Industrial IT

Industrial Router & Firewall IRF1000 series

Extended Technical Data Sheet

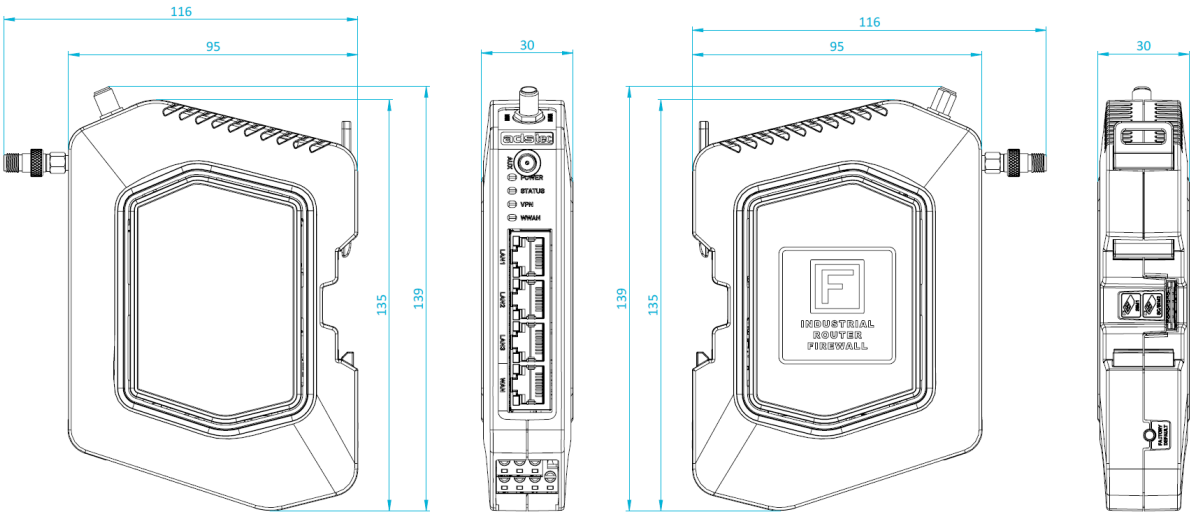
IRF14xx

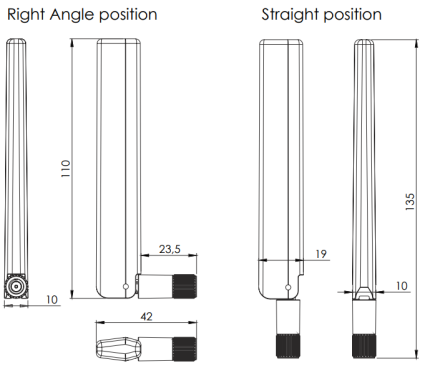
Variants	LAN	Wireless
IRF1401	4 x RJ45 100 Mbit/s	-
IRF1421	4 x RJ45 100 Mbit/s	LTE

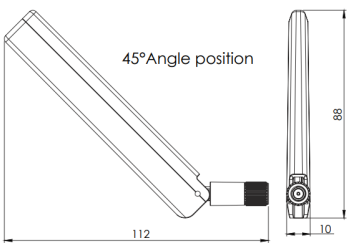
Hardware Specification	
Ethernet access	4 x RJ45 100BASE-TX
Power Supply	24 V +/- 20% Requirements for the power supply unit: • Class PS2 acc. to IEC 62368-1 – or – Limited Power Source (LPS) acc. to IEC 60950-1 • Short circuit current: < 8 A • For devices with UL approval: NEC Class 2
Current consumption	IRF1401: max. 0.5 A (12 W @ 24 V) IRF1421: max. 0.8 A (19.2 W @ 24 V)
Overvoltage category	I as per DIN EN 60664-1 (max. 1500 V)
Digital Input	24 V for, e.g., triggering VPN connections
SCM-Card Slot	For ADS-TEC memory- and smartcards
Memory Card (SIM)	Optional: Saves the complete configuration und enables easy replacement of the unit
WWAN	Optional: LTE via external antenna
Realtime Clock (RTC)	Supercap-buffered RTC integrated, approx. 1 week durability
Weight	Approx. 200 g
Vibration	IEC 60068-2-6
Shock	IEC 60068-2-27
EMC	ETSI EN 301 489-1 V2.2.3 ETSI EN 301 489-52 V1.2.1 EN 55032:2015 +AC:2016 +A1:2020 +A11:2020 EN IEC 61000-6-2:2019
Operating Temperature	-30...+70 °C
Storage Temperature	-40...+85 °C
Pollution degree	2 as per IEC 61010-1
Altitude during operation	2000 m or less
Humidity	5 ... 90 %, no condensation
Protection Class	IP30 for switching cabinet mounting
Fastening method	35 mm DIN-rail mounting

Technical data

External dimensions







Technical data

Industrial IT

Configuration and Monitoring	
Web interface	• Online help tooltips for all important options • German/English language support • Access via HTTPS • Free definition of unlimited user accounts with detailed access (write) control for any configuration option • Custom Menu configurable
SNMP	Protocols: SNMPv3 SNMPv3 read and write username/password and Pre-Shared-Key are configurable Supported SNMP MIBs: MIB-2, Groups: • system • interfaces • at • ip • tcp • udp • snmp ADS-TEC general MIB ADS-TEC firewall MIB
API	Software APIs from JSON RPC 2.0 to low level “adsdp” suitable even for microcontrollers
Modbus/TCP	The native Modbus/TCP interface enables the control of the device by a PLC. The following functions are imaged in the registers: Cut & Alarm, status request & acknowledgment IPsec, on/off switchable generally OpenVPN, separate status request and activation / deactivation of the 10 possible OpenVPN connections
Eventlog/Syslog	Eventlog can be sent to syslog server or accessed via web interface
Auditlog	**Anomaly:** Detects and records network anomalies (e.g. ARP spoofing, IP conflicts) **Configuration:** Logs all configuration changes for full traceability of administrative actions **Device:** Records external interface events such as USB insert/remove and link state changes **Packet Filter:** Logs forwarded traffic hits on firewall rules with audit enabled **Remote Service:** Tracks VPN requests and state changes for remote access monitoring **Authentication:** Records login attempts, session timeouts, and user logout events Auditlog can be sent to syslog server
Remote Capture	Remote capture interface for usage with Wireshark. Allows packet analysis with Wireshark through „rpcapd“. With this feature you can use every interface on the firewall as a remote capture interface on an additional diagnostics Windows PC.
Configuration Backup	Setups can be stored in files and read back
Reboot Scheduler	Timer can be set to reboot the device

Technical data

Industrial IT

Firewall/Filter	
Firewall in two Operating Modes	**Routing mode:** with stateful filtering of IPv4 traffic on two logical interfaces WAN and LAN, in this mode LAN is used as a 3 port switch and WAN as a single port interface **Transparent mode (bridged):** connects the ETH1 and ETH 2- 4 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 4-port switch is the result.
Firewall version	Stateful inspection
DNS based Filter	Host names can be used as Layer 3 filter criteria
Layer 2 Filter	Available filter criteria for transparent mode: • Source and target interfaces (Layer2, for example, OpenVPN, LAN,...) • Source and target MAC address • Ethernet protocol number • With VLAN: VLAN ID and VLAN QoS Tag • With IP: Source and target IP address & network mask, IP protocol • With IP + TCP/UDP: Source and target ports, TCP flags or automatic configuration of the way back • Activities: Log, Drop, Accept, Cut, Alarm
Network groups	Grouping of single IP or DNS based addresses and network addresses to groups which can be used on Layer2 or on Layer3 filter rule sets
Hardware groups	Grouping of MAC addresses to groups which can be used on Layer2 filter rule sets

IP Addressing, Routing, NAT, and DHCP	
IPv4	• One IP address for management in transparent bridge mode, two IP addresses in IP router mode • NAT (Masquerading), e.g. for outgoing traffic • All interfaces can be configured as DHCP clients • The default gateway can be configured manually. • DNS with DHCP client according to RFC 2136 • PPPoE support for all IP interfaces for usage with DSL modems
IP Routing	Static net or host routes are configurable Dynamic routing according to RIPv2 and OSPF (basic functions) Log level can be configured additionally
IP Forwarding & Port Forwarding	Port Forwarding for TCP/UDP Ports or complete IP addresses using IP aliases. Including the following features: • Optional source or reverse NAT for forwarding to hide the original source. • Conditional source matching to enable a forward only for special addresses. • IP Forwarding with IP aliases on VPN channels like IPsec or OpenVPN to run additional virtual IPs on the VPN which will be forwarded to the local network. • No limitation on the number of forwards
1:1 NAT Network Mapping	Network mapping to resolve IP subnet conflicts by mapping complete IP subnets to virtual address spaces • Map a single IP subnet to a complete virtual address space • Directly couple two identical IP sub networks by mapping both to two different virtual address spaces • Keep real IP sub network for the viewpoint of VPN channels • Connect and map up to 3 identical IP sub networks with a single router
DHCP Server	DHCP server on WAN and/or LAN interfaces, DNS and gateway are taken over dynamically if an interface is configured as DHCP client

Technical data

Industrial IT

VPN Parameter	
Big-LinX	Big-LinX: Smartcard or Software certificate based OpenVPN with cloud services
OpenVPN	OpenVPN is an open source alternative to IPsec. The software is freely available for Linux, MacOS/X and Windows. • Configurable as TCP/IP client or server alternatively • Authentication with X.509 certificates • HTTP proxy tunnel support in client mode, proxy authentication: Basic, NTLM • Maximum of 10 different OpenVPN processes (client or server) • Each single configuration has a separate interface which can be used for packet filter rulesets Further supported OpenVPN parameters: • IP address assignment and assignment of static routes to OpenVPN clients • IP address acquirement from OpenVPN servers in client mode • OpenVPN tls-auth certificates can be uploaded via certificate management • Forwarding of local subnets to OpenVPN servers. This enables the server to present selectable temporary routes to the web interface user. • Radius Server authentication for Client authentication on server processes
IPsec Policy	IPsec Policies are mostly used to create VPNs with other VPN routers. • 64 different IPsec policies for Subnet-to-Subnet configuration or as a Road warrior IPsec Server • Every VPN policy can be configured as active or passive • IPsec can generally be started and stopped via Modbus/TCP. • Authentication via PSK or X.509 certificates • IPsec NAT traversal • IPsec Limit-MTU option • Hardware crypto engine for high data throughput
X.509 Certificate Management	Separate certificate management for verification of the validity of all existing certificates Upload function for client, CA, Open-VPN tls-auth and CRL certificates Preinstalled set of demo-certificates for quick function tests SCEP for automated certificate enrollment Automated self-signed device certificate for easy deployment via Sub-CA

Signaling	
Ext. “CUT” Signal	Depending on input: • Configure Filter Rules • Disable the WWAN / Cellular Modem • Disable the Uplink Ethernet Port WAN
Ext. VPN KEY Signal	Start / Stop OpenVPN connections by external digital input signal

Edge Gateway/IIoT Functions	
Industrial Internet of Things (IIoT)	Easy setup for datasets with support of multiple sources and targets • Modbus/TCP interface: Enables the status request and control of VPN channels. Enables ModbusTCP for data collection • Modbus/RTU interface: Enables Modbus/RTU interface for data collection • OPC/UA: Enables OPC UA for data collection • Big-LinX data push: Enables data push with ADS-TEC WWH to Big-LinX • MQTT: Enables the sending of data to a defined target by MQTT

Technical data

Industrial IT

Time Synchronization Services	
Date & Time **NTP Relay**	• Three different remote NTP servers are configurable. • NTP server relay can be enabled to distribute the time in a local network. • Integrated RTC for high accuracy.
NTP (NTS-KE)	• Authenticated and integrity-protected NTP communication • Secure key negotiation via TLS • Support for client, server, and relay operation

Edge Computing/Docker	
Docker Container Support	Integrated Docker environment for running containerized applications directly on the device. Support for standard-compliant Docker images
Rootless Docker	Secure container execution without root privileges using isolated namespaces
Docker Network Modes	Support for bridge, host, and user-defined networks for flexible and secure integration
Private Docker Registries	Connectivity to private image registries for secure deployment and version control of custom containers.
Container Management	Container management and control via web-based GUI and standard Docker CLI
Docker Peripherals	RS485

WWAN	
WWAN module	Integrated multi-band wireless module for high-speed wireless internet access: LTE EU or LTE USEMEA
Data speed	LTE EU: Peak download rate: 150 Mbit/s Peak upload rate: 50 Mbit/s LTE USEMEA: Peak download rate: 400 Mbit/s Peak upload rate: 150 Mbit/s
Frequency Bands	LTE EU: • LTE (FDD): Band 1 / 3 / 5 / 7 / 8 / 20 / 28 (23 ± 1 dBm) • LTE (TDD): Band 38 / 40 / 41 (23 ± 1 dBm) • UMTS (WCDMA): Band 1 / 5 / 8 (23 ± 1 dBm) • GSM / GPRS / EDGE: 850 (32.5 ± 1 dBm) / 900 (32.5 ± 1 dBm) / 1800 MHz (29.5 ± 1 dBm) LTE USEMEA: • LTE (FDD): Band 1 / 2 / 3 / 4 / 5 / 7 / 8 / 12 / 13 / 14 / 18 / 19 / 20 / 25 / 26 / 28 / 29 (Rx only) / 32 (Rx only) / 66 / 71 (23 ± 1 dBm) • LTE (TDD): Band 38 / 39 / 40 / 41 (23 ± 1 dBm)/ 42 / 43 / 48 (22 ± 1 dBm)UMTS (WCDMA): Band 1 / 2 / 4 / 5 / 6 / 8 / 9 / 19 (23 ± 1 dBm)
Antennas	LTE: 1 antenna is included in the scope of delivery. Peak Gain (typ.): 617-960 MHz: -1.1 dBi 1427-2690 MHz: 0.5 dBi 3300-5000 MHz: 0.3 dBi 5150-5925MHz: 1.6 dBi Polarization: Vertical (linear, vertical)

Technical data

Operating Modes	• Permanent connection • Manual connection control via API or SMS • Fallback connection with active TCP-Ping monitoring of target Hostname
Requirements for separate external LTE antennas	• Antenna system: External multi-band 2x2 MIMO antenna system • 2 x SMA connectors, MAIN and AUX (AUX = Diversity/MIMO) • Coaxial cable: nominal impedance of 50 ohms, e.g. RG174 • VSWR of Ant1 and Ant2: < 2:1 (recommended); < 3:1 (worst case) • Total radiated efficiency of Ant1 and Ant2: > 50% on all bands • Radiation patterns of Ant1 and Ant2: Nominally omni-directional radiation pattern in azimuth plane. • Mean Effective Gain of Ant1 and Ant2 (MEG1, MEG2): ≥ -3 dBi • Isolation between antennas: > 10 dB

ads-tec Industrial IT GmbH
Heinrich-Hertz-Straße 1
72622 Nürtingen
Phone +49 70222522-200
Fax +49 70222522-402
sales@ads-tec.de
www.ads-tec-iit.com/en