SIEMENS

Data sheet 6GT2831-6AA60

product type designation



RF1060R USB reader

SIMATIC RF1000 Access control reader RF1060R; ISO 14443 A/B Mifare, ISO15693 USB port; IP65 front, -25 to +55 $^{\circ}$ C; 90 x 62 x 25 mm LxWxH; with integrated antenna, incl. 1.8 m USB connecting cable .

| suitability | for | operation |
|-------------|-----|-----------|
|-------------|-----|-----------|

ISO 15693 and ISO 14443 A/B transponder, for connecting to PC and control systems

| radio frequencies | | |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|--|
| operating frequency / rated value | 13.56 MHz | |
| range / maximum | 0.03 m; Range is dependent on transponder type: observe http://support.automation.siemens.com/WW/view/en/67384964 | |
| protocol / with radio transmission | ISO 15693, ISO 14443 A/B, Felica, NXP NTAG21x, HID iClass | |
| transfer rate / with radio transmission / maximum | 424 kbit/s | |
| product feature / multitag-capable | Yes | |
| nterfaces | | |
| standard for interfaces / for communication | USB 2.0 | |
| type of electrical connection | 1.8 m connecting cable with USB 2.0 type A connector | |
| nechanical data | | |
| material | PC-GF | |
| color | titanium gray | |
| mounting distance / relating to metal surfaces / recommended / minimum | 0 mm | |
| supply voltage, current consumption, power loss | | |
| supply voltage / at DC | | |
| rated value | 5 V | |
| • | 4.5 5.25 V | |
| consumed current / at DC | | |
| at 5 V / typical | 0.15 A | |
| • at 5 V / maximum | 0.3 A | |
| ambient conditions | | |
| ambient temperature | | |
| during operation | -25 +55 °C | |
| during storage | -25 +55 °C | |
| during transport | -25 +55 °C | |
| protection class IP | IP65; on front after cabinet installation, IP20 rear | |
| shock resistance | EN 60721-3-7 Class 7 M2 | |
| shock acceleration | 300 m/s² | |
| vibrational acceleration | 50 m/s² | |
| design, dimensions and weights | | |
| width | 90 mm | |
| height | 62 mm | |
| depth | 23.5 mm | |
| net weight | 0.12 kg | |
| fastening method | 4 M4 screws for cabinet installation | |
| product features, product functions, product components / gen | eral | |

| certificate of suitability • IECEX reference code • according to IEC 81346-2:2019 BYB accessories accessories card holder, USB cable 0.5 m, table/wall box, clean room cover, further information / internet links internet link • to web page: selection aid TIA Selection Tool • to web page: selection aid TIA Selection Tool • to web page: dentification and localization systems • to web page: SiePortal • to website: Image database • to website: Image database • to website: Industry Online Support bitps://www.siemens.com/ • 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 such do not expensive the 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 elements such do not expensive the 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 elements 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/lybersecurity-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 suppor | | | |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| standards, specifications, approvals certificate of suitability • IECEX No reference code • according to IEC 81346-2:2019 BYB accessories accessories card holder, USB cable 0.5 m, table/wall box, clean room cover, further information / internet links internet link • to web page: selection aid TIA Selection Tool • to web page: ReFID country approval • to web page: SiePortal • to web page: SiePortal • to website: Industry Chine Support • to website: Industry Online Support security information Security inf | display version | 3-color LED | |
| certificate of suitability • IECEX No reference code • according to IEC 81346-2:2019 BYB accessories accessories accessories internet link • to web page: Selection aid TIA Selection Tool • to web page: RFID country approval • to web page: SiePortal • to website: Image database • to website: Image database • to website: Industry Online Support sccurity information security informati | product feature / silicon-free | Yes | |
| certificate of suitability • IECEX reference code • according to IEC 81346-2:2019 BYB accessories accessories card holder, USB cable 0.5 m, table/wall box, clean room cover, further information / internet links internet link • 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: Industry Online Support by thos://www.siemens.com/ident https://www.siemens.com/ident https://www.siemens.com/ident https://www.siemens.com/ident https://www.siemens.com/ident https://www.siemens.com/ident https://www.siemens.com/ident https://www.siemens.com/ident https://www.siemens.com/ident 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. In order to protect plants is systems, machines and networks. In order to protect plants is 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 such do nyle 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 networks. Such 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 elements and components should only the 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 se | standards, specifications, approvals | | |
| reference code • according to IEC 81346-2:2019 accessories accessories card holder, USB cable 0.5 m, table/wall box, clean room cover, further Information / Internet links internet link • 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: Industry Online Support • to website: Industry Online Support bitos://seportal.siemens.com/ • 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 elements should only be connected to an enterprise network on 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-industry. Siemens products and solutions undergo continuous development to make them more secure. Siemens strongl 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 Induction Cybersecurity RSS Feed under | certificate of suitability | Radio according to R&TTE guidelines EN300 330 and EN 301489, FCC, cULus | |
| reference code | certificate of suitability | | |
| accessories accessories accessories card holder, USB cable 0.5 m, table/wall box, clean room cover, further information / internet links internet link • to web page: selection aid TIA Selection Tool • to web page: selection and localization systems • to web page: SiePortal • to website: Image database • to website: Industry Online Support bitps://www.siemens.com/clent https://www.siemens.com/bilddb https://www.siemens.com/cax https://www.siemens.com/cax bitps://www.siemens.com/bilddb https://www.siemens.com/cax bitps://www.siemens.com/cax https://www.siemens.com/cax h | • IECEx | No | |
| accessories accessories accessories card holder, USB cable 0.5 m, table/wall box, clean room cover, further information / internet links internet link • 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 web site: Image database • to website: Image database • to website: Inage database • to website: Industry Online Support https://www.siemens.com/cax • 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 against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cocepts. 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 and only when appropriate security measures (e.g. firewalls and/or networks. Such systems, machines and not or network and networks. Such systems, machines and networks and networks. Such systems, machines and networks against cyber threats, it 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 strongli 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 lindustrial Cyb | reference code | | |
| accessories card holder, USB cable 0.5 m, table/wall box, clean room cover, further information / internet links internet link • 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 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 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 in guestion-guestic for preventing unauthorized access to their plants, systems, machines and networks. Such systems machines and continuously maintain — a holistic, state-of-the-art industrial cybersecurity 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 to in internet 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 strongl 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 | according to IEC 81346-2:2019 | BYB | |
| internet link internet link to web page: selection aid TIA Selection Tool to web page: RFID country approval to web page: RFID country approval to web page: Identification and localization systems to web page: SiePortal to web site: 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 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 in 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. 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 firewalls and that the latest product versions are used. Use of product versions are an olonger supported, and failure to apply the latest updates may increase customer's | accessories | | |
| internet link • 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 web site: Image database • to website: CAx-Download-Manager • 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. In order to protect plants, systems, machines and networks 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 propromates 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 strongl 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 saty informed about product updates subscribe to the Siemens Industrial Cybersecurity RSS Feed under | accessories | card holder, USB cable 0.5 m, table/wall box, clean room cover, | |
| 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: CAx-Download-Manager 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 attained the resulting 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 segments) are only the security measures that may be implemented, please visit www.siemens.com/cybersecurity measures (e.g. firewalls and/or network segmentalon) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongl 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 web page: RFID country approval to web page: identification and localization systems to web page: SiePortal to website: Image database to website: Image database it 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. Clustomers 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 or 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 strongl 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: 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 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 strongl 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 | https://www.siemens.com/tstcloud | |
| 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 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 strongli 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: RFID country approval | https://www.siemens.com/rfid-approvals | |
| * to website: Image database * to website: CAx-Download-Manager * 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 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 strongli 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: identification and localization systems | https://www.siemens.com/ident | |
| • to website: CAx-Download-Manager • to website: Industry Online Support *** https://support.industry.siemens.com **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 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 strongl 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: SiePortal | https://sieportal.siemens.com/ | |
| ● to website: Industry Online Support Security information | • 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 strongl 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 | 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 strongl 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: 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 strongl 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 | security information | | |
| Approvals / Certificates | | 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 | |

IFCEx

General Product Approval

IECEx







Industry Canada (IC)

Radio Equipment Type Approval Certificate

Miscellaneous

Radio Equipment Type Approval Certificate

<u>FCC</u>

last modified:

9/12/2024