

SIEMENS

Installation Instructions Model FN2017-U1, FN2018-U1

FN2017-U1 Ethernet Module (Multi Mode Fiber Optic)
FN2018-U1 Ethernet Module (Single Mode Fiber Optic)

The optional models FN2017-U1 Ethernet Module (MM) and FN2018-U1 (SM) are media adapters which provides interconnecting fiber optic 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, as applicable.

FEATURES

The principal features of the FN2017-U1 (MM) and FN2018-U1(SM) include:

- Easily plugged into the host card

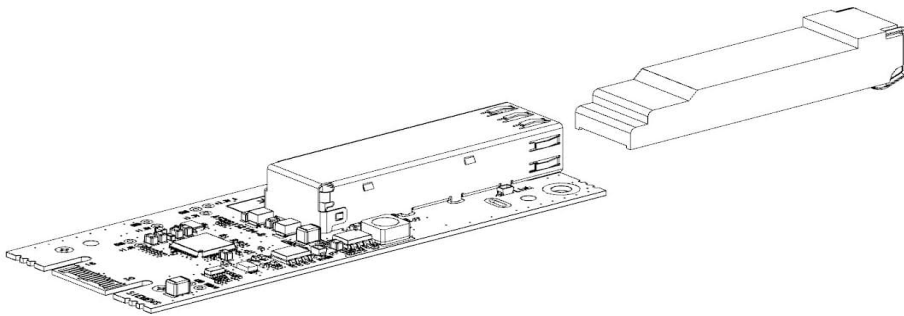


Figure 1. FN2017-U1/FN2018-U1 Ethernet Module with removable fiber media adapter

PRE-INSTALLATION

The fiber optic media adapters, either single-mode or multi-mode, come pre-installed into the FN2017-U1 and FN2018-U1. There are no configuration switches or jumpers on the FN2017-U1 or FN2018-U1.

OPERATION

The FN2017-U1 and FN2018-U1 can be used in both the Desigo CC Modular and the Cerberus Pro Modular systems and are compatible with the XINC Network Ring Card. The XINC provides two sockets for media adapters such as the FN2017-U1 and FN2018-U1 and they can be installed into either socket. Mixing of media adapters, such as the FN2016-U1, FN2017-U1, and FN2018-U1 media adapters on the XINC is allowed depending on the requirements of a specific installation. While the mixing of media adapter types on a given XINC is allowed they must be matched at each end of the connection between XINCs. Refer to *XINC Installation Instructions*, Document ID A6V12412368* for details regarding network configuration, media adapter installation and wiring instructions.

WIRING

The fiber optic cables use dual Mini LC type connectors.

ELECTRICAL RATING

Electrical Ratings	
FN2017-U1	49mA (max) @ 24VDC (100Mbps)
FN2018-U1	40mA (max) @ 24VDC (100Mbps)

OUTPUT SIGNAL ATTENUATION

As a signal travels down an optical fiber, its level is reduced due to absorption by the fiber. This sets the maximum length of an optical connection. The actual length is determined by the transmitter output level, the length of the fiber, and the receiver sensitivity. The maximum length is reached when the fiber attenuation is the same as the difference between the transmitter output and the receiver sensitivity less 3 dBm for an error margin. These values are different depending upon the module type used and the kind of optical fiber which is used to connect the modules.

The following table gives the maximum allowable signal attenuation for the different kinds of fiber used with each type of module. It also gives the maximum length of an optical link using that combination of module and fiber and are indicative only. Signal attenuation due to fiber loss, termination quality and splices determines maximum link length.

Ethernet Module Output Signal Maximum Attenuation and Link Length			
Module Type	Fiber Type	Signal Attenuation	Link Length
FN2017-U1 (MM)	50/125 μ m	7.5 dB	2.0 km
	62.5/125 μ m	11 dB	2.0 km
FN2018-U1 (SM)	9/125 μ m	30 dB	40 km

*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-cybersecurity.html](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>.