

EVOLVE Fire Network Application Guide

Copyright © 2026 Walter Kidde Portable Equipment, LLC
All rights reserved.

This document may not be copied in whole or in part or otherwise reproduced without prior written consent from Walter Kidde Portable Equipment, LLC, except where specifically permitted under US and international copyright law.

Trademarks and patents The EVOLVE name and logo are trademarks of Walter Kidde Portable Equipment, LLC.

EVOLVE is a trademark of Walter Kidde Portable Equipment, LLC.

Contact information For contact information, see www.kidde-esfire.com.

Content

	Important information	ii
Chapter 1	Overview	1
	About this guide	2
	Related publications	2
Chapter 2	Network applications	3
	Supported network topologies	4
	EVOLVE network overview	5
	EVOLVE network media	6
	EVOLVE network operation	8
	External communication services	12
Chapter 3	Cybersecurity	15
	Cybersecurity general information	16
	Airgap	16
	EVOLVE internal network	16
	EVOLVE-SNP module	17
	Access and authentication	17
Appendix A	Network application examples	21
	Network application examples	22

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Walter Kidde Portable Equipment, LLC be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Walter Kidde Portable Equipment, LLC shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Walter Kidde Portable Equipment, LLC has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Walter Kidde Portable Equipment, LLC assumes no responsibility for errors or omissions.

Advisory messages

Advisory messages alert you to conditions or practices that can cause unwanted results. The advisory messages used in this document are shown and described below.

WARNING: Warning messages advise you of hazards that could result in injury or loss of life. They tell you which actions to take or to avoid in order to prevent the injury or loss of life.

Caution: Caution messages advise you of possible equipment damage. They tell you which actions to take or to avoid in order to prevent the damage.

Note: Note messages advise you of the possible loss of time or effort. They describe how to avoid the loss. Notes are also used to point out important information that you should read.

Chapter 1

Overview

Summary

This section provides an overview of this guide.

Content

About this guide 2

Related publications 2

About this guide

This application guide is intended for use by sales, distribution, and application personnel. It is intended as a reference guide that provides solutions to typical network application scenarios using EVOLVE network components. This guide also provides an overview of cybersecurity.

EVOLVE fire alarm systems incorporate many diverse network application solutions that can be used to design your project. If you need additional help in designing your networked EVOLVE fire alarm system, contact your district sales manager.

Related publications

The following documents provide additional information related to EVOLVE network components:

- *EVOLVE Technical Reference Manual* (P/N 3102926)
- *EVOLVE-NET Series Fiber Optics SFP Network Controllers Installation Sheet* (P/N 3103134)
- *EVOLVE-NET-TP Twisted-Pair SFP Network Controller Installation Sheet* (P/N 3103151)
- *EVOLVE-MEDIA1 Media Converter Module Installation Sheet* (P/N 3103136)
- *EVOLVE-MEDIA2 Dual Port Media Converter Installation Sheet* (P/N 3103138)
- *EVOLVE-SNP Communication Services Module Installation Sheet* (P/N 3103140)

Chapter 2

Network applications

Summary

This chapter provides a discussion of EVOLVE including supported network topologies and media, network operation and performance, and supported communication services.

Content

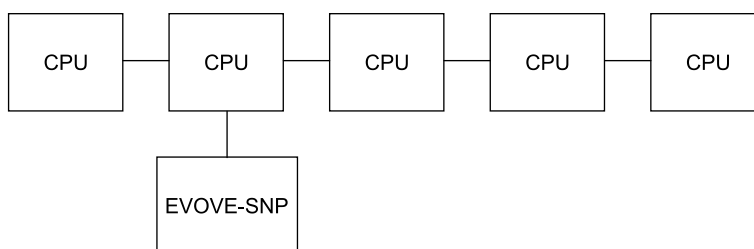
Supported network topologies	4
Linear daisy chain	4
Ring	4
EVOLVE network overview	5
EVOLVE network media	6
EVOLVE network operation	8
Configuration	8
State and command routing	8
Message routing	8
Event routing groups	9
Network time synchronization	9
Network performance	9
Network faults	10
Network reconciliation	10
Network off-normal operations	10
External communication services	12
External Communication Protocol (ECP) Service	13
Sur-Gard/IP Receiver Service	13
ConnectedSafety+ (CS+) Service	14

Supported network topologies

Networked EVOLVE fire alarm systems support the network topologies described below.

Linear daisy chain

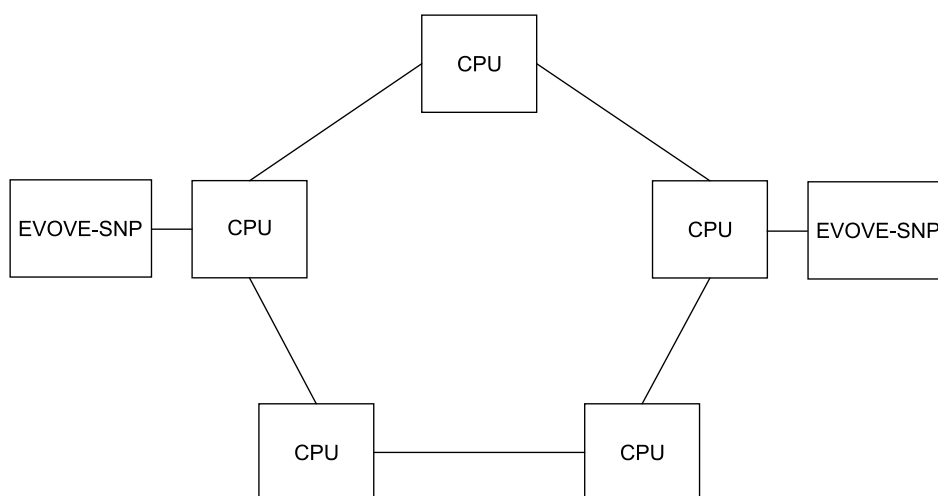
In EVOLVE fire alarm networks that use linear daisy chain topology, the fire panel CPU nodes are connected sequentially from beginning-to-end without a redundant return path to the originating node (see below). The data communication performance designation for fire alarm networks using this topology is Class B/DCLB.



In Class B/DCLB fire alarm networks, a single open or short condition results in loss of communication beyond the fault location. Nodes on the same side of the fault maintain communication with each other but not with nodes on the other side of the break. The EVOLVE fire alarm network provides protection should there be a short in a copper network offering the same recovery solution as found with an open. A short on network wiring creates a single disconnect between the nodes on either side of the short, while allowing nodes on the same side of the short to communicate with each other. Class B/DCLB networking provides a cost-effective solution for applications where full redundancy is not required, and system design allows for localized loss of network communication.

Ring

In EVOLVE fire alarm networks that use ring topology, the fire panel CPU nodes are connected sequentially from beginning-to-end and include a redundant return path to the originating node (see below). The data communication performance designation for fire alarm networks using this topology is Class A/DCLA or Class X/DCLC.



In Class A/DCLA and Class X/DCLC fire alarm networks, a single open or single short condition anywhere on the network does not impair communication between network nodes. Class A/DCLA and Class X/DCLC networking is ideal for facilities requiring high fault tolerance and continuous operation in the event of a single wiring fault.

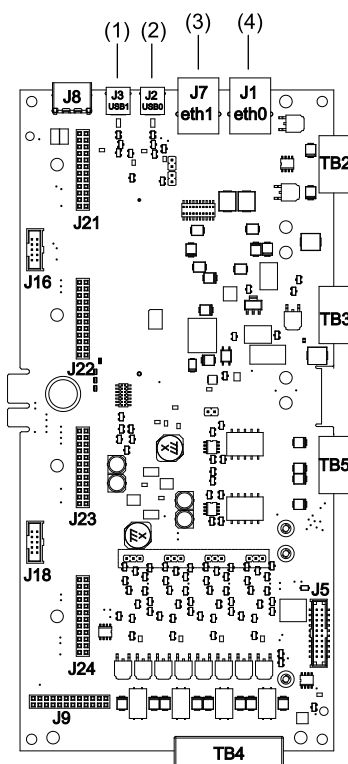
EVOLVE network overview

EVOLVE fire alarm networks support one to 24 nodes. Multiple network media types are supported including unshielded twisted-pair, fiber-optic, and CAT 5e or better cables using small form-factor pluggable (SFP) modules. Nodes communicate with other nodes over CAT 5e or better Ethernet using the on-board RJ-45 connections. Fiber-optic and twisted-pair are achieved using the EVOLVE-MEDIA1 media converter module and EVOLVE-MEDIA2 dual port media converter. Linear daisy chain and ring network topologies are supported. EVOLVE networked fire alarm panels also support connection to and from external IP services and central monitoring stations via an EVOLVE-SNP communication services module. See Appendix A “Network application examples” on page 21 for example block diagrams of supported network topologies.

The EVOLVE fire alarm network uses Internet protocol (IP) for data communication between nodes. The EVOLVE fire alarm network distributes network status, events, reports, instruction packets, and instruction log packets to all nodes in the network. The network also performs functions such as network-wide time synchronization, node supervision, and network reconcile activities.

An EVOLVE fire alarm control panel has four network interfaces as shown in Figure 1 below. A maximum of two nodes can reside in the same cabinet, an EVOLVE CPU node and an EVOLVE-SNP node.

Figure 1: Network interfaces



- (1) J3 – USB 1 (USB Type C) - to connect to the EVOLVE-CU or an EVOLVE-SNP
- (2) J2 – USB 0 (USB Type C) - to connect to the EVOLVE-CU
- (3) J7 – ETH1 - Ethernet connection to other nodes or external services
- (4) J1 – ETH0 - Ethernet connection to other nodes or external services

Adding an EVOLVE-SNP provides two additional Ethernet interfaces in the same cabinet. A USB-C cable connects an EVOLVE CPU to an EVOLVE-SNP. For additional details regarding mounting options, see *EVOLVE-SNP Communication Services Module Installation Sheet* (P/N 3103140). The EVOLVE-SNP provides communication with external networks using IPv4 or IPv6 and provides a secure communication barrier between the internal life safety network and the external internet or intranet. All requests and responses are handled by the EVOLVE-SNP, protecting the EVOLVE fire alarm network from malicious attacks.

Note: For maximum EVOLVE networked system capability, refer to *EVOLVE UL Listing Document* (P/N 3102923).

Table 1: EVOLVE nodes

Device name	Description
Panel CPU Board	The EVOLVE panel CPU board processes all information from modules installed in the same cabinet and from other nodes in the fire alarm network. The EVOLVE panel CPU board incorporates: • Two USB 2.0 Type C connectors • Two RJ-45 Ethernet ports
EVOLVE-SNP Communication Services Module	The EVOLVE-SNP communication services module provides additional connections for external communication services. It also acts as a firewall by blocking unauthorized access to the EVOLVE fire alarm network, while permitting outward communication. The EVOLVE-SNP module incorporates: • Two USB-C ports (USB 0 connects to panel CPU board; USB 1 is for future use) • Two RJ-45 Ethernet ports

EVOLVE network media

EVOLVE fire alarm systems provide many solutions that allow installations to use different media types to connect networked control panels. This is accomplished through the use of small form-factor pluggable (SFP) modules and media converters. The EVOLVE-MEDIA1 and EVOLVE-MEDIA2 media converters provide the ability to use a different network media between EVOLVE fire alarm control panels via SFP modules. They install in an expansion slot on the EVOLVE CPU. For additional mounting details, see *EVOLVE-MEDIA1 Media Converter Module Installation Sheet* (P/N 3103136) or *EVOLVE-MEDIA2 Dual Port Media Converter Installation Sheet* (P/N 3103138).

The SFP modules provide plug and play network changeability. These SFPs are hot-swappable, meaning the network, including the nodes being changed, can remain running while the SFP is swapped. There will be network communication faults while the SFPs are being swapped since links will be disconnected temporarily. Those faults clear once all reconnections are complete.

Selecting the appropriate media types listed in Table 2 on page 7 depends on several factors, including network size and operations, cost, and whether it is a new system or retrofit. The cabling must meet the minimum capacitance and resistance specifications. High speed CAT 5e or better, or fiber-optic media, is recommended particularly for large installations.

Refer to Table 2 on page 7 for a description of EVOLVE network SFPs. Refer to ““Related publications” on page 2 for specific SFP publications.

Table 2: EVOLVE network SFPs

Device	Cable type	Max wire run length	Description
EVOLVE-NET-MM	Fiber-optic	1.24 mi. (2 km.)	SFP network media interface, multi-mode fiber-optic, with a 50/125 μ (OM3/OM4) fiber pair up to 1.24 mi. (2 km), 62.5/125 μ (OM1) fiber pair up to 0.62 mi. (1 km), or a 100/140 μ fiber pair up to 150 m. The EVOLVE-NET series network controllers mount in one SFP slot in the EVOLVE-MEDIA1 media converter module or EVOLVE-MEDIA2 dual port media converter.
EVOLVE-NET-SM	Fiber-optic	8.7 mi. (14 km.)	SFP network media interface, dual filament, single-mode fiber-optic, with a 9/125 μ (G.652) fiber pair up to 8.7 mi. (14 km.). The EVOLVE-NET series network controllers mount in one SFP slot in the EVOLVE-MEDIA1 media converter module or EVOLVE-MEDIA2 dual port media converter.
EVOLVE-NET-SMH	Fiber-optic	24.8 mi. (40 km.)	SFP network media interface, dual filament, single-mode fiber-optic, high-power output, with a 9/125 μ (G.652) fiber pair up to 24.8 mi. (40 km.). The EVOLVE-NET series network controllers mount in one SFP slot in the EVOLVE-MEDIA1 media converter module or EVOLVE-MEDIA2 dual port media converter.
EVOLVE-NET-TP	See Table 3	See Table 3	The EVOLVE-NET-TP SFP network controllers support data communication over one unshielded twisted-pair wire. Each controller supports a single unshielded twisted-pair wired intranet connection. The EVOLVE-NET-TP-to-EVOLVE-NET-TP link is supervised for opens, shorts, ground faults, and continued communications. EVOLVE-NET-TP network controllers plug into one SFP slot in the EVOLVE-MEDIA1 media converter module or EVOLVE-MEDIA2 dual port media converter.

Table 3: EVOLVE-NET-TP cabling specifications

Wire type	Wire size	Circuit length [1]	Maximum circuit resistance	Maximum circuit capacitance	Communication speed
UTP - Unshielded twisted-pair (UTP) other than CAT cables [2]	16 to 22 AWG	5,000 ft. (1,524 m)	80 Ω	0.09 μ F	Up to 2 Mbps TX and RX Communication
CAT 5e or better - UTP that meets ANSI/TIA/EIA-568-A definition	22 to 24 AWG	328 ft. (100m)	N/A	N/A	Up to 2 Mbps TX and RX Communication
Shielded twisted-pair (STP) other than CAT cables [3]	Not supported				

[1] Circuit length is between any two nodes.

[2] Twisted-pair wiring should be a single unshielded twisted-pair with six twists per foot minimum. It is recommended to use 16 to 18 AWG for reliability and simplicity of installation. All specifications in Table 3 above should be met to maximize noise immunity.

[3] Shielded twisted-pair is not supported for the EVOLVE-NET-TP.

EVOLVE network operation

Configuration

The EVOLVE fire alarm network is a self-configuring (plug and play) network. Each Ethernet interface is assigned a MAC address during manufacturing. The programmer needs to add the MAC address (which is printed on the CPU or EVOLVE-SNP label) into the EVOLVE-CU. When the configuration is downloaded to the system, each CPU node is automatically assigned an IPv6 address. A new IPv6 address is assigned during each system boot up. Configuration of project settings for the entire network is performed from a single USB connection to one node.

Note: For all EVOLVE-CU versions, use the Transfer button on the Home tab to transfer configuration and firmware downloads.

State and command routing

Networked EVOLVE fire alarm systems use a feature called Network Routes to allow state changes, event messages (see “Message routing” below), and LCD user interface common control commands to be shared on multiple nodes as follows:

- A fire panel node’s State Network Route uses network routes to determine the group of fire panel nodes from which it processes state changes and event messages, in addition to its own
- A fire panel node’s LCD common controls use network routes to determine the group of fire panel nodes to which it sends common control commands to, in addition to itself

There are two default network routes: All and None. The All network route includes all fire panel nodes and all EVOLVE-SNP expander nodes in the project. The None network route does not include any nodes. These two network routes are nonconfigurable.

A project may have up to 256 user-defined network routes. A node may be a member of more than one network route.

Message routing

Networked EVOLVE fire alarm systems use a feature called Message Routes to determine where device state changes are displayed or printed.

There are two default message routes: All and None. The All message route includes all fire panel node LCDs and printers in the project. The None message route does not include any fire panel node LCDs or printers. These two message routes are nonconfigurable.

Message routes work in conjunction with a fire panel node’s state network routing. A fire panel node may not process event messages from another fire panel node if that fire panel node is not included in its state network routing.

A project may have up to 256 user-defined message routes. Fire panel node LCDs and printers may be a member of more than one message route.

Fire panel nodes and printer connections use a queues filter to determine which events are displayed or printed. There is no event filtering on a node’s FireWorks, FSB Service, ConnectedSafety+, and Custom ECP Service connections.

Notes

- A node's state network route setting determines whether it processes event messages from other nodes. A device's message route setting determines whether a node may display or print the event message. A fire panel node or printer's queue filter setting determines which event message types are displayed or printed.
- Setting a device's message route to None prevents its event message from being displayed or printed but does not prevent a node from processing its state change.

Event routing groups

Event routing groups specify the group of CMS accounts to which event activation and event restoration messages are sent, and can be added to an EVOLVE-CU project. Refer to *EVOLVE-CU Help* for more information on configuring event routing groups.

Network time synchronization

The EVOLVE network uses Network Time Protocol (NTP) to keep all nodes synchronized. Nodes are assigned as a server or client. When assigned as a server, a CPU node is the master timekeeper, and all nodes synchronize to its clock. It is also possible to make use of internet network time services to be the master, however the system must have an EVOLVE-SNP installed to provide the internet connection to the remote NTP server. By configuring the Fully Qualified Domain Name or IP address of an NTP server, all nodes on the EVOLVE network maintain synchronization to that clock.

Network performance

The EVOLVE network requires that all nodes must process any event on the network within the time specified by agency standards to maintain reliability and to make sure the building occupants are notified in a timely manner. The following sections describe how this requirement is met and factors to consider.

Bandwidth

The EVOLVE network bandwidth can vary depending upon the communication media used. Bandwidth versus media type is shown in Table 2 on page 7 and Table 3 on page 7. Depending on the media selected, the bandwidth supported is 100 Mbps to 1 Mbps of data. The amount of data that is sent and the bandwidth used in EVOLVE is impacted by the following factors:

- Number and topology of network nodes
- Number of simultaneous events and operations

The network under idle conditions, when there are no events or operations active, uses some bandwidth to maintain the network routing and supervision. This overhead bandwidth increases somewhat as the number of nodes increases, so when using low bandwidth media, this overhead should be considered as the number of nodes increases.

When operations and events occur, data volume over the network increases. Bandwidth usage due to events or operations varies based on number of events or operations and the quantity of information associated with each. Based on bandwidth needed for network overhead, event and control operations, EVOLVE has limits for concurrent operations.

When many events occur simultaneously, such as during a multiple fire event situation, the system requires more bandwidth. Each node in the EVOLVE system limitation can consume approximately 50 events per second. That number is based on worst case bandwidth usage where maximum data is present on low bandwidth media. The maximum bandwidth, used under these circumstances, averages well below what EVOLVE-NET-TP networks can support. As such, the EVOLVE system with its node count limit of 24 should not be constrained, even with EVOLVE-NET-TP networks.

Note: It is recommended to use fiber-optic or CAT 5e or better Ethernet for optimum network performance. Refer to *EVOLVE-NET Series Fiber Optics SFP Network Controllers Installation Sheet* (P/N 3103134) and *EVOLVE-NET-TP Twisted-Pair SFP Network Controller Installation Sheet* (P/N 3103151) for complete details.

Speed

In addition to the bandwidth capabilities of different media types, there are latencies within the system due to the firmware and device drivers that carry out the receive and transmit operations. EVOLVE has design requirements that assure timely delivery of events and execution of notification and other fire system operations.

Network faults

An EVOLVE fire alarm network has the capability to detect and annunciate network off-normal conditions. Communication fault detection/restoration mechanisms monitor the heartbeat messages sent from the nodes across the network. Communication failures are reported when messages from a node are not seen within agency time requirements. If the communication failure is recovered and the nodes are able to talk within the agency time requirement, the trouble will be restored and the system will go back to normal.

EVOLVE also supervises the network interfaces for faults and link failures. The network ports that should be active are selected in the EVOLVE-CU node properties. Based on this configuration, the EVOLVE nodes generate a trouble whenever a port is configured as active, but the link is not detected, or when a port is not configured as active and a link is detected (if a user inserts an SFP). Kidde Commercial supported SFPs are UL listed for this purpose and the system supervises for correct SFP types. If an incompatible SFP is installed, a fault event is reported, helping ensure network integrity and listings are maintained.

During high network traffic when there is demand for sending large amount of data from a single node, an EVOLVE node adjusts its transmissions to ease the traffic. A node generates a network overflow message if it cannot keep up with the amount of traffic being sent or consumed. EVOLVE nodes are intelligent enough to make sure that during high network demand, message loss is prevented. Refer to *EVOLVE Technical Reference Manual* (P/N 3102926) for pseudo points and troubleshooting guidance.

Network reconciliation

When the network recovers from failures, all active and restored events are sent over to the network so that all nodes are updated with the latest network status, i.e., reconciled. If network communication fails while there is an active request to control the system, the request is canceled and you must re-establish control. See *EVOLVE User Guide* (P/N 3102928) for more information on how to request and grant control.

Network off-normal operations

In addition to the network conditions described above, EVOLVE monitors versions of firmware and configurations resident on all nodes and the nodes themselves. Exceptions found result in a level of degraded operations as described in the following.

Fail-safe modes

The cases below are fail-safe modes that the network will enter under certain conditions.

Incompatible firmware:

- This case happens when the firmware version of one node is incompatible with other nodes. On the LCD user interface, the Network Incompatibility pseudo point (0300 + node address) displays with firmware mismatch information and location in the details. For example, the Network Incompatibility pseudo point for node one is 0301, node two is 0302, etc.

- Node state changes and remote write unlock (reprogramming capability) is accepted. Command and control messages to and from the incompatible node(s) are discarded.
- An alarm on the local node is annunciated as an alarm with the proper type. An alarm from a node with incompatible firmware is annunciated and the Unconfigured pseudo point (0032) displays on the remote nodes and any nodes with compatible firmware.

Incompatible database:

- This case happens when the database (or database version) of a node is not compatible with other nodes. On the LCD user interface, the Network Incompatibility pseudo point (0300 + node address) displays with the database mismatch and location information in the details. For example, the Network Incompatibility pseudo point for node one is 0301, node two is 0302, etc.
- Node state changes and remote write unlock are accepted while a node is in this state, so the installer can download a new database from any node in the network. Command and control messages to and from the incompatible node(s) are discarded.
- An alarm on this local node is annunciated as an alarm with the proper type. An alarm from a node that is part of the incompatible network is annunciated and the Unconfigured pseudo point (0032) displays on the remote nodes and any nodes with compatible firmware.

Duplicate node ID:

- When two networks are connected together and two or more nodes have the same node ID, the Network Incompatibility pseudo point (0300 + node address) displays on the LCD user interface with the duplicate node and location information in the details. For example, the Network Incompatibility pseudo point for node one is 0301, node two is 0302, etc. This could happen if proper steps are not taken when a large installation is brought up with small groups of nodes, and then connected together to form the full system.
- Remote write unlock is accepted, so the user can download a new database from any node in the network to correct the issue. Command and control messages to and from the incompatible node(s) are discarded. Node state changes are checked and processed by the nodes to determine if other nodes are in alarm (to annunciate un-configured alarm trouble), but the state changes are not saved to history.
- An alarm from either node that has the duplicate address network is annunciated and the Unconfigured pseudo point (0032) displays on the remote nodes.
- An alarm on the local node is annunciated as an alarm with the proper type and any nodes with compatible firmware.

Node ID out of bounds:

- In cases when either a node is in default fail-safe mode or the node ID is not in the project, the Network Out of Range pseudo point (031) displays on the LCD user interface.
- Remote write unlock is accepted so the user can download a new database from any node in the network to correct the issue. Command and control messages to and from the out-of-range node(s) are discarded. Node state changes are checked and processed by the nodes to determine if other nodes are in alarm (to annunciate un-configured Alarm trouble), but the state changes are not saved to history.
- An alarm from a node that is out of bounds is annunciated and the Unconfigured pseudo point (0032) displays on the remote nodes.
- An alarm on the local node is annunciated as an alarm with the proper type and any nodes with compatible firmware.

Node is currently operating as a single node configuration:

- In cases where a node is configured as a single node project but is wired into a multi-node network.
- In the single node configuration, the node will not start network processes to save resources and for security reasons. Therefore, this node will not have full communications with other nodes and will not be able to

receive the remote write unlock to be able to remotely download the correct configuration database to this node.

- An alarm on this local node is annunciated as an alarm with proper type.
- The solution to this scenario is to locally reconfigure the single node through direct USB connection with the proper multi-node network configuration prior to connecting it to the rest of the nodes.

External communication services

EVOLVE communications services are used to allow transmission of system events through an EVOLVE control panel to external devices such as central monitoring stations, building management systems, FireWorks Incident Management Platform, and printers. Communication occurs over Ethernet using communication services described in this section.

When external connections are needed, the design of EVOLVE protects the fire alarm system by implementing firewall protections on the EVOLVE main CPU board in single fire alarm control panel systems, and by using the UL listed EVOLVE-SNP communication services module for networked fire alarm control panel systems.

In a single fire alarm control panel system, you can use the CPU onboard Ethernet ports for external communication services. In networked fire alarm control panel systems, the EVOLVE-SNP completely separates the life safety network from outside networks and provides several services via the external network.

Table 4 below shows the maximum number of services that can be configured for a node type. The services can be any combination of different services but cannot exceed the maximum number.

Table 4: Communication services and node types

Service	Details (maximum services: 8)
Printer	External service; 1 per panel
ECP [1]	8 per panel
Sur-Gard/IP Receiver (IP Dialer) [2]	External service; up to 8 per panel
ConnectedSafety+ (CS+) [3]	External service; 1 per project
FireWorks [4]	External service; up to 8 per panel

[1] Uses the External Command XML (ECPxml) protocol, which requires customer or product licensing to allow communication with the control panel. Supports EVOLVE-FSB Field Server Bridge. To obtain a third-party license key, contact your local Kidde Commercial representative.

[2] A project can have up to eight Sur-Gard connections per fire panel node provided you do not specify any other external connections. Each Sur-Gard connection can send event codes to one or more CMS accounts, but you cannot have more than eight Sur-Gard CMS accounts in a project.

[3] A project can only have one CS+ service.

[4] A project with a single standalone fire panel node can have up to eight FireWorks connections provided you do not specify any other external connections. FireWorks version 10.0 is only compatible with non-networked EVOLVE control panels for monitoring only.

When connecting to external services with an EVOLVE-SNP module it is important to keep in mind the following configuration requirements:

- The EVOLVE-SNP Ethernet connections, ETH0 and ETH1, should not have connection to any Ethernet ports on the CPU nodes.
- When multiple Ethernet connections are used on a CPU node or EVOLVE-SNP module for external services: Both Ethernet port IP versions on the CPU node or EVOLVE-SNP module must be the same, either both IPv4 or both IPv6.

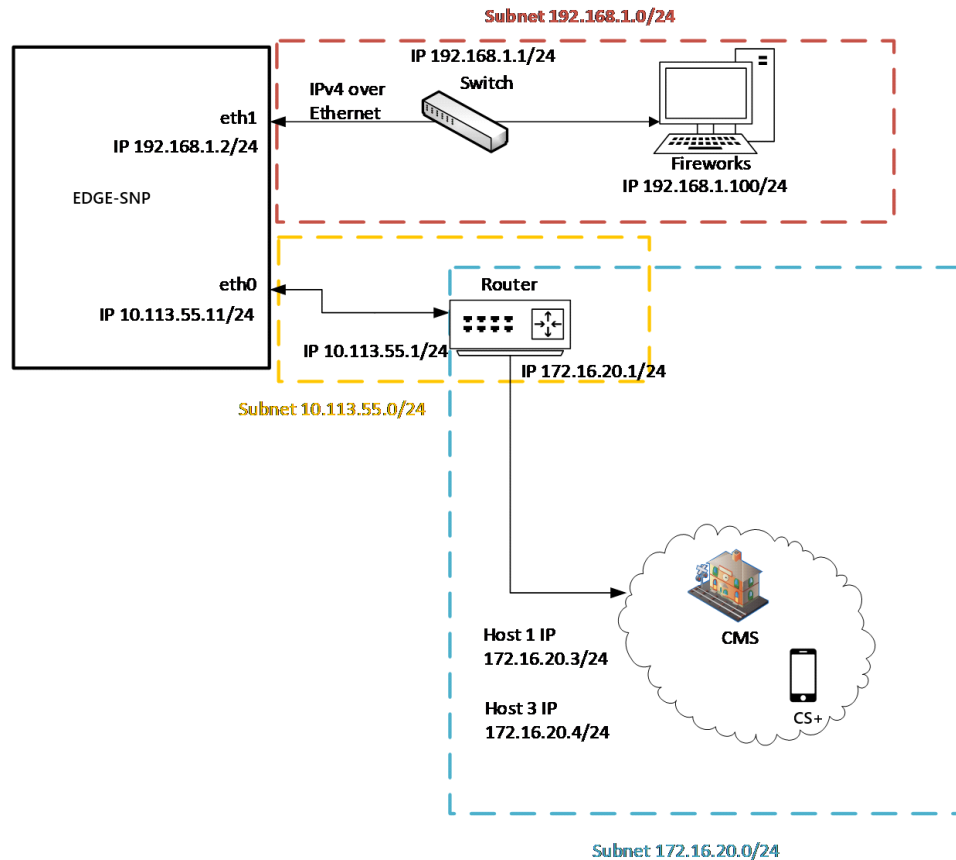
Each port, ETH0 and ETH1, must be connected to a different subnet. If auto-addressing is used, the ports must be connected to different DHCP servers.

Assure that the connected server(s) or hosts belong to the same subnet as the connected ETH0 or ETH1 port.

If your network setup necessitates reaching a host on a different subnet, use ETH0 for this configuration. See Figure 2 below.

If your configuration requires reaching a host or a server on the Internet, make sure that any DNS server you configure can resolve a public address.

Figure 2: Subnet hosts



External Communication Protocol (ECP) Service

The External Communication Protocol is a proprietary protocol used to communicate with FireWorks and third-party building management systems. The ECP is a secured protocol by which the system sends and receives requests as XML messages through the EVOLVE-SNP. A license is required to use the ECP for monitoring the system from an external application.

Sur-Gard/IP Receiver Service

The Sur-Gard/IP Receiver Service is a service also referred to as Central Monitoring Stations (CMS) that is used to communicate with the central monitoring station, so that the system is monitored 24/7 for any events. This service's communication is secured over a proprietary UDP protocol.

ConnectedSafety+ (CS+) Service

The ConnectedSafety+ (CS+) Service allows the panel to connect to the cloud and send live events and reports. The CS+ Service connects to the cloud and sends and receives data over secure MQTT protocol. The service is supervised by default. Any disconnection is reported as a trouble and displays the Communication Service pseudo point (0700 + service ID). In order for the service to function properly, the panel must be connected to the Internet and to a DNS server that can resolve public addresses.

The following is the preferred Internet connection to run the CS+ Service:

- Wire the connection from the EVOLVE-SNP to a router, as opposed to an unmanaged switch. Routers ensure that clients receive network traffic intended just for them.
- Use of a switch is not recommended. If a managed switch is used, configure the port used for the EVOLVE-SNP to be isolated so that traffic to/from other clients is not sent to the EVOLVE-SNP.
- Setup a VLAN dedicated to the EVOLVE-SNP running the CS+ service, as an option to isolate network traffic.

Chapter 3

Cybersecurity

Summary

This section provides a description of the cyber security related features of the EVOLVE system.

Content

- Cybersecurity general information 16
 - Cybersecurity industry accepted guidelines 16
- Airgap 16
- EVOLVE internal network 16
- EVOLVE-SNP module 17
 - EVOLVE-SNP cybersecurity features 17
- Access and authentication 17

Cybersecurity general information

The EVOLVE system provides levels of protection and the flexibility to deploy in a manner that can help with cybersecurity requests. The system's flexibility allows the installer to work with the building owner and local IT professionals to match the system to their IT and cybersecurity needs.

Whether a site has a detailed Security Incident and Event Management (SIEM) structure or is more ad hoc in its approach, understanding how EVOLVE addresses cybersecurity attack surfaces helps both installer and local IT to align the active protection, compensating controls, and audit trail capabilities available to the cybersecurity needs and the life safety needs.

Cybersecurity industry accepted guidelines

Common industry-accepted standards that include specific weakness-correcting guidelines are published by the following organizations:

- National Institute of Standards and Technology (NIST)
- Federal Information Processing Standards (FIPS)
- Secure Technical Implementation Guides (STIG)
- SysAdmin, Audit, Network and Security (SANS) Institute
- Center of Internet Security (CIS)
- International Organization for Standardization (ISO)
- Open Web Application Security Project (OWASP)
- Internet Engineering Task Force (IETF) - Request For Comments (RFC)
- Risk Management Framework (RMF)

Airgap

An airgap is a space between the life safety system and external threats. EVOLVE has multiple levels of physical security that can be used to meet simple airgap requirements in systems without firewalls.

An airgap does not allow the life safety system to connect or communicate to any external IT infrastructure.

EVOLVE internal network

EVOLVE has multiple levels of physical security that can be used, such as tamper switches and control panel keyed door locks. These methods can provide an audit trail of cabinet access. They also provide a level of protection in conjunction with EVOLVE history archives and in building security protocols.

EVOLVE addresses higher level cybersecurity needs starting with its internal network and the method used to connect the EVOLVE-CU configuration utility to outside networks.

The internal life safety network takes advantage of industry standards bringing a self-configuring IPv6 network. Eliminating the need for centralized servers, EVOLVE achieves an easily deployed, self-configuring peer-to-peer IPv6 network.

The EVOLVE nodes authenticate with each other allowing only interoperation with nodes of the same project. Man-in-the-middle attacks on the network are less likely and would be annunciated, captured in history, and auditable. Pseudo points indicate possible intrusions such as Network Communication (0050 + node ID), Network Incompatibility (0300 + node ID), and Network Out of Range (0031).

To further reduce risk and minimize the attack surface (areas that may be exploited) of EVOLVE hardware, all unnecessary I/O on all microcontrollers is removed during manufacturing and all physical connections are removed on all microcontroller PCB assemblies, making connection via product hardware difficult. All services and applications run non-root based including user accounts. No console access is provided.

EVOLVE-SNP module

When external connections are needed, EVOLVE protects the life safety network by offering the fire listed EVOLVE-SNP module. The EVOLVE-SNP acts as a firewall by blocking unauthorized access to the EVOLVE fire alarm network, while permitting outward communication. The EVOLVE firewall is designed as a proxy firewall – no network data packets are passed from one side of the firewall to the other. Protocols and ports can be restricted to only those needed by the EVOLVE operation; the firewall will block all other traffic.

EVOLVE-SNP cybersecurity features

- ECPxml and ConnectedSafety+(CS+) services are via 256-bit AES via SSL/TLS (FIPS-197).
- Central Station connections (IP receiver/Sur-Gard service): 128-bit AES Tyco Fibro Protocol, encryption/authentication key provided by central station on an account-by-account basis.
- CS+, IP receiver service and NTP are outgoing communication services only initiated by the EVOLVE system.
- ECPxml communications are incoming using a passphrase for authentication within a TLS session. ECP is hashed by port and requires a passphrase of up to 40 unicode characters and a hashed license key. CS+ uses the EVOLVE-CU license and a certificate to authenticate with the panel.
- Messages and data adhere to and are validated for conformance to the XML schema.
- EVOLVE-SNP incoming service requests can be turned off at startup, by time of day or via programming, with only outgoing requests allowed. This firewall policy allows the system to continue sending critical events to services like central monitoring stations.
- Session timeouts are enforced.
- Brute force access shuts down after five unsuccessful authentication tries, or in the case of flood attacks, and provides a monitor point indication.

Access and authentication

Access to EVOLVE is based on industry-standard, best practices. First a physical barrier, the locked door, provides a barrier to the system. Kidde Commercial advises that customers should have a tamper switch installed in all Fire Alarm Control Panels (FACP). When the cabinet door is opened, a trouble should be signaled. If an unscheduled trouble from door entry is enumerated, the door entry open trouble should be investigated by a person qualified to determine if the cabinet is being accessed by a technician who:

- has need to access
- is qualified to access

- has been authorized to access

As a security best practice, the facility security officer should also place a serialized frangible seal on the door to indicate if the cabinet has been accessed. The breaking of the seal, and/or opening of the cabinet and who accessed the cabinet should also be recorded in a logbook. When access to the cabinet is complete for the day's maintenance window, a replacement serialized seal should be attached to show unauthorized entry and logged into the FSO's logbook.

To gain access to higher level system operations, a seven-digit PIN entry is required. All control panel access is role-based; a user can only perform actions explicitly allowed by system configuration and the permissions policy set in the system configuration. For example, a user with a high level of access can enable and disable devices, but a lower-level user cannot. In the event of failed password attempts at a user interface, EVOLVE can be programmed by the installer to initiate a response based on five failed login attempts, which triggers the Internal, Reset Required pseudo point (0682) and shows this message on the LCD user interface: CU Client has exceeded allowed failed login attempts. The response can initiate any action needed by the EVOLVE system, including off site notifications such as CS+ notification, central station notification and so on. EVOLVE does not lock the LCD user interface if the maximum number of log in attempts is exceeded, keeping the primary objective of life safety system in place, active, available, and unobstructed. To further enhance access security, a timeout is also put in place to force a user logout after a period of inactivity. All password attempts, successful or not, are logged to history for audit trail access.

When connecting the system configuration software, authentication of the EVOLVE-CU project encryption and hashing utilizes FIPS 140.2 infrastructure for AES256 and SHA256. The control panel meets FIPS 197 standard for encryption.

Salting increases the password hashing strength by adding a random value to the end of the input. This method extends the length of the original password to protect against rainbow table attacks and brute-force attacks. No passphrases, access codes, or PINs are stored in any database as plain text. All are in a one-way SHA256 hash. All access to the control panel is logged to history including the user information. No password is exposed in any EVOLVE database or report as plain text. The EVOLVE-CU enforces lockout after five attempts to access a project. Two-factor authentication is needed for configuration access to the control panel:

- A project passphrase that is up to 40 Unicode characters combined with a licensed PC
- A six-digit session access code that is randomly generated by the control panel

As an additional security best practice, the computer running the CU needs to be secure. In order to not compromise the security of the control panel and the CU, hardening of the operating systems running the CU must be used. To accomplish this hardening process, an industrially recognized standardized security framework should be employed, not limited to:

- A robust anti-virus installed
- Operating system and application security patches applied to protect the system
- Inbound and outbound firewall rules that permit only required ports to enter and leave
- Applications and users running with least privileges
- Only authorized users may access the CU
- The operating system checks to verify programs installed on the operating system are signed
- Disable unused services and users
- Utilize secure boot
- Enable Data Execution Prevention (DEP)

Common industry-accepted standards that include specific weakness-correcting guidelines are published by the following organizations:

- Center for Internet Security (CIS)
- International Organization for Standardization (ISO)

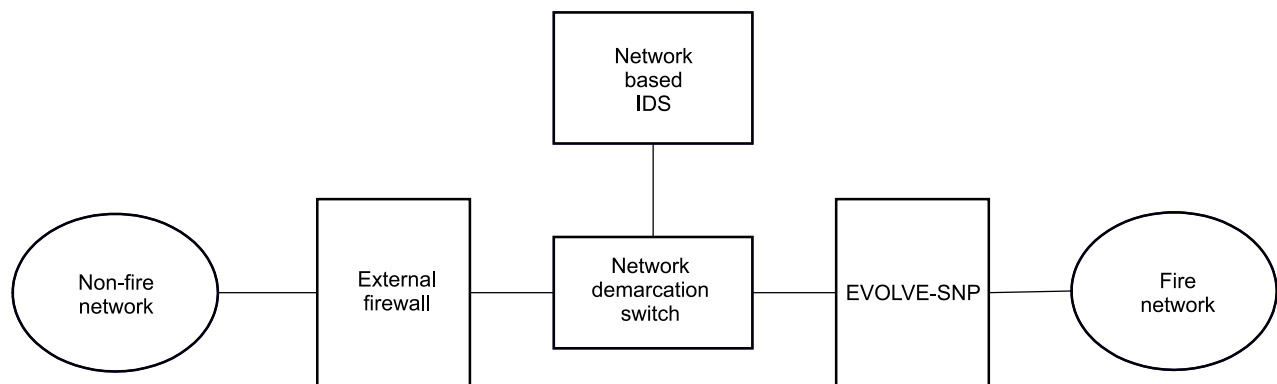
- SysAdmin, Audit, Network, and Security (SANS) Institute
- National Institute of Standards and Technology (NIST) and Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGS)

External network firewall

As a best practice, to protect the fire network and the fire control panel's attack surface at the point of demarcation when the EVOLVE firewall is connected to an external network, the building network (external to the fire system network) provider should provide their own Industrial Grade Stateful Packet Inspection firewall and a network based intrusion detection device (IDS) which supplies unexpected traffic back to a Security Operations Center's (SOC's) Security Incident and Event Management (SIEM). The demarcation configurable smart Ethernet switch needs to have its intrusion detection port placed in listen all mode.

A conceptual configuration example is shown in Figure 3 below.

Figure 3: External network firewall example



Appendix A

Network application examples

Summary

Some examples of network topologies supported by the EVOLVE network are presented in this section.

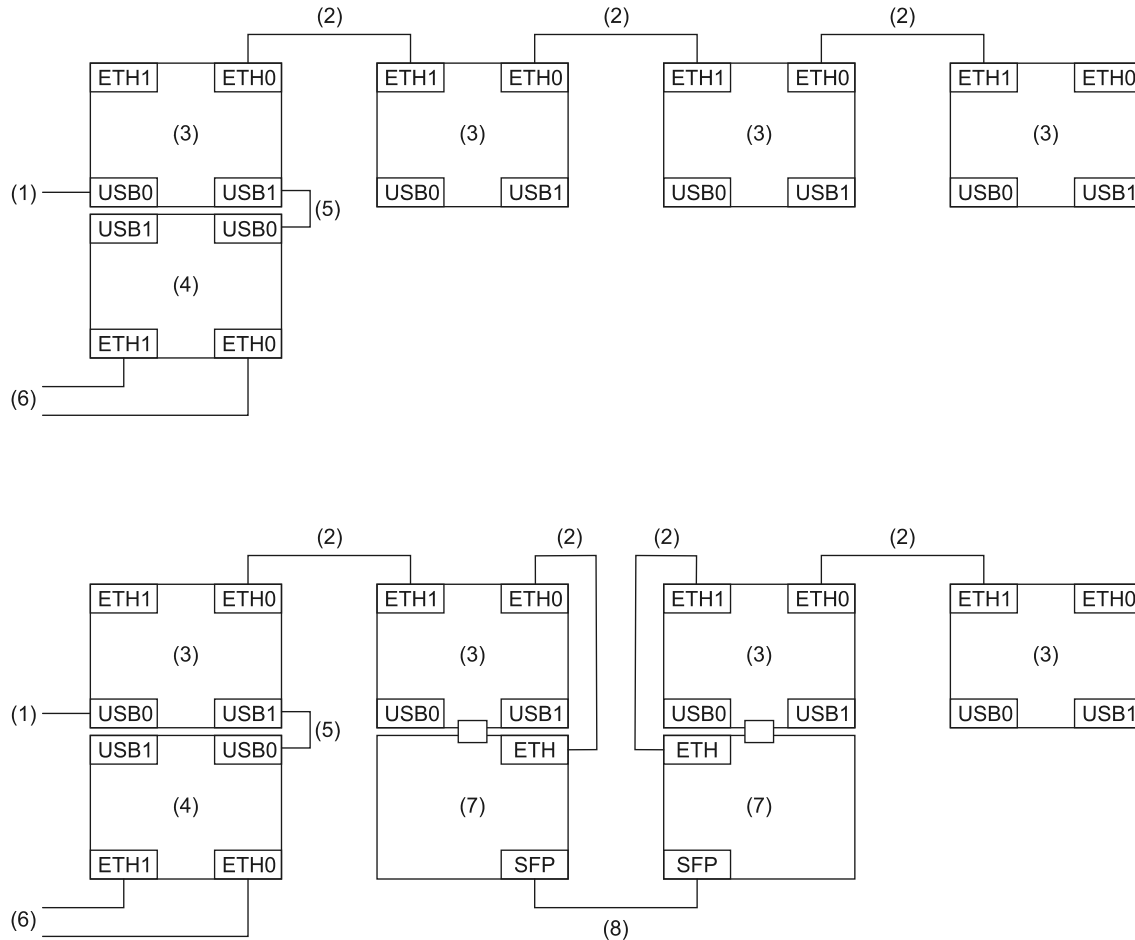
Content

Network application examples 22

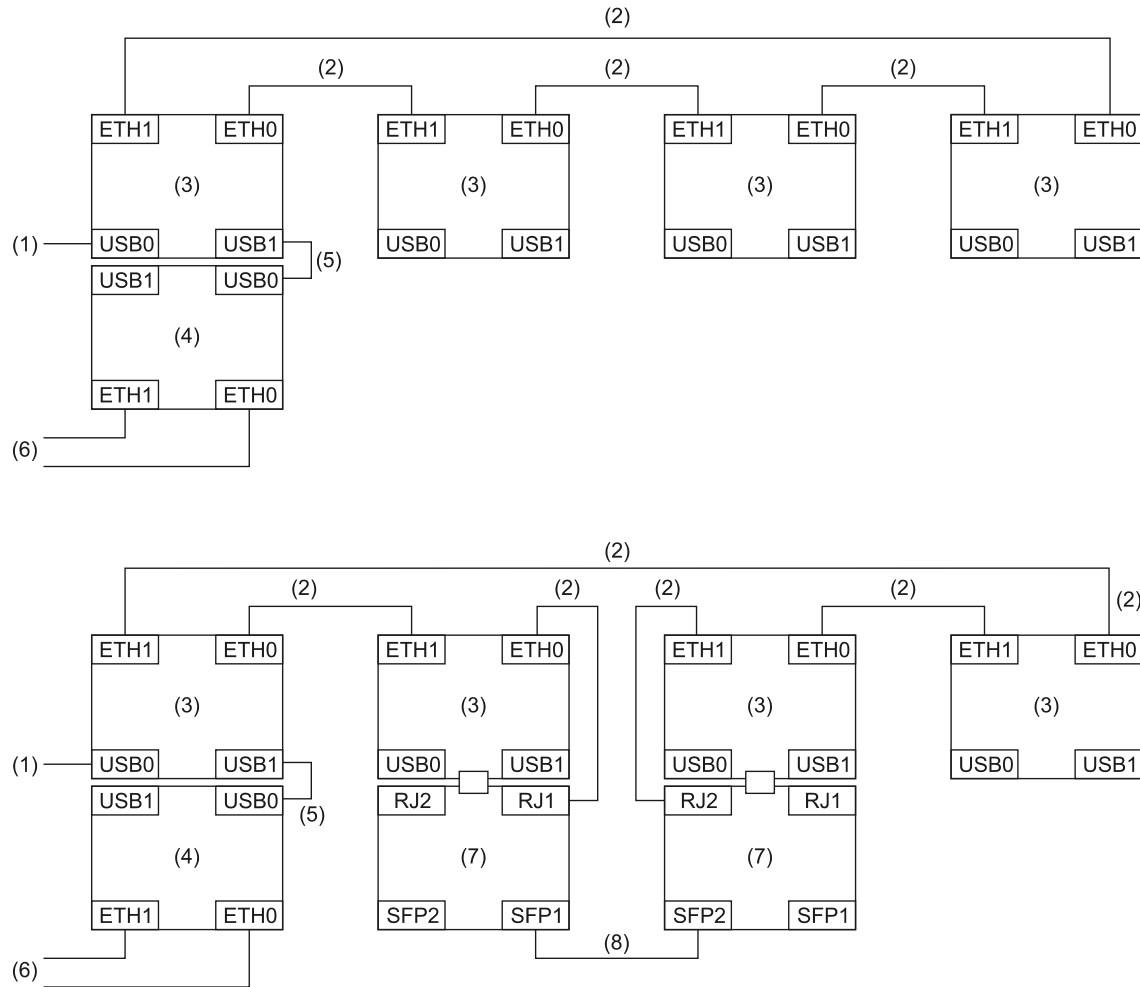
Network application examples

Network connection from node to node is accomplished using small form-factor pluggable (SFP) modules.

Figure 4: Typical linear daisy chain (Class B) network wiring

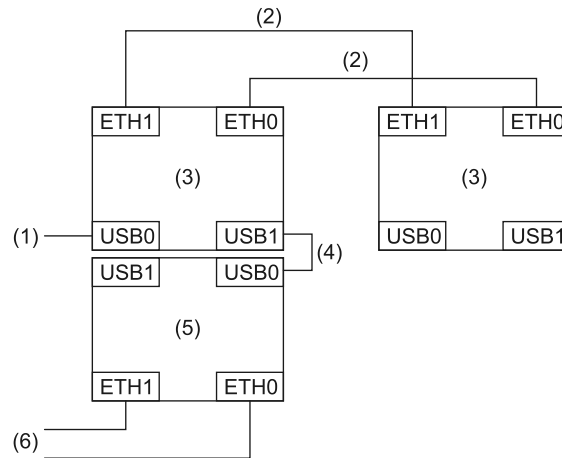


- (1) EVOLVE-CU computer USB-C cable
- (2) RJ-45 Ethernet cable, CAT 5e or better
- (3) Fire panel CPU board
- (4) EVOLVE-SNP module
- (5) USB-C cable
- (6) RJ-45 Ethernet cable, CAT 5e or better to external equipment
- (7) EVOLVE-MEDIA1 module
- (8) Fiber-optic or unshielded twisted-pair cable and compatible SFP module

Figure 5: Typical ring (Class A/Class X) network wiring

- (1) EVOLVE-CU computer USB-C cable
- (2) RJ-45 Ethernet cable, CAT 5e or better
- (3) Fire panel CPU board
- (4) EVOLVE-SNP module
- (5) USB-C cable
- (6) RJ-45 Ethernet cable, CAT 5e or better to external equipment
- (7) EVOLVE-MEDIA2 module
- (8) Fiber-optic or unshielded twisted-pair cable and compatible SFP module

Figure 6: Typical Class A two nodes



- (1) EVOLVE-CU computer USB-C cable
- (2) RJ-45 Ethernet cable, CAT 5e or better
- (3) Fire panel CPU board
- (4) USB-C cable
- (5) EVOLVE-SNP module
- (6) RJ-45 Ethernet cable, CAT 5e or better to external equipment