SIEMENS

Data sheet

6GK7242-5DX30-0XE0

product type designation



CM 1242-5

communications module CM 1242-5; for connection of SIMATIC S7-1200 to PROFIBUS as DP slave module.

transfer rate	
transfer rate	
 at the 1st interface / according to PROFIBUS 	9.6 kbit/s 12 Mbit/s
interfaces	
number of interfaces / according to Industrial Ethernet	0
number of electrical connections	
 at the 1st interface / according to PROFIBUS 	1
• for power supply	0
type of electrical connection	
 at the 1st interface / according to PROFIBUS 	9-pin Sub-D socket (RS485)
supply voltage, current consumption, power loss	
type of voltage / of the supply voltage	DC
supply voltage / 1 / from backplane bus	5 V
consumed current	
• from backplane bus / at DC / at 5 V / typical	0.15 A
power loss [W]	0.75 W
ambient conditions	
ambient temperature	
 for vertical installation / during operation 	0 45 °C
 for horizontally arranged busbars / during operation 	0 55 °C
during storage	-40 +70 °C
during transport	-40 +70 °C
relative humidity	
 at 25 °C / without condensation / during operation / maximum 	95 %
protection class IP	IP20
design, dimensions and weights	
module format	Compact module S7-1200 single width
width	30 mm
height	100 mm
depth	75 mm
net weight	0.115 kg
fastening method	
 35 mm top hat DIN rail mounting 	Yes
S7-300 rail mounting	No
wall mounting	Yes
product features, product functions, product components / general	
number of units	
per CPU / maximum	3

service / as DP slave	performance data / PROFIBUS DP		
OPYO OPYO Pes OPYO Pes OPYO Pes OPYO O			
OPV1 data volume		Yes	
data volume • of the address range of the inputs / as DP slave / total • of the address range of the outputs / as DP slave / total • of the address range of the outputs / as DP slave / total protocol / is supported • *CP/IP protocol / is supported • *CP/IP No STEP 7 Basic/Professional **STEP 7 B			
of the address range of the outputs / as DP slave / total porformance data / telecontrol protocol / is supported			
of the address range of the outputs / as DP slave / total porformance data / telecontrol protocol / is supported	of the address range of the inputs / as DP slave / total	240 byte	
performance data / telecontrol protocol / is supported		*	
TECP/IP No TOTAL functions / management, configuration, engineering STEP 7 Basic/Professional STEP			
TECP/IP No TOTAL functions / management, configuration, engineering STEP 7 Basic/Professional STEP	protocol / is supported		
configuration software		No	
* required **standards, specifications, approvals / hazardous environments* certificate of suitability / CCC / for hazardous zone according to GB standard* certificate of suitability / CCC / for hazardous zone according to GB standard / 3s marking standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Yes Global Warning Potential [CO2 eq] • total • during manufacturing • during operation • after end of life • 0.18 kg further information / internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industrial communication • to website: Image database • to website: Image database • to website: Image database • to website: Industry Online Support • to website: Industry Online Support **Support Industry siemens.com/sismatic.net **https://www.aiemens.com/sismatic.net **https:/	product functions / management, configuration, engineering		
certificate of suitability / CCC / for hazardous zone according to GB standard (as marking) certificate of suitability / CCC / for hazardous zone according to GB standard / as marking standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Ciobal Warming Potential (CO2 eq) • total • during manufacturing • during operation • after end of life • on the by page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: SiePortal • to website: Industrial communication • to website: Industry Online Support • to website: Industry Online Support * to website: Industry Online Support * to website: Industry Online Support * Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks, longer to protect plants, systems, machines and networks. Such systems, semens products and solutions constitute one element of such a concept. Siemens products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. Such systems, machines and networks and networks. Such systems, machines and networks and solutions constitute one element of such a concept. Siemens products and solutions constitute one element of such a concept. Siemens products and solutions constitute one element of such a concept. Siemens products and solutions constitute one element of such a concept. Siemens products and networks. Such 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 membrane and networks and networks. Such systems, machines and components should only be conne	configuration software		
certificate of suitability / CCC / for hazardous zone according to GB standard certificate of suitability / CCC / for hazardous zone according to GB standard / as marking standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration Pes Global Warming Potential [CO2 eq] • total • during manufacturing • during operation • after end of life • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web site: Industrial communication • 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. Such systems, machines and networks. Such 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 connection is necessary and only when appropriate security connection is necessary and only when appropriate security. Siemens 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. 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. 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 are in place. For additional information on ind	• required	STEP 7 Basic/Professional	
GB standard / as marking standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration (Slobal Warming Potential (CO2 eq) • total • during manufacturing • during operation • after end of life • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: industrial communication • to website: image database • to website: image database • to website: image database • to website: industry Online Support • to be website: industry Online Support • to selection industry Online Support • thiss://www.siemens.com/cax • the selection online Support • 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. Customers are responsible for preventing unauthorized access reproducts and solutions ounstitute one element of such a concept. Customers are responsible for preventing unauthorized access reproducts and solutions undergo continuously maintain – a holistic, state-of-the-art industrial cybersecurity measures (e.g. firewalls and/or networks. Such systems, machines and networks against cyber undergo. 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 measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity i	standards, specifications, approvals / hazardous environments		
Saturdard / as marking standards, specifications, approvals / Environmental Product Declaration [Environmental Product Declaration Yes Global Warming Potential [CO2 eq] • total 89.58 kg • during manufacturing 14.29 kg • during operation 75.11 kg • after end of life 0.18 kg further information / Internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to website: Industry Online Support • to this support the secure operation of plants, systems, machines and networks against cyber threats, it is necessary to implement—and continuously amintain —a holistic, state-of-the-art industrial cybersecurity concept. Siemens provides 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 against cyber threats, it is necessary of onlipement—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 networks against cyber threats, it is necessary of onlipement — 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 networks or holistic, state-of-the-art industrial cybersecurity concept. Siemens for products and so		Yes; GB3836.1, GB3836.8	
Environmental Product Declaration Global Warming Potential (CO2 eq) • total • during manufacturing • during operation • after end of life • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: slee's product and the selection of thitps://www.siemens.com/istcloud • to web page: slee's product and thitps://www.siemens.com/istcloud • to website: Industrial communication • to website: Industrial communication • to website: Industrial product product and thitps://www.siemens.com/simatic-net • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support **Security information** **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, machines and one tworks should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when approliate security 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 are used available and hat the latest product versions are used available and late the latest product updates are applied as soon as they are available and late the latest product versi		Ex nA IIC T4 Gc	
Solobal Warming Potential [CO2 eq] total	standards, specifications, approvals / Environmental Product Declaration		
total during manufacturing during operation after end of life o.18 kg further information / internet links internet link to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Image database to website: Image database to website: Image database to website: Industry Online Support to website: Industry Online Support thtps://www.siemens.com/simatic-net https://www.siemens.com/cax 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. Stemens 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, 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 (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 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	Environmental Product Declaration	Yes	
during manufacturing during operation after end of life 0.18 kg further information / internet links internet link to web page: selection aid TIA Selection Tool to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal thtps://www.siemens.com/simatic-net thtps://www.siemens.com/simatic-net thtps://www.siemens.com/simatic-net thtps://www.siemens.com/cax thtps://support.industry.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 with 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 that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber t	Global Warming Potential [CO2 eq]		
 during operation after end of life 0.18 kg further information / internet links internet link to web page: selection aid TIA Selection Tool to website: Industrial communication to website: Industrial communication to website: Image database to website: Image database 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. 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. 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/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 intenset. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under 	• total	89.58 kg	
after end of life further information / internet links internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to web page: SiePortal • to website: Image database • to website: CAx-Download-Manager • 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 also 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 (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 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 treats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under	during manufacturing	14.29 kg	
intermet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to web page: SlePortal • to web site: Image database • to website: Image database • to website: Industry Online Support • to website: Industry Online Support • 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 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	during operation	75.11 kg	
internet link • to web page: selection aid TIA Selection Tool • to website: Industrial communication • to web page: SiePortal • to web site: Image database • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • to website: Industry Online Support • 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' 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 updates are applied as soon as they are available and that the latest product updates are applied as soon as they are available and that the latest product updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under	after end of life	0.18 kg	
to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal to web page: SiePortal to website: Image database to website: Image database to website: CAx-Download-Manager 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' 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 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	further information / internet links		
to website: Industrial communication to web page: SiePortal to website: Image database https://www.automation.siemens.com/bilddb to website: CAx-Download-Manager 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	internet link		
to web page: SiePortal to website: Image database to website: CAx-Download-Manager 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' 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 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	 to web page: selection aid TIA Selection Tool 		
• to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support https://support.industry.siemens.com/cax https://support.industry.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			
to website: CAx-Download-Manager to website: Industry Online Support			
• to website: Industry Online Support https://support.industry.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	G		
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://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			
		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

General Product Approval



Declaration of Conformity









EMV

For use in hazardous locations



<u>KC</u>





<u>FM</u>





Marine / Shipping









NK / Nippon Kaiji Kyokai



Environment

Confirmation



last modified:

5/17/2024

