SIEMENS

## Data sheet 6GK1716-1CB25-0AA0

| | |
|---|---|
| **product type designation** | **HARDNET-IE S7 V21** |
| | HARDNET-IE S7 V21; software for S7, open communication,: OPC, PG/OP communication, configuration software; up to 120 connections; floating license; runtime software, software + electronic manual and license key on USB flash drive; class A; 3 languages (de, en, zh-CHS); for Windows® 10 Professional/Enterprise Windows® 10(IoT) Enterprise 2019 LTSC Windows® 10(IoT) Enterprise 2021 LTSC Windows® 11 Professional/Enterprise; Windows® 11(IoT) Enterprise 2024 LTSC Windows® Server 2022, 2025 (Standard Edition, Datacenter); |



Figure similar

| | |
|---|---|
| product brand name | NET |
| Technical Product Detail Page | https://i.siemens.com/1P6GK1716-1CB25-0AA0 |
| software version | V21 |
| **further information / internet links** | |
| internet link | |
| ● to web page: selection aid TIA Selection Tool | https://www.siemens.com/tstcloud |
| ● to website: Industrial communication | https://www.siemens.com/simatic-net |
| ● 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) |

**last modified:** 8/2/2026


Subject to change without notice
© Copyright Siemens