



Figure similar

Powerpack HARDNET-IE S7-REDCONNECT V17 SP1; for extension HARDNET-IE S7 V17; to HARDNET-IE S7 REDCONNECT V17; Floating License; License key on USB flash drive class A; 2 languages (de, en), for Windows® 10 Professional/Enterprise (64 bit) version 1909, 2004, 20H2; Windows® Server 2016 (Standard Edition, Datacenter); Windows® Server 2019 (Standard Edition, Enterprise) Windows® 10(IoT) Enterprise 2016 LTSC Windows® 10(IoT) Enterprise 2019 LTSC .

software version	V17
standards, specifications, approvals	
reference code	
<ul style="list-style-type: none"> according to IEC 81346-2:2019 	010307
further information / internet links	
internet link	
<ul style="list-style-type: none"> to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support 	<ul style="list-style-type: none"> https://www.siemens.com/tstcloud https://www.siemens.com/simatic-net https://sieportal.siemens.com/ https://www.automation.siemens.com/bilddb https://www.siemens.com/cax https://support.industry.siemens.com
security information	
security information	<p>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)</p>

last modified:

9/7/2025