

### product type designation



### ASM 475 communication module

MOBY communications module ASM475 for SIMATIC S7 300 and ET200M parameterizable (without front connector).

### suitability for operation

SIMATIC S7-300, ET200M together with RF200/300, MV400/500, MOBY D/E/I/U

### transfer rate

transfer rate / at the point-to-point connection / serial / maximum	115.2 kbit/s
---------------------------------------------------------------------	--------------

### interfaces

design of the interface / for point-to-point connection	RS422
number of readers / connectable	2
type of electrical connection	
• of the backplane bus	S7-300 backplane bus
• of the PROFIBUS interface	(according to the head module)
• of Industrial Ethernet interface	(according to the head module)
• for supply voltage	Screw-type or spring-loaded terminals
design of the interface / to the reader / for communication	Screw-type or spring-loaded terminals

### mechanical data

material	Noryl
color	anthracite

### supply voltage, current consumption, power loss

supply voltage / at DC	
• rated value	24 V
•	20 ... 30 V
consumed current	
• at DC / at 24 V / without connected devices / typical	0.1 A
• from supply voltage 1L+ / maximum	1 A

### ambient conditions

ambient temperature	
• during operation	0 ... 60 °C
• during storage	-40 ... +70 °C
• during transport	-40 ... +70 °C
protection class IP	IP20
shock resistance	According to IEC 61131-2
shock acceleration	150 m/s²
vibrational acceleration	10 m/s²

### design, dimensions and weights

width	40 mm
height	125 mm
depth	120 mm
net weight	0.2 kg
fastening method	S7-300 rack
wire length / for RS 422 interface / maximum	1000 m

product features, product functions, product components / general	
display version	4 LEDs per reader connection, 2 LEDs for device status
product function / addressable transponder file handler	Yes
protocol / is supported	
• S7 communication	Yes
product functions / management, configuration, engineering	
type of parameterization	Object manager, GSD
type of programming	FB 45, FB 55, FC 56 (FC 45/55 with limited functionality)
type of computer-switched communication	acyclic communication
standards, specifications, approvals	
certificate of suitability	CE, FCC, UL/CSA
reference code	
• according to IEC 81346-2:2019	KEC
product function / is supported / identification link	No
standards, specifications, approvals / Environmental Product Declaration	
Environmental Product Declaration	Yes
Global Warming Potential [CO2 eq]	
• total	101.43 kg
• during manufacturing	16 kg
• during operation	85.3 kg
• after end of life	0.13 kg
accessories	
accessories	Front connector with screw-type or spring-loaded terminals
further information / internet links	
internet link	
• to website: Selection guide for cables and connectors	<a href="https://support.industry.siemens.com/cs/ww/en/view/109766358">https://support.industry.siemens.com/cs/ww/en/view/109766358</a>
• to web page: selection aid TIA Selection Tool	<a href="https://www.siemens.com/tstcloud">https://www.siemens.com/tstcloud</a>
• to web page: identification and localization systems	<a href="https://www.siemens.com/ident">https://www.siemens.com/ident</a>
• to web page: SiePortal	<a href="https://sieportal.siemens.com/">https://sieportal.siemens.com/</a>
• to website: Image database	<a href="https://www.automation.siemens.com/bilddb">https://www.automation.siemens.com/bilddb</a>
• to website: CAX-Download-Manager	<a href="https://www.siemens.com/cax">https://www.siemens.com/cax</a>
• to website: Industry Online Support	<a href="https://support.industry.siemens.com">https://support.industry.siemens.com</a>
security information	
security information	Siemens provides products and solutions with industrial cybersecurity 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 cybersecurity 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 cybersecurity measures that may be implemented, please visit <a href="https://www.siemens.com/cybersecurity-industry">www.siemens.com/cybersecurity-industry</a> . 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 Cybersecurity RSS Feed under <a href="https://www.siemens.com/cert">https://www.siemens.com/cert</a> . (V4.7)
Approvals / Certificates	
General Product Approval	

[Declaration of Con-  
formity](#)



[Miscellaneous](#)

General Product Ap- proval	EMV	Environment
-------------------------------	-----	-------------



[KC](#)

[Confirmation](#)



---

last modified:

11/22/2024 