DESIGNED FOR SMALL REMOTE SITES THAT REQUIRE A SECURE CONNECTION TO A LIMITED NUMBER OF DEVICES

The iSEG RF-1031 offers security solutions for both M2M (Machine to Machine) and H2M (Human to Machine) traffic by incorporating a DPI (Deep-Packet Inspection) firewall, as well as a user-identity firewall.

The iSEG RF-1031 includes a distributed DPI firewall or monitoring all network traffic and managing physical and remote access control systems. The whitelist-based firewall is installed at every port for both Serial and Ethernet traffic. Each SCADA protocol packet is validated by the firewall for source, destination, protocol and packet content.

The firewall’s two states (Monitoring and Blocking) allow blocking suspicious traffic or just monitoring, in addition to triggering an alarm at the control center.

The iSEG RF-1031 supports VPN tunnels for secure inter-site connectivity with IPsec, DMVPN, mGRE tunnels (among others) with key management certificates, supporting layer-3 services.

In addition, the iSEG RF-1031 fully supports L3 switches (VLANs, Routing, etc.) for Ethernet and serial ports.

The iSEG RF-1031 offers a built-in APA (Authentication Proxy Access), for compliance with the NERC CIP V6 requirement for identifying and granting privileges to users prior to granting network access.

Once validated, specific access is granted to predefined devices and functions, and each operation is logged. The iSEG RF-1031 is also integrated with a physical identity server system, for other authentication methods (e.g. magnetic card.)

Continued...
### SPECIFICATIONS

#### SECURITY
- Distributed DPI Firewall
- Profile-based firewall
- Security rules planning per service group
- Firewall modes: Monitoring, Enforcement
- IEC 104 DPI Firewall
- Modbus TCP DPI Firewall
- DNP3 TCP DPI Firewall
- S7 TCP DPI Firewall
- **VPN**
  - IPsec Certificates X.509
  - IPsec Dynamic Key Exchange
  - IPsec encryption AES, 3DES
  - L3 IPsec VPN policy based L3
  - IPsec VPN route based
  - L3 mGRE DM-VPN
- **Access control**
  - Access Lists L3, L4
  - NAT
  - User-based/Task-based access control for local devices via local APA (Authentication Proxy Access)
  - OS image encryption

#### INTERFACES
- 1 or 2 x RS-232 RJ45 Serial port
- 1 x RS-485 RJ-45 Serial port
- 1 x 10/100TX RJ-45 Ethernet port
- 1x100/1000 SFP Ethernet port
- Cellular Modem with dual SIM for HSPA + LTE/CDMA 450MHz
- Discrete lines: 2 In, 2 Out
- Console

#### PHYSICAL DESIGN
- DIN rail mounting, optional wall mount
- Rugged enclosure - IP 30
- Fanless, self-cooling
- Wide range of ambient temperature: min. -40°C, max +70°C (-40°F to +158°F)
- Storage Temperature: min -40°C, max +85°C
- Operating humidity up to 90%
- Dimensions (HxWxD) 106 x 44.7 x 120mm
- Power consumption: 9W
- Power supply 9-60V
- DC IEC 61850-3 conformance
- MTBF 25 years

#### MANAGEMENT
- Console serial port
- Backup/Restore running config
- Conditioned/scheduled system reboot
- Remote management and upgrade
- TFTP/SFTP Client
- Safe Mode
- Syslog

#### PROTECTION
- Protection over wired and cellular connections
- Protection between Cellular ISPs (SIM cards backup)
- Conditioned/scheduled system reboot

### NETWORKING
- **Serial**
  - SCADA gateway IEC 101/104 and DNP3
- **Routing**
  - Terminal Server Byte/Frame modes
  - Serial transparent tunneling byte mode
- **Switching**
  - Auto Crossing
  - Auto Negotiation IEEE 802.3ab
  - VLAN Tagging
- **Time**
  - Local Time settings
  - SNTP
- **Diagnostic**
  - Counters & statistics per Port
  - LED diagnostics
  - Ping
  - RMON
  - DDM

#### SPECIFICATIONS
- Typical implementation, with remote site access over redundant cellular networks

---

**About Radiflow**

Radiflow is a leading provider of industrial cyber security solutions for critical business operations. Our comprehensive portfolio of cybersecurity solutions empowers critical infrastructure and industrial enterprises to maintain visibility, control and security of their operational environment. Our intelligent threat management for Industrial cybersecurity minimizes potential business interruption and loss within your OT environment.

The Radiflow team consists of professionals from diverse backgrounds, from veterans of military cyber and communications units to former employees of leading players in the industry. Founded in 2009, Radiflow’s first solutions were launched in late 2011, validated by leading research labs and successfully deployed by major utilities worldwide. More at radiflow.com.