SIEMENS

## Data sheet 6GK1711-1EW16-0AA0

| | |
|---|---|
| **product type designation** | **SOFTNET-IE RNA V16** |
| | SOFTNET-IE RNA V16 Redundant network access, network access software for PRP Network structures; integrated SNMP Floating License Runtime software, software and electr. manual on DVD, License key on USB stick; Class A; 2 languages (de, en); for Windows 7 SP1 Professional/Enterprise/Ultimat e (64 bit); Windows® 10 Professional/Enterprise (all 64 bit) version 1809, 1903; Windows® Server 2012 R2 Update (Standard Edition); Windows® Server 2016 (Standard Edition, Datacenter); Windows® Server 2019 (Standard Edition, Enterprise) . |




Figure similar

| | |
|---|---|
| Technical Product Detail Page | https://i.siemens.com/1P6GK1711-1EW16-0AA0 |
| software version | V16 |
| **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:** 10/29/2025


Subject to change without notice
© Copyright Siemens