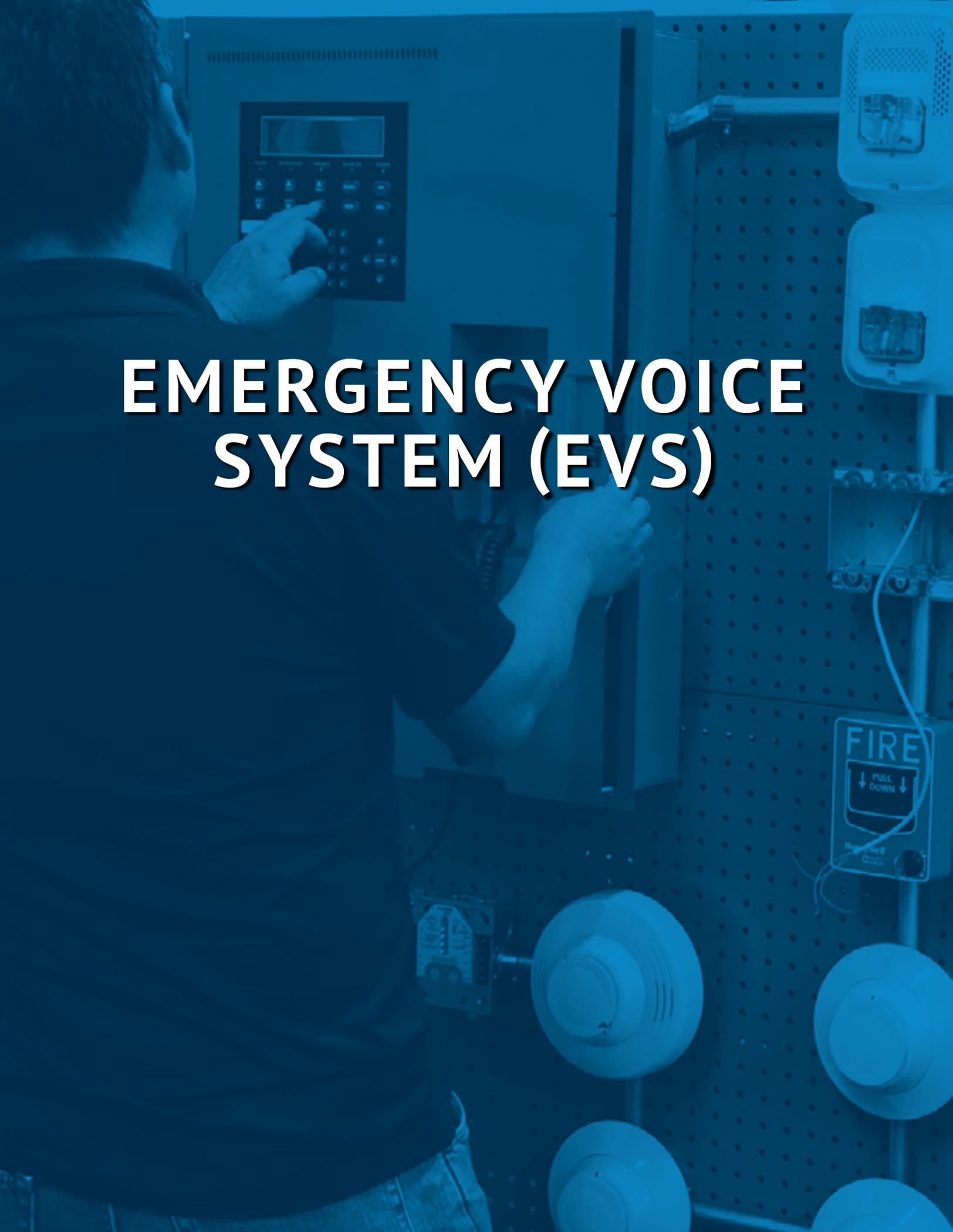
EMERGENCY VOICE SYSTEM (EVS)

Mass Notification System (MNS)

NFPA72 – 2010

National Fire Alarm and Signaling Code
- Systems used for more than just fire hazards
- EVS message can be higher priority than Fire
- Weather, terrorist attacks, chemical hazards

Risk Analysis
- To be developed for each facility
- Basis for emergency response plan
- Consider fire and non-fire emergencies
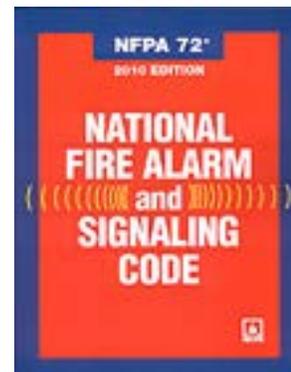
New Chapter 24 – Emergency Communications Systems
- "Protection of life by indicating the existence of an emergency situation and communicating information necessary to facilitate an appropriate response and action"

Visual Appliances NFPA 72 2010

In-Building EVS
- Where audible notification is provided, MNS shall also provide visible notification information to serve the hearing impaired and for high-noise areas

  NFPA 72 2010 24.4.2.19.1

- Strobes used in combination systems where the same strobe is used for MNS and fire alarm, it shall be clear and meet UL1971, have no marking or be marked "ALERT"

  NFPA 72 2010 24.4.2.20.4

- Strobes used for mass notification shall meet the synchronization requirements

  NFPA 72 2010 24.4.2.20.10

Visual Appliance Network

Individual Building MNS
- Strobes are located as required for a fire alarm

  UFC 4-3.4.2

- Combined MNS/FACP systems may use either one clear strobe or two strobes ...clear for fire and amber for MNS as specified by the AHJ

UFC 4-3.4.2

- Clear strobes activated by the fire alarm system shall not operate during periods when the amber strobes are in operation, but otherwise shall operate continuously until the fire alarm system is reset

UFC 4-6.2.3

NFPA Voice Evacuation Control Locations

- Control locations shall be secured to allow access only by trained and authorized personnel

NFPA 72 2016   24.4.5.2

- If there are multiple voice/alarm control locations, only one shall be in control at any given time

NFPA 72 2016 24.4.5.4

6820-EVS

EVS-VCM

- 15 messages
- 8 programmable EVS events
- 16 audio switches
- Slot for additional switches EVS-SW24
  - Total of 40 audio switches

Flexible Event Programming for Fire and EVS

Voice Load Software

Specific Reporting Codes for EVS events
- List in manual

Up to 8 Amplifiers (1000 watts)
- Any combination
  - EVS-INT50W
  - EVS-50W
  - EVS-125W
  - EVS-100W

Up to 4 EVS-LOCs

EVS-LOC (Local Operating Console)

UL Version EVS-LOC

Contains
- EVS-RVM
- SK-6860
- Microphone

8 Programmable EVS Events

Installation

Connect EVS to at least 1 amplifier
- Connect via SBUS

Wire VBUS to each amplifier
- Class A
- Class B
  - Needs 15k EOL resistor
- No T-tapping allowed

Amplifiers

EVS-INT50W
- 1 circuit, 50 watts
- 25 or 70 volts

Mounted internally on SK-6820EVS
- EVS-LOC or SK-5895XL

Power by FACP
- Constant aux power - 2.9 Amps

UL listed for 520Hz tone output when used with compatible speakers

EVS-INT50W Layout

Amplifiers

EVS-50W and EVS-125W
- 4 circuits

Class A or Class B
- Add an EVS-CE4 to gain an additional 4 circuits

EVS-50W
- 50 watts total
- All circuits rated for 50 watts
- 25 and 70.7 volt RMS options

EVS-125W
- 125 watts total
- Circuit 1 – 100 W capable
- Other circuits are good for 50 W
- 25 volts RMS only

EVS-50W & EVS-125W Amplifier Layout
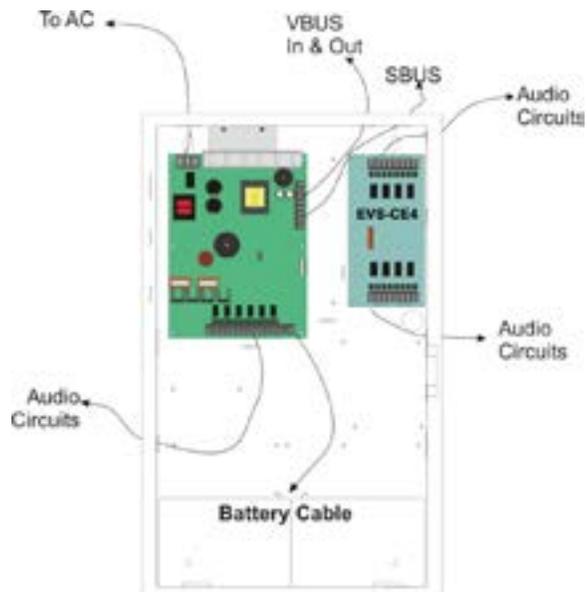
EVS-100W

8 speaker circuits
- Class A or Class B
- All circuits rated for 50 watts

Program as 50 W
- 50 W as backup

Program as 100 W
- 50 W backup using optional EVS-50WBU

25 Vrms or 70.7 Vrms operation

Has built-in test switches to test backup amp

UL listed for 520 Hz signaling when used with compatible speakers
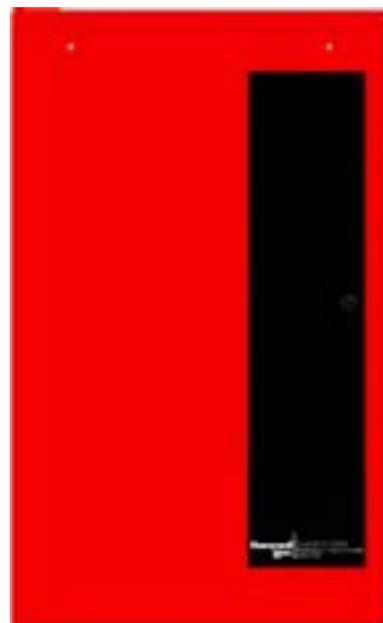
EVS-100W
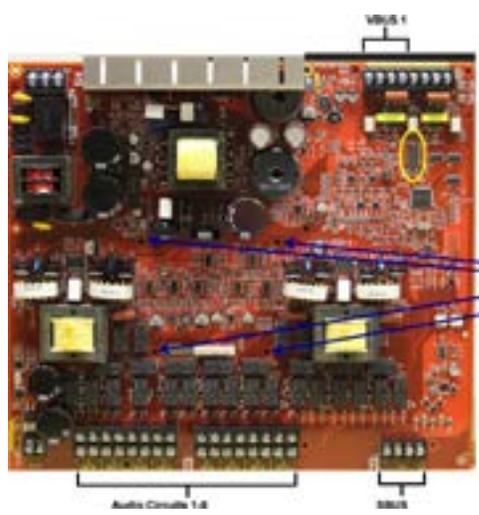
- Dipswitch for SBUS address
- EVS-50WBU mounting holes

EVS-50WBU

Provides 50 watts backup
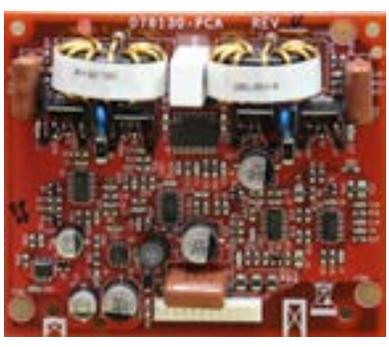
EVS-100W Test Switches

SW 1 Amp A
  - "ON" during normal operation
  - "Test" to test back up amp

SW 2 Amp B
  - "ON" during normal operation
  - "Test" to test back up amp
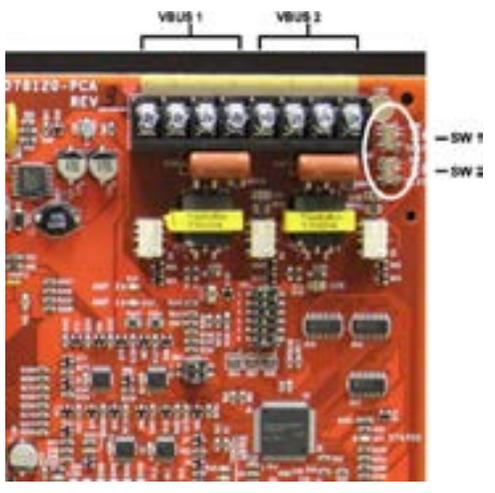
NOTE: Please allow up to 3 mins for backup amp to engage

EVS Amplifier Speaker Wiring
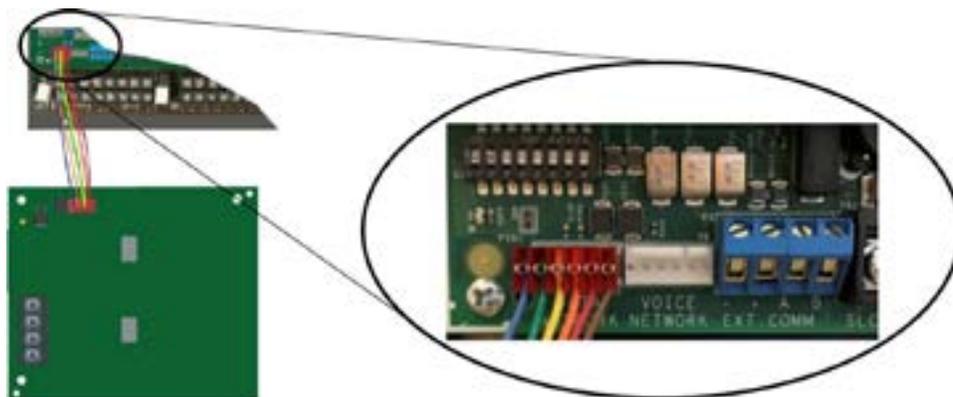
Figure 5-6 Panel to SK-NIC connection

The IN terminals are used for Class A speaker circuits
- No EOL required for Class A
- Twisted, shielded wire recommended

Wire Lengths

Number of Speakers		Total Load		Wire Distance in Feet			
@1/2 W	@1 W	Vrms	Watts	18 AWG	16 AWG	14 AWG	12 AWG
10	5	25Vrms	5W	3600	6200	9800	15600
		70Vrms		25000	39700	63200	100520
20	10	25Vrms	10W	2125	3380	5375	8540
		70Vrms		15200	24150	38400	61100
30	15	25Vrms	15W	1460	2320	3690	5870
		70Vrms		11000	17500	27800	44200
40	20	25Vrms	20W	1100	1750	2780	4420
		70Vrms		8500	13510	21500	34175
52	26	25Vrms	26W	760	1200	1920	3050
		70Vrms		6100	9700	15400	24520
80	40	25Vrms	40W	550	875	1390	2200
		70Vrms		4100	6500	10360	16480
100	50	25Vrms	50W	450	715	1130	1800
		70Vrms		3500	5560	8850	14070

Silent Knight recommends shielded wire for all speaker loops

EVS-VCM and EVS-RVM

8 dedicated buttons for activating EVS

Still has 16 Voice Output Group Selections
- 24 additional with EVS-SW24
- Up to 40 total SK-6820EVS

V-Bus
- Class A or Class B
- Twisted pair, shielded
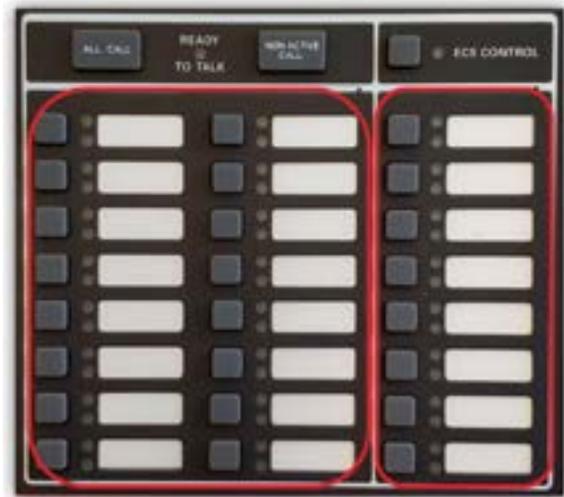
EVS-VCM or RVM Board Layout
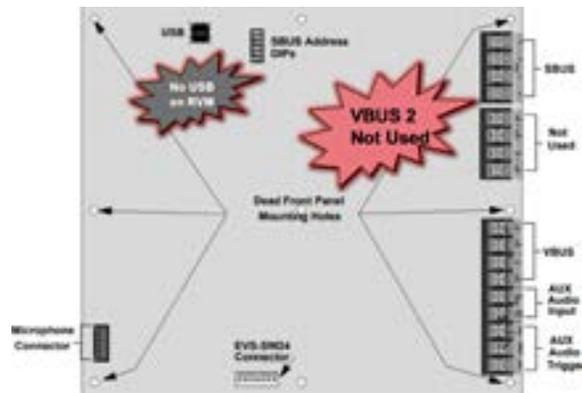
EVS-VCM or RVM board layout, take note that V BUS 2 is not used, and on the EVS-RVM there is no USB port.

EVS-VCM VBUS

VBUS
An analog voice bus the carries the recorded voice messages or messages created from the microphone from the EVS-VCM to the amplifier/RVM

Class A or Class B
- The maximum loop resistance on the VBUS is 20 ohms
- Twisted, shielded wire recommended on the VBUS 1 OUT
- VBUS 2 not used

Wire V BUS from EVS-VCM V BUS one OUT, to each amplifier, can be wired Class A or Class B. V BUS requires fifteen k EOL resistor. No T-tapping allowed
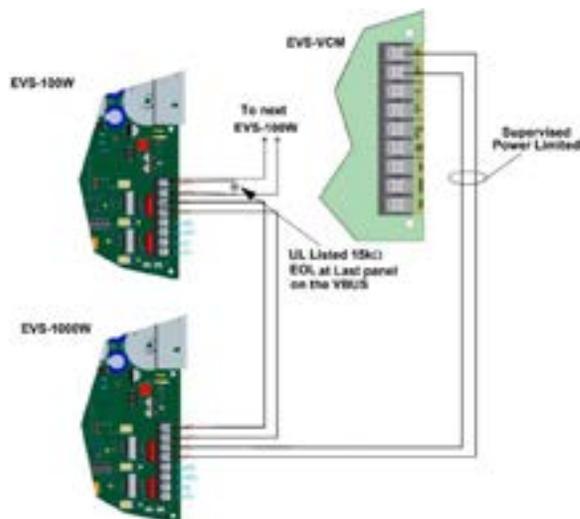
Line Input from Another Source

Using AUX Audio Input
- Recording messages
- Play messages from another source
  - PA system, Muzak, Reveille and Taps

AUX Audio Triggers
- Additional FACP input points
- EVS triggers (CDM1 or CDM2)
  - Voice aux status no alarm LED
    - Displays "Voice Aux 1 Active"
  - Voice aux EVS general alarm LED
    - Displays "EVS Aux 1 Active"
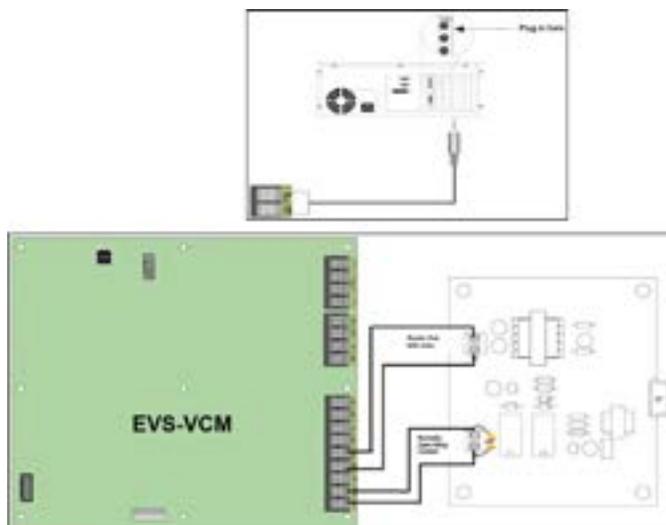
EVS Operations

EVS control can be gained at:
- Main panel
- EVS-LOC

Fire Fighter's profile
- Defaulted for EVS Control
  - Priorities are set through the Software Suite

User profiles
- Can be set to have EVS access

Super User profile
- Can override and gain control
- Installer profile (123456) has super user access by default

EVS Control Lockout
- Prevents two EVS devices from gaining control and changing EVS events in a short amount of time

Gaining EVS Control
- There are three things that govern whether or not EVS Control can be obtained
  - 1. LOC Priority
  - 2. LOC Lockout
  - 3. User profile access control

LOC Priority
- LOCs are assigned (by editing the EVS-VCM, or EVS-RVM) with a LOC priority of low, normal, or high
- LOCs with a higher priority are always able to gain control from a lower priority LOC
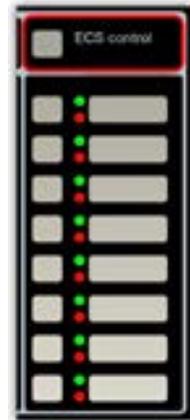
LOC Lockout

When LOCs are programmed to the same priority, LOC lockout timer applies

Lockout timer can be set between immediate and 12 hours in increments of 1 second or it can be set to never expire

- The default setting is 30 seconds and will restart upon any key press at the LOC with EVS control

LOC lockout will not allow an LOC to gain EVS control from the LOC with EVS control until one of three things happen:

- The LOC lockout timer expires. Once the LOC lockout timer expires, an attempt to gain EVS control can be made again
- The user at the second LOC requests EVS Control from the LOC with EVS control and that LOC grants the request. If the EVS lockout timer expires while an EVS control request is in progress, the system will automatically pass EVS control to the requesting LOC
- The user at the second LOC enters an access code with the EVS super user profile option

User Profile Access Control

- The user will need to enter an access code containing the EVS Control Request or EVS Super User profile option to gain EVS Control
  - If the access code has EVS super user, the EVS control request is ignored and activations by that user are always as EVS super user

Microphone Functions

Any microphone can provide live messages
- EVS or Fire System
  - If EVS is the highest active system, the user at an LOC must gain EVS control to do a EVS page
  - If fire system is the highest active system, any station can do a fire page
  - Risk assessment will determine priority levels
- Selective paging
  - Voice groups can be programmed to switches
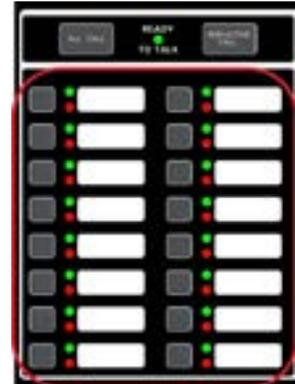
Paging

To use the microphone for paging
1. Push the PTT (push to talk) button on the microphone
2. Use the Select Keys on the LOC to toggle the output areas to page to with the microphone (illuminates the green LEDs)
3. Speak into the microphone
4. Release PTT button when finished

NOTE: The Ready to Talk LED will illuminate after an output area has been activated.

Recording Custom Messages

EVS-VCM has 15 recordable message slots
- Recording methods
  - Microphone
  - Aux input
  - EVS message management software tool
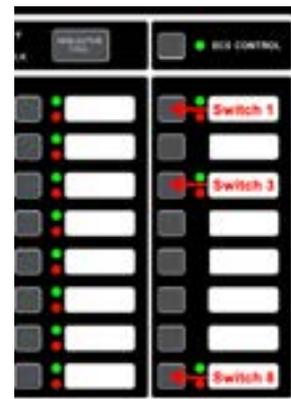
While in local recording mode, EVS-VCM switches will function as:

Key	Function
EVS Message Key 1	Select message slot to record to
EVS Message Key 3	Start and stop recording from Aux Audio Input
EVS Message Key 8	Erase user message 1-15
Select Keys 1-15	Message slot 1-15

Red LED when active

Local Recording

While in local recording mode voice switches 1-15 represents message slots 1-15

Switches 1-15 will function as:

Switch LED	Active LED Status	Meaning
Select Key 1-15 Green LED	On	Message is currently programmed in this slot
Select Key 1-15 Red LED	On	Message recording in progress
Select Key 1-15 Green/Red LED	Off/Off	Message slot is empty
Select Key 1-15 Red LED	Flashing	Message is being played back or message is selected for recording

Aux Audio Input Recording

Allows downloading of pre-recorded messages to any message slots 1-15, using Aux Audio input terminals

- Wire 1/8" mini plug to Aux Audio ground and IN terminals
- Plug mini plug into Line Out/ Headphone jack of PC or laptop
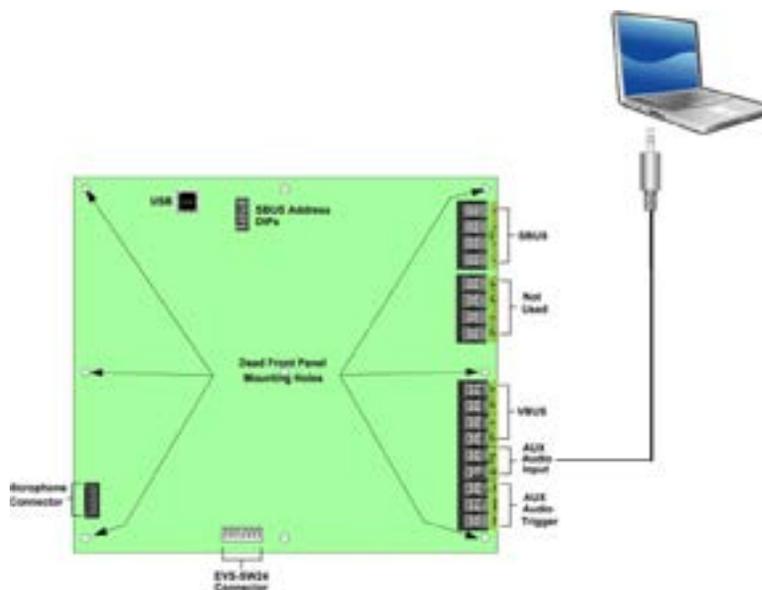
Erasing Messages 1-15
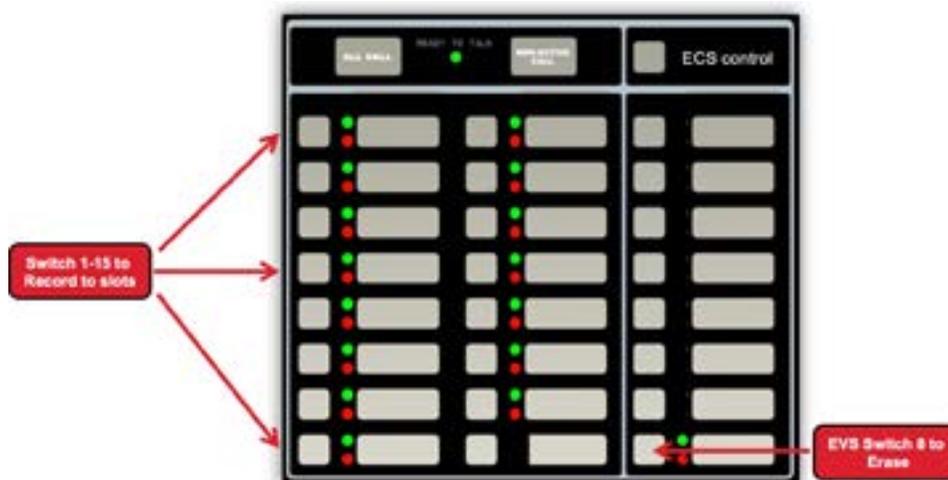
Switch 1-15 to Record to Slots

- EVS switch 8 to erase
- Enter "Panel Programming" at FACP
- Select option 8 "VCM Maintenance"
- Select amp and speaker circuit for playback
- All occupied message slots 1-15 will have
  - Green LED "ON"
- Press ECS switch 8
  - Red LED will be "ON"
- Choose a switch between 1-15 to erase message
  - Example – switch 5 (message 5)
  - When message delete process is complete
    - The LEDs for EVS switch 8 and switch 5 will turn off
- Cannot leave message slot empty
  - Panel will be in trouble

Microphone Recording
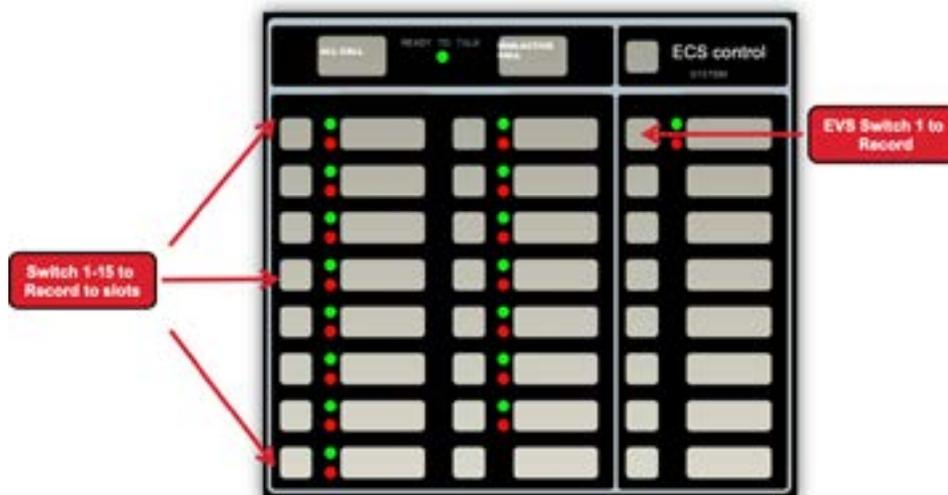
Recording a Message

- Enter "Panel Programming" at FACP
- Select option "VCM Maintenance"
- Select amp and speaker circuit for playback
- All occupied message slots 1-15 will have a Green LED "ON", empty slots will be off
- Press EVS switch 1 to record
- Red LED will be "ON"
- Choose an empty message switch
- Example – switch 5 (message 5)
- Red LED will be "FLASHING"
- Press push-to-talk button on microphone to record message
- Red LED will be on while recording
- Release push-to-talk button, when finished recording
- The LEDs for EVS switch 1 will turn off
- Message 5 Green LED will turn "ON" indicating message saved and Red LED will turn "OFF"
- Exit programming menu when completed

HFSS Message Management Software Tool

Utility software used to Upload and Download ".SKE" or new ".SKE1" messages
- Compatible with older generation VIP and EVS/ECS panels
- Connect directly to the USB port on the VCM
- Pre-recorded messages saved on PC or laptop
- Messages downloaded from Silent Knight website
  - Contact Tech Support (messages not available on website)

Can move messages from various message slots

Download from any EVS/ECS series panel page

ECS=Farenhyt Emergency Communication System
EVS=Silent Knight Emergency Voice System

Panel must be in normal condition

Connect PC or laptop to the VCM with standard USB printer cable

Select either:
- Get voice message
  - Upload message from the VCM and store onto PC or laptop
- Set voice message
  - Transfer a ".SKE1 file" from PC or laptop onto the VCM
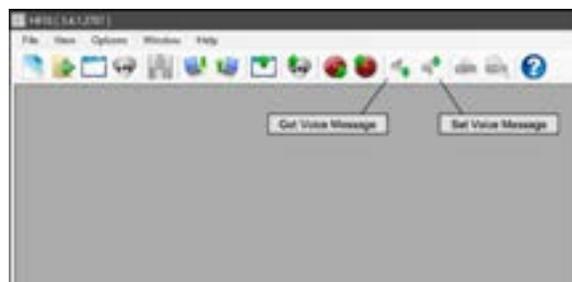
Get Voice Message

Used to download the message to the computer
- USB icon must be green and connected

Select message ID
- Selects the message to extract from the VCM

Select file location
- Choose where you want to save the message on the PC

Click download voice

Set Voice Message

Used to upload the message to the VCM
- USB icon must be green and connected

Select message ID
- Selects the message to send to the VCM

Select file location
- Locate the message stored on the PC

Click upload voice

EVS-VCM Keys and LEDs

Select Keys

The Select Keys are used to toggle which output areas are active
- If **Message Mode** is active, the select keys will toggle which areas the active message is distributed to
  - Also activates the red select key LEDs that are assigned to the mapped groups
- If **Microphone Mode** is active, the select keys will toggle which areas the microphone audio is distributed to
  - Also toggles the green select key LEDs that are assigned to the mapped groups
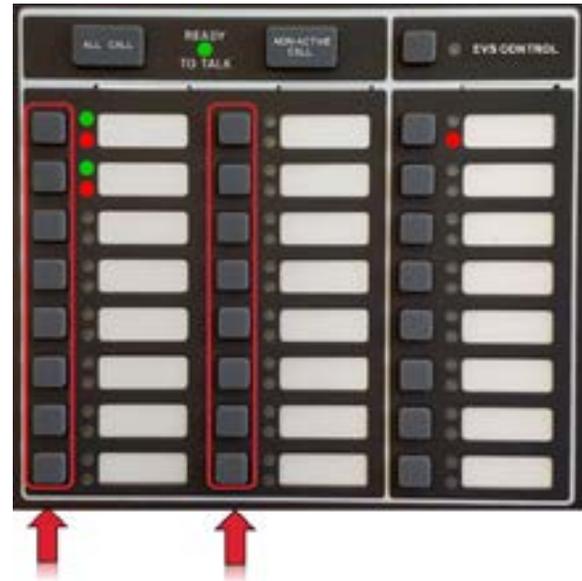
NOTE: For LOC activated EVS events, if an area is programmed through mapping to be active that area is automatically selected and can not be deactivated using the Select Keys

Select Key LEDs

Used to indicate which output areas are active for a microphone page or system events
- Green LEDs: active areas for microphone paging
  - These are only active when the microphone PTT (Push To Talk) is engaged
- Red LEDs: active areas for system events
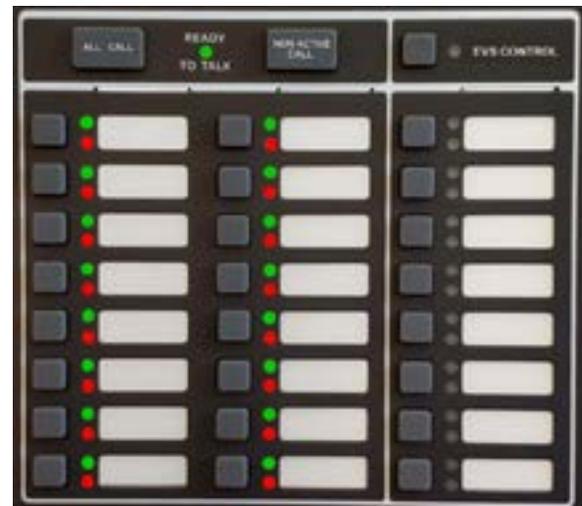
EVS Control Key

Pressing the EVS Control Key will do one of two things:
- Enter Message Mode of the LOC EVS interface
  - Including trying to gain EVS Control if the user doesn't have it already
- Relinquish EVS control if pressed while in message mode

EVS Control LED

The EVS Control LED is used to indicate the status of EVS Control in the system
- Solid
  - The LOC has EVS control within the system
- Blinking
  - Another LOC has gained EVS control in the system

EVS Message Keys

Used in Message Mode to select which EVS Message is to be played
- If LOC does not have EVS control
  - The system will automatically try to gain EVS control before allowing the EVS event to be activated
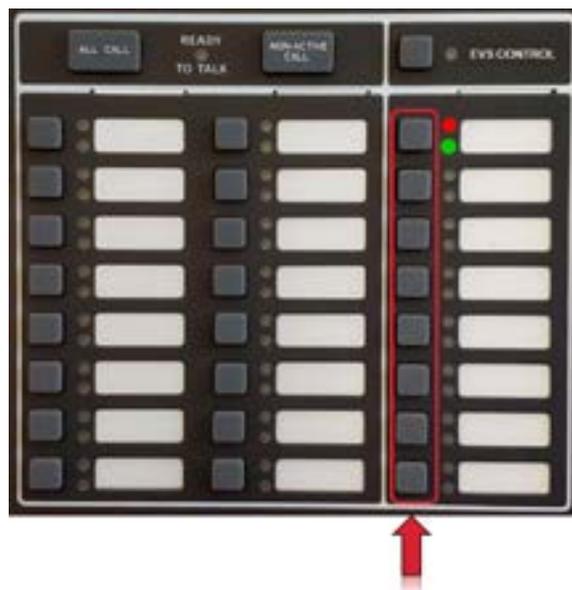
EVS Message LEDs

The red EVS Message LEDs indicate the active EVS message and any previously active EVS messages
- If the EVS message was activated by a point, the red LEDs on the LOC will turn on to indicate what messages have been activated
- In manual EVS state, the red EVS message LEDs will indicate which EVS message has been activated at an LOC

The green LEDs indicate the EVS message was selected in message mode and that the LOC has EVS control
- The green EVS message LEDs will activate for the LOC that activated the EVS message

HFSS with EVS

Site General Parameters

- Auto upgrade emergency commands
- Auto upgrade fire commands
  - Will automatically override active message to the highest priority event message selected

Site Parameters

- Chirp bypassed system NACs
- Chirp On full silence
  - Will activate outputs every 30 seconds
- Enable EVS button priority
  - When selected EVS switches 1-8, will follow priority sequentially
- LOC lockout timer
  - Never expire
  - Immediate
  - 0-12 hrs

Select: EVS Event Names

- Can rename EVS events up to 40 characters
- Auto reset time
  - Never
  - Disable event
  - 0-240 minutes

Select: Event Priority

- Can change priority of events
  - Click and drag desired event to proper priority
- Determined by risk assessment

Select: Voice Settings

- Can change per event type

Tone
- Plays between message

Message Repeat

Initial Message Delay
- Tone plays prior to start of message

Message Repeat Delay
- Tone will play during delay

Message 1-15

Voice Settings

Can change per event type
- Restart message after mic
  - Yes or NO
- Restart message on new group activation
  - Yes or NO

HFSS With EVS

Editing EVS-50W Amp

- Module ID
- Name
- Add EVS-CE4 speaker expansion card
- 25 Vrms or 70 Vrms

*Options that are grayed out are not available for the selected module
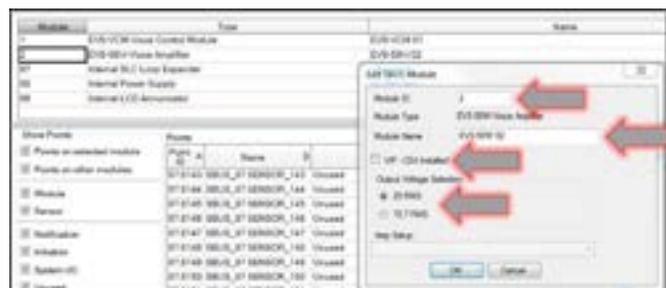
EVS-VCM Voice Module 1
- Aux trigger points 1 (CMD1) and point 2 (CMD2)

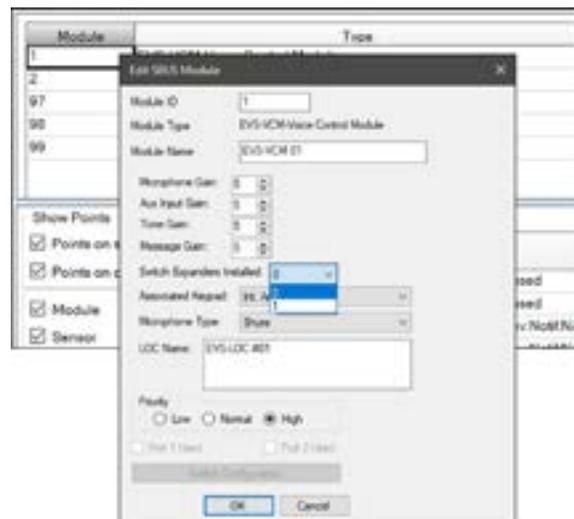EVS-50W Voice Amplifier Module 2
- 4 speaker circuits
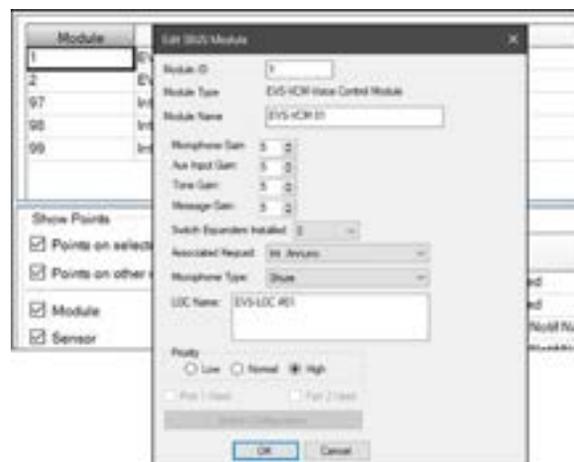
Editing EVS-VCM

- Name
- Gain levels
- Switch expander enabled when using
  EVS-SW24
  - 1 up to 40 switches
- Each EVS-VCM must be associated
  to a keypad
- Microphone type
  - Shure
  - Astatic

Must have an Associated Keypad to Reset events

Editing EVS-VCM

- LOC name
- Device priority
  - Low
  - Normal
  - High

Output Groups

Allow System Override
- Allows any output group, whether activated by fire system or EVS, to be superseded by highest priority event. Defaulted as "YES"

Example: Allow System Override "YES"
- If a fire system and EVS event are both active, there will be no outputs for the fire event if the EVS system event is of higher priority

Example: Allow Override "NO"
- If a fire system event is active to recall elevators, when the EVS event is activated to override speakers, it will not override the elevator

Voice
- Must be selected to use for voice output groups
  - Speaker circuits

Select/Activation Switch
- Can be assigned to individual Voice switches on EVS-VCM for selective paging or manual activation of EVS outputs with cadence patterns
  - EVS-VCM switches 1-64

Editing Select/Activation Switch
- Left click/Right click
- Switch setting box will appear
  - Enter switch number from 1-40
- Left click/Right click on activation cadence for output patterns
  - EX: Sync for EVS Strobes
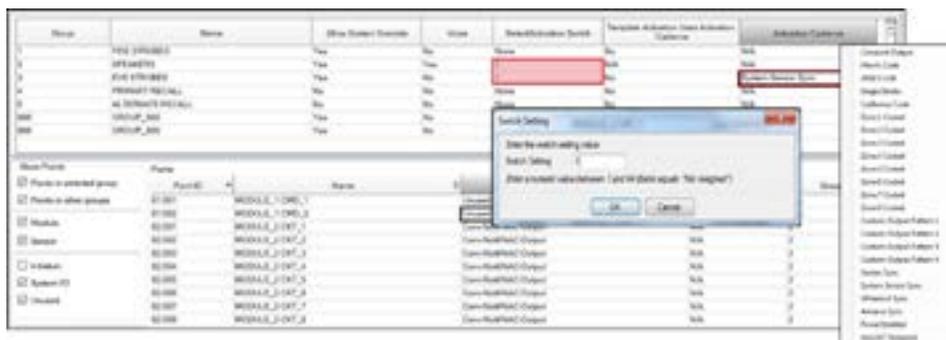
Mapping tab

Options to Map by
- Zone
  - Standard mapping
- Panel
  - Custom LED annunciator
- Site
  - EVS, function keys and other options
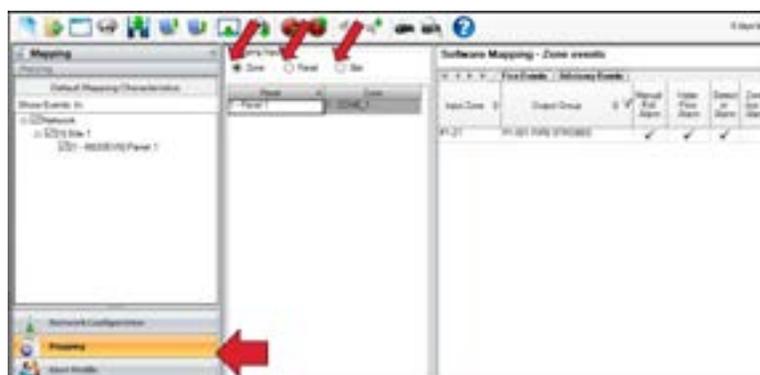
Panel Mapping
- Fire Events
  - System Aux 1 alarm
  - System Aux 2 alarm

Panel Mapping
- Advisory Events
  - Output group trouble, SBUS expander trouble, SBUS Class A trouble, SLC loop trouble, AC loss trouble, battery trouble, ground fault trouble, phone line trouble, report AC count trouble, printer trouble, aux power trouble, system switch trouble
- Scrollbar can be moved to the right to view more events types

Site Mapping
- Fire Events
  - General fire, fire drill, general fire pre-alarm, general fire supervisory, general CO alarm & general CO supervisory

Mapping Speaker Groups

Adding a speaker group to mapping is the same as adding any other group

- Right-click the zone under mapping input, click select group(s) to map, add the speaker(s)

Once added, left-click/right-click on the group under zone events for manual pull alarm

- You can edit voice groups for enabled/disabled, latching, silenceable, alert, timers, and map inhibit
  - No output pattern can be selected. All speaker output information is done under network configuration>voice settings
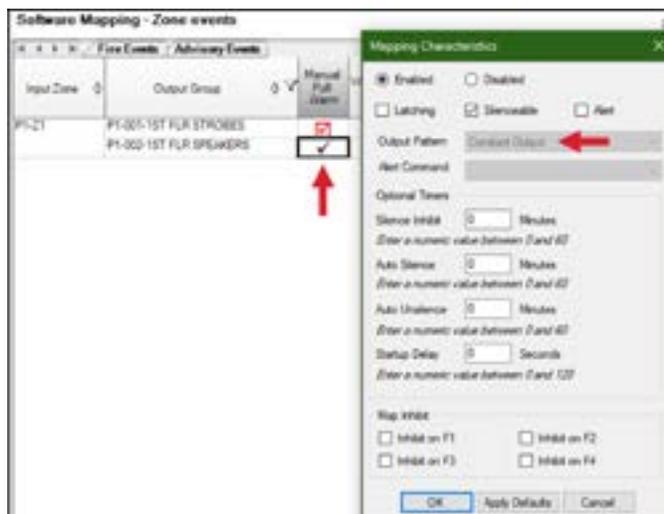
Mapping EVS switches

All mapping of EVS switches occurs under EVS events in site in mapping input

- LOC EVS 1 – 8 represent the 8 EVS switches
- Right-click on site 1 under mapping input and click select group(s) to map
  - Add in all groups that will be activated by that switch
- In the example below, LOC EVS 1 (EVS SWITCH 1) is programmed to do the following;
  - Activate both EVS strobes with System Sensor Sync
  - Activate both speaker groups
    - Speakers must be mapped to the EVS switch in order for an EVS message to audibly play during an event

References

- NFPA 70 - National Electrical Code
- NFPA 72 - National Fire Alarm and Signaling Code
- NFPA 101 - Life Safety Code
- UFC
- UL 2572

SMART WIRELESS INFORMATION FIRE TECHNOLOGY (SWIFT)

What is SWIFT?

SWIFT is a commercial smart wireless integrated fire technology. SWIFT uses a robust, Class-A mesh network that integrates with existing hard wired fire systems.
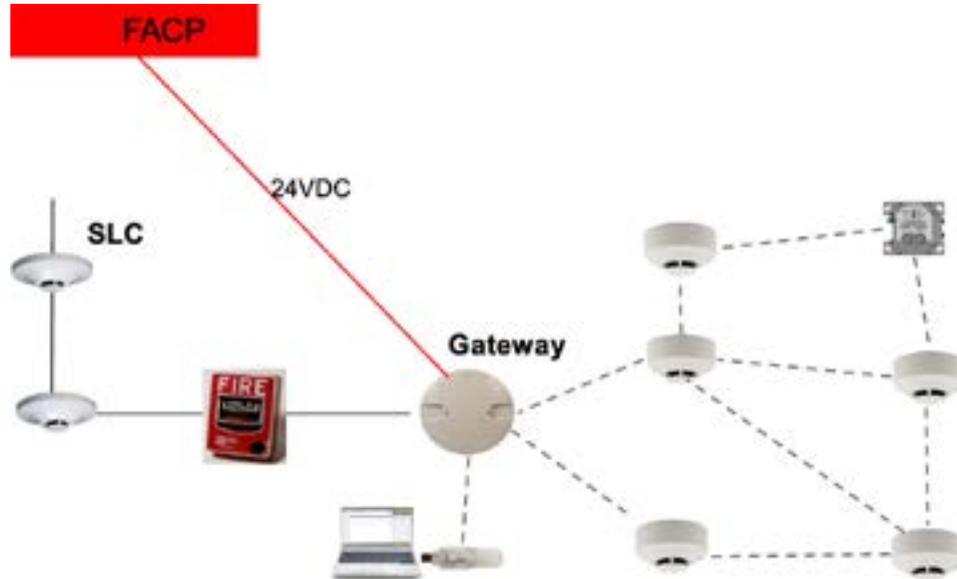
Applications

- Difficult or impossible to wire
- Visually sensitive or historical integrity
- Restricted access – hazardous or secure
- Temporary construction
- Remodels
- Dangerous applications where asbestos may be present.

System Specifications

- **Up to 50 devices per mesh**
  - Including W-gate measure
  - 4 overlapping systems permitted

- **902MHz-928MHz**
  - License free band
  - Frequency hopping

- **50mW transmitter (+17 dBm)**
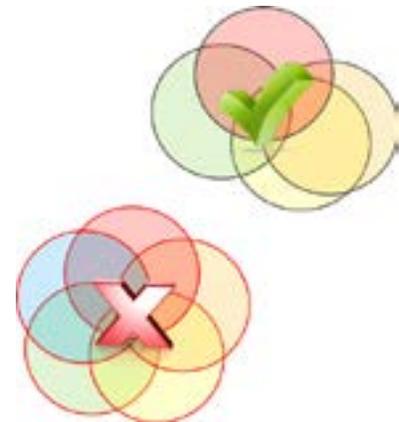
- **Multiple antennas to overcome orientation issues**

- **Distance @-55 dBm**
  - Completely dependent on the environment
  - For starters, treat as you would a wired detector (spaced 30' on center)

When a wireless relay, wireless AV base, or wireless sync module is in use, module device count must be limited to 109 modules per loop. This includes wired and wireless modules that are on the same loop. The module address range must be within 1-109.

This is for SK modules only, you will still have 1-159 addresses for your sensors

WIDP-WGI (Gateway)

- Bridges communication from wired to wireless

- Powered by the SLC or external 24 VDC
  - Maximum current using SLC power: 24 mA
  - Maximum current using External supply: 40 mA (recommended)
  - SLC removing & adding

- 6815 only

- Each mesh requires 1 gateway

- Occupies 1 SLC module address

Consider powering from an external 24 VDC power supply. When powered by the SLC, a trouble on the SLC can put the gateway out of service. It could take at least 30 minutes or more for the wireless network to recover.

Power – Filtered, non-resettable

WSK-WGI (Gateway Wiring)

Powered by SLC

If powered by the SLC, ANY
trouble shooting requiring you to remove
the SLC, will result in a reconfiguration
of the mesh.
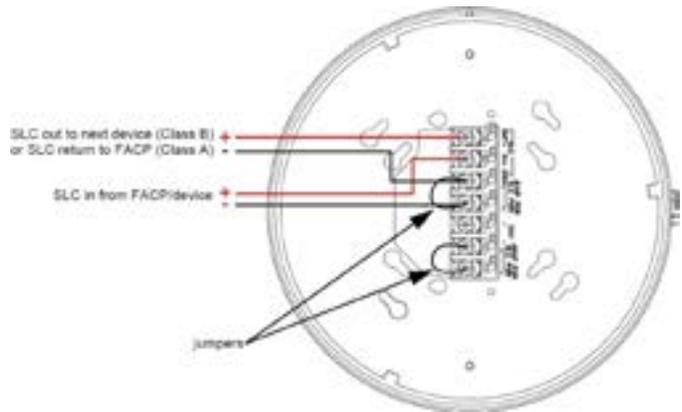
Powered by External 24 VDC
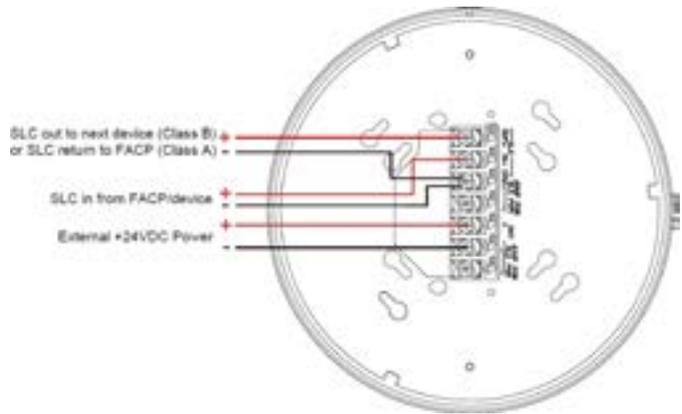
Detectors

- Basic operation identical to wired version
- Panel makes alarm decision
- Detector LEDs flash in alarm
- Each operates on (4) CR123A batteries (Included with detector)
  - UL Listed for 2 years of expected battery life
- 4" base shipped with each detector
  - Magnet built into the base to detect tamper condition

Type	Model Number
Photo	WSK-PHOTO
Heat (Fixed)	WSK-HEAT
Heat (ROR)	WSK-HEAT-ROR
Photo/Heat	WSK-PHOTOT
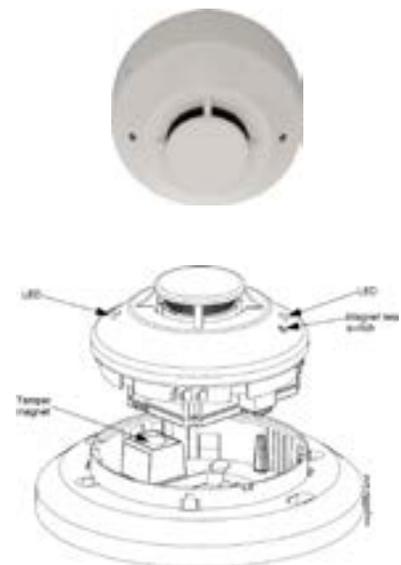
UL listed battery life = 1 yr. Listing for 2 years is in progress.

WSK-MONITOR

- Used to monitor any normally open contact
  - Conventional pull station, waterflow etc.
- Operates on (4) CR123A batteries (Included)
  - UL listed for 2 years of expected battery life
- Module plate included
  - Magnet included to detect tamper condition
- Use a plastic SMB500 4 inch box
- 3' limit on wiring length
  - Due to lack of ground fault detection
- 3.9K EOLR included with each module

WSK-PULL-DA

- Integrated LED display status
- Requires (4) CR-123A batteries (included)
  - UL listed for 2 years of expected battery life
- Compatible with wireless battery cartridge (W-BATCART)

WSK-RELAY

- Equivalent contact ratings to the wired relay
  - UL limitations – only one set of contacts permitted
- Equivalent battery specifications to all wireless devices
  - Specified for 2 years of battery life
  - Latching relay only draws power to change state
  - A relay in the off-normal or active position will draw more power due to the LED drawing more power
- Relay will go to the normal state during startup
- Relay will go to & stay in the normal state during installation
  - Bootloader (mode for updating a device)
  - Factory default (including site survey)
  - Mesh formation

- Activation of the relay as follows:
  - Relay will activate first
  - Then the LED changes state (next message lower priority)
- Relay will "hold" its last state if it drops from the mesh
  - Tampered device
  - Jammed device
  - Dropped device (out of range/communication)
  - Dead batteries

WSK-RELAY Limitations

- Wireless relay cannot control multiple devices
- Emergency control function interface wiring within 3'
  - NFPA requirement 21.2.4
- Wireless initiating and output devices must be in the same mesh to meet 9 second activation
  - If a relay is controlling a power supply
- Not for releasing service use

> **21.2.4*** Emergency control function interface devices shall be located within 3 ft (1 m) of the component controlling the emergency control function.
> **3.3.137.1.2*** Emergency Control Function Interface. The interface between the fire alarm system emergency control function interface device and the component controlling the emergency control function. (SIG-PRO)

The root cause of this limitation is the NFPA committee does not want the neglect of a primary battery powered device (such as our battery powered relay) to result in the loss of multiple "points". The committee wants to avoid a situation where all fire doors in a building or zone fail to close if someone forgets to change the batteries in a single relay.

SWIFT AV BASES

- Compatible with System Sensor L-Series AV notification appliances
- Can also be combined with hard-wired devices
- Requires (8) CF-123A batteries (included)
- Compatible with wireless battery cartridge (W-BATCART)
- Compatible with SWIFT synchronization module (W-SYNC)
- Power supplied by two sets of 4 batteries
  - One set provides power for wireless communication
    - UL listed for at least 2 years
  - One set provides power for notification appliance's audio and/or visual signal
    - Battery life depends upon activation time and output level of the audio or visual signal

Battery Life at Temporal 3, Ambient Conditions

Model	Model Type	Battery Life (Minutes), per Candela Setting									
		15 cd	30 cd	75 cd	95 cd	110 cd	115 cd	135 cd	150 cd	177 cd	185 cd
Strobe-only	Ceiling	1305	849	482	399	-	339	-	283	237	-
Chime-only	Ceiling	115	764	461	388	-	324	-	269	225	-
Horn-Strobe	Ceiling	754	594	374	324	-	286	-	247	211	-

Note: Battery life will decrease using continuous tone or other coded patterns and under-ambient environmental conditions.

211 minutes = roughly 3.5 hours

Each AV device requires two (2) consecutive SLC addresses on the fire panel. Use the rotary code wheels on the AV device to set the base address. The AV device will also occupy the address following the base address.

(Base +1) The base address on the AV base will require the following configuration:
• Type code: Wireless Relay – Output

Base+1 address will use the following configuration:
• Type code: NAC Module - Output Point

Point ID ▲	Name ◊	Type ◊	Zone ◊	Group
97.M001	AV BASE 1 NORHT HALL	Addr Notif Wireless Relay Output	N/A	1
97.M002	AV BASE+1 NORHT HALL	Addr Notif Output	N/A	1
97.M003	AV BASE 2 SOUTH HALL	Addr Notif Wireless Relay Output	N/A	1
97.M004	AV BASE +1 SOUTH HALL	Addr Notif Output	N/A	1
97.M005	SBUS_97 MODULE_5	Unused	N/A	N/A

W-SYNC

- Provides audio and visual synchronization of a wireless notification device to a wired notification device and is intended to be used with a wireless gateway
- Sync module outputs a "Master" synchronization signal, optional control output, and monitor input
- One sync module can drive up to 4 power supplies or 4 MDL3R/W with a sync pattern
- Supports System Sensor SpectrAlert, SpectrAlert Advance, and L-Series sync protocols

Powered by 24VDC!

SWIFT Synchronization Module
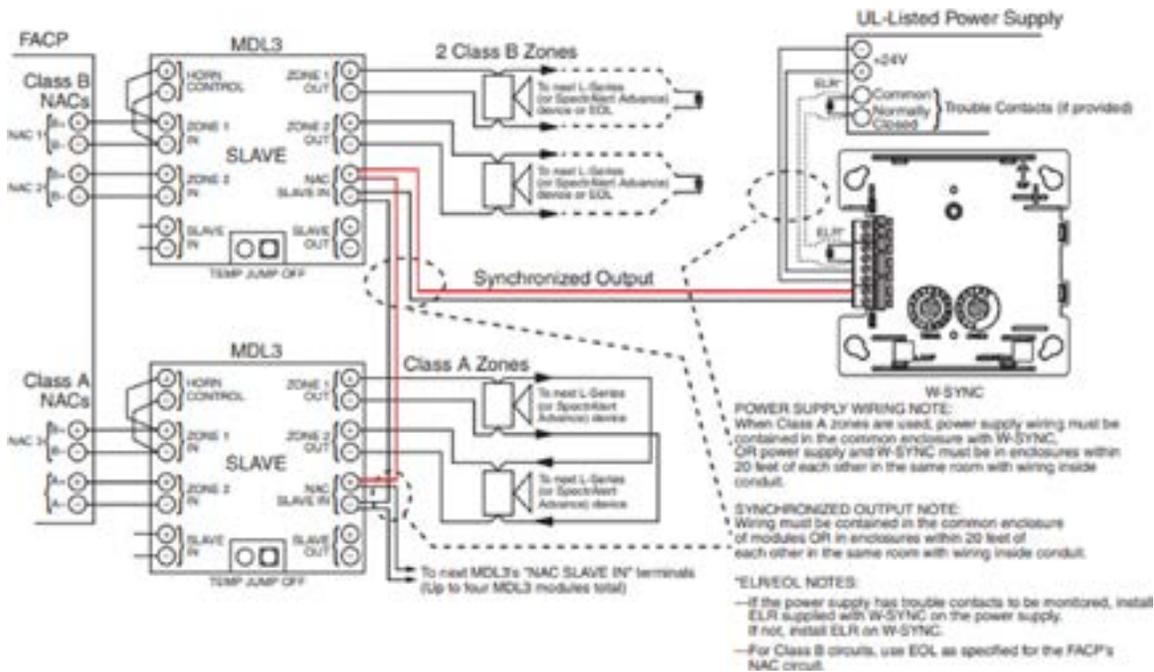
W-SYNC

Faceplate includes magnet for activation and tamper resistance
Occupies two module SLC addresses via rotary switches:
  • Base Address – RELAY1FC – wireless true
  • Base Address + 1 CONTROL – wireless false

Mounts directly to an SMB500 electrical box

Please Note!
Synchronization of only wireless notification appliances within a single mesh network is inherent in the wireless system and a wireless synchronization module is not needed

USB Adapter (W-USB)

  • Made by System Sensor
  • Connects to a PC (Windows XP, 7, 8, 10)
  • Communicates to wireless devices for configuration and diagnostics

SWIFT Tools

PC-based application for:
- Collecting and analyzing site survey data
- Configuring and installing a system
- Diagnostics
- Battery level
- History
- Statistics

SWIFT Testing & Setup

SITE SURVEY
Link Test – Quick test for signal strength
RF Scan – Test for channel activity
and background noise (70 minutes)

SWIFT TOOLS
Site survey
Create mesh
Formation
Diagnostics

Site Survey

Evaluate the site prior to installation
- Verify the connectivity to challenging locations
- Measure the interference and activity
- Measure the background noise

Link Quality Test

Requirements:
- Two or more devices (detectors) required
- Devices must be in factory default state
- Addresses can be set in a range of 1 to 150
- The addresses being used are for testing only

Conduct a Link Quality Test

Remove batteries from device and set device address
- 1st device starts at 001, 2nd device 002, 3rd device 003, etc.
  - Bring 1st device (001) to the first location to conduct the test
  - Insert one battery into the device (will blink Yellow every 5 seconds then turn red)
    - One battery per device during link quality test
  - Clear tamper condition
    - (By placing detector in base and twist to lock into position)
- Bring 2nd device (002) to the second location and insert one battery
- Clear tamper condition
  - (By placing detector in base and twist to lock into position)
- Repeat for subsequence devices
- Results appear in about 20 seconds

The device will conduct a link test to the next lowest address
- The results from the link test from device 001 to 002 is displayed by the LEDs on device 002
- Once test is complete between 002 and 001, continue for address 003, 004, etc.
- Test must be repeated, if desired, within five minutes of the last concluded test or the devices will start an RF scan test
  - (When devices are set to an address or 101 and higher)

Site Survey – Link Quality Test
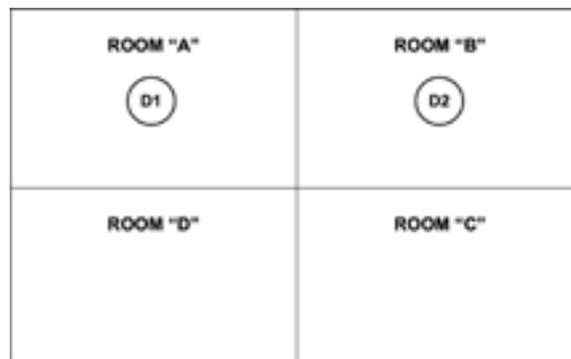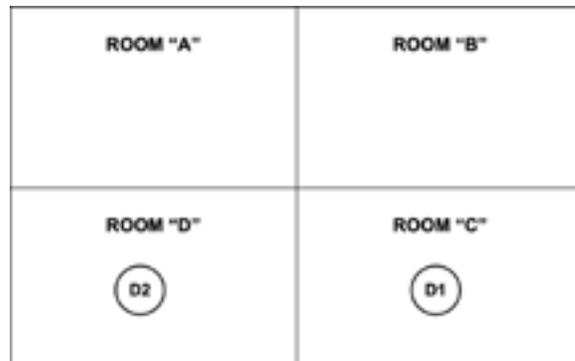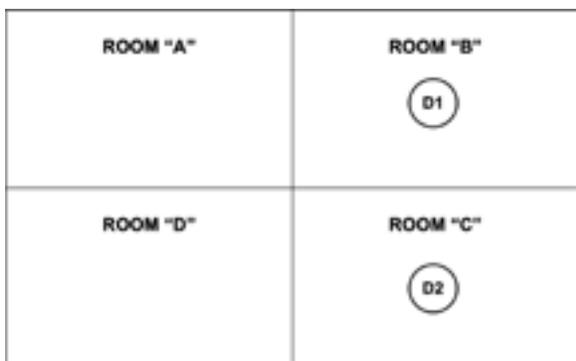
Link Quality Test Results

LED Pattern	Color	Results/Description
On steady	Red	Failure – no data received
Single blink every 5 seconds	Red	Poor – partial data received, or signal strength measured lower than the acceptable limit for a primary or secondary link (-81 dBm or lower)
2 blinks every 5 seconds	Green	Marginal – all data received at a signal strength acceptable for a secondary link but not a primary link (-61 dBm to -80 dBm)
3 blinks every 5 seconds	Green	Good – all data received at a signal strength acceptable for a secondary link and marginally acceptable for a primary link (-51 dBm to -60 dBm)
4 blinks every 5 seconds	Green	Excellent – all data received at a signal strength acceptable for a primary link (-50 dBm or better)
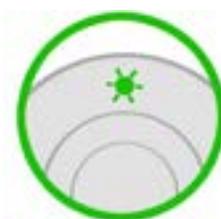
4 blinks = Excellent link
3 blinks = Great link
2 blinks = Good link
1 blink = Poor link
Solid Red (on steady) = No link

Devices Act as Repeaters

- Every device is also a repeater
  - Extending the distance at each location
  - Dedicated repeater network is not required
- Class A fault and weak link troubles
  - SWIFT tools identifies poor connections
  - SWIFT tools recommends placement of repeaters
  - Add a device in between to improve the signal strengths
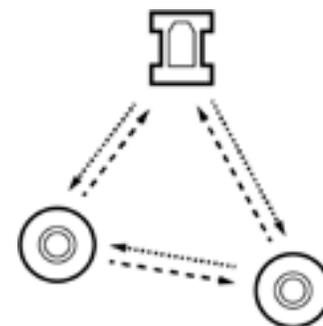
RF Scan Test

Definition
- A radio frequency scan to assess and measure the background noise and interference from other wireless systems if any, in the site

To conduct an RF scan test, follow the same procedure for the link quality test
- RF scan test requires the use of addresses from 101 to 150

The RF scan test can be conducted individually or following a link quality test
- RF scan test will be conducted for any device with an SLC address set between 101 and 150 at the end of the link quality test
- The addresses being used are for testing only

RF Scan Test Status

State	Pattern	LED	Status
In Progress – 70 minutes remaining	7 short blinks every 30 seconds	Red	Bad
		Green	Good
In Progress – 60 minutes remaining	6 short blinks every 30 seconds	Red	Bad
		Green	Good
In Progress – 50 minutes remaining	5 short blinks every 30 seconds	Red	Bad
		Green	Good
↓	↓		
In Progress – 10 minutes remaining	1 short blink every 30 seconds	Red	Bad
		Green	Good
RF Scan Test Complete	On Steady	Red	Bad
		Green	Good

Videos

YouTube videos to explain the instructions

Installation Steps with SWIFT Tools

A 2-step process:

- Assigning profiles
  - Create or upload a profile
  - Select devices to assign the to the profile
  - Assign the profile
- Create mesh network
  - Start the process
  - Stop the process
  - Mesh network will restructure automatically
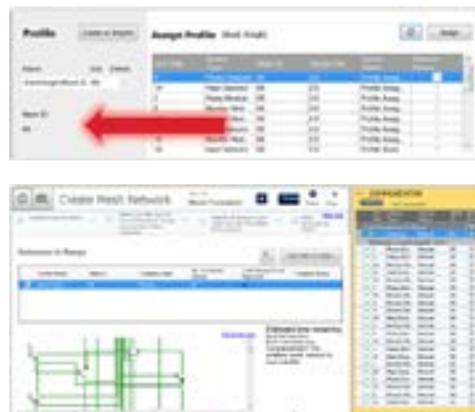
Mesh restructuring can be activated manually.

Swift Tools provides visibility in the process!

Assign Profiles

- Each wireless device comes from factory in a default state
- A profile is assigned to associate a wireless device with it's gateway and other devices in the same network
- Profile assignment doesn't create the network – it lays the foundation for it
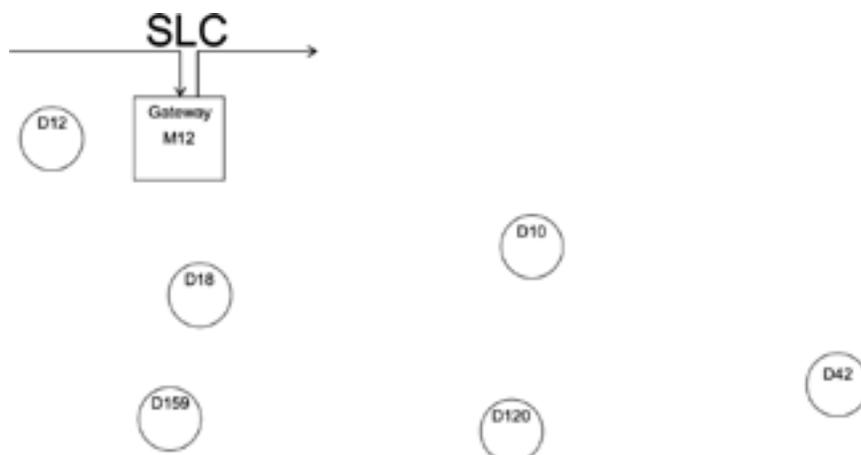
What is a profile? It's the first step in creating a MESH network. Each wireless device comes from factory in a default state. A profiles is assigned to associate a wireless device with it's gateway and other devices in the same network. Profile assignment doesn't create the network – it lays the foundation for it.

Profiles Assigned

- Now, all devices within a given Mesh network have matching profiles
- That profile instructs each device to communicate only with its corresponding gateway
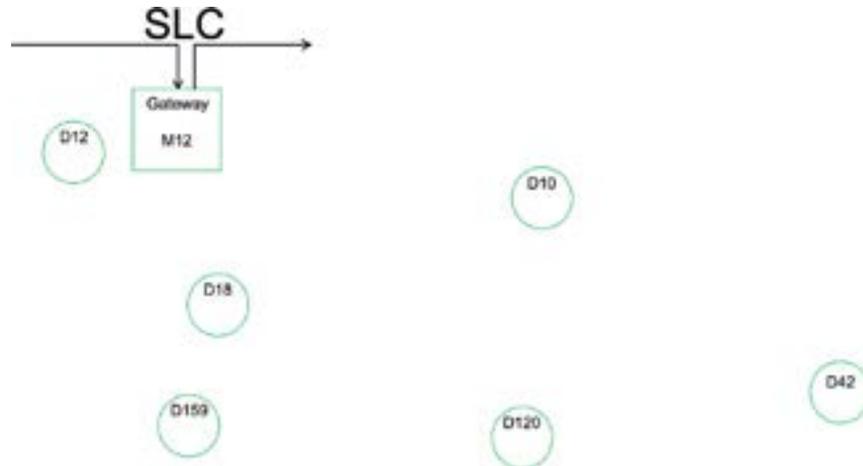
Profiles Define Association/Enrollment

So if we have overlapping networks...like this, we don't have confusion. Two separate networks that can co-exist without conflict. Think of it as SWIFT nirvana.
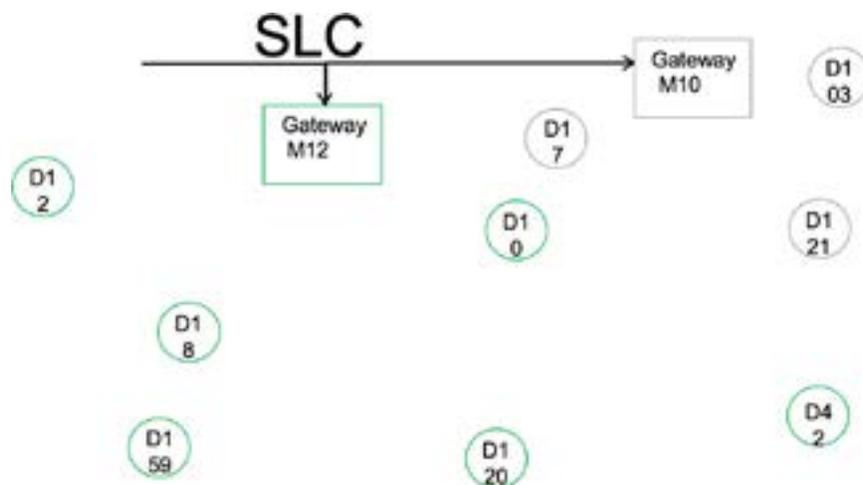
Mesh Formation Mode

- Gateway must have a profile before entering mesh formation mode:
- No fire protection in this mode
  - Device is an active participant in a mesh forming
  - LED blinks green then yellow every 6 seconds

Mesh Formation in Progress

The gateway is instructed to start MESH formation.
- Devices start seeking the strongest and most reliable path to the gateway
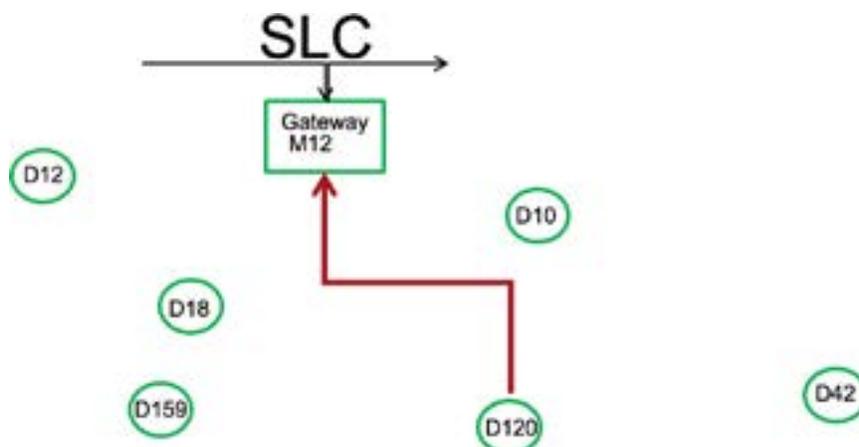
Back to a single network. The gateway is instructed to start MESH formation. Devices start seeking the strongest and most reliable path to the gateway.

Mesh Formed

- The Mesh if formed but it may not be configured in the best way – it's sort of random at this point
- We want devices to have the strongest signal strength between each other.
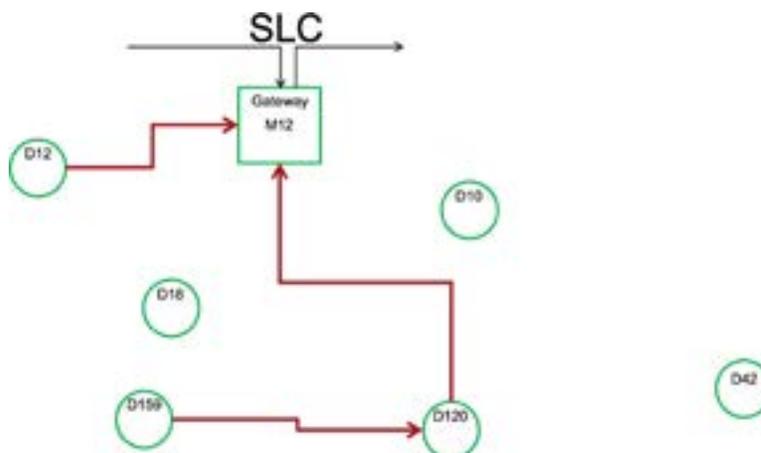
Mesh Restructuring

- Changes to the environment
  - Renovations
  - Obstructions
- Device is moved
- Devices are added or deleted
- Panel sends a restructure trouble
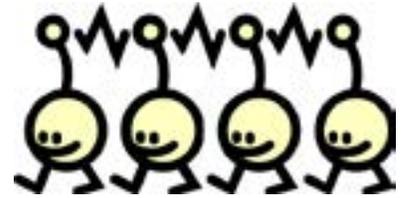
Mesh restructuring uses considerably more battery power (elevator power)

Mesh Restructuring in Progress

- The gateway conducts a restructuring process where it measures the signal strength
- from device to device in ALL paths possible – in every configuration
- That's what these next diagrams show.
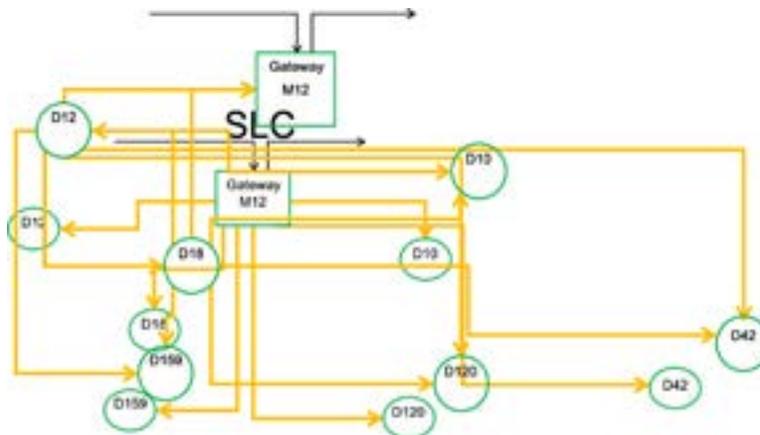
Mesh Restructured (Optimized)

Now the gateway has the signal strength of every device in every possible configuration and it can put the network together in the most optimum configuration

Note: D10 is only talking to one device, this will happen on any mesh. To keep class A it reports twice.
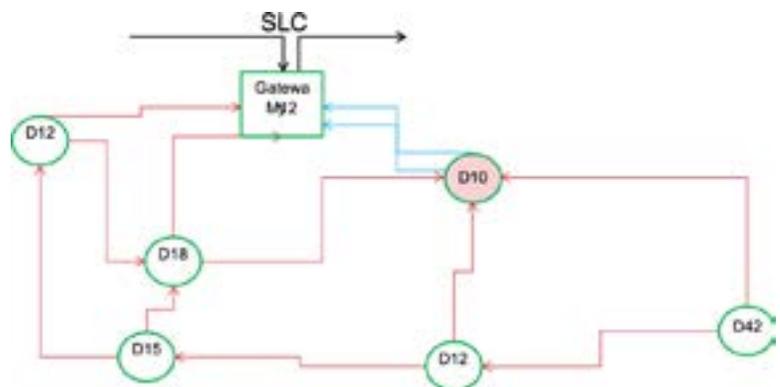
Normal Mode

- The mesh network has been formed
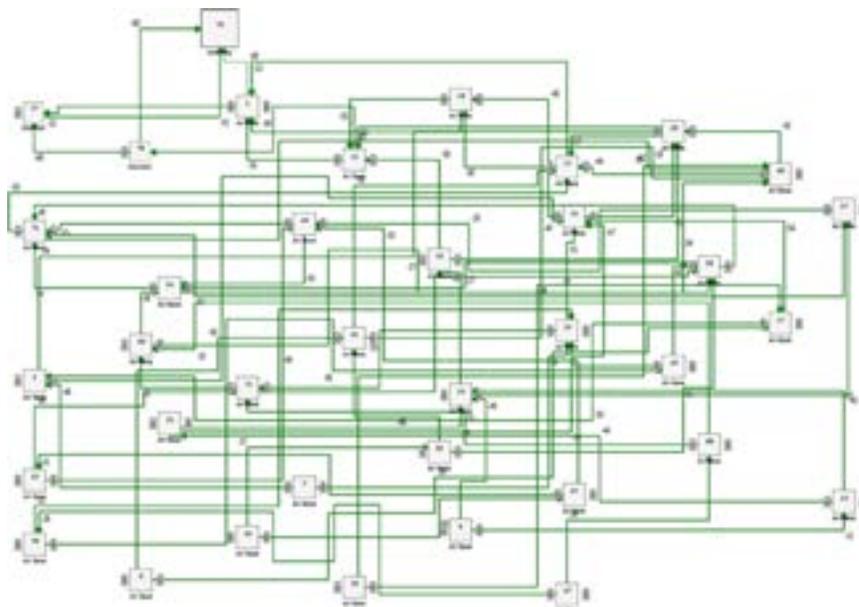
Rescue Mode

- If you loose a device on the mesh
  - Lost battery
  - Unable to communicate
- All the other devices start searching
  - for the lost device
- LED blinks every 12 sec
- Does not report trouble in this mode
- Still have fire protection in this mode

If a Device Falls Out of the Mesh….

After a certain period of time, the system assumes a missing device has fallen out of the mesh (missing person report)
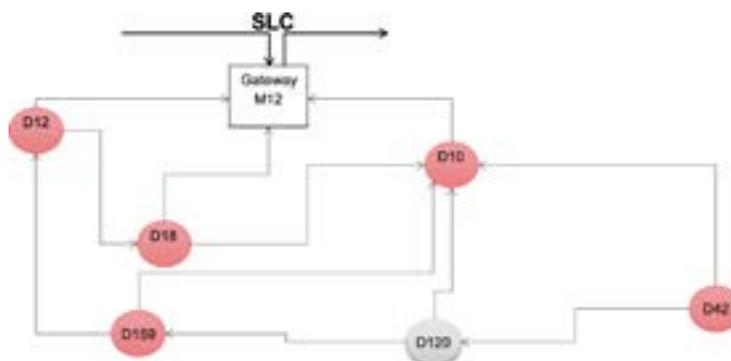
The System Will Repair Connections…
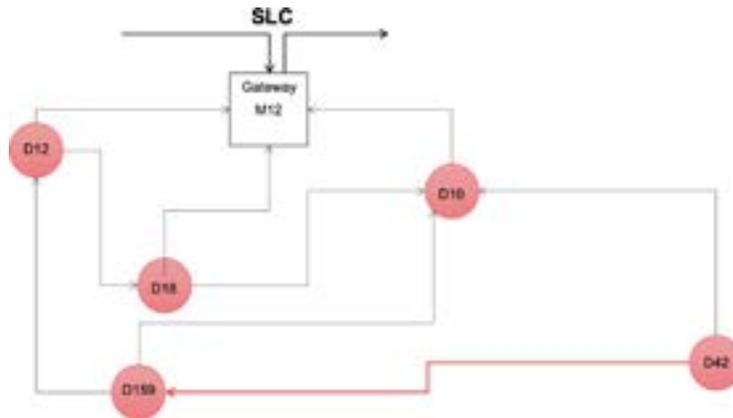
And Search for the Lost Device…
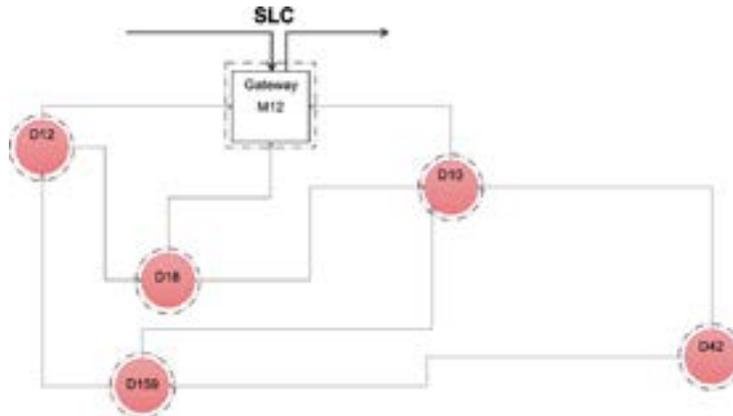
Even if it's placed in a New location…
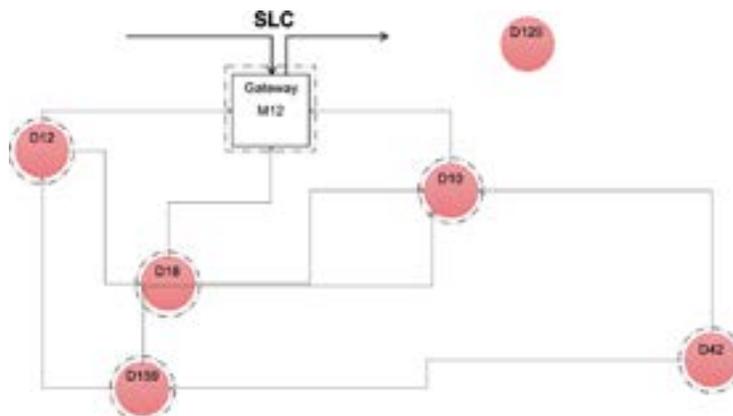
Say someone removes a detector to paint the room. They put it in the office. The gateway will find it even if…

Recover it Using "Rescue Mode"...

Rescue mode is an automatic mode where all devices in the mesh get upset and start looking for the device. Devices draw a lot of power here
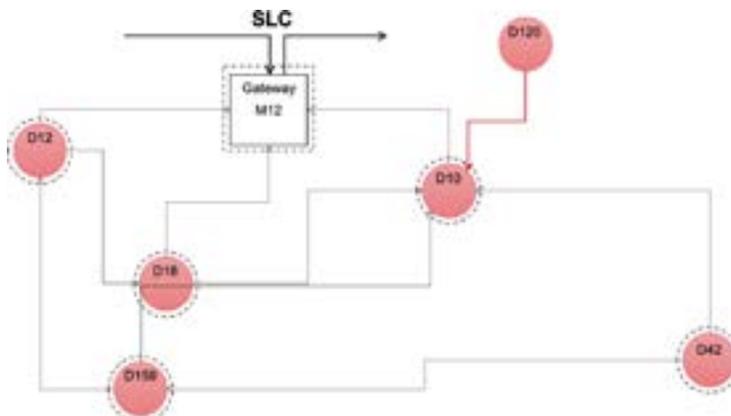
And Use Mesh Restructuring...
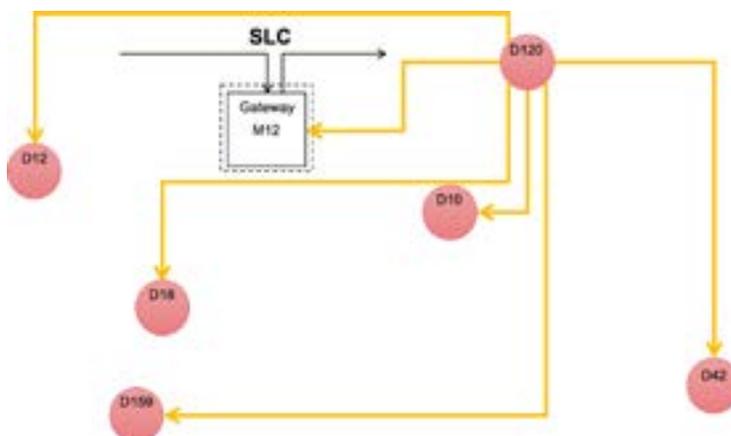
To Reestablish the Mesh Network
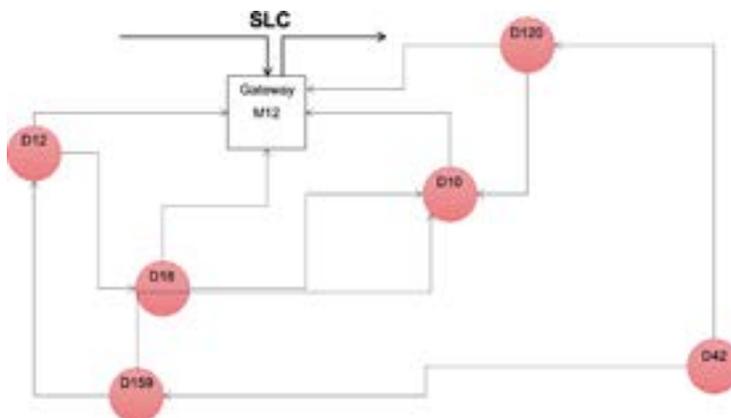
Patented Cascading Alarm Technology

When one device goes into alarm, it
tells it's other two devices.
Those two devices tell their two
devices and so on.

This keeps the system within the UL
286 Standard of 10 seconds.
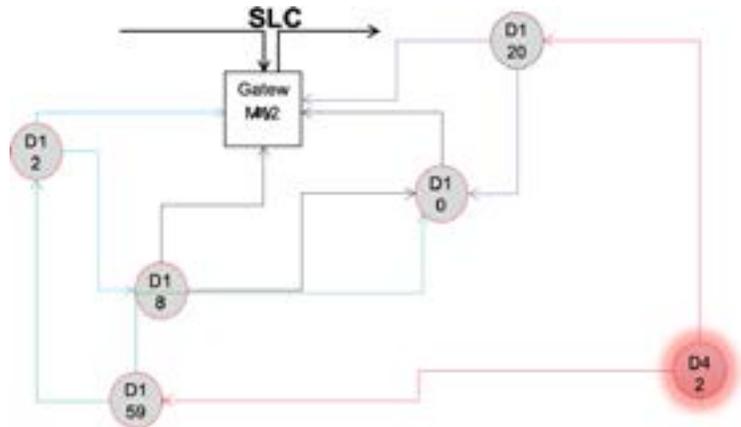
Operation

Latching wireless events need to be "Reset"
 • Tamper
 • Water flow
 • Low battery
 • RF device – no answer

The wireless devices are just like intelligent hard wired devices.
You can set all the same parameters for them (drift compensation
- MORE EXAMPLES). UL requires all wireless events to latch.
So all wireless devices will have to be reset. UL requires troubles
associated with wireless devices to resound every four hours.

Interference Sources

What sources of interference are anticipated?
 • Walkie-talkie radios using our frequencies
 • Some RFID readers
 • Some wireless clock networks
 • Older cordless phones
 • Long distance LAN links

Interference only comes from sources in our band

What does NOT cause Interference

- Walkie-talkies that are NOT using the same frequencies
- WiFi networks and devices (2.4 GHz and 5.2 GHz)
- North American Cell phones
- Bluetooth devices

Silence Mode

- Must select in SWIFT Tools
- Temporarily shuts down devices without uninstalling them
- Timed shutdown helps determine whether or not SWIFT is causing
  RF interference to other systems
- Select timeout in software
- From 30 minutes to 24 hours
- No fire protection in this mode

Batteries

- Four CR123A batteries (included with each device)
  - Panasonic or Duracell ONLY
- UL listed for 2 years of life expectancy
- 2 year battery life expected
  - 2.6 years currently, but with additional features in the roadmap
  this will drop, but not lower than 2 years

- Low battery indication with 1 week of life remaining
  - Battery status indication using SWIFT tools
  - Fresh, greater than 6 months, less than 6 months, low
- Individual battery voltages available in statistics
- Battery status indicated by LEDs
  - Battery status indicated upon installation
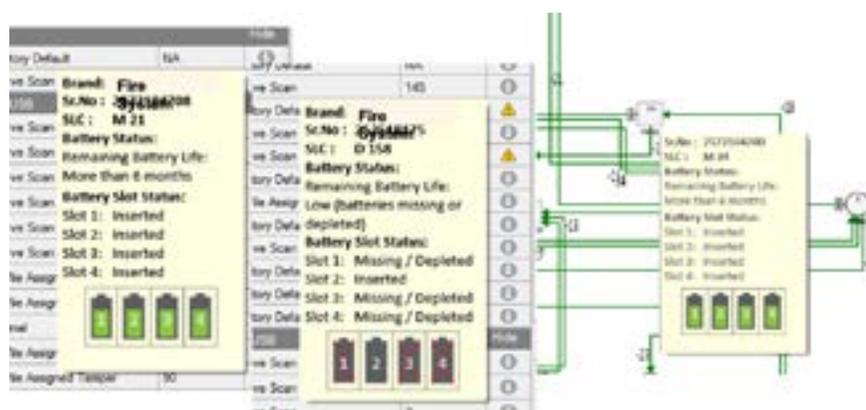
SWIFT Summary

- Redundant
  - Class A connections for each device
  - A single device loss does not stop other device communication

- Self Healing
  - Rescue mode, mesh restructuring
  - Automatically adjusts for most building environment changes

- Robust – interference immunity
  - Uses multiple frequencies for each transmission
  - Withstands walkie-talkie interference at 2 feet
  - Alternate channel hop set used to avoid interference

- Every device repeats and extends the system range
  - Extending the distance at each location
  - Dedicated repeater network is not required
  - Added on an existing fire system in cases of hard to wire or no access

Agency Approvals

- Underwriters Laboratory
  - UL 864
  - UL 268
- Factory Mutual
- CSFM approved
- FDNY approved

SWIFT Agency Info

- Devices comply with UL 268 Standards:
  - 200 second polling and system response of devices within 10 seconds.
- Devices comply with Part 15 of the FCC rules
  - The device may not cause harmful interference and the device must accept any interference received, including interference that may cause undesired operation.

CLSS
CLOUD
COMMUNICATION

What is CLSS?

CLSS is an innovative, all-in-one cloud platform that enables systems integrators and facilities managers to deliver an enhanced fire safety service, while maximizing the performance efficiencies offered by Honeywell's trusted detection and alarm systems.

By harnessing the power of data, it delivers the connectivity and intelligence needed for secure, compliant and more efficient fire system management. CLSS answers dealers pain points by driving efficiency, maximizing retention and increasing win rates.

Provides real time visibility and increases user confidence by reducing complexities, cost and uncertanity.

Who Do We Serve?

CLSS Serves 6 market segments of the fire industry:
- Dealers
- Fire marshalls
- Building owner/facility managers
- Central stations
- 911 centers
- First responders

CLSS is the center hub for everything commercial fire. More specifically, CLSS increases user confidence by connecting dealers and end users to their sites. This platform provides real time visibility while reducing cost, complexities, and uncertainty.

What Does CLSS Offer You?

What do we offer to you?
- Rid your site of deregulated POTS lines.
  - Fewer nuisance signals.
  - Cost savings
  - Phoneline fault
  - Corrupted account numbers
  - Simple connection for quicker installations
  - No re-programming of panel needed
  - No need for a 24-hour fire watch

LESS TECHNICAL SUPPORT CALLS !!

Upgrading from POTS will ultimately provide cost savings throughout a dealer's business while adding reliability and redundancy to their fire systems.

Solution. Reduce T1 Lines - less pots traffic cost CS money and must have PRI and Sec Ans. We are IP lower cost.

More reliable signaling, No mismatch of signals causing wrong dispatch

Industry Sunset Reminders

Be a solution provider – 2022 Sunsets
- Mobile sunsets
  - December 2022 Verizon

- POTS deregulation!
  - As of August 2022
  - What does this mean?
    - Dealers may see an increase on their telephone bill.
    - Carriers have the option to deny service or repair POTS connections.

Share customer testimonials on tower removals before sunset dates.

To eliminate possible service disruptions, upgrade all remaining 3g and POTS lines with pathways today!

Your Solution!

The **CLSS Pathway** combines dial capture functionality with the powerful capabilities of Honeywell's CLSS Cloud. It represents the latest alarm communications technology for the fire industry. The CLSS Pathway allows data transmission by utilizing LTE CAT-M1 networks, serving as a bridge between the fire system and the CLSS Cloud. This device provides a single site-to-cloud path ensuring all CLSS Cloud services use the same audited and monitored method to access the on-premises life safety system.

Universal Contact ID Support

HW-AV-LTE-M

HW-AV-ENC

Features & Benefits: Hardware Features:
- Dual SIM automatically picks from AT&T or Verizon networks for ultimate redundancy and reliability
- LTE-CAT-M1 network is 5G-ready for deep signal penetration inside buildings
- Meets UL 864 requirements for sole, primary or backup path communications
- Universal fire alarm control panel (FACP) compatibility and direct power from 24-volt FACP
- Introductory offer includes first year of cellular/IP service included in purchase price

CLSS Pathway is : a 5G dual path, dual sim dialer capture which communicates over AT&T or Verizon cell networks depending on the strongest signal.

Can be used as a sole path communicator by enabling the LAN connectivity.

Compatible with any fire, burg or combo panel communicating via contact ID.

How Much Does It Cost?

Cost to the Dealer:
Approximately $150.00 per device.
$12.00 per month for airtime
- Includes 5 min supervision
- No over activity fees
- No activation fees
- 12 months free service

What included!
- Unlimited access to CLSS web and mobile app.
- End-user facility management access.
- CLSS check-point (test and inspection reports)
- Real-time alerts and notifications.

The introductory price is $150 but may vary depending on the local distributor.
$12 monthly, or $144 yearly will be due after the 13th month for continued cell services.

Over 60 Central Stations and Growing!!

- Affiliated Monitoring, Inc.
- Alarm Central, LLC
- Alarm Monitoring Services
- Alarm Tech Central Station
- Alert Alarm Inc.
- Alert Security Alarms
- Alert360
- All American Monitoring
- Amcest Corporation
- Audio Sentry Corporation
- AvantGuard Monitoring
- Blue Ridge Monitoring
- Cen-Signal
- CenterPoint Technologies Inc.
- Central Alarm Control
- Central Dispatch Alarm Monitoring
- Central Station Monitoring
- Central Station, Inc.
- Centralarm Monitoring Inc.
- Coastal Burglar Alarm
- Com-Linq Central Station

- Cooperative Response Center Inc.
- COPS Monitoring, Inc.
- Counterforce Central Alarm
- Countryside Alarms
- Criticom Monitoring Services CMS
- Design Communications
- Dispatch Center
- Doyle Security
- Dynamark Monitoring
- Emergency Systems Inc.
- EMERgency24
- ESC Central
- General Monitoring Services
- Global Monitoring Solutions
- Grand Central Station
- Home Security Monitoring Center
- METRODIAL Central Station
- Michigan Monitoring
- Monitoring America

- Nationwide Digital Monitoring
- NEXgeneration Central Station
- NMC (National Monitoring Center)
- Per Mar Security
- Quick Response Monitoring
- Rapid Response
- Securall Monitoring Corporation
- Securatech
- Security Central
- Southwest Dispatch
- Statewide Central Station
- TMS Total Monitoring Services
- United Central Control, Inc.
- Universal Monitoring
- US Monitoring
- USA Monitoring
- Vector Security
- Z-Tech Central

Currently we have over 60+ Central Stations supporting CLSS Pathway.

If you don't see your CS, no worries! Raise a request through CLSS and we'll contact them in efforts to get them onboarded to support CLSS.

What's Your Part?

To request access to CLSS, download the Mobile App for CLSS and request access to CLSS.
www.Fire.Honeywell.com

To configure a pathway, request the following information from your central station.
1. The prefix (prefix does not get sent to central station)
2. The DNIS (should be 5 digits)
3. Unique account number

After submitting a request for CLSS access, you will receive 3 emails. The first, confirming your request to sign up.

The 2nd and 3rd emails could take up to 2 hours to receive and will contain a generic alpha numeric password used to access CLSS.

Technical Support

For General Technical and Pathway Support Call:
CLSS Support – (800) 627-3473

https://buildings.honeywell.com/us/en/brands/our-brands/firelite/support/technical-support

If Dealer is using the below products, call the respective support line.
Fire-Lite Alarms – (800) 627-3473
Notifier – (800) 289-3473
Gamewell-FCI – (800) 606-1983
Farenhyt – (800) 328-0103

Live CLSS trainings will be held through the end of September with Pathway overview being held every Wednesday,

Site and Facility Manager on Thursdays.
Test and Inspect on Fridays.
Provide contact info should they need it.

FED
LEARNING CENTER

#FEDLC #FireFam
#GenerationTrained
#NFPA10 #FireSafety #NFPA
#OurWorkSavesLives #NFPA72
#NFPA17A #FireExtinguisher
#HandsOnTraining #FlameGame #NFPA101
#NFPA96 #KitchenSuppression #FireProtection

www.FEDLearningCenter.com

@FEDLearningCenter