SIEMENS

Data sheet 6GT2821-4AC10

product type designation



RF240R reader

SIMATIC RF200 Reader RF240R; RS422 interface (3964R); IP67, -25 to +70 °C; 50x 50x 30 mm; with integrated antenna.

suitability for operation	ISO 15693 Transponder (MDS Dxxx), for connecting to communication modules	
radio frequencies		
operating frequency / rated value	13.56 MHz	
range / maximum	65 mm; Range is dependent on transponder type: observe http://support.automation.siemens.com/WW/view/en/67384964	
protocol / with radio transmission	ISO 15693, ISO 18000-3	
transfer rate / with radio transmission / maximum	26.5 kbit/s	
product feature / multitag-capable	No	
electrical data		
transfer rate / at the point-to-point connection / serial / maximum	115.2 kbit/s	
transmission time / for user data		
 for write access / per byte / typical 	0.6 ms	
 for read access / per byte / typical 	0.6 ms	
interfaces		
standard for interfaces / for communication	RS422	
type of electrical connection	M12, 8-pin	
mechanical data		
material	PA6.6	
color	anthracite	
tightening torque / of the screw for securing the equipment / maximum	1.5 N·m	
mounting distance / relating to metal surfaces / recommended / minimum	0 mm	
supply voltage, current consumption, power loss		
supply voltage / at DC		
• rated value	24 V	
•	20.4 28.8 V	
consumed current / at DC		
at 24 V / typical	0.05 A	
ambient conditions		
ambient temperature		
 during operation 	-20 +70 °C	
during storage	-25 +80 °C	
during transport	-25 +80 °C	
protection class IP	IP67	
shock resistance	EN 60721-3-7 Class 7 M2	
shock acceleration	500 m/s ²	
vibrational acceleration	200 m/s ²	
design, dimensions and weights		

width leight 30 mm legeth 50 mm levelight 30 m		
So mm So m	width	50 mm
net weight fastering method vire length of the RS 422 interface / maximum product features, product functions, product components / general display version ground feature / silicon-free yes standards, specifications, approvals certificate of suitability effects No MTBF A30 a reference code a cocording to IEC 81346-2-2019 Serial and suspendiations, approvals / Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration Environmental Product Declaration United States	height	30 mm
dastening method 2 x M5 screws	depth	50 mm
were length of nRS 422 interface / maximum roduct features, product functions, product components / general display version product features silicon-free standards, specifications, approvals certificate of suitability of IECEX No MTBF reference code according to IEC 81346-2-2019 BYB standards, specifications, approvals / Environmental Product Declaration Further Information / Information after end of life outlines persisted in the second of life life persisted in the second of life life life life life life life lif	net weight	0.06 kg
For RS 422 interface / maximum product fanctions, product components / general factors product factors, product factors, product factors of substitutions, product components / general factors, specifications, approvals	fastening method	2 x M5 screws
For RS 422 interface / maximum product fanctions, product components / general factors product factors, product factors, product factors of substitutions, product components / general factors, specifications, approvals	wire length	
display version	-	1000 m
display version	product features, product functions, product components / ge	neral
product feature / silicon-free standards, specifications, approvals certificate of suitability • IECEX No MTBF 430 a coording to IEC 81348-22019 BYB standards, specifications, approvals reference code • according to IEC 81348-22019 BYB standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration global warming potential [CO2 eq] • total • during manufacturing • total • during operation • after end of life • to website: Selection guide for cables and connectors • to web page: Identification and localization systems • to web page: Identification and localization systems • to web page: Identification and localization systems • to website: Image database • to website: Image database • to website: Industry Online Support bittps://www.siemens.com/fat.bittps://www.siemens.com/cat.bittps		
certificate of suitability e IECEX No MTBF Asocording to IEC 81348-2-2019 Standards, specifications, approvals / Environmental Product Declaration 112.4 kg during operation offer and of life offer offer of Sk internet link to website: Selection guide for cables and connectors to web page: Identification and localization systems to website: CAx-Download-Manager to website: CAx-Download-Manager to website: Industry Online Support blips://www.slemens.com/fats blips://www.slemens.com/fats blips://www.slemens.com/cax	· · ·	
certificate of suitability EICCEX No MTBF	·	
certificate of suitability • IECEX No MTBF 430 a reference code • according to IEC 81346-2:2019 BYB standards, specifications, approvals / Environmental Product Declaration Environmental Product Declaration global warming potential (CO2 eq) • total • during manufacturing • total • during operation • after end of life • 0.3 kg further information / intornet 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 and localization systems • to web page: Sie-Portal • to web page: Sie-Portal • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support • to website: Industry Online Support • thiss://www.siemens.com/fided-phrovals • https://www.siemens.com/cax • thiss://www.siemens.com/cax • thiss://w		Padia according to PRITE guidalines EN200 220 and EN 201490, ECC, all lus
MTBF 430 a reference code	·	Radio according to No.11E guidelines EN300 330 and EN 301409, PCO, COLUS
MTBF reference code according to IEC 81346-22019 BYB	•	Ala
reference code		
** according to IEC 81346-2:2019 **standards, specifications, approvals / Environmental Product Declaration Yes		430 a
Environmental Product Declaration Environmental Product Declaration global warming potential [CO2 eq] • total • during manufacturing • during operation • after end of life • after end of life • to website: Selection guide for cables and connectors • to web page: 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 web page: selection aid TIA Selection Tool • 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 web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web site: Image database • to web page: selection aid TIA Selection Tool • to website: Image database • 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. In order to protect plants, systems, machines and networks. Such systems, machines and and tworks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Guerners' products and solutions constitution element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks such as 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. Siemen's products and solutions undergo continuous development to make them mo		
Environmental Product Declaration Yes		
e total • total • during manufacturing • during operation • after end of life • during operation • after end of life • 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 and localization systems • to web page: SiePortal • to web page: SiePortal • to web page: SiePortal • to website: CAx-Download-Manager • to website: industry Online Support • to website: Industry Online Support * 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. In order to protect plants, systems, machines and networks. In order to protect 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 onetworks 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 threats, it is necessary to implement and continuously maintain — a holistic, state-of-the-art industrial cybersecurity 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 that are no longer supported, and failure to apply the latest updates may increase customer's exposures to cyber freats. To stay informed about product updates, subscribe to the Siemens Inodustrial Cybersecurity R	standards, specifications, approvals / Environmental Product	Declaration
• total • during manufacturing • during operation • after end of life • during manufacturing • after end of life • 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: RFID country approval • to web page: RFID country approval • to web page: selection and localization systems • to web page: sleentification and localization systems • to web site: Image database • to website: Image database • to website: CAx-Download-Manager • to website: CAx-Download-Manager • to website: Industry Online Support • thips://swww.siemens.com/cax • thips://swww.siemens.com/cax • thips://support.industry.siemens.com/ • thips://support.industry.siemens.com/cax • thips://support.industry.siemens.com/ca/	Environmental Product Declaration	Yes
during manufacturing during operation diffe during operation during duri	global warming potential [CO2 eq]	
after end of life after end of life o.3 kg 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 and localization systems to web page: SlePortal 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 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 functions on a networks super submitorized access the thirp lanks, systems, machines and networks and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access the their plants, systems, machines and networks and networks super submition and networks submitions or networks that may be implemented, please visit www.siemens.com/cybersecurity measures for poduct versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exponentiation are in place. For additional information on industrial cybersecurity measures 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 had are no longer supported, and failure to apply the latest upd	• total	124.25 kg
after end of life 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: identification and localization systems • 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 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. Such systems, machines and networks. Such systems, machines and one properties are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and one properties executly measures (e.g. firewalls and/or networks segaral and only when appropriate security measures (e.g. firewalls and/or networks segaral and on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/corest. Customers execure. 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 a publy 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)	during manufacturing	11.24 kg
internet link intern	 during operation 	112.71 kg
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: RFID country approval • to web page: identification and localization systems • to web page: identification and localization systems • to web page: SiePortal • to website: Image database • to website: CAx-Download-Manager • 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, and networks. In order to protect plants, systems, and networks. In order to protect plants, systems, machines and networks. Such systems, and plants 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, and only when appropriate security measures (e.g. firewalls and/or networks such systems, 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 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 updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under intips://www.siemens.com/cet. (V4.7)	after end of life	0.3 kg
to website: Selection guide for cables and connectors to to web page: selection aid TIA Selection Tool to web page: RFID country approval to web page: identification and localization systems to web page: identification and localization systems to web page: SiePortal 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 Security information Siemen 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 flustrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) Approvals / Certificates	further information / internet links	
to web page: selection aid TIA Selection Tool to web page: RFID country approval to web page: identification and localization systems to web page: SiePortal to website: Image database to website: Image database 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 provides 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 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 are applied as soon as they are available and that the latest product versions are sued. 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	internet link	
to web page: RFID country approval to web page: identification and localization systems to to web page: SiePortal to website: 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 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: Selection guide for cables and connectors	https://support.industry.siemens.com/cs/ww/en/view/109766358
to web page: identification and localization systems to web page: SiePortal to website: Image database to website: CAx-Download-Manager 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. 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 web page: selection aid TIA Selection Tool	https://www.siemens.com/tstcloud
to web page: identification and localization systems to web page: SiePortal to website: Image database to website: CAx-Download-Manager 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 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) Approvals / Certificates	 to web page: RFID country approval 	https://www.siemens.com/rfid-approvals
to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support https://www.siemens.com/cax 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 lustrial 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 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 web page: identification and localization systems	https://www.siemens.com/ident
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 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		https://sieportal.siemens.com/
• to website: CAx-Download-Manager • 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		https://www.automation.siemens.com/bilddb
• 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) Approvals / Certificates	· ·	
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)	2	Integral Support and distribution of the Control of
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	nups.//www.siemens.com/cert. (v4.7)

UK CA









<u>KC</u>

Radio Equipment Type Approval Certificate

Environment

Miscellaneous FCC Miscellaneous Confirmation



last modified: 8/18/2024 🖸