SIEMENS

## Data sheet 6GK6050-0AL30-0EA0

| | |
|---|---|
| | CONTROL MODULE WITH LAYER 3 SECURITY EDITION LAYER-2-HARDWARE |
| **product type designation** | **RUGGEDCOM RX5000PN CM01 L3SECL2HW** |
| Technical Product Detail Page | https://i.siemens.com/1P6GK6050-0AL30-0EA0 |
| **standards, specifications, approvals / Environmental Product Declaration** | |
| Environmental Product Declaration | Yes |
| global warming potential [CO2 eq] | |
| ● total | 439.49 kg |
| ● during manufacturing | 109.62 kg |
| ● during operation | 328.65 kg |
| ● after end of life | 1.22 kg |
| **further information / internet links** | |
| internet link | |
| ● to website: Selection guide for cables and connectors | https://support.industry.siemens.com/cs/ww/en/view/109766358 |
| ● to website: Industry Mall/RUGGEDCOM selector | https://www.siemens.com/ruggedcom-selector |
| ● to website: Industrial communication | https://www.siemens.com/simatic-net |
| ● to website: Siemens RUGGEDCOM | https://www.siemens.com/ruggedcom |
| ● to web page: SiePortal | https://sieportal.siemens.com/ |
| ● to website: Image database | https://www.automation.siemens.com/bilddb |
| ● to website: CAx-Download-Manager | https://www.siemens.com/cax |
| ● to website: Industry Online Support | https://support.industry.siemens.com |
| **security information** | |
| security information | Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement - and continuously maintain - a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under https://www.siemens.com/cert. (V4.7) |

**Approvals / Certificates**

| General Product Approval | Test Certificates | other | Environment |
|---|---|---|---|
| Manufacturer Declaration | CB | inspection certificate | EPD |

**last modified:** 9/11/2026


Subject to change without notice
© Copyright Siemens