SIEMENS

Data sheet 6GK5903-2SA40-0AA0

product type designation	**Layer 3 Lizenz für XCM/XCH-300 und XRM/XRH-300**
	SCALANCE layer 3 function, extension of XCM/XCH-300 and XRM/XRH-300 to include layer 3 features , type of delivery OSD download, unlimited license, transfer via ALM to end devices, consignee email address required for delivery
Technical Product Detail Page	https://i.siemens.com/1P6GK5903-2SA40-0AA0
software version	V1.0
product functions / routing	
service / routing / note	Layer 3 software license
product function	
● static IP routing	Yes
● dynamic IP routing	Yes
protocol / is supported	
● RIPv2	Yes
● OSPFv2	Yes
● VRRP	Yes
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: 6/28/2026

Subject to change without notice
© Copyright Siemens