R&S®SITLine ETH
Ethernet Encryptor

Secure data transmission via landline, radio relay and satellite links

ROHDE&SCHWARZ

Secure Communications

Product Brochure | 04.00

R&S®SITLine ETH Ethernet Encryptor

At a glance

The R&S®SITLine ETH is a family of devices for Ethernet encryption and creating secure "layer 2 virtual private networks" (L2 VPN). The R&S®SITLine ETH protects companies and organizations against espionage and manipulation of data that is transported via Ethernet over landline, radio relay or satellite links. The devices in this product family are BSI-approved and can be used in a flexible manner in many stationary and mobile applications.

The R&S®SITLine ETH performs encryption on an Ethernet basis – in the ISO/OSI model's data link layer (layer 2) – and is thus ideal to protect applications where throughput and time are critical. Communications links over public and private networks can be protected. Using R&S®SITLine ETH, the security requirements can be represented fully independently of the existing or planned network structure.

Because Ethernet significantly reduces costs, it has become established in recent years as a true networking alternative to "managed IP connections". The R&S®SITLine ETH provides different models and performance classes. The R&S®SITLine ETH family is a flexible solution to meet changing requirements for a high level of investment protection.

Key facts

- Ethernet encryptor in performance classes from 25 Mbit/s to 1 Gbit/s
- Advanced cryptographic methods and standards (elliptic curves, AES, X.509)
- Flexible deployment in both simple and complex network structures
  - Safeguarding lines (point-to-point), star structures (point-to-multipoint) and fully meshed networks (multipoint-to-multipoint)
  - Maximum bandwidth efficiency, avoidance of overhead
  - For Ethernet connections via landline, radio relay and satellite links
- Extremely compact design (1 HU), very low specific energy consumption, low total cost of ownership (TCO)
- BSI-approved up to German restricted ("VS-NfD") and NATO restricted

R&S®SITLine ETH100.

R&S®SITLine ETH50.

R&S®SITLine ETH Ethernet Encryptor

Benefits and key features

Secure civil, official and military communications

- Confidential communications between sites and within a single site (L2 VPN)
- Safeguarding of radio relay and satellite links (SatCom)
- Integrity protection for public transport (railway, road tolls)
- Secure data center interconnection, secure storage area networks

▷ page 4

Low system costs

- Minimum investment for installation and configuration
- Low space and energy costs
- Lower transmissions costs than with managed IP
- Low maintenance and service requirements

▷ page 6

Professional, certified security

- Secure authentication
- Flexible encryption hardware
- Manipulation-proof devices
- Variable operating modes

▷ page 7

Independent, secure management

- Separation of network management and security management

▷ page 8

Automatic link setup

- Redundant link structure to the security management system
- Self-organizing and self-healing
- Automatic setup of encrypted links

▷ page 9

R&S®SITLine ETH1G.

Safeguards civil, official and military communications

Originally used only in local area networks (LANs), today Ethernet is a universal transmission technology for wide area networks (WANs). This makes interconnecting sites over global networks just as easy as in-house cabling. Unfortunately, this also means a greater susceptibility to attacks from the public network: These networks are just as easy to eavesdrop on, manipulate and disrupt as ordinary computer networks. The BSI-approved R&S®SITLine ETH safeguards communications through consistent encryption on the Ethernet layer.

Confidential communications between sites and within a single site (L2 VPN)

Video conferences, VoIP calls, database queries – the confidentiality of communications links within organizations must be safeguarded in order to prevent espionage and undesired manipulation of data. This is especially important if parts of the communications links are established over long distances, as is the case for organizations with geographically dispersed sites or for networking within a larger campus. Here, the flexibility and variability of the R&S®SITLine ETH are highly beneficial: All of the devices are interoperable. Depending on the site to be integrated, the optimal device can be selected based on criteria such as the required transmission capacity, the number of necessary connections and the environmental conditions. From the encryption of individual lines or applications to the safeguarding of complex structures, the interoperability allows the security solution to grow along with the network. This provides long-term investment protection for users.

R&S®SITLine ETH safeguards public and private Ethernet connections over landline, radio relay and satellite links.

Safeguarding of radio relay and satellite links (SatCom)

Precise, timely information is necessary for strategic command and control of armed forces. Situation reports with image and video material often need to be transmitted over long distances. Here, radio relay and SatCom links are used to connect field units to the central unit (e.g. control center, headquarters), which in many cases might even be on a different continent. In order to ensure information superiority, the data must be completely free from any manipulation, and must not fall into the hands of third parties – reason enough to use strong encryption. However, the encryption must not place any additional loading on the already very narrow bandwidth of the radio relay or SatCom link.

Especially in scenarios with narrow bandwidth allocations, the basic design concept of the R&S®SITLine ETH provides clear benefits: Compared with classic IP encryption, the R&S®SITLine ETH requires significantly less protocol information (overhead) for encrypted transmissions. During the entire radio relay transmission or during satellite hops, the information is protected against eavesdropping and manipulation despite throughput limitations.

Integrity protection for public transport (railway, road tolls)

Public transport networks are managed in central control centers, which are supplied with information from transport hubs (e.g. railway stations, signal boxes) that may be unattended. Automation enables tighter scheduling of trains and greater punctuality. However, unattended transport hubs require a higher level of protection against manipulation, especially if they are connected to the control center over public networks. In this case, cryptographic functions can safeguard the integrity and confidentiality of the transmitted data. Special R&S®SITLine ETH models are available for use in more challenging environments (e.g. extended temperature range, installation with top-hat rail/ DIN rail, external emergency erasure).

Secure data center interconnection, secure storage area networks

Central data centers in a corporation typically have a redundant design. The centers must be securely interconnected via high-performance lines. The state-of-the-art transmission technology for this application are Ethernet services with a transmission capacity of at least 100 Mbit/s and typically several Gbit/s. The R&S®SITLine ETH can be scaled for connections in the Mbit/s and Gbit/s range. The R&S®SITLine ETH multiport model can also be used to efficiently safeguard dedicated Ethernet lines that are connected in parallel.

R&S®SITLine ETH protects communications within critical infrastructures, such as public transport systems.

Low system costs

Compared with other communications and security solutions, Ethernet carrier services protected by the R&S®SITLine ETH have the dual benefits of higher security and lower operating costs.

Minimal investment for installation and configuration

The R&S®SITLine ETH integrates into a network in a fully transparent manner. Except for the security parameters, no other network-specific configuration steps are required. Ethernet is a plug&play technology and therefore requires almost no configuration effort. This saves installation time and expense.

Low space and energy costs

The compact design, low module height and different device classes make it possible to save on both installation space and energy. The multiport device provides the functionality of up to four devices while consuming only the space and power of a single device. The option to safeguard up to four physical lines with a single device is unique worldwide.

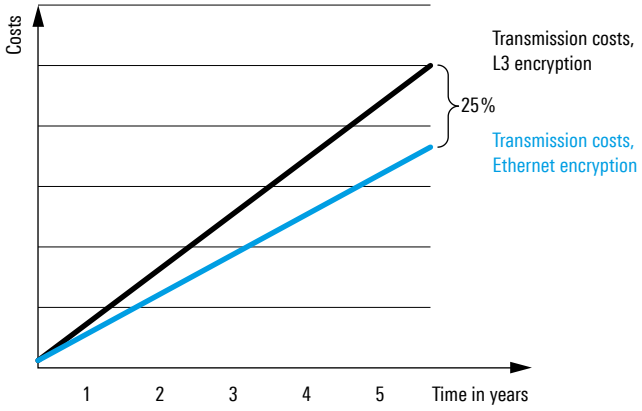
Lower transmissions costs than with managed IP

The significantly lower overhead for Ethernet encryption and the resulting improvement in the net-to-gross transport ratio reduces the transport costs for the payload. Depending on the traffic profile and the selected security functions, the net payload rate only drops by 0% to 13% when using Ethernet encryption. By way of comparison: An IPsec-secured L3 VPN reduces the net payload rate by up to 60% due to the overhead. In addition, purchasing Ethernet as a WAN service from a carrier is usually significantly more economical than, for example, managed IP services.

Low maintenance and service requirements

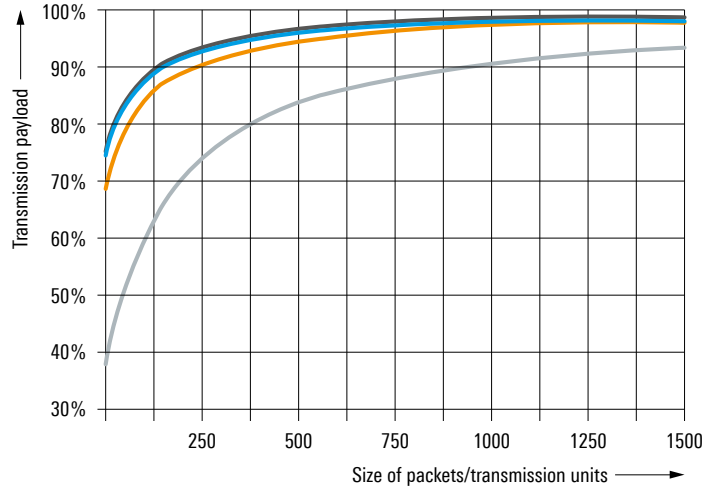
Ethernet operates independently of the logical IP network structures. This eliminates the need for adaptations when integrating new applications, changing providers or migrating to higher-level network protocols (e.g. IPv4 to IPv6). Experience has shown that the service costs for layer 2 systems resulting from major update and upgrade cycles is significantly lower than for other solutions.

Low system costs



Compared with IPsec, Ethernet encryption with R&S®SITLine ETH reduces the TCO by 25% within 5 years.

Net payload rate (capacity utilization)



For a medium-sized packet size of 250 byte, the R&S®SITLine ETH has a significantly higher net payload than IPsec encryption:
R&S®SITLine ETH: > 90% (L2 encryption)
IPsec encryption: 75%

Professional, certified security

Ethernet is a fixed, universal standard for data transmission via cable and radio. However, it does not protect the confidentiality or integrity of the transmitted data. The R&S®SITLine ETH provides the necessary protection in a significantly more efficient and effective manner than other solutions. It has been approved by the Federal Office for Information Security (BSI) for handling of classified documents up to the German restricted ("VS-NfD") level.

Secure authentication

The R&S®SITLine ETH uses the following technologies and standards for secure authentication:

- Asymmetric cryptography using elliptic curves with a 257-bit key (roughly corresponds to 3200-bit RSA key)
- X.509 v3 certificates for persons and equipment
- Secure storage and transport of confidential parameters using smart card technology

Before a link is set up, users are securely authenticated using the certificate issued by the security management system and parameters that are securely provided via a smart card token. A unique set of keys is generated for each management connection and for each of the up to 4000 data connections per device. Key agreement is performed in accordance with the Diffie-Hellman protocol. For key generation, the R&S®SITLine ETH uses a true hardware-based random number generator which is certified in accordance with Common Criteria EAL4+.

Flexible encryption hardware

Symmetric algorithms (AES 256) are used. These are integrated into powerful hardware. Special customer requests regarding the cryptographic method can be taken into account upon request.

Manipulation-proof devices

The R&S®SITLine ETH features not only cryptographic core functions but also an intricate system of mechanical and electromechanical security functions. This includes layered security zones, protected memory, protective mechanisms against mechanical manipulation and further security functions to counteract attempts to steal or manipulate secure confidential information.

Variable operating modes

Depending on the traffic profile and the device model, the R&S®SITLine ETH supports different operating modes:

- Point-to-point: Ethernet private line (EPL) – dedicated Ethernet line
- Point-to-multipoint: Ethernet virtual private line (EVPL) – logical channels on one line
  - With VLAN IDs from the customer network and EVPL service in the WAN (VID EVPL)
  - Without VLAN IDs from the customer network and EVPL service in the WAN (MAC-EVPL)
- Multipoint-to-multipoint: Ethernet LAN (ELAN) in the WAN (MAC-ELAN) – without VLAN IDs from the customer network

Each operating mode can be used in transport mode and in tunnel mode.

In scenarios where two devices are directly interconnected without a switch, the R&S®SITLine ETH100 and the R&S®SITLine ETH1G can alternatively be operated in bulk mode. Bulk mode encrypts all Ethernet packets (including protocol information) without additional overhead, offering a higher degree of confidentiality with maximum data throughput.

R&S®SITLine ETH50.

Independent, secure management

The R&S®SITLine ETH combines high-quality, reliable protection of sensitive data with the ability to separately monitor the network structures involved in the data transfer.

Separation of network management and security management

Due to the strict separation of the security management system (SMS) and the network management system (NMS), connection monitoring can be delegated to the network operator without compromising security. The encryption parameters can be configured for the individual communications relationships completely independently of the transported network structure (e.g. IP subnets). This makes it possible to outsource network responsibility while keeping security under the user's full control.

The R&S®SITLine ETH combines two strictly separated management instances:

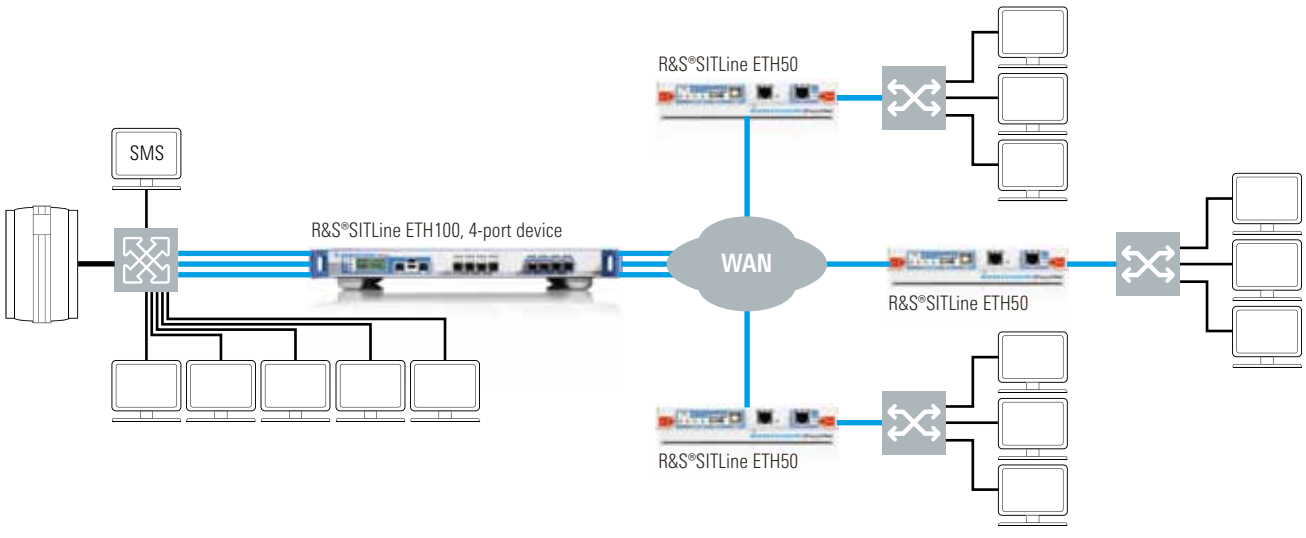
- Security management system (SMS)
- Network management system (NMS)

The security management system is an autonomous instance with the user's security officer as its central point. The security officer has complete control over all security parameters and functions. All communications between the SMS and the individual devices are just as highly protected as the actual data links. Syslog can be used for integration into any existing log book systems from third-party suppliers,

The network management system can be used to independently control parameters for participating networks. For reporting purposes, the devices use traps to send status messages. These messages can be evaluated by the supplied R&S®SITLine administration software or by any SNMP-capable management program.

The two independent reporting mechanisms (Syslog for SMS, traps for NMS) monitor the availability of the infrastructure in two different ways.

Security management

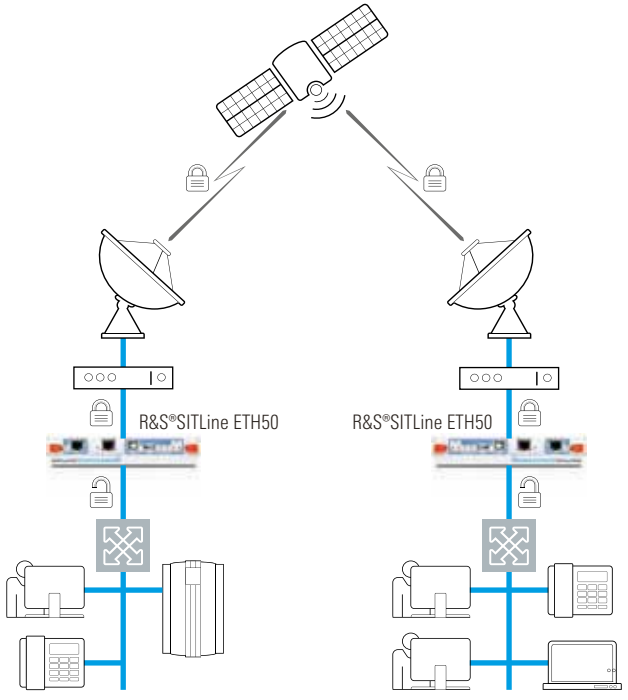


Security management is global for all locations and takes place online for all R&S®SITLine ETH devices in the network.
Security management does not affect network management.

Automatic link setup

Putting additional systems into operation in an existing complex network can be a challenge. This is particularly true for the configuration and organization of the links to the security management system. Ethernet encryptors must offer excellent security encompassing confidentiality, authenticity and integrity while simultaneously meeting demanding requirements for network performance and availability. The R&S®SITLine ETH simplifies this process through self-organization of encrypted links, thereby eliminating the risk of faulty configurations.

Automatic link setup



The R&S®SITLine ETH can be preconfigured before it is sent to the operating site. On startup, it automatically sets up encrypted L2 links. The same applies to backup devices.

Redundant link structure to the security management system

The SMS can directly access an R&S®SITLine ETH via each of the device's interfaces (local management ports as well as data ports). Only the device's IP address for the SMS functions and the associated gateway address need to be entered.

Self-organizing and self-healing

Only a small amount of initial configuration data needs to be transferred offline to the devices (smart card token). All other settings take place dynamically and securely online. The security concept also provides the flexibility to quickly replace a device (e.g. after servicing) without time-consuming reconfiguration. This also helps to maximize the availability of secure communications. Automatic configuration adaptation takes place continually: If the management connection fails, the R&S®SITLine ETH will automatically search for alternative connections to the SMS.

Automatic setup of encrypted links

The individual certificates for the devices are used to determine which parties are authorized to set up connections. Encrypted links can be configured without detailed network data. Encrypted links are automatically set up even when the network configuration changes. Each connection with another authorized communications party is always set up as an encrypted link. If it is not possible to set up an encrypted link because the agreed security procedure could not be completed, data is blocked for this network area. This eliminates the possibility of unintentional or unnoticed communications via unencrypted links. This behavior can only be modified by the security officer by actively setting up an exception rule.

Specifications in brief

Specifications in brief			
	R&S®SITLine ETH1G	**R&S®SITLine ETH100**	**R&S®SITLine ETH50**
Ethernet, ports			
Number of lines per device	1	1, 2 or 4	1
Connector/transceiver	optical, electrical, exchangeable (SFP)	electrical, replaceable (SFP)	electrical, built-in
Performance/throughput per line	1 Gbit/s	100 Mbit/s	25 Mbit/s, 50 Mbit/s, 100 Mbit/s
Number of links	4000	4000	64
Supported Ethernet services			
EPL, Ethernet link encryptor, Ethernet dedicated line	•	•	•
EVPL, VLAN-based encryption	•	•	•
MAC-EVPL, MAC-address-based encryption	•	•	•
MAC-ELAN, MAC-address-based encryption via port-based E-LAN	•	•	•
Cryptography and security			
Transport/tunnel mode	•	•	•
Bulk mode (back-to-back)	•	•	–
Asymmetric	257-bit ECC key (roughly corresponds to 3200-bit RSA key)		
Key agreement	Diffie-Hellman (DH-ECKAS) protocol		
Digital signature	ECDSA		
Authentication	X.509 v3 certificates		
Symmetric	AES with 256-bit key, CFB interleaved mode; other standard algorithms or customer-specific algorithms upon request		
External emergency erasure	–	–	•
Emergency erasure after loss of power	after two days	after two days	after one to seven days (can be configured and deactivated)
Management system			
Standard port for management system	inband	inband	inband
Separate port for R&S®SITScope ETH security management	•	•	–
Network management	independent of security management, supports SNMP versions v1, v2c and v3		
	R&S®SITLine administration software for stand-alone operation	R&S®SITLine administration software for stand-alone operation	
Security management	R&S®SITScope		
Approvals/certifications			
BSI	German restricted (VS-NfD)	German restricted (VS-NfD)	German restricted (VS-NfD)
	NATO restricted	NATO restricted	NATO restricted
EANTC	interoperability test	interoperability test	interoperability test
Key generation (TRNG)	Common Criteria EAL 4+	Common Criteria EAL 4+	Common Criteria EAL 4+
CE approval	•	•	•
General data			
Operating temperature range	+5 °C to +50 °C		–20 °C to +70 °C
Storage temperature range (not initialized)	–20 °C to +70 °C		–40 °C to +70 °C
MTBF	51 000 h	49 000 h	350 000 h (without fan)
Power supply	110 V or 240 V/50 Hz or 60 Hz	110 V or 240 V/50 Hz or 60 Hz	24 V DC to 60 V DC
Dimensions and weight			
Form factor	rack format (19")/1 HU		half rack format (7.5")/1 HU, top-hat rail (DIN rail)
Dimensions (W × H × D)	438 mm × 61 mm × 498 mm (17.2 in × 2.4 in × 19.6 in)		190 mm × 36 mm × 190 mm (7.5 in × 1.4 in × 7.5 in)
Weight	max. 5.2 kg (11.5 lb) (including installation fixtures)		max. 1.5 kg (3.3 lb)
Shipping weight	max. 16 kg (35.3 lb)		max. 3 kg (6.6 lb)

Ordering information

Designation	Type	Order No.
R&S®SITLine ETH50, half rack format (7.5"), 1 HU		
1 line, 25 Mbit/s	R&S®SITLine ETH50-25	5401.8830K02
1 line, 50 Mbit/s	R&S®SITLine ETH50-50	5401.8830K02
1 line, 100 Mbit/s	R&S®SITLine ETH50-100	5401.8830K02
R&S®SITLine ETH100, rack format (19"), 1 HU		
1 line, 100 Mbit/s	R&S®SITLine ETH100-110	5401.7004K11
2 lines, 100 Mbit/s	R&S®SITLine ETH100-210	5401.7004K12
4 lines, 100 Mbit/s	R&S®SITLine ETH100-410	5401.7004K13
R&S®SITLine ETH1G, rack format (19"), 1 HU		
1 line, 1 Gbit/s	R&S®SITLine ETH1G-110	5401.6820K11
R&S®SITLine device token (one token required per device)		
USB token, smart card		5410.0650.04
R&S®SITScope ETH, security management		
Server hardware set, consisting of: server hardware, keyboard and mouse, basic software, unrestricted GUI license, 1 R&S®SITLine terminal license, 3 root tokens, 2 supervisor tokens, 2 manager tokens	R&S®SITScope ETH-HW	5410.8400K13
Server software set, consisting of: basic software, unrestricted GUI license, 1 R&S®SITLine terminal license, 3 root tokens, 2 supervisor tokens, 2 manager tokens	R&S®SITScope ETH-SW	5410.8400K53
R&S®SITLine ETH manuals		
User manual, R&S®SITLine ETH100/R&S®SITLine ETH1G, German		5401.8900.31
User manual, R&S®SITLine ETH50, German		5401.8875.31
User manual, R&S®SITLine ETH100/R&S®SITLine ETH1G, English		5401.8900.32
User manual, R&S®SITLine ETH50, English		5401.8875.32

Data sheet for R&S®SITLine ETH100/1G, see PD 5214.0724.22.
Data sheet for R&S®SITLine ETH50, see PD 5214.4607.22.
Product brochure for R&S®SITScope, see PD 5213.8351.11
and www.rohde-schwarz.com

Service you can rely on

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

About Rohde&Schwarz

Rohde&Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde&Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability

Certified Quality System
ISO 9001

Rohde&Schwarz SIT GmbH
Am Studio 3 | D-12489 Berlin
Phone +49 30 65884-223 | Fax +49 30 65884-184
E-Mail: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

Regional contact

- Europe, Africa, Middle East | +49 89 4129 12345
  customersupport@rohde-schwarz.com
- North America | 1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Latin America | +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asia/Pacific | +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com
- China | +86 800 810 8228/+86 400 650 5896
  customersupport.china@rohde-schwarz.com

PD 5214.0724.12 | Version 04.00 | February 2012 | R&S®SITLine ETH

5214072412