SIEMENS

Data sheet 6GK8553-0BB00-1DA1

product brand name	SCALANCE
interfaces	
number of electrical/optical connections / for network components or terminal equipment / maximum	1; SFP+
number of electrical connections / for external antenna(s)	4; 4x4 MIMO, N-type antenna connectors for external connections
type of electrical connection / for external antenna(s)	N socket, N bulkhead jack
number of interfaces / according to USB	1; debug interface USB (Type C)
type of electrical connection / at the digital inputs/outputs	M12 (4-pole, L-coded)
WAN connection	
type of wireless network / is supported / 5G private networks	Yes
frequency band / is supported / 5G Standalone (SA)	n78
wireless & modem	
operating frequency	3 600 ... 3 800 MHz
operating mode / time-division duplexing (TDD)	Yes
size of channel bandwidths	40/80/100 MHz
transmit power / maximum	0.25 W; 24 dBm per channel and antenna port (with DPD enabled), PII > 18%
type of modulation	QPSK/16QAM/64QAM/256QAM
supply voltage, current consumption, power loss	
supply voltage / rated value	
•	24 V
•	16.8 ... 31.2 V
type of voltage / of the supply voltage	DC
consumed current	
• at rated supply voltage / maximum	1.5 A
power loss [W] / typical	36.2 W
supply voltage / 1 / from M12 power Connector (L-coded) for redundant voltage supply	24 V
ambient conditions	
ambient temperature	
• during operation	-30 ... +60 °C
• during storage	-40 ... +70 °C
• during transport	-70 ... +90 °C
relative humidity / at 25 °C / during operation / maximum	95 %
protection class IP	IP65
design, dimensions and weights	
design	compact
width	258 mm
height	53 mm
depth	258 mm
net weight	3 382 g
material / of the enclosure	aluminum
fastening method	ceiling, mast and wall mounting; 4 M5 screws on the back for VESA, 4 mounting devices with d=5.5 mm for wall or ceiling installation
standards, specifications, approvals	
standard	
• for EMC	frame standards: ETSI EN 301 489-1 V2.2.3 and basic standards: EN 55011:2016 + A1:2017 + A2: 2021 + A11:2020 CISPR 11:2019 (CISPR 11 (2015-06) + AMD 1 (2016-06) + AMD 2 (2019-01))
• for emitted interference	basic standards: EN 55032:2015 + A1: 2020 + A11: 2020 CISPR 32 EDITION 2.1: 2019, EN IEC 61000-6-3: 2021, EN IEC 61000-6-4: 2018
• for interference immunity	basic standards: EN 55035:2017 + A11: 2020 CISPR 35:2016, EN IEC 61000-6-1: 2019, EN IEC 61000-6-2: 2019 (burst: 5 kHz and 100 kHz)
certificate of suitability	EN IEC 61000-6-2: 2019 (burst: 5 kHz and 100 kHz)

product conformity	
● according to IEEE 1588 v2-Precision Time Protocol	Yes
● SyncE	Yes
MTBF / at 40 °C	25 a

further information / internet links

internet link	
● to website: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
● to web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
● to website: Mobile radio national approval	https://www.siemens.com/mobile-approvals
● 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

CE
EG-Konf.

last modified: 4/9/2025