

height	125 mm
depth	120 mm
net weight	0.22 kg
fastening method	Yes
• S7-300 rail mounting	
performance data / open communication	
number of possible connections / for open communication / by means of SEND/RECEIVE blocks / maximum	8
data volume	
• as user data per ISO on TCP connection / for open communication / by means of SEND/RECEIVE blocks / maximum	8 Kibyte
• as user data per TCP connection / for open communication / by means of SEND/RECEIVE blocks / maximum	8 Kibyte
• as user data per UDP connection / for open IE communication / by means of SEND/RECEIVE blocks / maximum	2 Kibyte
number of Multicast stations	8
performance data / S7 communication	
number of possible connections / for S7 communication	
• maximum	4
service	Yes
• of SIMATIC communication / as server	
performance data / multi-protocol mode	
number of active connections / with multi-protocol mode	12
performance data / PROFINET communication / as PN IO controller	
product function / PROFINET IO controller	No
performance data / PROFINET communication / as PN IO device	
product function / PROFINET IO device	Yes
data volume	
• as user data for input variables / as PROFINET IO device / maximum	512 byte
• as user data for output variables / as PROFINET IO device / maximum	512 byte
• as user data for input variables / for each sub-module as PROFINET IO device	240 byte
• as user data for output variables / for each sub-module as PROFINET IO device	240 byte
• as user data for the consistency area for each sub-module	240 byte
number of submodules / per PROFINET IO-Device	32
performance data / telecontrol	
protocol / is supported	Yes
• TCP/IP	
product functions / management, configuration, engineering	
product function / MIB support	Yes
protocol / is supported	
• SNMP v1	Yes
• DCP	Yes
• LLDP	Yes
configuration software	
• required	STEP 7 V5.4 or higher / STEP 7 Professional V11 (TIA Portal) or higher
identification & maintenance function	
• I&M0 - device-specific information	Yes
• I&M1 - higher level designation/location designation	Yes
product functions / diagnostics	
product function / web-based diagnostics	Yes
product functions / switch	
product feature / switch	Yes
product function	
• switch-managed	No
• with IRT / PROFINET IO switch	No
• configuration with STEP 7	Yes

product functions / redundancy

product function	
• ring redundancy	Yes
• redundancy manager	No
protocol / is supported / Media Redundancy Protocol (MRP)	Yes

product functions / security

product function	
• password protection for Web applications	No
• ACL - IP-based	Yes
• ACL - IP-based for PLC/routing	No
• switch-off of non-required services	Yes
• blocking of communication via physical ports	Yes
• log file for unauthorized access	No

product functions / time

product function / SICLOCK support	Yes
product function / pass on time synchronization	Yes
protocol / is supported	
• NTP	Yes

standards, specifications, approvals

reference code	
• according to IEC 81346-2:2019	KEC

further information / internet links

internet link	
• to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
• to website: Industrial communication	https://www.siemens.com/simatic-net
• to web page: SiePortal	https://sieportal.siemens.com/
• to website: Image database	https://www.automation.siemens.com/bilddb
• to website: CAx-Download-Manager	https://www.siemens.com/cax
• to website: Industry Online Support	https://support.industry.siemens.com

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 www.siemens.com/cybersecurity-industry . 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 https://www.siemens.com/cert . (V4.7)
----------------------	--

Approvals / Certificates

General Product Approval



[Declaration of Conformity](#)



EMV For use in hazardous locations

[KC](#)



[FM](#)

[CCC-Ex](#)



Marine / Shipping other Environment



[Confirmation](#)

[Confirmation](#)

last modified:

8/22/2024 