

SIEMENS

INSTALLATION INSTRUCTIONS

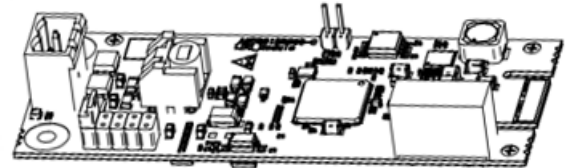
Model LDC Long Distance Copper Module

The Model LDC is an interface card which provides an interconnecting copper wire link for networked systems. The Operating Temperature Range and Humidity is 0 to 49 C, and 93% @ 32 C.

FEATURES

The principal features of the LDC card include:

- Easy insertion into the host card or assembly
- Automatic identification by the system at power up
- Protection of the external signal path from overvoltage caused by electrostatic discharge (ESD) or electrical fast transients (EFT)
- Line supervision for open and short circuits for Class B (DCLB) or Class X (DCLC) wiring
- Ground fault detection at 5k ohms or less
- Galvanically isolated communications link to prevent ground loops



LDC Long Distance Copper Module

NOTE: A very low ohmic ground fault may trigger the reporting of both ground fault and line fault conditions.

PRE-INSTALLATION

1. Determine from the site-specific shop drawings whether the LDC should be set for either supervising the link (Ring-OUT) or terminating the link (Ring-IN). Ground fault supervision must be enabled for the link supervising module (Ring-OUT).
2. For link supervising module, set the jumpers as illustrated in Figure 1. For link terminating module without ground fault detection, set the jumpers as illustrated in Figure 2.

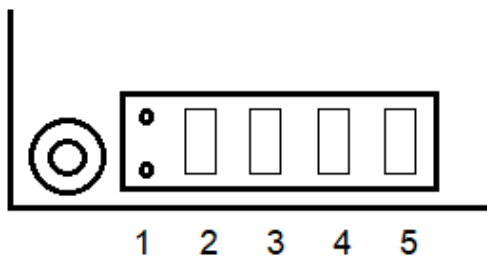


Figure 1
Link Supervising Module (Ring-OUT configuration)

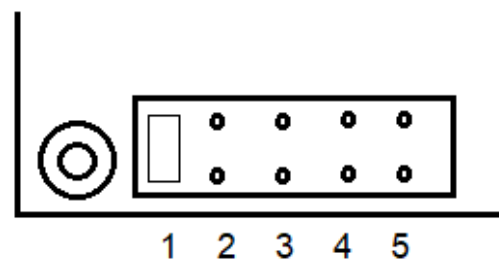


Figure 2
Link Terminating Module (Ring-IN configuration) without Ground Fault Supervision

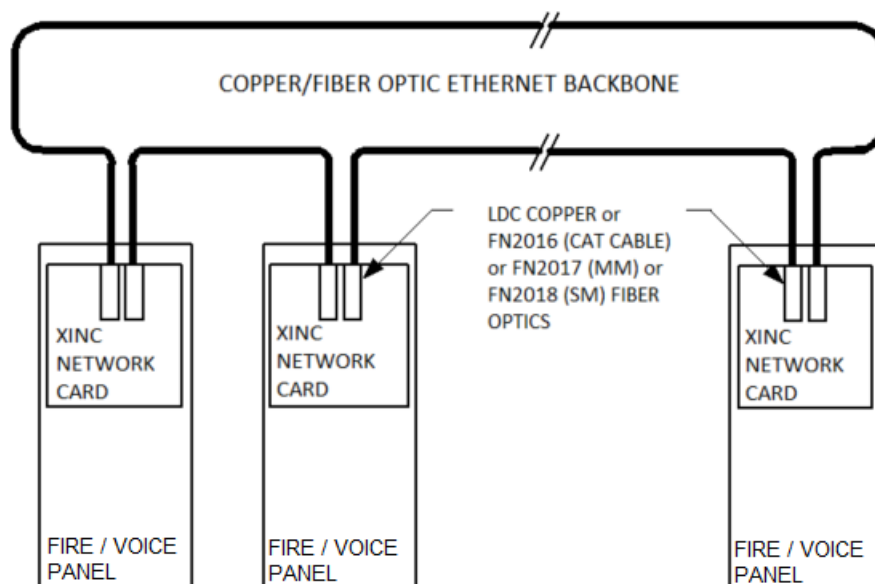
NOTICE: Install in accordance with National Electrical Code, ANSI/ NFPA 70, the Standard for Installation and Classification of Burglar and Holdup Alarm Systems, UL 681, and the Standard for Central-Station Alarm Services, UL 827, as applicable.

OPERATION

The LDC Module can be used in ring networks in a Desigo Fire Safety Modular / Cerberus PRO Modular System Panel.

Operation in a Ring Network in Desigo Fire Safety Modular / Cerberus PRO Modular System Panel

The LDC Module is a card that plugs into the XINC card to provide an electrical interface for an Ethernet backbone network (see Figure 3). Each link in the backbone is independent of any other link. Each segment can be implemented as either copper wire, Ethernet CAT5 or single-mode (SM) or multi-mode (MM) fiber-optic cable without any regard to what is used for the other segments in the backbone network.



*Figure 3
Ethernet backbone network of a Desigo Fire Safety Modular / Cerberus PRO Modular System Panel*

Controls and Indicators

The LDC Module contains a single LED located at the copper cable connector. The following table describes the various color outputs and their functions.

COLOR	DESCRIPTION
No Color	No power/ No link is established
Green	Link is established; No active communication with link partner
Yellow	Blinking yellow indicates communication with a link partner; data sharing
Red	Momentary red indicates a search for link partner

MOUNTING

Mounting the LDC Module in a Desigo Fire Safety Modular / Cerberus PRO Modular system

CAUTION: Power down the Desigo Fire Safety Modular / Cerberus PRO Modular System Panel before mounting the LDC and its associated XINC card.

1. Place the XINC card on a flat work surface with the DIN connectors facing towards you.
2. Insert the LDC into either Ring slot on the right side of the XINC card.
3. Secure the LDC module with the included screws to the XINC card.

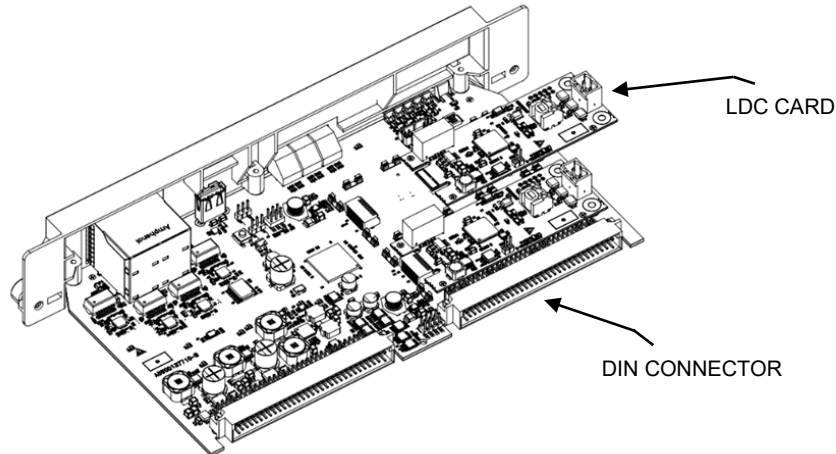


Figure 4
LDC partially inserted into XINC card

4. Configure the supervision jumpers according the previous Pre-Installation section in this document.
5. Refer to the site specific shop drawing (Figure 5) to determine which slot position on the card cage the XINC card is to be installed in. Tighten the captive bezel retaining screws on the XINC card bezel at the top and bottom mating surfaces so that the XINC card is securely held in place in the Card Cage. Install the XINC card into the card cage slot according to instructions provided in Siemens Industry, Inc., Building Technologies Division Document number A6V12412368 *Installation Instructions for the Model XINC Card*.

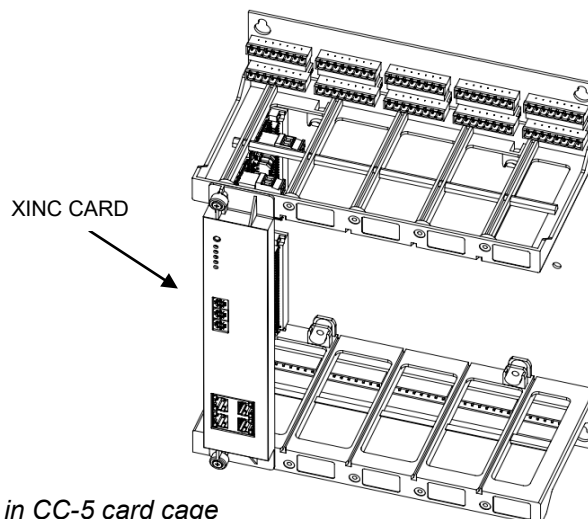


Figure 5
LDC/XINC installed in CC-5 card cage

NOTICE: If it becomes necessary to uninstall the XINC Card, first remove the copper wiring connection terminal from the LDC Module from the top card cage slot guide. Refer to Figure 6. If alternate technology modules are used, refer to respective module installation instructions for disconnection method.

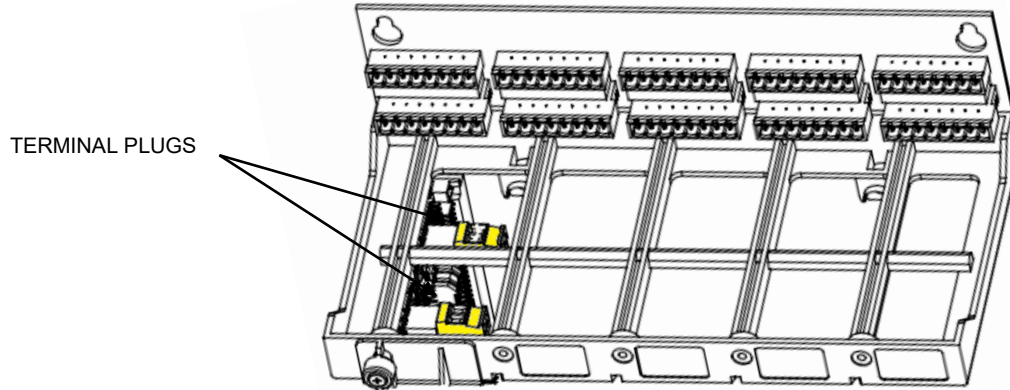


Figure 6
Top of CC-5 card cage slot

WIRING

There are no wiring operations for installing the LDC Module onto the XINC Card. When using the LDC Module to connect Designo Fire Safety Modular / Cerberus PRO Modular System panels, consult the table below on cabling the panels together to establish Ethernet rings. A single multi-conductor cable is used to connect from one module to the next in the ring.

Cable	Maximum Wire Length	Maximum Impedence (Capacitance)
Unshielded 18AWG FPLR	2500 feet	15 ohms (75 nF)
Shielded 18AWG FPLR	1500 feet	9 ohms (128 nF)
Unshielded 14AWG FPLR	2500 feet	10 ohms (75 nF)
Shielded 14AWG FPLR	1500 feet	6 ohms (135 nF)
12AWG THHN (single conductor)	5000 feet	12 ohms (85 nF)
Twisted 14AWG THHN	2500 feet	6 ohms (125 nF)
CAT 5 (single pair)	3000 feet	188 ohms (39 nF)

ELECTRICAL RATINGS

The following table lists the power requirements for the LDC Module:

Input Power (Power derived from Power Supply via XINC Card)	
24V Screw Terminal Current	120 mA
24V Back Plane Current	0 mA
6.2V Back Plane Current	0 mA
Standby Current	120 mA

Cyber security disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept. You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit <https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html>

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under <https://www.siemens.com/cert/en/cert-security-advisories.htm>.