

# IRF2601, IRF2621 – Industrial Router & Firewall

Variants	LAN	Connectivity
<b>IRF2601</b>	6 x RJ45 1000Mbit/s	-
<b>IRF2621</b>	6 x RJ45 1000Mbit/s	4G LTE / UMTS



## Data sheet

Capability Characteristics	
<b>VPN key</b>	Control state of OpenVPN connections by means of an external signal
<b>6 x Gbit/s Ethernet</b>	6 integrated 1Gbit/s Ethernet interfaces running as Switch or stand-alone
<b>Firewall in three Operating Modes</b>	<ul style="list-style-type: none"> <li>Routing mode with statefull filtering of IPv4 traffic on two logical interfaces WAN and LAN, where LAN is used as a 4 port switch and WAN as a 2 port switch</li> <li>In the extended routing mode all 6 Ethernet interfaces can be operated and filtered as independent IP interfaces</li> <li>The transparent mode (bridged) connects the WAN1 and WAN2 adapter directly to the LAN network and enables additional filtering on Layer 2, based on Ethernet criteria via VLAN, MAC addresses or protocol and thus a 6-port switch is the result.</li> </ul>
<b>Packet Filter</b>	Enables the use of pre-defined rule sets for standard communication requirements and an easy controlled production of new filter sets
<b>Network Traffic Prioritization and Shaping</b>	Supports prioritization based on VLAN tag, Ethernet or IP header properties. Bandwidth limitation with Ethernet and IP header criteria.
<b>Configuration</b>	Configuration via web interface (HTTP, HTTPS) and SNMP.
<b>VPN</b>	Supports three different VPN protocols: <ul style="list-style-type: none"> <li>OpenVPN: Layer2 (Ethernet) and Layer3 (IP) transport with SSL-based encryption. Support for tunneling via HTTP proxy and packet filtering</li> <li>IPsec: Standard IPsec encryption with 1:1 NAT support and data filtering.</li> <li>Big-LinX: Smartcard based OpenVPN VPN with cloud services</li> </ul>
<b>Modbus/TCP Interface</b>	Enables the status request and control of VPN channels and Cut & Alarm.
<b>4G / LTE / HSPA+</b>	Optional integrated LTE/HSPA+ multi-band wireless module (2G/3G/4G) for high speed wireless internet access.
<b>SNMP</b>	SNMP basis support enables the integration in existing network monitoring tools.
<b>Memory Card</b>	Saves the complete configuration und enables easy replacement of the unit.
<b>Big-LinX</b>	ADS-TEC Big-LinX smartcard based VPN System
<b>Java / OSGi</b>	Additional Java Virtual Machine with OSGi 4.2 Framework for a open Development of own Applications on the device
<b>API</b>	Rich set of software APIs from JSON RPC 2.0 (for Java) to low level "adsdp" suitable even for microcontrollers.

Basic Parameter	Software Specification
<b>IPv4</b>	<ul style="list-style-type: none"> <li>• One IP address for management in transparent bridge mode, two IP addresses in IP router mode</li> <li>• NAT (Masquerading), e.g. for outgoing WAN traffic</li> <li>• All interfaces can be configured as DHCP clients.</li> <li>• The default gateway can be configured manually.</li> <li>• Dynamic DNS with DHCP client according to RFC 2136</li> <li>• PPPoE support for all IP interfaces for usage with DSL modems</li> </ul>
<b>IP Routing</b>	<p>10 static net or host routes are configurable Dynamic routing according to RIPv2 and OSPF (basic functions) RIPv2 parameters:</p> <ul style="list-style-type: none"> <li>• „simple password“ authentication</li> <li>• interfaces can be switched as active or passive</li> </ul> <p>OSPF parameters:</p> <ul style="list-style-type: none"> <li>• „simple password“ authentication</li> <li>• interfaces can be switched as active or passive</li> </ul> <p>Log level can be configured additionally</p>
<b>IP Forwarding &amp; Port Forwarding</b>	<p>Port Forwarding for TCP/UDP Ports or complete IP addresses using IP aliases. Including the following features:</p> <ul style="list-style-type: none"> <li>• Optional Source NAT for forwardings to hide the original source.</li> <li>• Conditional source matching to enable a forward only for special addresses.</li> <li>• IP Forwarding with IP aliases on VPN channels like IPsec or OpenVPN to run additional virtual IPs on the VPN which will get forwarded to the local network.</li> <li>• No limitation on the number of forwards</li> </ul>
<b>1:1 NAT Network Mapping</b>	<p>Network mapping to resolve IP subnet conflicts by mapping complete IP subnets to virtual address spaces.</p> <ul style="list-style-type: none"> <li>• Map a single IP subnet to a complete virtual address space.</li> <li>• Directly couple two identical IP sub networks by mapping both to two different virtual address spaces.</li> <li>• Keep real IP sub network for the viewpoint of VPN channels.</li> <li>• Connect and map up to 6 identical IP sub networks with a single router</li> </ul>
<b>DHCP Server</b>	DHCP server on WAN and/or LAN interfaces, DNS and gateway are taken over dynamically if an interface is configured as DHCP client
<b>DHCP Relay</b>	Enables the transmission of all DHCP queries to a central DHCP server.

VPN Parameter	Software Specification												
<b>OpenVPN</b>	<p>OpenVPN is an open source alternative to IPsec. The software is freely available for Linux, MacOS/X and Windows.</p> <ul style="list-style-type: none"> <li>• Configurable as TCP/IP client or server alternatively</li> <li>• Authentication with X.509 certificates</li> <li>• HTTP proxy tunnel support in client mode, proxy authentication: Basic, NTLM</li> <li>• Maximum of 10 different OpenVPN processes</li> <li>• ~50 VPN Clients on a pure OpenVPN server setup (depending on system RAM usage)</li> <li>• Each single configuration has a separate interface which can be used for packet filter rulesets</li> <li>• Layer2 Ethernet Tunnels for bridging industrial Ethernet protocols over IP networks</li> </ul> <p>Further supported OpenVPN parameters:</p> <ul style="list-style-type: none"> <li>• IP address assignment and assignment of static routes to OpenVPN clients</li> <li>• IP address acquirement from OpenVPN servers in client mode</li> <li>• Pushing of local subnets to OpenVPN servers. This enables the server to present selectable temporary routes to the webinterface user.</li> <li>• Radius Server authentication for Client authentication on server processes</li> </ul> <p>Detailed list of configurable OpenVPN Options: LZO, TUN/TAP, UDP/TCP, Ciphers, Client-to-Client, redirect gateway, route pushing, HTTP Proxy, Layer 2/3, additional username/password authentication, static client IP address table with iroutes and client specific routes, IP Pool.</p>												
<b>IPsec Policy</b>	<p>IPsec Policies are mostly used to create VPNs with other VPN routers.</p> <ul style="list-style-type: none"> <li>• 64 different IPsec policies for Subnet-to-Subnet configuration or as a Road warrior IPsec Server</li> <li>• Every VPN policy can be configured as active or passive</li> <li>• IPsec can generally be started and stopped via Modbus/TCP or LCD.</li> <li>• Authentication via PSK or X.509 certificates</li> <li>• IPsec NAT traversal</li> <li>• IPsec Limit-MTU option</li> <li>• Hardware crypto engine for high data throughput</li> </ul> <p>IPsec detail specification:</p> <table border="1"> <tr> <td>Key Exchange</td> <td>IKE (Internet Key Exchange) based on ISAKMP (Internet Security Association and Key Management Protocol)</td> </tr> <tr> <td>IKE Phases</td> <td>Main-Mode, Quick-Mode</td> </tr> <tr> <td>DH Groups</td> <td>DH-Group 1 MODP 768, DH-Group 2 MODP 1024, DH-Group 5 MODP 1536</td> </tr> <tr> <td>Data integrity</td> <td>MD5 (128bit), SHA1 (160bit)</td> </tr> <tr> <td>Encryption</td> <td>DES (64bit), 3DES (192bit), AES (128bit), AES (192bit), AES (256bit)</td> </tr> <tr> <td>IPsec Mode</td> <td>ESP-Tunnel</td> </tr> </table>	Key Exchange	IKE (Internet Key Exchange) based on ISAKMP (Internet Security Association and Key Management Protocol)	IKE Phases	Main-Mode, Quick-Mode	DH Groups	DH-Group 1 MODP 768, DH-Group 2 MODP 1024, DH-Group 5 MODP 1536	Data integrity	MD5 (128bit), SHA1 (160bit)	Encryption	DES (64bit), 3DES (192bit), AES (128bit), AES (192bit), AES (256bit)	IPsec Mode	ESP-Tunnel
Key Exchange	IKE (Internet Key Exchange) based on ISAKMP (Internet Security Association and Key Management Protocol)												
IKE Phases	Main-Mode, Quick-Mode												
DH Groups	DH-Group 1 MODP 768, DH-Group 2 MODP 1024, DH-Group 5 MODP 1536												
Data integrity	MD5 (128bit), SHA1 (160bit)												
Encryption	DES (64bit), 3DES (192bit), AES (128bit), AES (192bit), AES (256bit)												
IPsec Mode	ESP-Tunnel												
<b>X.509 Certificate Management</b>	<p>Separate certificate management for verification of the validity of all existing certificates</p> <p>Upload function for client, CA and CRL certificates</p> <p>Preinstalled set of demo-certificates for quick function tests</p> <p>SCEP for automated certificate enrollment</p>												

Configuration and Monitoring	
<b>Web interface</b>	<ul style="list-style-type: none"> <li>• Online help tooltips for all important options</li> <li>• German/English language support</li> <li>• Access via HTTP/HTTPS is configurable freely for any interface, access violations may be logged</li> <li>• Configurable HTTPS certificate</li> <li>• HTTP access can be deactivated</li> <li>• Free definition of unlimited user accounts with detailed access (write) control for any configuration option</li> </ul>
<b>SNMP</b>	<p>Protocols: SNMPv1, SNMPv2, SNMPv3, SNMPv2 read and write community are configurable SNMPv3 read and write username/password and Pre-Shared-Key are configurable</p> <p>Supported SNMP MIBs: MIB-2, Groups:</p> <ul style="list-style-type: none"> <li>• system</li> <li>• interfaces</li> <li>• at</li> <li>• ip</li> <li>• tcp</li> <li>• udp</li> <li>• snmp</li> </ul> <p>ADS-TEC general MIB ADS-TEC firewall MIB</p>
<b>Modbus/TCP</b>	<p>The native Modbus/TCP interface enables the control of the device by a PLC. The following functions are imaged in the registers: Cut &amp; Alarm, status request &amp; acknowledgment</p> <p>IPsec, on/off switchable generally</p> <p>OpenVPN, separate status request and activation / deactivation of the 10 possible OpenVPN connections</p> <p>Much more options are available if Java /OSGi is used with a Java based Modbus/TCP stack on the device.</p>
<b>Eventlog/Syslog</b>	<p>Eventlog can be sent to syslog server</p> <p>Eventlog can be sent to an email address periodically</p> <p>Eventlog visible via webinterface</p>
<b>Client Monitoring</b>	<p>Monitoring of TCP/IP terminals by means of ICMP:</p> <ul style="list-style-type: none"> <li>• Limit values for packetloss and delay are configurable</li> <li>• In case of violation of the limit values an eventlog input is generated</li> <li>• An email can be sent</li> <li>• CUT or ALARM can be released</li> </ul>
<b>Remote Capture</b>	<p>Remote capture interface for usage with Wireshark. Allows packet analysis with Wireshark through „rpscap“.</p> <p>With this feature you can use every interface on the firewall as a remote capture interface on an additional diagnostics Windows PC.</p>

Signaling	
<b>Int. CUT Signal</b>	Releasing per: filter rule (possible rules targets: Cut & Allow, Cut & Reject), ICMP Client Monitoring alarm.
<b>Ext. CUT Signal</b>	WAN disconnect through CUT input signal.
<b>ALARM Signal</b>	Releasing per: filter rule (can be combined with all rules targets like: Reject, Cut, Allow, etc.), ICMP Client Monitoring.
<b>Ext. VPN KEY Signal</b>	Start / Stop OpenVPN connections by external input signal
<b>Acknowledging</b>	The internal signals can be acknowledged automatically with a configurable timer or manually via the web interface.
<b>RS232</b>	Integrated RS232 interface with SUB-D9 connector is available for complete control out of the JAVA/OSGi environment or via COM server.

Firewall Filter	
<b>Generally</b>	All filter rules are fast and easily configured with the web interface packet filter. 10 sub-rules per rule set are possible. The source and target interfaces must be defined firmly per rule set.
<b>SecureNow!</b>	With SecureNow! you can run an automatic analysis of the traffic passing through the firewall. It will then generate a set of firewall rules on Layer2 or on Layer3 for the traffic analyzed.
<b>Layer2 Filter</b>	Available Filter criteria: <ul style="list-style-type: none"> <li>• Source and target interfaces (Layer2, for example, OpenVPN, LAN,...)</li> <li>• Source and target MAC address</li> <li>• Ethernet protocol number</li> <li>• With VLAN: VLAN ID und VLAN QoS Tag</li> <li>• With IP: Source and target IP address &amp; network mask, IP protocol</li> <li>• With IP + TCP/UDP: Source and target ports, TCP flags or automatic configuration of the way back</li> <li>• Activities: Log, Drop, Accept, Cut, Alarm</li> </ul>
<b>Network groups</b>	Grouping of single IP addresses and network addresses to groups which can be used on Layer2 or on Layer3 filter rule sets.
<b>Hardware groups</b>	Grouping of MAC addresses to groups which can be used on Layer2 filter rule sets.

Prioritization and Traffic Shaping	
<b>Operating mode</b>	Traversing network traffic can be differentiated, prioritized and limited according to criteria
<b>Parameter</b>	Maximum 10 classes with priority 0-9 and respective maximum bandwidth Maximum bandwidth of interface Classes can be defined according to the following criteria: <ul style="list-style-type: none"> <li>• IP addresses</li> <li>• MAC addresses</li> <li>• Ethernet protocol number</li> <li>• VLAN criteria: ID &amp; QoS Tag</li> <li>• IP ToS Feld</li> <li>• IP Protocol</li> <li>• TCP/UDP Ports</li> </ul>

Miscellaneous	
<b>Date &amp; Time</b> <b>NTP Relay</b>	<ul style="list-style-type: none"> <li>• Three different remote NTP servers are configurable.</li> <li>• NTP server relay can be enabled to distribute the time in a local network.</li> <li>• Integrated RTC for high accuracy.</li> </ul>
<b>Configuration Backup</b>	Setups can be stored in files and read back
<b>Network Share</b>	Access up to 10 CIFS (Windows file share) network shares via one central mount point, provided by the router.
<b>USB to Serial converter support</b>	RS232 and RS485 USB to Serial converts with one of the following chipsets: FTDI, CP2101 or PL2303. Can be used from the Java/OSGi Extensions with the supplied RXTX library only.

<b>4G LTE (optional)</b>	
<b>LTE/HSPA+ wireless module</b>	Optional integrated LTE/HSPA+ multi-band wireless module (4G/3G/2G) for high speed wireless internet access.
<b>Standards</b>	<p>LTE: 3GPP Release 9  UMTS: 3GPP Releases 5, 6, 7, 8  GSM/GPRS/EDGE: 3GPP Release 99, GERAN Feature Package #1</p> <p>CDMA (Americas):</p> <ul style="list-style-type: none"> <li>– TIA/EIA/IS-2000.1 through .6. cdma2000® Standards for Spread Spectrum Systems. Release 0. April 2000</li> <li>– TIA/EIA/IS-2000.1-1 through .6-1. cdma2000® Addendum 1. April 2000</li> <li>– TIA/EIA/IS-2000.1-2 through .6-2. cdma2000® Addendum 2. June 2001</li> <li>– TIA/EIA/IS-95-B. Mobile Station-Base Station Compatibility Standard for Dual-Mode Spread Spectrum Systems. December 4, 1998</li> <li>– TIA/EIA/IS-. cdma2000® High Rate Packet Data Air Interface Specification. Nov.2000</li> </ul>
<b>Data speed</b>	Peak Download Rate: 100 Mbit/s Peak Upload Rate: 50 Mbit/s
<b>Frequency Bands</b>	<p>EMEA and Australia</p> <ul style="list-style-type: none"> <li>– LTE: 2100(B1),1800(B3), 2600(B7), 900(B8), 800(B20)</li> <li>– UMTS/WCDMA: 2100(B1),1900(B2), 850(B5), 900(B8)</li> <li>– GSM/GPRS/EDGE: Quad-Band (850/900/1800/1900)</li> </ul> <p>Americas</p> <ul style="list-style-type: none"> <li>– LTE: Band 2 (1900 MHz); Band 4 (AWS) (1700/2100 MHz); Band 5 (850 MHz); Band 13 (700 MHz); Band 17 (700 MHz); Band 25 (1900 MHz G Block)</li> <li>– CDMA EVDO Release 0 and EVDO Release A: BC0 (Cellular 800 MHz); BC1 (PCS 1900 MHz); BC10 (Secondary 800 MHz)</li> <li>– UMTS: Band 1 (2100 MHz); Band 2 (1900 MHz); Band 4 (AWS 1700/2100 MHz); Band 5 (850 MHz); Band 8 (900 MHz)</li> <li>– GSM/GPRS/EDGE: Quad-Band (850/900/1800/1900)</li> </ul>
<b>Transmit power</b>	<ul style="list-style-type: none"> <li>• LTE Bands 1, 2, 3, 4, 5, 8, 13, 17, 20, 25: +23 dBm ± 1 dB; LTE Band 7: +22 dBm ± 1 dB</li> <li>• UMTS Bands 1, 2, 4, 5, 8 : +23 dBm ± 1 dB</li> <li>• GSM850 CS and EGSM900 CS : +32 dBm ± 1 dB (GMSK mode) +27 dBm ± 1 dB (8PSK mode)</li> <li>• DCS1800 CS and PCS1900 CS : +29 dBm ± 1 dB (GMSK mode); +26 dBm ± 1 dB (8PSK mode)</li> <li>• CDMA: Band Class 0 (Cellular) +24 dBm +0.5/-1 dB Band Class 1 (PCS) +24 dBm +0.5/-1 dB Band Class 10 (Cellular) +24 dBm +0.5/-1 dB</li> </ul>

<p><b>Antennas</b></p>	<p>2 antennas are included in the scope of delivery.</p> <p>Antenna gain and frequencies:</p> <p>0 dBi @ 790-960 MHz</p> <p>1 dBi @ 1710-2170 MHz</p> <p>3 dBi @ 2500-2700 MHz</p> <p>Polarisation: linear</p>	
<p><b>Operating Modes</b></p>	<ul style="list-style-type: none"> <li>• Permanent connection</li> <li>• Manual connection control via API</li> <li>• Fallback connection with active ICMP monitoring of target IP via Ethernet</li> </ul>	
<p><b>Requirements for separate external LTE antennas</b></p>	<ul style="list-style-type: none"> <li>• Antenna system: External multi-band 2x2 MIMO antenna system</li> <li>• 2 x SMA connectors, MAIN and AUX (AUX = Diversity/MIMO)</li> <li>• Coaxial cable: nominal impedance of 50 ohms, e.g. RG174</li> <li>• EMEA/Australia - Operating bands - Ant. 1: 791–960 MHz; 1710–1990 MHz; 2110–2170 MHz; 2500–2690 MHz</li> <li>• EMEA/Australia - Operating bands - Ant. 2: 791–960 MHz; 1805–1990 MHz; 2110–2170 MHz; 2620–2690 MHz</li> <li>• Americas - Operating bands - Ant. 1: 704–960 MHz; 1710–1995 MHz; 2110–2170 MHz</li> <li>• Americas - Operating bands - Ant. 2: 734–960 MHz; 1930–1995 MHz; 2110–2170 MHz</li> <li>• VSWR of Ant1 and Ant2: &lt; 2:1 (recommended); &lt; 3:1 (worst case)</li> <li>• Total radiated efficiency of Ant1 and Ant2: &gt; 50% on all bands</li> <li>• Radiation patterns of Ant1 and Ant2: Nominally omni-directional radiation pattern in azimuth plane.</li> <li>• Envelope correlation coefficient between Ant1 and Ant2:             <ul style="list-style-type: none"> <li>&lt; 0.4 on 791–894 MHz and 925–960 MHz bands</li> <li>&lt; 0.2 on 1805–1995 and 2110–2170 MHz bands</li> <li>&lt; 0.1 on 2620–2690 MHz band</li> </ul> </li> <li>• Mean Effective Gain of Ant1 and Ant2 (MEG1, MEG2): ≥ -3 dBi</li> <li>• Isolation between antennas: &gt; 10 dB</li> </ul>	
<p><b>GNSS specifications</b></p>	<ul style="list-style-type: none"> <li>• Frequency range: GPS: 1575.42 MHz; GLONASS: 1602 MHz</li> <li>• Assisted GPS (A-GPS) SUPL1.0</li> <li>• Assisted GNSS (A-GNSS) SUPL2.0</li> <li>• gpsOneXTRA 2.0 with GPS + GLONASS support</li> <li>• Satellite channels: Maximum 30 ch. (16 GPS, 14 GLONASS), simultaneous tracking</li> <li>• Protocols: NMEA 0183 V3.0</li> <li>• Acquisition time (= Time to first fix): Hot start: 1 s; Warm start: 29 s; Cold start: 32 s</li> <li>• Accuracy: Horizontal: &lt; 2 m (50%); &lt; 5 m (90%); Altitude: &lt; 4 m (50%); &lt; 8 m (90%); Velocity: &lt; 0.2 m/s</li> <li>• Sensitivity*: Tracking: -161 dBm; Acquisition (assisted, non-LTE): -158 dBm; Acquisition (assisted, LTE): -153 dBm; Acquisition (standalone): -145 dBm</li> <li>• *) Sensitivity is the lowest GNSS signal level for which the device can still detect an in-view satellite 50% of the time.</li> <li>• Operational limits: Altitude &lt;6000 m or velocity &lt;100 m/s. Either limit may be exceeded, but not both.</li> </ul>	
<p><b>GNSS host software</b></p>	<ul style="list-style-type: none"> <li>• GPS daemon: gpsd (<a href="http://www.catb.org/gpsd/">http://www.catb.org/gpsd/</a>)</li> <li>• Cycle time: 1 s</li> </ul>	

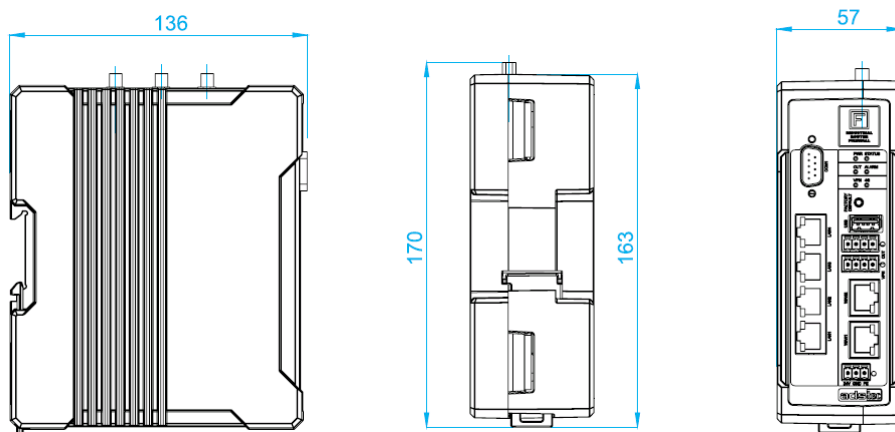
<b>GNSS connector</b>	<ul style="list-style-type: none"> <li>• DC bias on GNSS connector to support an external active GNSS antenna: max. 100 mA @ 3.3 V</li> <li>• Connector type: RSMA (female connector on the housing side, male connector with union nut on the cable side)</li> <li>• Coaxial cable: nominal impedance of 50 ohms, e.g. RG174</li> </ul>
<b>GNSS antenna requirements</b>	<ul style="list-style-type: none"> <li>• Frequency range: Narrow-band GPS: 1575.42 MHz <math>\pm</math>2 MHz (minimum); Wide-band GPS and GLONASS: 1565–1606 MHz (recommended)</li> <li>• Field of view (FOV): Omni-directional in azimuth; -45°...+90° in elevation</li> <li>• Polarization (average Gv/Gh): &gt; 0 dB</li> <li>• Free space average gain (Gv+Gh) over FOV: &gt; -6 dBi (preferably &gt; -3 dBi)</li> <li>• Gain: Maximum gain and uniform coverage in the high elevation angle and zenith. Gain in azimuth plane is not desired.</li> <li>• Average 3D gain: &gt; -5 dBi</li> <li>• Isolation between GNSS and LTE antennas: &gt; 10 dB in all uplink bands</li> <li>• Typical VSWR: &lt; 2.5:1</li> <li>• Polarization: Any other than LHCP (left-hand circular polarized) is acceptable.</li> </ul>



Hardware Specification	
<b>Ethernet accesses</b>	6 x RJ45 1000BaseTx FD: WAN1, WAN2 LAN1, LAN2, LAN3, LAN4
<b>Power Supply</b>	24 VDC <sup>*</sup> , max. 800mA @ 24 VDC NEC class 2
<b>Cut &amp; Alarm</b>	Software controlled disconnection of the WAN network connector with acknowledging of the event. Either triggered by an external signal or by means of filter rules. Outgoing signal triggered by a filter rule or ICMP monitoring. 24 VDC <sup>*</sup> input – for activation of Cut (external) & Alarm function, for example, with a SPS or per key switch (7V@3ma -36V@16mA) 24 VDC <sup>*</sup> alarm output for status signaling to a SPS or display (max. 1000mA)
<b>VPN Key &amp; Up</b>	24 VDC <sup>*</sup> VPN Key input signal for triggering VPN connections. (max 10mA) 24 VDC <sup>*</sup> VPN Up output signal for signaling a working VPN channel (max. 1000mA)
<b>SCM-Card Slot</b>	For ADS-TEC memory- and smartcards
<b>USB</b>	External USB 2.0 plug
<b>Housing</b>	Rugged aluminum die-cast case for top hat rail mounting VESA75
<b>Realtime Clock (RTC)</b>	Capacity buffered RTC integrated
	*) 7...36 VDC. For use in conformity with UL specifications: 7...30 VDC.

ADS-TEC Software Extensions	
<b>Java VM</b>	Java Virtual Machine supporting Java specification 1.3 and most parts of 1.4, 1.5 and 1.6
<b>Equinox OSGi Framework</b>	OSGi 4.2 Framework based on Equinox 3.8.2. The following OSGi bundles are prepared as extension: <ul style="list-style-type: none"> <li>• Java Modbus Library, Jamod from jamod.sf.net</li> <li>• RXTX, Java RS232/RS485 library from rtx.qbang.org</li> <li>• Simple HTTP server: Equinox javax.servlet.http 2.5.0</li> <li>• JSON RPC bundles: com.thetransactioncompany.jsonrpc and net.minidev.json</li> <li>• ADS-TEC Log2Eventlog</li> <li>• ADS-TEC configuration manager</li> </ul>
<b>SSH / SFTP</b>	Included with the OSGi extension <ul style="list-style-type: none"> <li>• SSH access the OSGi console</li> <li>• SSH port forwarding features are available!</li> <li>• SFTP access to the internal Flash storage for general data storage or OSGi bundle upload.</li> </ul>
<b>Hardware resources for Extensions</b>	Available for all extensions: <ul style="list-style-type: none"> <li>• ~110 MB RAM</li> <li>• ~55 MB SLC NAND Flash</li> </ul> The bare bone JavaVM OSGi environment will take about 30 MB RAM and 20 MB flash from these resources. PowerPC CPU with 666MHz, all extensions run with secondary process priority.

General Data	
External sizes	See dimensional drawings below.
Weight	Approx. 1 kg
Vibration	IEC 60068-2-6
Shock	IEC 60068-2-27
EMC	EN 61000-6-4 Emission standard for industrial environments EN 61000-6-2 Immunity for industrial environments FCC Part 15, class A
Operating Temperature	-20°C ... + 70°C
Storage Temperature	-20°C ... + 85°C
Humidity	5 ... 90% no condensation
Protection Class	IP 20 for switching cabinet mounting



OSGi™ is a trademark or registered trademark of the OSGi Alliance in the United States, other Countries or both.  
 Java™ is a registered trademark of Oracle and / or its affiliates.