SIEMENS

Data sheet   **6GK1901-0DM20-2AA5**

product type designation	**IE M12 Panel Feedthrough**
product description	Control cabinet feedthrough M12 (D-coded) / RJ45
	IE M12 panel feedthrough control cabinet bushing to transition from M12 connection (D-coded)- connection method (IP65) on RJ45 connection technology (IP20) 1 pack=5 units.

suitability for use	Control cabinet feedthrough for transition from M12 connection type (D-coded), IP65/67 to RJ45 connection type (IP20)

transfer rate	
transfer rate / for Industrial Ethernet	10 Mbit/s, 100 Mbit/s

interfaces	
number of electrical connections	
● for network components or terminal equipment	2
type of electrical connection	
● for network components or terminal equipment	M12 socket (D-coded) and RJ45
type of electrical connection / FastConnect	No

mechanical data	
material / of the enclosure	plastic
locking mechanism design	Screwed joint
tightening torque / for M12 round connector / maximum	0.6 N·m
connector coding / of the M12 circular connector	D

design, dimensions and weights	
type of cable outlet	90° cable outlet
width	24 mm
height	45 mm
depth	35.4 mm
net weight	40 g

ambient conditions	
ambient temperature	
● during operation	0 ... 70 °C
● during storage	0 ... 70 °C
● during transport	0 ... 70 °C
protection class IP	IP65/67 (M12), IP20 (RJ45)

product features, product functions, product components / general	
product feature	
● PoE capability	Yes
● PoE+capability	Yes
● silicon-free	Yes
product component	
● strain relief	Yes

standards, specifications, approvals	
certificate of suitability	
● RoHS conformity	Yes
● UL approval	Yes

2/22/2024

● railway application in accordance with EN 50155	No
standard for structured cabling	Cat5
further information / internet links	
internet link	
● to website: Image database	https://www.automation.siemens.com/bilddb
● to website: Industry Online Support	https://support.industry.siemens.com
security information	
security information	Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. 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 industrial security concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components 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. For additional information on industrial security measures that may be implemented, please visit https://www.siemens.com/industrialsecurity. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under https://www.siemens.com/cert. (V4.6)

last modified: 2/15/2024 ⬈

2/22/2024