# **SIEMENS**

### **Data sheet**

## 6GK5734-1FX00-0AA0

### product type designation



## W734-1 RJ45

IWLAN client, SCALANCE W734-1, RJ45, 1 radio, 2 R-SMA antenna port, iFeatures Support via KEY-PLUG, IEEE 802.11a/b/g/h/n, 2.4/5GHz, gross data rate 300 Mbit/s, 2x RJ45 max. 100 Mbit/s, PoE integrated 2-port switch, redundant 24 V DC, joint block, IP30, -20... 60 °C, plug slot WPA2/802.11i/e, observe national approvals! CERT ID: MSN-W1-RJ-E2, scope of delivery: Manuals on CD-ROM, German/English, 1x joint block; for operation outside of USA/Israel .

transfer rate			
transfer rate			
<ul> <li>with WLAN / maximum</li> </ul>	300 Mbit/s		
for Industrial Ethernet	10, 100 Mbit/s		
transfer rate / for Industrial Ethernet			
• minimum	10 Mbit/s		
• maximum	100 Mbit/s		
interfaces			
number of electrical connections			
<ul> <li>for network components or terminal equipment</li> </ul>	2		
<ul><li>for power supply</li></ul>	1		
<ul> <li>for redundant voltage supply</li> </ul>	1		
type of electrical connection			
<ul> <li>for network components or terminal equipment</li> </ul>	RJ45 socket		
<ul><li>for power supply</li></ul>	4-pole screw terminal, PoE		
memory			
design of the removable storage			
• C-PLUG	Yes		
• KEY-PLUG	Yes		
interfaces / wireless			
number of radio cards / permanently installed	1		
transmission mode / for multiple input multiple output (MIMO)	2x2		
number of spatial streams	2		
number of electrical connections / for external antenna(s)	2		
type of electrical connection / for external antenna(s)	R-SMA (socket)		
product feature / external antenna can be mounted directly on device	Yes		
supply voltage, current consumption, power loss			
type of voltage / of the supply voltage	DC		
supply voltage			
<ul> <li>from Power-over-Ethernet according to IEEE802.3at for type 1 and IEEE802.3af</li> </ul>	48 V		
consumed current			
at DC / at 24 V / typical	0.25 A		
<ul> <li>with Power-over-Ethernet according to IEEE802.3at for type 1 and IEEE802.3af / typical</li> </ul>	0.125 A		
power loss [W]			
• at DC / at 24 V / typical	6 W		
<ul> <li>with Power-over-Ethernet according to IEEE802.3at for type 1 and IEEE802.3af / typical</li> </ul>	6 W		

supply voltage / 1			
from terminal block	19.2 V		
supply voltage / 2			
from terminal block	28.8 V		
ambient conditions			
ambient temperature			
during operation	-20 +60 °C		
during storage	-40 +85 °C		
during transport  Addition to wait the Vet ACE SO Coultboard and deposition Vetwering	-40 +85 °C		
relative humidity / at 25 °C / without condensation / during operation / maximum	95 %		
ambient condition / for operation	When used under hazardous conditions (Zone 2), the SCALANCE W774-1 RJ45 or W734-1 RJ45 product must be installed in an enclosure. To comply with EN 50021, this enclosure must meet the requirements of at least IP 54 in compliance with EN 60529.		
protection class IP	IP30		
design, dimensions and weights			
width	26 mm		
height	156 mm		
depth	127 mm		
width / of the enclosure / without antenna	26 mm		
height / of the enclosure / without antenna	147 mm		
depth / of the enclosure / without antenna	127 mm		
net weight	0.52 kg		
fastening method	wall mounting only if flat mounted		
S7-300 rail mounting	Yes		
S7-1500 rail mounting	Yes		
35 mm top hat DIN rail mounting	Yes		
wall mounting	Yes		
radio frequencies			
operating frequency			
for WLAN in 2.4 GHz frequency band	2.41 2.48 GHz; depending on the country approvals		
for WLAN in 5 GHz frequency band	4.9 5.8 GHz; depending on the country approvals		
product features, product functions, product components / gener			
product function / Access Point Mode	No		
product function / client Mode			
product function	Yes		
	Yes		
• iPCF client	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'		
<ul><li>iPCF client</li><li>iPCF-MC client</li></ul>	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG		
	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG		
• iPCF-MC client	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'		
iPCF-MC client  number of iPCF-capable radio modules	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP  product functions / management, configuration, engineering	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only		
iPCF-MC client  number of iPCF-capable radio modules product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client product function	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only		
iPCF-MC client  number of iPCF-capable radio modules product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client product function	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8 Yes		
iPCF-MC client  number of iPCF-capable radio modules product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client product function     CLI     web-based management	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8 Yes Yes		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client  product function      CLI     web-based management     MIB support	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes		
iPCF-MC client  number of iPCF-capable radio modules product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client product function     CLI     web-based management     MIB support     TRAPs via email     configuration with STEP 7	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client  product function      CLI     web-based management     MIB support     TRAPs via email	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes		
iPCF-MC client  number of iPCF-capable radio modules product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client product function	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes Yes		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP   product functions / management, configuration, engineering  number of manageable IP addresses / in client  product function      CLI     web-based management     MIB support     TRAPs via email     configuration with STEP 7     configuration with STEP 7 in the TIA Portal     WDS  protocol / is supported	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes Yes Yes		
number of iPCF-capable radio modules product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client product function  CLI  web-based management  MIB support  TRAPs via email  configuration with STEP 7  configuration with STEP 7 in the TIA Portal  WDS  protocol / is supported  Address Resolution Protocol (ARP)	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes Yes Yes No		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP   product functions / management, configuration, engineering number of manageable IP addresses / in client  product function      CLI     web-based management     MIB support     TRAPs via email     configuration with STEP 7     configuration with STEP 7 in the TIA Portal     WDS  protocol / is supported     Address Resolution Protocol (ARP)     ICMP	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP   product functions / management, configuration, engineering  number of manageable IP addresses / in client  product function      CLI     web-based management     MIB support     TRAPs via email     configuration with STEP 7     configuration with STEP 7 in the TIA Portal     WDS  protocol / is supported     Address Resolution Protocol (ARP)     ICMP     Telnet	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye		
number of iPCF-capable radio modules product function / iPRP  product functions / management, configuration, engineering number of manageable IP addresses / in client product function  CLI  web-based management  MIB support  TRAPs via email  configuration with STEP 7  configuration with STEP 7 in the TIA Portal  WDS  protocol / is supported  Address Resolution Protocol (ARP)  ICMP  Telnet  HTTP	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye		
iPCF-MC client  number of iPCF-capable radio modules  product function / iPRP   product functions / management, configuration, engineering  number of manageable IP addresses / in client  product function      CLI     web-based management     MIB support     TRAPs via email     configuration with STEP 7     configuration with STEP 7 in the TIA Portal     WDS  protocol / is supported     Address Resolution Protocol (ARP)     ICMP     Telnet	Yes; Only in combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' Yes; Only in combination with 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures'  1 Yes; In combination with the 'KEY-PLUG W780 iFeatures' or 'KEY-PLUG W740 iFeatures' only  8  Yes Yes Yes Yes Yes Yes Yes Yes Yes Ye		

• LLDP	No		
identification & maintenance function	INU		
I&M0 - device-specific information	Yes		
I&M1 - higher level designation/location designation	Yes		
product functions / diagnostics			
product function			
PROFINET IO diagnosis	Yes		
• link check	No		
connection monitoring IP-Alive	No		
SysLog	Yes		
protocol / is supported	100		
• SNMP v1	Yes		
• SNMP v2	Yes		
• SNMP v3	Yes		
product functions / VLAN			
product function			
function VLAN with IWLAN	No		
product functions / DHCP			
product function			
DHCP client	Yes		
DHCP server	Yes		
DHCP Option 82	Yes		
product functions / redundancy			
protocol / is supported			
• STP/RSTP	Yes		
• MSTP	Yes		
• RSTP	Yes		
product functions / security			
product function			
ACL - MAC-based	Yes		
<ul> <li>management security, ACL-IP based</li> </ul>	Yes		
• IEEE 802.1x (radius)	Yes		
NAT/NAPT	Yes		
<ul> <li>access protection according to IEEE802.11i</li> </ul>	Yes		
WPA/WPA2	Yes		
• TKIP/AES	Yes		
protocol / is supported			
• SSH	Yes		
• RADIUS	Yes		
product functions / time			
protocol / is supported			
• NTP	Yes		
• SNTP	Yes		
SIMATIC time synchronization (SIMATIC Time)	Yes		
standards, specifications, approvals			
standard	FM 0044, Olsse I Bisisis a Co. A D O D TAYOU A TO CO.		
• for FM	FM 3611: Class I, Division 2, Groups A,B,C,D, T4 / Class 1, Zone 2, Group IIC, T4, FM16US0205X		
for safety / from CSA and UL	UL 60950-1 E115352, CSA C22.2 No. 60950-1		
certificate of suitability			
EC Declaration of Conformity	Yes		
CE marking	Yes		
• C-Tick	Yes		
• E1 approval	No		
railway application in accordance with EN 50155	No		
• NEMA TS2	No		
● IEC 61375	No		
• IEC 61850-3	No		
• NEMA4X	No		
Power-over-Ethernet according IEEE802.3at for type 1	Yes		
and IEEE802.3af			

standard for versions communication  IEEE 802.11b  IEEE 802.11b  IEEE 802.11b  IEEE 802.11b  IEEE 802.11c  IEEE 80	Power-over-Ethernet according to IEEE802.3at for type 2	Yes			
HEEE 802.11b					
FIEEE 802.116		Yes			
FEET 802.11g					
FIEE 802-111   Yes					
IEEE 802.111  IEEE 802.111  Ves  Ves  Ves  Ves  Ves  Ves  Vouvill find the current list of countries at: www.siemens.de/funkzulassungen  Annorana Register of Shipping Europe Ltd. (ABS)  French marine classification association  Annorana Register of Shipping (KRS)  French marine classification society (RV)  DNV GL  French marine classification society (RV)  DNV GL  Ves  I korrana Register of Shipping (KRS)  Ves  I korrana Register of Shipping (KRS)  Ves  I koppe Register of Shipping (LRS)  Ves  Ves  Ves  I koppe Register of Shipping (LRS)  Ves  Ves  Ves  I koppe Register Station (PRS)  Ves  I koppe Register (Shipping (LRS)  Ves  I koppe Register (Shipping (LRS)  Ves  I koppe Register (Shipping Register)  Ves  I koppe Register (Shipping Register)  Ves  Ves (GB3838 I Register)  Ves  Ves  Ves  Ves  Ves (GB3838 I Register)  Ves  Ves  Ves  Ves  Ves  Ves (GB3838 I Register)  Ves  Ves  Ves  Ves  Ves  Ves  Ves  Ve					
FIEEE 802.111   Yes	9	1.00			
Yes   You will find the current list of countries at: www.siemens.defunkzulgassungen   Standards, approvals / marrine classification   Yes   Yes					
weeless approvals  **Indiractis, specifications, approvals / marine classification  **American Bureau of Shipping Europe Ltd. (ABS)  **American Bureau of Shipping (Europe Ltd. (ABS)  **Pers					
Marine classifications, approvals / marine classification  Marine classification association  - American Bureau of Shipping Europe Ltd. (ABS)  - French marine classification society (BV)  - NoV CL  - Koream Register of Shipping (KRS)  - Licyds Register of Shipping (KRS)  - Negor Institution of Naval Architects (RINA)  - Possitive Register of Shipping (KRS)  - Royal institution of Naval Architects (RINA)  - Problik Regist Statkow (PRS)  - Royal institution of Naval Architects (RINA)  - Royal institution of					
Marine classification association  American Bureau of Shipping Europe Ltd. (ABS)  American Bureau of Shipping Europe Ltd. (ABS)  American Bureau of Shipping (RTS)  Nes  Nov Cl.  Novan Register of Shipping (RTS)  Nes  Noyal Institution of Naval Architects (RINA)  Res  Royal Institution of Naval Architects (RINA)  Res  Res  Royal Institution of Naval Architects (RINA)  Res  Res  Res  Res  Res  Res  Res  Re		Tod will find the current list of countries at. www.sichichs.dc/funkzulassungen			
American Bureau of Shipping Europe Ltd. (ABS)     French marine dassification society (BV)     Yes     NoN Cd.     Korean Register of Shipping (KRS)     Non Cd.     Note an Register of Shipping (LRS)     Non Cd.     Noper Kalji Kyokai (NK)     Polski Rejestr Statikow (PRS)     Nopin Kalji Kyokai (NK)     Polski Rejestr Statikow (PRS)     Nopin Kalji Kyokai (NK)     Nopin Kyokai (NK)     Nopin Kalji Kyokai (NK)     Nopin Kyokai					
Finneth marine classification society (BV)  Pres  Norwan Register of Shipping (KRS)  Loyds Register of Shipping (KRS)  Pres  Loyds Register of Shipping (LRS)  Pres  Reyal institution of Naval Architects (RINA)  Pres  Standards, specifications, approvals / hazardous environments  standard / for hazardous zone  ANSI/ISA 12.12 01-2013, CANICSA C22.2 No 213-M1987, CL 1, div. 2, GP, A, B, CD, Ta / CL 1, Zone 2, GP IIC E240480  Prival institution of Naval Architects (RINA)  Pres  Standards, specifications, approvals / hazardous environments  Standard / for hazardous zone  ANSI/ISA 12.12 01-2013, CANICSA C22.2 No 213-M1987, CL 1, div. 2, GP, A, B, CD, Ta / CL 1, Zone 2, GP IIC E240480  Pres  Prival institution of Naval Architects (RINA)  Pres  Standards, specifications, approvals / Environmental Product Declaration  Environmental Product Declaration  Pres  Global Warming Potential [CO2 eq]  Intelligency of the Carbon o		Vec			
Non-real Register of Shipping (KRS)     Nosean Register of Shipping (KRS)     Nippon Kaji Kyoka (RK)     Poski Register Statkow (FRS)     Nippon Kaji Kyoka (RK)     Poski Register Statkow (FRS)     Nosean Register Register Statkow (FRS)     Nosean Register Register Statkow (FRS)     Nosean Register Re					
Korean Register of Shipping (KRS)     Lloyds Register of Shipping (LRS)     Yes     Nippor Maily Kyokai (KN)     Polski Registr Satkow (PRS)     Royal Institution of Naval Architects (RINA)     Yes     Standards, specifications, approvals / Insuradous environments     standard / for hazardous zone     ANSURSA 12-12-01-2013, CANICSA C22.2 No 213-M1987, CL 1, div. 2, GP. A,     Royal Institution of Naval Architects (RINA)     *from CSA and UL     Standards / For hazardous zone according to     Bis standard     *as marking     *sa marking     *as marking     *Ex Na ILC 14 Ge     *standards, specifications, approvals / Environmental Product Declaration     Test (Sibal Warming Potential (CO2 eq)     *otol     *otol     *during manufacturing     *during operation     *otol 14     *otol 14     *during operation     *otol 60     *otol 15     *otol 15     *otol 15     *otol 16     *otol 16     *otol 17     *otol 17     *otol 18     *otol 18     *otol 19					
Lloyds Register of Shipping (LRS) Nippon Kaji Kyoka (NK) Posis Regist Stattow (PRS) Royal Institution of Naval Architects (RINA) Pes Royal Institution of Naval Architects (RINA) Pes Standard's peedifications, approvals / hazardous environments  standard's peedifications, approvals / hazardous environments  Standard's of brazardous zone  from CSA and UL  ANSINSA 12.12.01-2013, CAN/CSA C22.2 No.213-M1987, Cl. 1, div. 2, GP. A. B. C. D. T.4 / Cl. 1, Zone 2, CP IIC E240480 Pes G83838.1, G83836.8  Ex nA IIC T4 Ge  standards, specifications, approvals / Environmental Product Declaration  Environmental Product Declaration  Yes  Standards, specifications, approvals / Environmental Product Declaration  Finder of the product Declaration  Yes  Standards, specifications, approvals / Environmental Product Declaration  Finder of the product Declaration  Yes  Standards, specifications, approvals / Environmental Product Declaration  Finder of the product Declaration  Yes  Standards, specifications, approvals / Environmental Product Declaration  Finder of the product Declaration  Yes  Standards, specifications, approvals / Environmental Product Declaration  Yes  Standards, specifications, approvals / Environmental Product Declaration  190.081 kg  during potential (CO2 eq)  100.081 kg  accessories  24 V DC screw terminal included in scope of delivery  Standards of the product Declaration  Internet link  100 web page: WLAN country approval  100 two basis: industry Online Support  100 two basis: industry Online Support  100 websis: industrial online Support websis on the product of the secure operation of plants, systems, machines and networks. Such apport in secure operation of plants, systems, machine		1.77			
Nippon Kaiji Kyokai (NK)     Polski Rejestr Statkow (PRS)     Royal Institution of Nava Architects (RINA)     Yes     Royal Institution of Nava Architects (RINA)     Yes     standards, specifications, approvals / hzzardous environments     standard / for hazardous zone     # From CSA and UI.     ANSI/SA 12.12.01-2013, CAN/CSA C22.2 No.213-M1987, Cl. 1, div. 2, GP. A, B. C. D. Tal / Cl. 1, Zone 2, GP I/C E240480     Standard    * as marking     Ex na I/C 14. Ge     standards, specifications, approvals / Environmental Product Declaration     Environmental Product Declaration     Per and I/C 14. Ge     Standard    * as marking     Standard    *		1.77			
Polski Rejestr Statkow (PRS)  **Royal Institution of Naval Architects (RINA)  **Standards, **specifications, approvals** hazardous environments**  standard / for hazardous zone  **In Bo079-15:2005, EN 60079-0:2006, II 3 G Ex na II T4 KEMA 07 ATEX  **Offeet Offeet Offe					
Royal Institution of Naval Architects (RINA)     Standards, specifications, approvals / hazardous environments  standard / for hazardous zone		1.77			
standards, specifications, approvals / hazardous environments standard / for hazardous zone	•	1.77			
standard / for hazardous zone  • from CSA and UL  • from CSA and UL  certificate of suitability / CCC / for hazardous zone according to GB standard  • as marking  standards, specifications, approvals / Environmental Product Declaration  Environmental Product Declaration  (Sibal Warming Potential [CQ2 eq]  • total  • during manufacturing  • after end of life  accessories  24 V DC screw terminal included in scope of delivery  further information / internet links  internet link  • to web page: WLAN country approval  • to web page: SiePortal  • to web page: WLAN country approval  • to web page: SiePortal  • to web page: SiePortal  • to web page: SiePortal  • to web page: WLAN country operation  • to web page: SiePortal  • to web page: SiePortal  • to web page: WLAN country operation  • to web page: SiePortal  • to see page: WLAN country operation  • 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. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks. In order to protect plants, systems, machines and networks and networks. Such systems, machines and networks against cyber threats, it is necessary to implement—and continuous divisions and networks. Such systems, machines and networks against cyber orework of the internet if and to plants, systems, machines and networks against cyber oreworks. Such systems, machines and networks against cyber oreworks. Such a concept. Customers are responsible for preventing unauthorized access to their plants and solutions and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to plants, systems, anchines and networks. Such systems, machines and components shoul		165			
or from CSA and UL		EN 00070 45 0005 EN 00070 0 0000 # 0 0 E + 111 - 117 - 117			
B, C, D, T4 / Cl. 1, Zone 2, GP IIC E240480  Yes; GB3836.1, GB3836.8  Ex nA IIC T4 GC  Exna II		0145X			
as marking  as marking  Ex nA IIC T4 Gc  standards, specifications, approvals / Environmental Product Declaration  Environmental Product Declaration  Yes  Global Warming Potential (CO2 eq)  • total  • during manufacturing  • during operation  • after end of life  • on 190.081 kg  accessories  accessories  accessories  accessories  24 V DC screw terminal included in scope of delivery  further information / internet links  internet link  • to web page: WLAN country approval  • to web page: SiePortal  • to website: Industry Online Support  • to website: Industry Online Support  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 maritain—a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such exponents 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 industry. Siemens products and solutions constitute one element of such when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial 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 that are no longer s		B, C, D, T4 / Cl. 1, Zone 2, GP IIC E240480			
Standards, specifications, approvals / Environmental Product Declaration  Environmental Product Declaration  Sibal Warming Potential [CO2 eq]  • total  • during manufacturing  • during operation  • after end of life  accessories  accessories  accessories  accessories  accessories  by the formation / internet links  internet link  • to web page: SiePortal  • to website: Industry Online Support  https://www.aitomation.siemens.com/  security information  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, such 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 appropriates early when appropriates with a connection in enterprise network or the internet if and to the extent such a connection is necessary and only when appropriates 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 appropriates are applied as a dollations in development to make them more secure. Siemens strongly recommends that product versions that are no longer supported, and failure to apply the lettest updates may increase customer's exposure to cyber freats, To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed un	GB standard				
Environmental Product Declaration Yes  Global Warming Potential [CO2 eq]  • total 445.68 kg  • during operation 190.081 kg  • during operation 190.081 kg  • after end of life 0.16 kg  accessories  accessories  24 V DC screw terminal included in scope of delivery  further information / internet links  internet link  • to web page: WLAN country approval https://www.siemens.com/wireless-approvals  • to website: Image database https://www.automation.siemens.com/  • to website: Industry Online Support https://www.automation.siemens.com/  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 induntorized access to their plants, systems, 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 networks on 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 networks. Such systems, machines and such connection is necessary and only when appropriate security measures (e.g., firewalls and/or networks. Such systems, machines and such such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or networks or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewalls and/or networks symmetries 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 networks symmetries networks or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g., firewall					
Signature   Sign		eclaration			
• total		Yes			
during manufacturing     during operation     during operation of plants, systems, and industrial cybersecurity functions that support industry, siemens, com/bilddb     https://support.industry.siemens.com/     security information     security information 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 inform					
during operation		9			
accessories accessories 24 V DC screw terminal included in scope of delivery  turther Information / internet links  internet link  • to web page: WLAN country approval • to web page: SiePortal • to website: Image database • to website: Image database • to website: Image database • to website: Industry Online Support  **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 and networks are 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, and only when appropriate 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, and only when appropriate 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 and networks such systems, and only when appropriate security concept. 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 are used use for product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)  Approvals / Certificates	during manufacturing	<u> </u>			
accessories  accessories  24 V DC screw terminal included in scope of delivery  further information / internet links  internet link  • to web page: WLAN country approval  • to web page: SiePortal  • to website: Image database  • to website: Industry Online Support  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 dybersecurity concept. Siemens provides 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 plants, systems, fractional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity measures that may be implemented, please visit on 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)	<b>.</b>	190.081 kg			
accessories  24 V DC screw terminal included in scope of delivery  further information / internet links  internet link  • to web page: WLAN country approval  • to web page: SiePortal  • to website: Image database  • to website: Image database  • to website: Industry Online Support  security information  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 provides products and solutions with industrial cybersecurity concept. Sciemens 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 peasures 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)		0.16 kg			
internet link  • to web page: WLAN country approval • to web page: SiePortal • to website: Image database • to website: Industry Online Support  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 or to retere the accessary and only when appropriate security measures (e.g. firewalls and/or networks segmentation) are in place. For additional information on industrial cybersecurity measures (e.g. firewalls and/or network segmentation) are in place. For additional information on understrial cybersecurity measures 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 Siemen industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7)	accessories				
internet link  • to web page: WLAN country approval  • to web page: SiePortal  • to website: Image database  • to website: Image database  • to website: Industry Online Support  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, systemy, 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		24 V DC screw terminal included in scope of delivery			
to web page: WLAN country approval     to web page: SiePortal     to website: Image database     https://www.automation.siemens.com/     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	further information / internet links				
to web page: SiePortal	internet link				
to website: Image database     to website: Industry Online Support      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	<ul><li>to web page: WLAN country approval</li></ul>	https://www.siemens.com/wireless-approvals			
security information  Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of 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 networks 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)	• to web page: SiePortal	https://sieportal.siemens.com/			
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	• to website: Image database	https://www.automation.siemens.com/bilddb			
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)	• to website: Industry Online Support	https://support.industry.siemens.com			
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)	security information				
Approvals / Certificates	Security information	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			
	Approvals / Certificates				



Declaration of Conformity







<u>FM</u>

For	use	in	hazard-
OUS	loca	atio	ons

**Radio Equipment Type Approval Certificate** 

Marine / Shipping

CCC-Ex

Miscellaneous

Miscellaneous







Marine / Shipping

Environment



NK / Nippon Kaiji Kyokai







Confirmation

last modified:

6/3/2024

