Security Expert

Security Purpose Mini Output Expansion

Installation Manual

SP-MO8
June 2024

Schneider Electric

Legal Information

Contents

Introduction

The Security Expert Security Purpose Mini Output Expansion extends the number of outputs on the system by 8, featuring high current Form C relays for controlled automation of building systems including lighting and HVAC.

Flexible module network architecture allows large numbers of modules to be connected to the RS-485 module network, over a distance of up to 900M (3000ft). Further span can be achieved with the use of a network repeater module.

The current features of the output expander include:

- RS-485 module communications
- 8 outputs
- Industry standard DIN rail mounting
- Online and remote upgradable firmware

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- UL 294 - Access Control System Units
- UL 681 - Installation and Classification of Burglar and Holdup Systems
- UL 827 - Central-Station Alarm Services
- CAN/ULC-S301, Central and Monitoring Station Burglar Alarm Systems
- CAN/ULC-S302, Installation and Classification of Burglar Alarm Systems for Financial and Commercial Premises, Safes and Vaults
- CAN/ULC-S561, Installation and Services for Fire Signal Receiving Centres and Systems
- CAN/ULC-60839-11-1, Alarm and Electronic Security Systems – Part 11-1: Electronic Access Control Systems – System and Components Requirements
- The National Electrical Code, ANSI/NFPA 70
- The Canadian Electrical Code, Part I, CSA C22.1
- AS/NZS 2201.1 Intruder Alarm Systems
- The Local Authority Having Jurisdiction (AHJ)

Wiring

For UL/cUL installations the following wiring specifications must be observed.

Aux Wiring: Minimum 22AWG, maximum 16AWG (depends on length and current consumption).

For wire/cable size, a maximum of 5% voltage drop at the terminals of the powered device has to be observed.

Module Network Wiring:

- Minimum 24AWG (0.51mm) shielded twisted pair with characteristic impedance of 120ohm. Maximum length 900m (3000ft).
- CAT5e / CAT6 also supported for data transmission when using ground in the same cable. Maximum length 100m (330 ft).

Do not use extra wires in the cable to power devices.

Grounding Requirements

An effectively grounded product is one that is *intentionally connected to earth ground through a ground connection or connections of sufficiently low impedance and having sufficient current-carrying capacity to prevent elevated voltages which may result in undue hazard to connected equipment or to persons*.

Grounding of the Security Expert system is done for three basic reasons:

1. Safety
2. Component protection
3. Noise reduction

Safety Grounding

The object of safety grounding is to ensure that all metalwork is at the same ground (or earth) potential. Impedance between the Security Expert system and the building scheme ground must conform to the requirements of national and local industrial safety regulations or electrical codes. These will vary based on country, type of distribution system and other factors. The integrity of all ground connections should be checked periodically.

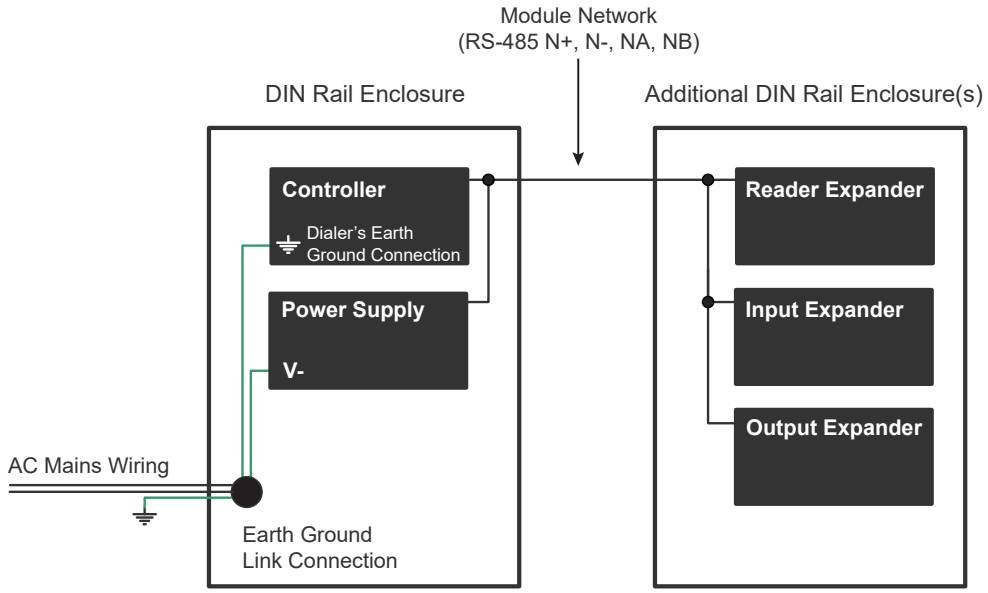
General safety dictates that all metal parts are connected to earth with separate copper wire or wires of the appropriate gauge.

Earth Ground Connection

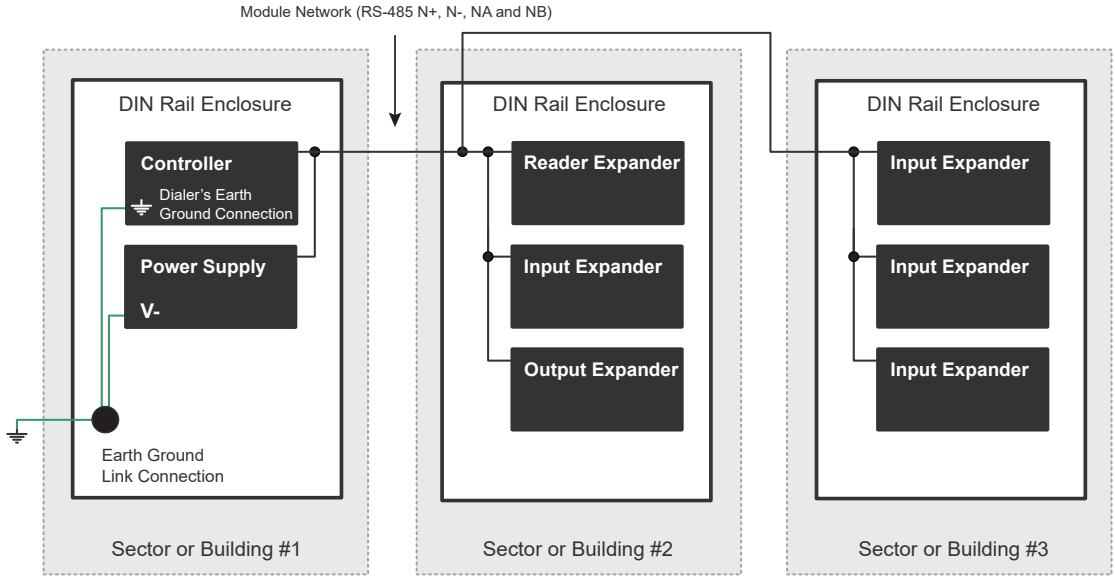
The DIN rail enclosure and the DIN rail modules must be grounded to a suitable single-point earth ground connection in the installation. A minimum 14AWG solid copper wire (or thicker, in accordance with local authorities) shall be used from the Security Expert system's earth connection points.

The DIN rail enclosure includes an earth ground single-point link connection via the metallic enclosure. This single-point link is the Security Expert system's earth ground. All modules that have earth ground connections and that are installed in the same enclosure shall be connected to this single point. A single-point earth ground connection avoids the creation of ground loops in the system and provides a single reference point to earth ground.

DIN Rail Ground Connections (one or more cabinets installed in the same room)



DIN Rail Ground Connections (multiple cabinets in different rooms, sectors, or buildings)



The *Dialer's Earth Ground Connection* applies to modem model controllers only.

Note that the DIN rail enclosure earth terminal is connected to the power supply V- terminal.

There must be only **one** single earth grounding point per system.

Mounting

Security Expert half DIN rail modules are designed to mount on standard DIN rail either in dedicated DIN cabinets or on generic DIN rail mounting strip.

They can also be hung from the top mount screw and permanently fastened using the hole in the attachment clip.

When installing a DIN rail module, ensure that there is adequate clearance around all sides of the device and that air flow to the vents of the unit is not restricted. It is recommended that you install the module in a location that will facilitate easy access for wiring. It is also recommended that the module is installed in an electrical room, communication equipment room, secure cabinet, or in an accessible area of the ceiling.

1. Position the DIN rail module with the labeling in the correct orientation.
2. Hook the mounting tabs (opposite the tab clip) under the edge of the DIN rail.
3. Push the DIN rail module against the mount until the tab clips over the rail.

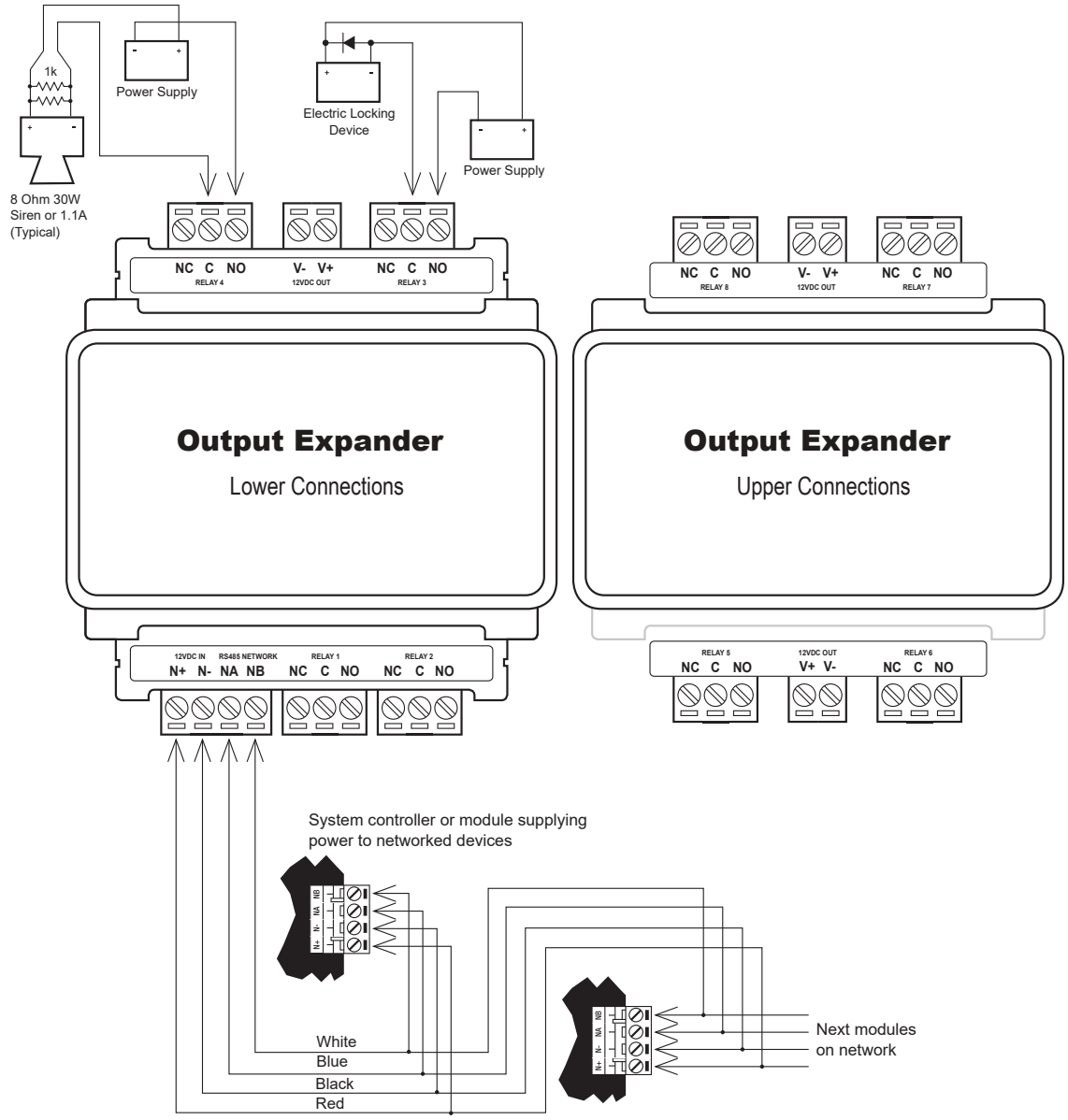
Removal

A Security Expert DIN rail module can be removed from the DIN rail mount using the following steps:

1. Insert a flat blade screwdriver into the hole in the module tab clip.
2. Lever the tab outwards and rotate the unit off the DIN rail mount.

Wiring Diagram

CAUTION: Incorrect wiring may result in damage to the unit.



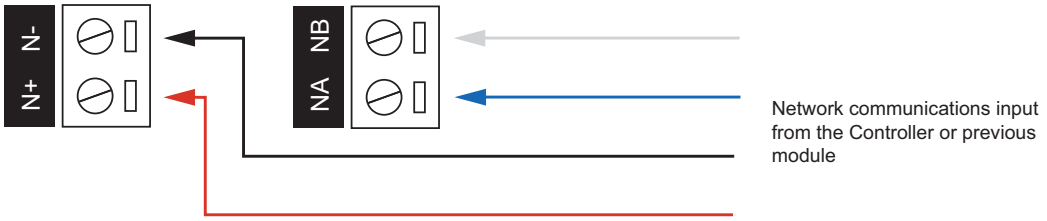
Dual Stack Connector Warning

This half DIN rail product employs an economical dual stack design which accommodates a double layer PCB with two rows of connectors. This requires the use of a specific connector configuration in which the design of the upper connectors is slightly different to the lower connectors. Pin positions on one row are incompatible with the connections on the other, and swapping upper and lower connectors may damage the connectors and the PCB.

Please check carefully before inserting connectors as incorrect placement can cause damage to the PCB.

DC Power & Encrypted Module Network

The expander incorporates encrypted RS-485 communications technology, and both module and network power are supplied by the N+ and N- terminals.



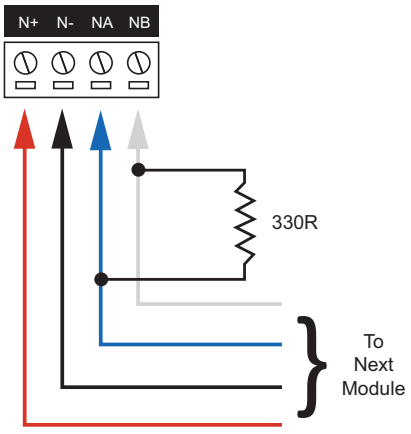
Connection of the communications and DC supply should be performed according to the diagram shown above. It is important that the N+ network communications power be 12VDC supplied from an independent battery backed power supply unit capable of supplying the required voltage to all devices on the RS-485 network.

Warning:

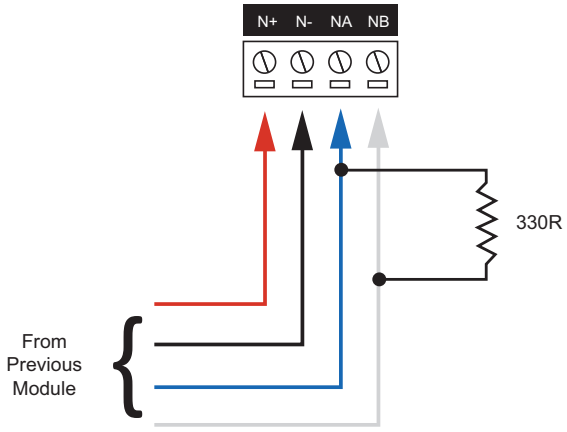
- The 12V N+ and N- communication input must be supplied from only **one** point. Connections from more than one 12V supply may cause failure or damage to the unit or the device supplying network power.
- The 330 ohm EOL (End of Line) resistor provided in the accessory bag **must** be inserted between the NA and NB terminals of the **first** and **last** modules on the RS-485 network. These are the modules physically located at the ends of the RS-485 network cabling.

End of Line Resistors:

First Module on RS-485 Network



Last Module on RS-485 Network

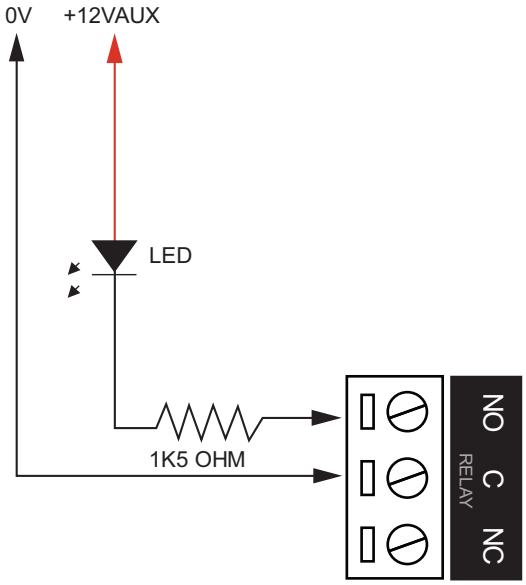


Outputs

The output expander has 8 programmable outputs. These outputs are used to activate bell sirens, lighting circuits, door locks, relay accessory products and other automation points.

Outputs 1 to 8

The 8 outputs each have a Form C output relay. The connection example below shows the control of an external LED indicator.



Warning: Switching inductive loads that can produce high back EMF voltages or large voltage-induced spikes can cause the module to behave unexpectedly and should be avoided. A suitable isolation circuit must be installed between the relay contacts of the module and the inductive load.

Trouble Inputs

Each output expander can monitor up to 8 trouble inputs.

Trouble inputs are used to monitor the module status and in most cases are not physically connected to an external input.

The following table details the trouble inputs that are configured in the system and the trouble groups that they are associated with.

Input Number	Description	Default Trouble Group	Default Trouble Group Option
PXxxx:01-07	Reserved	None	None
PXxxx:08	Module Offline	System	Module Offline

Replace 'xxx' with the appropriate address of the module that you are programming.

Address Configuration

The module address is configured via programming and will require knowledge of the module serial number. The serial number can be found on the identification sticker on the product.

Refer to the Security Expert system controller configuration guide for address programming details.

The controller has a set limit on the number of modules of each type that it can support. When adding and configuring modules always refer to the *Maximum Module Addresses* table in the controller configuration guide.

LED Indicators

Security Expert DIN rail modules feature comprehensive diagnostic indicators that can aid the installer in diagnosing faults and conditions. In some cases an indicator may have multiple meanings depending on the status indicator display at the time.

Status Indicator

The status indicator displays the module status.

State	Description
Fast flash (green)	Module attempting registration with controller
Slow flash (green)	Module successfully registered with controller
Flashing (red)	Module communications activity

When the fault and status indicators are flashing alternately, the module is in identification mode, enabling the installer to easily identify the module in question. Upon either a module update or the identification time period expiring, the module will return to normal operation.

Fault Indicator

The fault indicator is lit any time the module is operating in non-standard mode. If the fault indicator is flashing, the module requires a firmware update or is in firmware update mode. When the fault indicator is on, the status indicator will flash an error code.

State	Description
Continuous slow flash (red)	Module is in boot mode awaiting firmware update
Constantly on (red)	Module is in error state and will flash an error code with the status indicator

Power Indicator

The power indicator is lit whenever the correct module input voltage is applied across the N+ and N- terminals.

State	Description
Constantly on (green)	Correct module input voltage applied
Constantly off	Incorrect module input voltage applied

Output Indicators

The output indicators will show the status of the outputs.

State	Description
Constantly on (red)	Output is ON
Constantly off	Output is OFF

Error Code Indication

When the module attempts to register or communicate with the system controller a registration error can be generated indicating that it was not successful.

Error Code Display

The following table is only valid if the **fault** indicator is *constantly on* and the **status** indicator is *flashing red*.

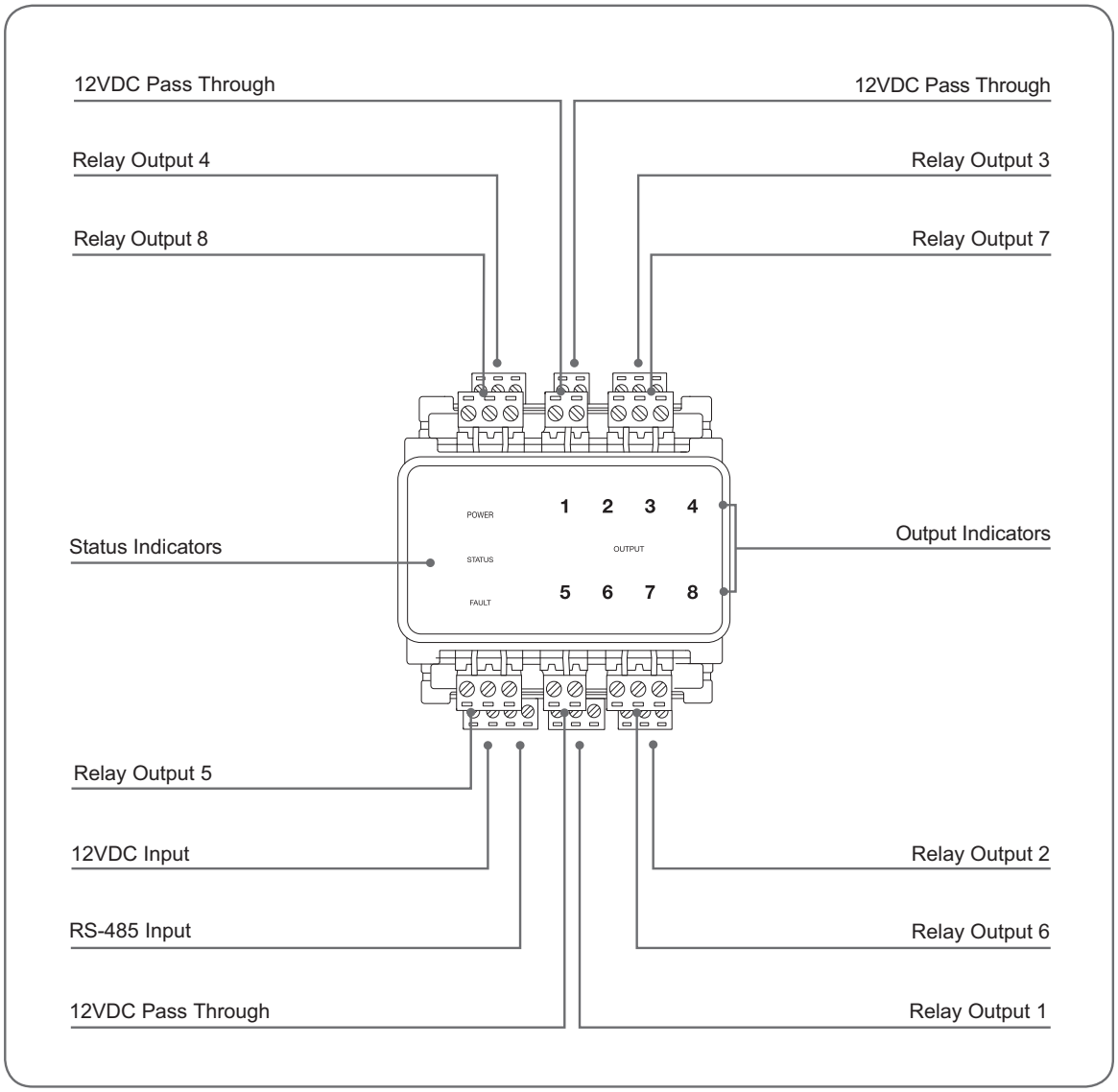
If the fault indicator is *flashing* the module requires a firmware update or is currently in firmware update mode.

The status indicator will *flash red* with the error code number. The error code number is shown with a 250ms on and off period (duty cycle) with a delay of 1.5 seconds between each display cycle.

Flash	Error Description
1	**Unknown Error Code** The error code returned by the system controller could not be understood by the module.
2	**Firmware Version** The firmware version on the module is not compatible with the system controller. To clear this error, update the module using the module update feature in the controller's web interface.
3	**Address Too High** The module address is above the maximum number available on the system controller. To clear this error change the address to one within the range set on the system controller, restart the module by disconnecting the power.
4	**Address In Use** The address is already in use by another module. To clear this error set the address to one that is not currently occupied. Use the view network status command to list the attached devices, or the network update command to refresh the registered device list.
5	**Controller Secured Registration Not Allowed** The controller is not accepting any module registrations. To allow module registrations use the network secure command to change the setting to not secured.
6	**Serial Number Fault** The serial number in the device is not valid. Return the unit to the distributor for replacement.
7	**Locked Device** The module or system controller is a locked device and cannot communicate on the network. Return the unit to the distributor for replacement.

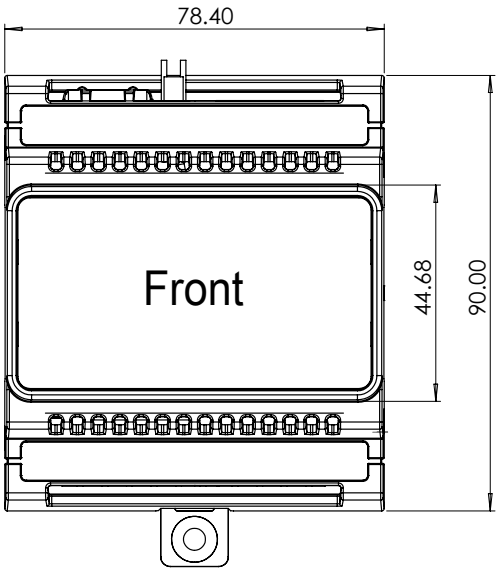
Mechanical Diagram

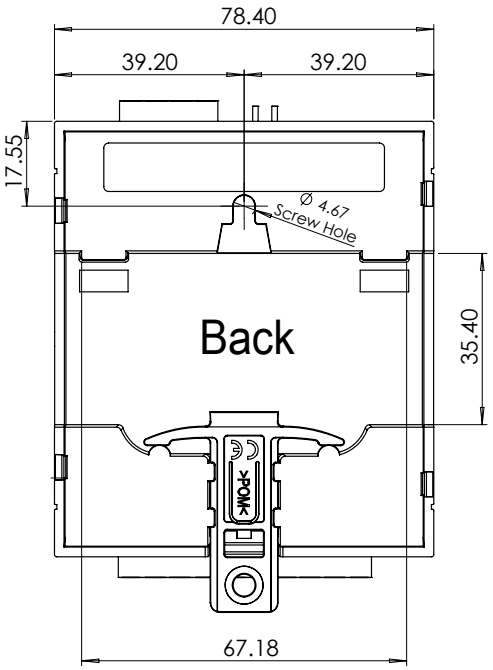
The mechanical diagram shown below outlines the essential details needed to help ensure the correct installation of the output expander.



Mechanical Layout

The mechanical layout shown below outlines the essential details needed to help ensure correct installation and mounting. All measurements are shown in millimeters.





Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Ordering Information	
SP-MO8	Security Expert Security Purpose Mini Output Expansion
Power Supply	
DC Input Voltage	11-14VDC
DC Output Voltage (DC IN Pass-Through)	10.83-14.0VDC 0.7A (Typical) Electronic Shutdown at 1.1A
Operating Current	80mA (Normal Standby)
Total Combined Current*	3.25A (Max)
Low Voltage Cutout	8.7VDC
Low Voltage Restore	10.5VDC
Communication	
RS-485	Module Network
Outputs	
Relay Outputs	8 Form C relays - 7A N.O/N.C. at 30 VAC/DC resistive/inductive
Dimensions	
Dimensions (L x W x H)	78 x 90 x 60mm (3.07 x 3.54 x 2.36")
Net Weight	240g (8.5oz)
Gross Weight	300g (10.6oz)
Operating Conditions	
Operating Temperature	UL/cUL 0° to 49°C (32° to 120°F) : EU EN -10° to 55°C (14° to 131°F)
Storage Temperature	-10˚ to 85˚C (14˚ to 185˚F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)
Mean Time Between Failures (MTBF)	587,177 hours (calculated using RDF 2000 (UTE C 80-810) Standard)

* The total combined current refers to the current that will be drawn from the external power supply to supply the expander *and* any devices connected to its outputs. The auxiliary outputs are directly connected via thermal resettable fuses to the N+ N- input terminals, and the maximum current is governed by the trip level of these fuses.

It is important that the unit is installed in a dry cool location that is not affected by humidity. Do not locate the unit in air conditioning or a boiler room that can exceed the temperature or humidity specifications.

Schneider Electric continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting our website (www.schneider-electric.com) for the latest documentation and product information.

New Zealand and Australia

General Product Statement

The RCM compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.

European Standards

CE Statement CE

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED)2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).

WEEE 

Information on Disposal for Users of Waste Electrical & Electronic Equipment

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

Information on Disposal in other Countries outside the European Union

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

Security Grade 4
Environmental Class II
Equipment Class: Fixed
Readers Environmental Class: IVA, IK07
SP1 (PSTN – voice protocol)
SP2 (PSTN – digital protocol)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)
SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + USB-4G modem)

Tests EMC (operational) according to EN 55032:2015
Radiated disturbance EN 55032:2015
Power frequency magnetic field immunity tests (EN 61000-4-8)

To comply with EN 50131-1, EN 60839-11 Security Grade 4 and AS/NZS2201.1 class 4&5 Vibration Detection for PreTamper Alarm, protection is provided by a DSC SS-102 Shockgard Seismic vibration sensor mounted within the system enclosure. Alarm output is provided by a pair of non-latching, N.C. (normally closed) relay contacts, opening for a minimum of 1 second on detection of an alarm connected in series with the 24Hr tamper input (TP) on the PSU (or any other system input designated/programmed as a 24Hr Tamper Alarm).

This relay is normally energized to give fail-safe operation in the event of a power loss. Indication of detection is provided by a LED situated on the front cover. The vibration sensor is fully protected from tampering by a N.C. micro switch operated by removal of the cover.

Enclosure SX-DIN-24 has been tested and certified to EN50131.

By design, all Security Expert EN-DIN-XX DIN Rail Enclosures comply with the EN50131 standards. Tamper protection against removal of the cover as well as removal from mounting is provided by tamper switch.

Warning: Enclosures supplied by 3rd parties may not be EN50131-compliant, and should not be claimed as such.

UK Conformity Assessment Mark

General Product Statement

The UKCA Compliance Label indicates that the supplier of the device asserts that it complies with all applicable standards.

UL and cUL Installation Requirements

Only UL / cUL listed compatible products are intended to be connected to a UL / cUL listed control system.

UL/cUL Installation Cabinet Options

cUL Fire Monitoring

Cabinet Model	cUL Installation Listings
SX-DIN-12	ULC-S559
SX-DIN-24	

Electronic Access Control System Installations

Cabinet Model	UL/cUL Installation Listings
SX-DIN-12	UL294, UL1076, ULC-ORD-C1076-86, ULC 1076, ULC 60839-11-1, CAN/ULC-S319
SX-DIN-24	

All cabinet installations of this type must be located **inside the Protected Area**.

Not to be mounted on the exterior of a vault, safe or stockroom.

All cabinet internal covers and lids/doors must be connected to the cabinet's main ground point for electrical safety and static discharge protection.

cUL Compliance Requirements

CAN/ULC-S304

- **Auto Arming**

  Control units that support auto arming shall provide an audible signal throughout the protected area not less than 10 min prior to the auto arming taking place. The control unit shall allow authorized users to cancel the auto arming sequence and transmit such cancelation to the signal receiving center with the identification of the authorized user that canceled the action.

  The following options must be enabled in the Security Expert system when using the Auto Arming feature. When the defer warning time is programmed to 10 minutes, the output group will be activated 10 minutes before the system performs the Auto Arming in the associated Area.

  - The **Defer Output or Output Group** must be programmed. Refer to the section *Areas* | *Outputs* in the Operator Reference Manual for programming instructions.
  - The **Defer Warning Time** must be programmed to not less than 10 minutes. Refer to the section *Areas* | *Configuration* in the Operator Reference Manual.
  - The **Defer Automatic Arming** option must be enabled. Refer to the section *Areas* | *Options (2)* in the Operator Reference Manual.
- **Arming Signal**

A bell or visual indicator used as an arming acknowledgment signal must be listed to a cUL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.

- **Double EOL Input Configuration**

  Only double EOL Input Configuration shall be used. Refer to the *Inputs* section of this manual and the section *Inputs* | *Options* in the Operator Reference Manual.

- **Multiplex System and Poll Time**

  The Security Expert controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

  In the Security Expert system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:

  - The **Log Polling Message** option must be enabled. Refer to the section *Report IP* | *Options* in the Operator Reference Manual.
  - The **Poll Time** must be programmed to 40 seconds. Refer to the *Report IP* | *General* section in the Operator Reference Manual.

- **Central Station Signal Receiver**

  The common equipment of each signal receiving center control unit shall be limited to 1000 alarm systems.

- **Number of attempts**

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Security Expert system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dial Attempts** option must be programmed. Refer to the section *Contact ID* | *Settings* in the Operator Reference Manual.

  If the SP-4G-USB cellular modem is being used as the secondary reporting option in the installation, the Report IP service assigned to the cellular modem must be programmed as above.

- **Check-In Time**

  DACT communication channel check-in time is not to exceed 24 hrs.

- **Trouble Input Service Test Report**
  - The **Test Report Time** must be programmed. Refer to the section *Controllers* | *Configuration* in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section *Controller* | *Options* in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section *Controller* | *Options* in the Operator Reference Manual.

- **Primary Communication Channel**

  The first attempt to send a status change signal shall utilize the primary communication channel.

  An ethernet Report IP service must be used as the primary service. The backup service may use Contact ID over the phone line or Report IP over the cellular network if the SP-4G-USB cellular modem is being used as the secondary communication channel.

  The following options are required:

  - The primary service (Report IP) must have the **Backup service** set to the secondary reporting service (Contact ID or Report IP over 4G modem). The **Service mode** must be set to *1 - Start with controller OS*.

- The backup service must have **Service operates as backup** enabled. For ULC-S304 P3 applications, **Enable offline polling** must be enabled and configured so that the backup service is monitored even when it is not active.
- For Report IP services, the **Reporting protocol** must be set to *Armor IP*.
- Refer to the *Services* section in the Operator Reference Manual.

- **Status Change Signal**

  An attempt to send a status change signal shall utilize both primary and secondary communication channels.
- **Local Annunciation if Signal Reporting Failure**

  Failure of the primary communication channel or secondary communication channel shall result in a trouble signal being transmitted to the signal receiving center within 240 seconds of the detection of the fault. Failure of either communication channel shall be annunciated locally within 180 seconds of the fault.

  The following options must be enabled in the Security Expert system:
  - The **Ethernet Link Failure** trouble input must be programmed.
  - The **Trouble Input Area** must be armed. Refer to the section *Trouble Inputs* | *Areas and Input Types* in the Operator Reference Manual.
- **Network and Domain Access**

  Neither the subscriber control unit nor the signal receiving center receiver shall be susceptible to security breaches in general-purpose operating systems.

  Network access policies should be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.
- **Ethernet Connections**

  All ethernet network connections shall be installed within the same room as the equipment.
- **Encryption**

  For active communications channel security, encryption shall be enabled at all times.

  The ArmorIP-E (UDP) protocol must be used and the Encryption Type must be set to AES-256.

  The following options must be enabled for the Report IP service in the Security Expert system.
  - The **Reporting Protocol** must be set to ArmorIP (UDP) Encrypted. The AES key must be set as specified by monitoring station.
  - Refer to the section *Report IP* | *General* in the Operator Reference Manual.
- **Server Configuration**

  Where a server is employed for control over network addressing, encryption or re-transmission, such shall be designed to remain in the "on state" at all times.

  Communicators are not suitable for active communication channel security and medium or high risk applications unless such can be "online" at all times, have a minimum 128 bit encryption scheme, have encryption enabled, network and domain security implemented.

  Network access policies shall be set to restrict unauthorized network access and "spoofing" or "denial of service" attacks.
- **Internet Service Provider (ISP)**

  The Internet Service Provider (ISP) providing service shall meet the following requirements:
  - redundant servers/systems
  - back-up power
  - routers with firewalls enabled and
  - methods to identify and protect against "Denial of Service" attacks (i.e. via "spoofing")
- **Information Technology Equipment, Products or Components of Products**

Products or components of products, which perform communications functions only, shall comply with the requirements applicable to communications equipment as specified in CAN/CSA-C22.2 No. 62368-1, Audio/video, information and communication technology equipment - Part 1: Safety requirements. Where network interfaces, such as the following, are internal to the subscriber control unit or receiver, compliance to CAN/CSA-C22.2 No. 62368-1 is adequate. Such components include, but are not limited to:

- A) Hubs;
- B) Routers;
- C) Network interface devices;
- D) Third-party communications service providers;
- E) Digital subscriber line (DSL) modems; and
- F) Cable modems.

- **Backup Power Requirements**

  Power for network equipment such as hubs, switchers, routers, servers, modems, etc., shall be backed up or powered by an uninterruptible power supply (UPS), stand-by battery or the control unit, capable of facilitating 24h standby, compliant with Clauses 16.1.2 and 16.4.1 of CAN/ULC-S304.

  For communications equipment employed at the protected premises or signal receiving center and intended to facilitate packet switched communications, as defined in CAN/ULC-S304, 24h back-up power is required.

- **Compromise Attempt Events**

  ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

  The event is sent with the following details:

  - **Account Code** as defined in the Serial Receiver settings
  - **Event Code** 0x163
  - **Group Code** as defined in the Serial Receiver settings
  - **Point Code** as defined in the Serial Receiver settings

  Refer to the section *Global Settings* | *Serial Receiver* in the ArmorIP Version 3 Internet Monitoring Application User Manual.

  For UL and cUL installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.

- **Power Supply Mains Power Connection**

  If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

  The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S319

- The Security Expert controller and reader expander module are intended to be mounted within the enclosure (refer to UL/cUL Installation Cabinet Options), installed inside the protected premise, and are CAN/ULC-S319 Listed for Class I applications only.
- Exit devices and wiring must be installed within the protected area.
- For the Security Expert controller and reader expander module, all RS-485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgment signal must be listed to a cUL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.

- Fail secure locking mechanisms shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to ULC-S533 and CAN/ULC-S104.
- Must be installed with CAN/ULC-S319 listed portal locking device(s) for cUL installations.
- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

CAN/ULC-S559

- **Signal Reporting**

  Any fault of an active communication system shall be annunciated and recorded at the signal receiving center within 180 s of the occurrence of the fault.

  The Report IP and Contact ID services must be programmed and enabled within the Security Expert system. The following options are required:

  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section *Contact ID* in the Operator Reference Manual.
  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section *Report IP* in the Operator Reference Manual.
  - The **Trouble Area** must be armed. Refer to the section *Trouble Inputs* | *Areas and Input Types* in the Operator Reference Manual.

  In the ArmorIP Internet Monitoring Software the **Poll Time** must be set to 40 seconds and the **Grace Time** must be set to 20 seconds. Refer to the section *Poll/Grace Time* in the ArmorIP Version 3 Internet Monitoring Application User Manual.
- **Central Station Signal Receiver**

  The maximum number of signal transmitting units connected to any transmission channel shall conform to the manufacturer's recommendations. The ArmorIP Receiver supports up to 10000 simultaneous connections.

  Refer to the section *Internet Connections Requirements* in the ArmorIP Receiver Installation Manual for further details.
- **Number of attempts**

  In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

  In the Security Expert system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The **Dialing Attempts** option must be programmed. Refer to the section *Contact ID* | *Settings* in the Operator Reference Manual.

  If the SP-4G-USB cellular modem is being used as the secondary reporting option in the installation, the Report IP service assigned to the cellular modem must be programmed as above.
- **Check-In Time**

  DACT communication channel check-in time is not to exceed 24 hrs.
- **Trouble Input Service Test Report**
  - The **Test Report Time** must be programmed. Refer to the section *Controllers* | *Configuration* in the Operator Reference Manual.

- The **Generate Input Restore on Test Input** option must be enabled. Refer to the section *Controller* | *Options* in the Operator Reference Manual.
- The **Test Report Time is Periodic** option must be enabled. Refer to the section *Controller* | *Options* in the Operator Reference Manual.

- **Ethernet Connections**

  All ethernet network connections shall be installed within the same room as the equipment.
- **External Wiring**

  All wiring extending outside of the enclosure must be protected by conduit.
- **Power Supply Mains Power Connection**

  If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.

  The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.
- **Arming Signal**

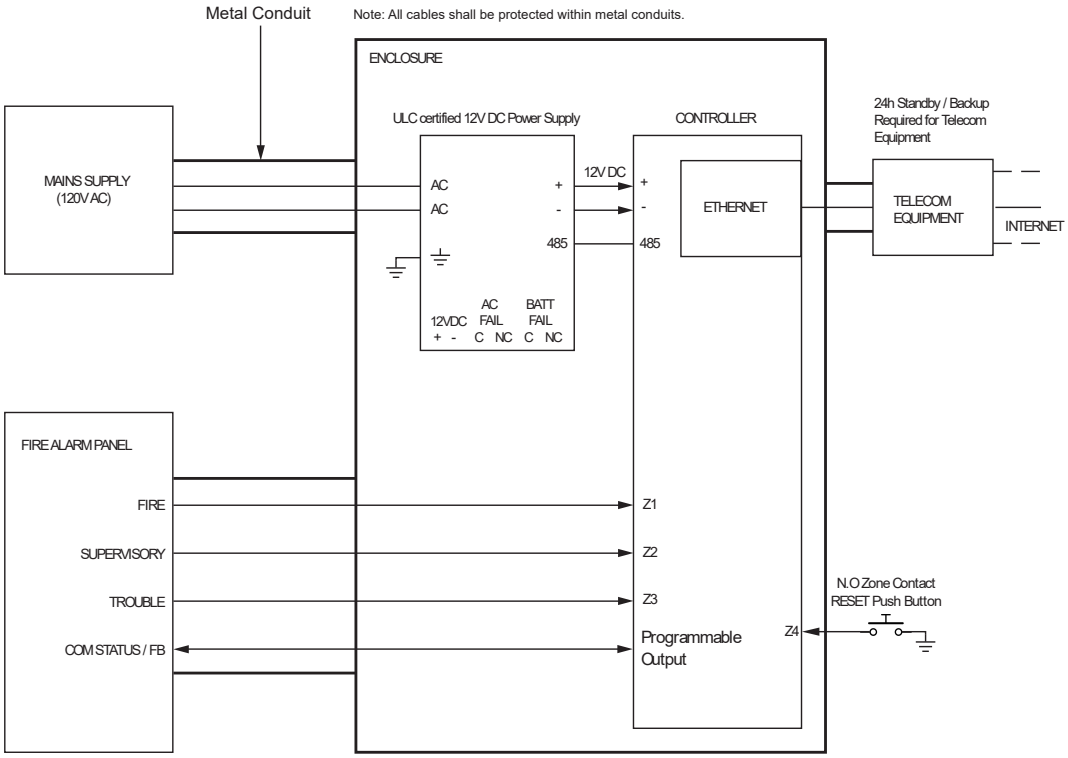
  A bell or visual indicator used as an arming acknowledgment signal must be listed to a cUL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- **Keypad Wiring**

  The RS-485 connection to the keypad must be wired such that the shorts and other faults on the RS-485 line connection of the keypad will not cause the controller to malfunction.
- **Fire Areas**

  Fire areas shall be separated from burglar areas through area partitioning.

  NOTE: Any available dry relay contact on the Security Expert controller or output expander may be used for the FACP system, provided the selected output is programmed as the Report OK output.

CAN/ULC-S559
CONTROLLER
ACTIVE COMMUNICATION

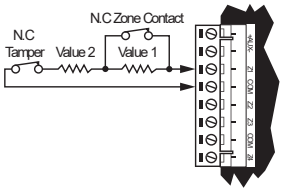


* The AC FAIL output on the Power Supply MUSTbe programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail

* Fire zones shall be separated from burglar zones through area partitioning.
* Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output
* Fire Zone Z4 N.O Push Button to be used as monitoring reset switch.

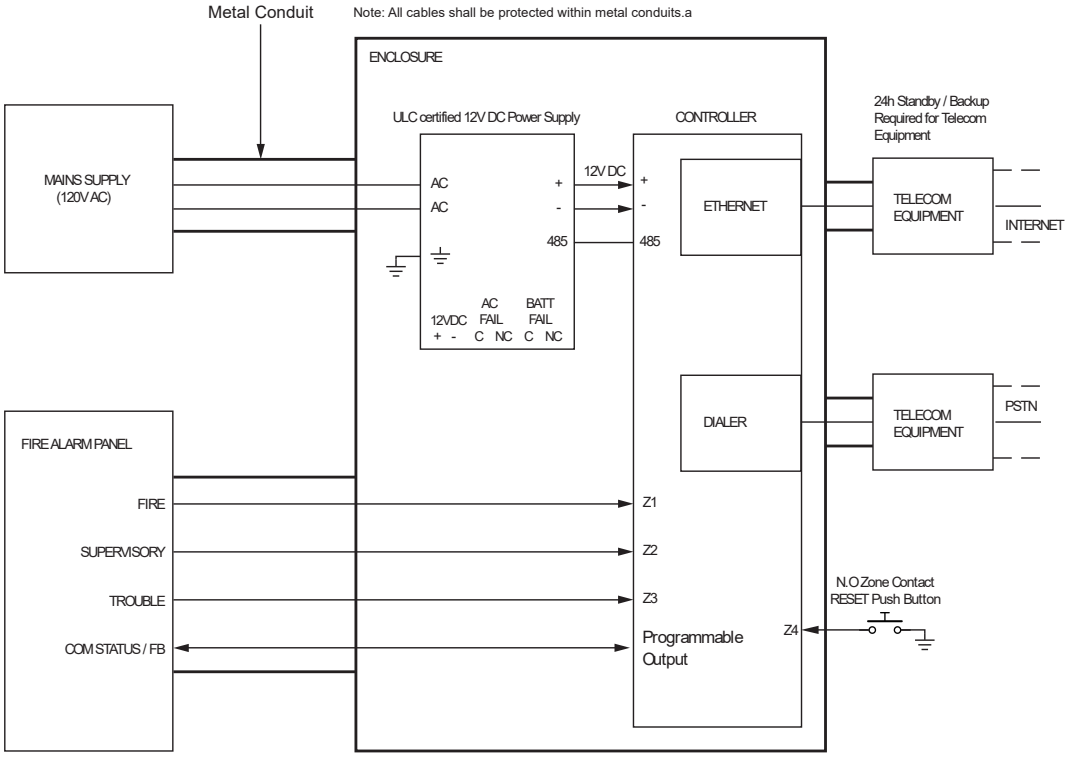
Typical Zone Circuits

EOL Resistor Zone Configuration		
Value 1	Value 2	Monitored Status
1K	1K	Open, Close, Tamper, Short
6K8	2K2	Open, Close, Tamper, Short
10K	10K	Open, Close, Tamper, Short
2K2	2K2	Open, Close, Tamper, Short
4K7	2K2	Open, Close, Tamper, Short
4K7	4K7	Open, Close, Tamper, Short



* EOL resistor must be installed at the Fire Alarm Control Panel Output.

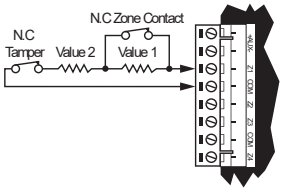
CAN/ULC-S559
CONTROLLER
PASSIVE COMMUNICATION: MODEM DIALER



* The AC FAIL output on the Power Supply MUSTbe programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail
* Fire zones shall be separated from burglar zones through area partitioning.
* Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output
* Fire Zone Z4 N.O Push Button to be used as monitoring reset switch.

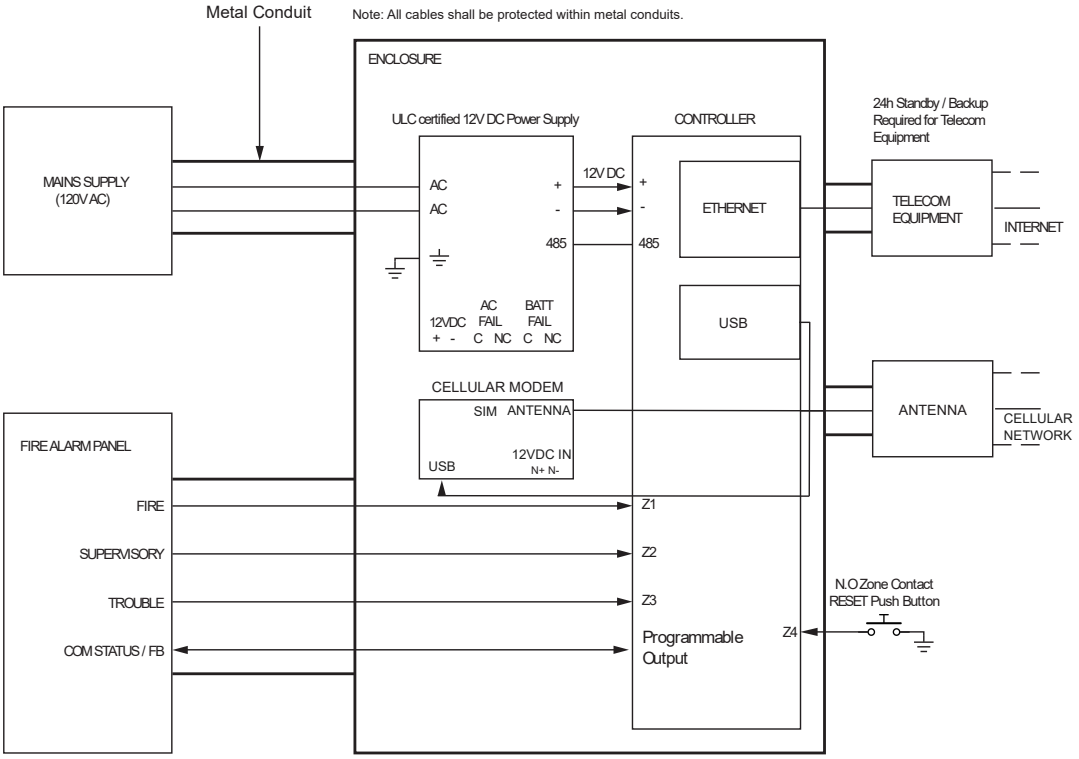
Typical Zone Circuits

EOL Resistor Zone Configuration		
Value 1	Value 2	Monitored Status
1K	1K	Open, Close, Tamper, Short
6K8	2K2	Open, Close, Tamper, Short
10K	10K	Open, Close, Tamper, Short
2K2	2K2	Open, Close, Tamper, Short
4K7	2K2	Open, Close, Tamper, Short
4K7	4K7	Open, Close, Tamper, Short



* EOL resistor must be installed at the Fire Alarm Control Panel Output.

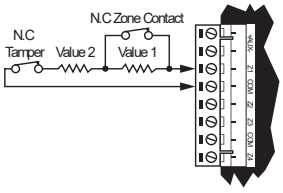
CAN/ULC-S559
CONTROLLER
ACTIVE COMMUNICATION: CELLULAR MODEM



* The AC FAIL output on the Power Supply MUSTbe programmed to follow the AC Trouble Input as follows:
AC FAIL = OPEN on fail
* Fire zones shall be separated from burglar zones through area partitioning.
* Fire zones Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output
* Fire Zone Z4 N.O Push Button to be used as monitoring reset switch.

Typical Zone Circuits

EOL Resistor Zone Configuration		
Value 1	Value 2	Monitored Status
1K	1K	Open, Close, Tamper, Short
6K8	2K2	Open, Close, Tamper, Short
10K	10K	Open, Close, Tamper, Short
2K2	2K2	Open, Close, Tamper, Short
4K7	2K2	Open, Close, Tamper, Short
4K7	4K7	Open, Close, Tamper, Short



* EOL resistor must be installed at the Fire Alarm Control Panel Output.

Fire area inputs must be programmed as follows:

- FACP Fire Alarm Signal input type must be programmed as Fire.
- Supervisory Trouble Signal input type must be programmed as 24 HR Silent.
- Trouble Signal input type must be programmed as 24 HR Silent.

Please refer to the section *Inputs* | *Areas and Input Types* in the Operator Reference Manual.

- All fire area inputs must be placed into an area and this area must be armed. Please refer to the section *Inputs* | *Areas and Input Types* in the Operator Reference Manual.
- COM Status

  FACP system with a COM STATUS input must have this input connected to one of the dry relay contacts of the Relay1 or Relay2 outputs of the Security Expert controller and the selected output must be programmed as the Report OK output in the Contact ID Service.

Note: Any available dry relay contact on the Security Expert controller or output expander may be used for the FACP system, provided the selected output is programmed as the Report OK output.

Please refer to section *Contact ID* | *Settings* in the Operator Reference Manual.

- Fire inputs Z1-Z3 shall be used exclusively for fire monitoring and cannot be programmed to activate the bell output.

UL Compliance Requirements

UL1610

For Security Grade 4 installations, two forms of reporting are required. This can be satisfied using the onboard 2400bps modem included with the modem controller model, or through the incorporation of the SP-4G-USB cellular modem module into the installation with the non-modem controller model.

- A local alarm sounding device, alarm housing, and control unit shall comply with the mercantile requirements in the Standard for Police Station Connected Burglar Alarm Units and Systems, UL365.
- A bell or visual indicator used as an arming acknowledgement signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Exit and entry delay must not exceed 60 seconds. To program the entry and exit delay time, refer to the section *Areas* | *Configuration* in the Operator Reference Manual.
- All ethernet network connections shall be installed within the same room as the equipment.
- Signals between the premises control unit and the receiving equipment, when not carried by wireless means, shall be protected by the following method:
  - Onboard modem telco connection must be dedicated to the Security Expert controller.

    Modem model only.
  - Ethernet connection to the Internet Service Provider (ISP) with a fixed IP Address must be dedicated to the Security Expert controller.
- To comply with the dual signal line transmission system requirement, *both* transmission lines (onboard modem and IP reporting) must be enabled. Signals shall be sent simultaneously to both the primary communications channel and the Backup Service.

  The Report IP and Contact ID services must be programmed and enabled within the Security Expert system. The following options are required:
  - The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
  - Refer to the section *Contact ID* in the Operator Reference Manual.
  - The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
  - Refer to the section *Report IP* in the Operator Reference Manual.
- When more than one means of signal transmission is used, loss of communication with the receiving system shall be annunciated at the receiver within 200 seconds. If a fault is detected on any of the signal transmission means, at least one of the signal transmission channels shall send a signal to the central-station to report the fault within 200 seconds.

  The Report IP and Contact ID services must be programmed and enabled within the Security Expert system.

  The Security Expert controller is compatible with the ArmorIP Internet Monitoring Receiver. Poll Time must be set to 40 seconds and the Grace Time must be set to 20 seconds.

In the Security Expert system, the reporting service must be configured to 40 seconds. The following options are required for the service selected as Report IP type:

- The **Poll Time** must be programmed to 40 seconds. Refer to the *Report IP* | *General* section in the Operator Reference Manual
- The **Contact ID Reporting Service** must be enabled and the **Service Mode** must be configured to start with the operating system.
- Refer to the section *Contact ID* in the Operator Reference Manual
- The **Report IP Service** must be enabled as the primary communication channel, the **Service Mode** must be configured to start with the operating system, and the **Reporting Protocol** must be set to ArmorIP.
- Refer to the section *Report IP* in the Operator Reference Manual.
- The **Trouble Input Area** must be armed in 24h mode. Refer to the section *Trouble Inputs* | *Areas and Input Types* in the Operator Reference Manual.

In the event of unsuccessful communication, a digital alarm communicator transmitter shall make a minimum of 5 and a maximum of 10 attempts. Where the maximum number of attempts to complete the sequence is reached, an indication of the failure shall be made at the premises.

In the Security Expert system, the reporting service selected as Contact ID must have the number of attempts programmed to 5 attempts. The following options are required:

- The **Dial Attempts** option must be programmed. Refer to the section *Contact ID* | *Settings* in the Operator Reference Manual.

- DACT communication channel check-in time is not to exceed 24 hrs.
- Trouble Zone Service Test Report
  - The **Test Report Time** must be programmed. Refer to the section *Controllers* | *Configuration* in the Operator Reference Manual.
  - The **Generate Input Restore on Test Input** option must be enabled. Refer to the section *Controller* | *Options* in the Operator Reference Manual.
  - The **Test Report Time is Periodic** option must be enabled. Refer to the section *Controller* | *Options* in the Operator Reference Manual.
  - ArmorIP detects the reception of any invalid packet on the programmed port as a potential system **compromise attempt**. Each compromise attempt sends a notification to the receiver, and logs a Compromise Attempt event under the Live Panel Events.

    The event is sent with the following details:

    - **Account Code** as defined in the Serial Receiver settings
    - **Event Code** 0x163
    - **Group Code** as defined in the Serial Receiver settings
    - **Point Code** as defined in the Serial Receiver settings

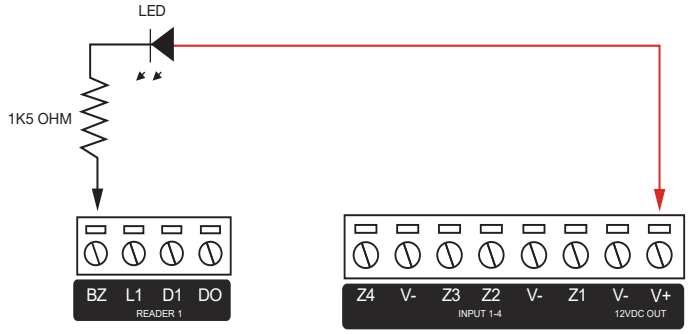
    Refer to the section *Global Settings* | *Serial Receiver* in the ArmorIP Version 3 Internet Monitoring Application User Manual.

    For UL and cUL installations the Central Station Receiving software must have the Contact ID details as specified, programmed for the **Compromise Attempt** event.
- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

UL294

- The Security Expert controller and reader expander module are intended to be mounted within the enclosure (refer to UL/cUL Installation Cabinet Options), installed inside the protected premise, and are UL 294 Listed for Attack Class I applications only.
- Exit devices and wiring must be installed within the protected area.

- For the Security Expert controller and reader expander module, all RS485 and reader terminal connections must be made using shielded grounded cable.
- All readers must be connected with shielded, grounded cable.
- A bell or visual indicator used as an arming acknowledgment signal must be listed to a UL security, signaling or fire standard. If intended to be mounted outside, it must be rated for outdoor use.
- Fail secure locking mechanism shall only be installed where allowed by the local authority having jurisdiction (AHJ) and shall not impair the operation of panic hardware and emergency egress.
- If fire resistance is required for door assembly, portal locking device(s) must be evaluated to UL10B or UL10C.
- Must be installed with UL 1034 listed electronic locks for UL installations.
- AC power on shall be indicated by an external panel mount LED (Lumex SSI-LXH312GD-150) and fitted into a dedicated 4mm hole in the cabinet to provide external visibility. This shall be wired between 12V and a PGM output that is programmed to follow the AC trouble input as shown below:



- If a flexible cord is used to connect to line voltage, strain relief must be provided for the cord inside the enclosure or at the knockout.
- The power supply is not intended to be mounted on the exterior of vault, safe, or stockroom.

FCC Compliance Statements

FCC Rules and Regulations CFR 47, Part 15, Subpart B

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Industry Canada Statement

ICES-003

This class A digital apparatus complies with Canadian ICES-003.
Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

Schneider Electric

www.schneider-electric.com

June 2024