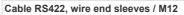
SIEMENS

Data sheet 6GT2891-4EH20

product type designation

product description



Highly flexible communication line (6-core)

SIMATIC RF, MV plug-in cable, with bare end, between ASM 475 and reader, or 24 V cable for RF61XR, RF650R, RF68XR, PUR, trailing, length 2 m.



suitability for use	Plug-in cable for connecting a reader to the ASM 475 communication module or 24V power supply of the RF61xR, RF650R and RF68xR readers
cable designation	L-YC11Y 6x1x0.25 6x24AWG CM
wire length	2 m
electrical data	
number of electrical connections	2
type of electrical connection	wire end sleeves (labeled) / M12 (female, 8 pin, straight)
loop resistance per length / maximum	160 mΩ/m
insulation resistance coefficient	20 GΩ·m
operating voltage	
• maximum	300 V
mechanical data	
number of electrical cores	6
design of the shield	Braided shield made of tin-plated copper wires
outer diameter	
of cable sheath	5.4 mm
symmetrical tolerance of the outer diameter / of cable sheath	0.2 mm
material	
 of the wire insulation 	PVC
of cable sheath	PUR
color	
 of the insulation of data wires 	DIN 47100
of cable sheath	Black
bending radius	
with single bend / minimum permissible	21.6 mm
 with multiple bends / minimum permissible 	43 mm
with continuous bending	75 mm
number of bending cycles	3000000
tensile load / maximum	200 N
weight per length	45 kg/km
ambient conditions	
ambient temperature	
during operation	-30 +80 °C
during storage	-30 +80 °C
during transport	-30 +80 °C
during installation	-30 +80 °C
fire behavior	flame resistant according to IEC 60332-1-2
class of burning behaviour / according to EN 13501-6	Eca

esistant to grease resistant resista		
resistant radiological resistance / to UV radiation resistant radiological resistance / to UV radiation resistant reproduct feature • halogen-free • halogen-free • silicon-free • silicon-free • product feature • halogen-free • silicon-free • silicon-free • silicon-free * Ves * standards, spocifications, approvals ULFET, listing / 300 V Rating Certificate of suitability • EAC approval • according to IEC 81346-2 • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to website: Iradge database • to website: CAx-Download-Manager • to website: Iradge database • to website: Iradge database • to website: industry Online Support * to buse the industry Online Support * security information **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 enviorks against contentions and one theories in order to protect plants, systems, machines and one theories in order to protect plants, systems, machines and one networks against should only be connected to an enterprise network or the internet of such a constitute on element of such a constitute and element of such a constitute and element of such a constitute and element of such a constitute on element of such a constitute and elements should only be connected to an enterprise network	chemical resistance	
radiological resistance / to UV radiation resistant product features, product functions, product components / general product feature		
product feature halogen-free halogen-free halogen-free product feature halogen-free halogen-fre		
product feature		
• halogen-free • silicon-free • silicon-free • silicon-free • standards, specifications, approvals UL/ETL listing / 300 V Rating Certificate of suitability • EAC approval reference code • according to IEC 81346-2 • according to IEC 81346-2 • according to IEC 81346-2:019 WGB further information / Internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: selection silicon aid TIA Selection Tool • to website: riange database • to to website: GAx-Download-Manager • to to website: Mage database • to to website: Mage database • to to website: Industry Online Support		nerai
Silicon-free Standards, specifications, approvals UL/ETI. listing / 300 V Rating Yes; CM (only cable without plug) certificate of suitability EAC approval Yes reference code according to IEC 81346-2 according to IEC 81346-2:2019 WGB further linformation / Internet links internet link to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web page: selection aid TIA Selection Tool to website: Image database to website: Industry Online Support thttps://www.siemens.com/listcloud https://www.siemens.com/listcloud https://www.siemens.com/cawwien/view/109768358 https://www.siemens.co	•	N.
### Security information ### Security infor	-	
UL/ETL listing / 300 V Rating certificate of suitability • EAC approval Yes Yes Yes Yes Yes Yes Yes Ye		Yes
reference code according to IEC 81346-2 according to IEC 81346-2-2019 WGB further information / internet links internet link to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web page: SiePortal to website: Image database to website: Image database to website: Industry Online Support thttps://www.uutomation.siemens.com/cax thttps://www.siemens.com/cax thttps://www.siemens.com/cax thttps://www.siemens.com/cax thttps://www.siemens.com/cax thttps://www.siemens.com/cax thttps://www.siemens.com/cax thttps://www.siemens.com/cax 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 not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is not enterprise network or the internet if and to the extent such a connection is n		
reference code • according to IEC 81346-2 • according to IEC 81346-2:2019 WG further information / internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to website: Image database • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • 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. Saints with the systems, machines and networks against veyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Ustomers 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 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.siem		Yes; CM (only cable without plug)
reference code according to IEC 81346-2 according to IEC 81346-2:2019 WGB further information / internet links internet link a to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to website: Image database to website: Image database to website: CAx-Download-Manager to website: Industry Online Support bittps://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cs/ww/en/view/109766358 https://www.siemens.com/cb/ to website: Image database https://www.siemens.com/cb/ bittps://www.siemens.com/cb/ to website: 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 against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-ari 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 connection is necessary and only when appropriate security measures teal. Ge, firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures teal may be implemented, please visit www.siemens.com/cybersecurity measures teal rung be implemented, please visit www.siemens.com/cybersecurity understore 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	•	
according to IEC 81346-2 according to IEC 81346-2:2019 WGB further information / internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: SiePortal • to website: Image database • to website: Image database • to website: Image database • to website: Industry Online Support • to website: Industry Online Support **Security information **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, 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 entity		Yes
according to IEC 81346-2:2019 WGB further Information / Internet links internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • 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 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 concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and networks against cyber executive their plants, systems are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and netwo		
internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: SiePortal • to website: Image database • to website: Image database • to website: Industry Online Support • to receive 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 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 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 RSS Feed under https://www.siemens.com/cert. (V4.7)	9	
internet link • to website: Selection guide for cables and connectors • to web page: selection aid TIA Selection Tool • to web page: SiePortal • to web site: Image database • to website: Image database • to website: Image database • to website: Industry Online Support • to website: Industrial cybersecurity 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 on 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, subscri		WGB
to website: Selection guide for cables and connectors to web page: selection aid TIA Selection Tool to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support thttps://swww.siemens.com/cax thttps://support.industry.siemens.com/bilddb thttps://support.industry.siemens.com/cax thttps://support.industry.siemens.com/sax thttps://support.industry.siemens.sax support.industry.siemens.sax support.industry.siemens.com/sax thttps://support.industry.siemens.sax support.industry.siemens.com/sax thttps://support.industry.siemens.sax support.industry.siemens.sax support.industry.siemens.com/sax thttps://support.industry.siemens.com/sax support.industry.siemens.com/sax support.industry.siemens.com/sax support.industry.siemens.com/sax support.industry.siemens.com/sax support.industry.sieme	further information / internet links	
to web page: selection aid TIA Selection Tool to web page: SiePortal to website: Image database https://www.automation.siemens.com/bilddb 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 (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 web page: SiePortal to website: Image database 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 onetworks against cyber such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and 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 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: Selection guide for cables and connectors 	https://support.industry.siemens.com/cs/ww/en/view/109766358
to website: Image database to website: CAx-Download-Manager to website: Industry Online Support https://www.siemens.com/cax 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/cycrt. (V4.7)	 to web page: selection aid TIA Selection Tool 	https://www.siemens.com/tstcloud
• to website: CAx-Download-Manager • to website: Industry Online Support **https://support.industry.siemens.com/cax* **https://support.industry.siemens.com/cax* **https://support.industry.siemens.com/cax* **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 https://www.siemens.com/cert. (V4.7)	to web page: SiePortal	https://sieportal.siemens.com/
• 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 https://www.siemens.com/cert. (V4.7)	to website: Image database	https://www.automation.siemens.com/bilddb
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)	to website: CAx-Download-Manager	https://www.siemens.com/cax
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	

General Product Approval EMV Environment









<u>KC</u>

Confirmation

last modified: 8/8/2024 🖸