SIEMENS

INSTALLATION INSTRUCTIONS
Model FN2016-U1

FN2016-U1 Ethernet Module (10/100 BaseTx)

The optional Model FN2016-U1 Ethernet Module (10/100 BaseTx) is a media adapter which provides interconnecting copper wire links for networked systems.

NOTE: The Operating Temperature Range and Humidity is 0 to 49 C, and 93% @ 32 C. Install in accordance with the 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

FEATURES

The principal features of the FN2016-U1(10/100 BaseTx) include:

- Easily plugged into the host card.
- Automatically identified by the system at power up.
- Protects the Ethernet signal path from over-voltage caused by electrostatic discharge (ESD), electrical fast transients (EFT) and surge events.
- Provides ground fault detection at 10k ohms or less.
- Can be configured as Class B (DCLB) or Class X (DCLC) wiring.
- Field wiring is Power Limited

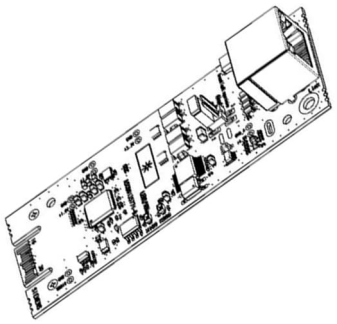

Figure 1 FN2016-U1 Ethernet Module

PRE-INSTALLATION

1. The FN2016-U1 must be installed in pairs. For each pair, one, and only one, FN2016-U1 must be configured to provide ground fault detection.

2. A jumper block is used to enable or disable ground fault detection on the FN2016-U1. Determine which FN2016-U1 in the pair will provide ground fault detection and place its jumper in the enabled position. Ensure that the other FN2016-U1 in the pair has its jumper in the disabled position. Refer to Figure 2.

Note: *When the FN2016-U1 detects a ground fault yellow LED H201 will illuminate.*

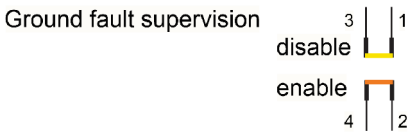

Figure 2 Ground fault detection jumper settings

Siemens Industry, Inc.
Smart Infrastructure

OPERATION

The FN2016-U1 can be used in both the Desigo CC Modular and the Cerberus Pro Modular systems and is compatible with the XINC Network Ring Card. The XINC provides two sockets for media adapters such as the FN2016-U1 and the FN2016-U1 can be installed into either socket. Mixing of media adapters, such as the FN2017-U1 and FN2018-U1 fiber optic media adapters, on the XINC is allowed depending on the requirements of a specific installation. Refer to XINC Installation Instructions, Document ID A6V12412368 for details regarding network configuration, media adapter installation and wiring instructions.

CONTROLS AND INDICATORS

The two LEDs on the FN2016-U1 which are located at the copper cable connector indicate the following:

Color	Function
Green	Link established
Yellow	Transmit or receive activity

WIRING

Cat 5/5e (shielded or unshielded) cable, 100 Meters max.

ELECTRICAL RATING

Electrical Ratings	
14 mA (max)	@ 24VDC (@10 Mbps)
16 mA (max)	@ 24VDC (@100 Mbps)
Ground Fault Detection Threshold:	10K ohms

* Use this QR code to access the XINC Installation and wiring diagrams.

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-cybersecu-rity.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.

Siemens Industry, Inc.
Smart Infrastructure
2 Gatehall Drive
Parsippany, NJ 07054

Doc ID A6V13300924_en--b