VALIANT COMMUNICATIONS

VCL-2243
RTU Firewall
IEC -104, IEC 61850, MODBUS Firewall

Introduction:

VCL-2243 is a high-security, high-reliability, ruggedized, failsafe transparent RTU Firewall that is designed to be installed between the RTU and the SCADA server without having to reconfigure any element of the network. VCL-2243 firewall supports IEC 60870-5-104 (IEC 104), IEC 61850 MMS protocol, MODBUS protocol options with extremely advanced features that may be installed to secure and protect RTUs (Remote Terminal Units) in critical infrastructure such as Sub-Stations, Smart Grid Distribution Systems, Oil and Gas Infrastructure and Railway Signalling Networks from being compromised, attacked, or accessed by hostile elements.

Ultra-Resilient and Failsafe – VCL-2243 RTU Firewall never itself becomes a point of failure. In the event of equipment or power failure, an external, dry-contact alarm is triggered and the incoming Ethernet link from the network is automatically bypassed from the firewall section and directly connected to the RTU. This ensures that the RTU always remains in service in any event. It is the only such firewall solution available in the industry that never, itself, becomes a point of failure.

The VCL-2243 secures RTU Terminals and corresponding central server(s) located in Load Dispatch Centre(s) / SCADA Management Centre(s) and Rail Traffic Control Room(s).

Protocols supported:

IEC 60870-5-104 (IEC 104):
10/100BaseT Ethernet Port

IEC 61850 MMS:
10/100BaseT Ethernet Port

MODBUS TCP/IP:
10/100BaseT Ethernet Port

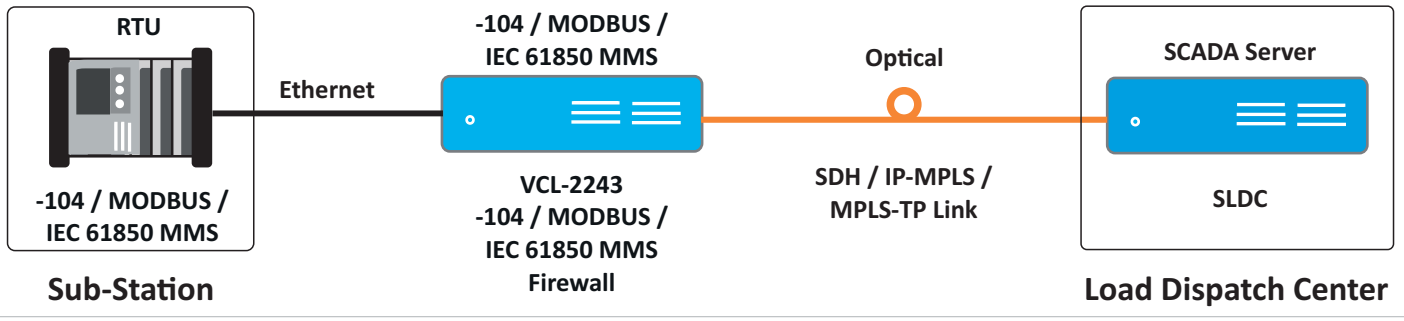
Access to the VCL-2243 RTU Firewall equipment is password protected that meet and exceed NERC requirements. VCL-2243 RTU Firewall can optionally be managed, centrally, from a RADIUS Server to provide enhanced levels of access security and centralized password authentication, management and control.

Application Diagram:

Versions and Technology Deployment:

- High-Security, High-Reliability, Ruggedized RTU Firewall
- Failsafe – Never itself becomes a point of failure, even in a power down condition.
- Transparent Firewall – No modification required in the existing network.
- Does not add any measurable latency. The latency added under full load conditions is less than 1ms.
- Installed in sub-stations to protect RTUs from network side intrusion and hostile access.
- MAC based lock. Allows user to lock to specified MAC addresses of known network devices in the utility network such as SCADA servers, and network management devices, computers etc. The RTU shall only accept or transmit data to known network devices in the MAC white-list.
- IP Address based lock. Allows lock to user specified IP address. The RTU shall only accept or transmit data to known network devices in the IP address white-list.
- Port based lock. Allows transmission only on user selected ports. Blocks communication and access on all other ports.
- Deep Packet Inspection. Allows only SCADA (-104/MODBUS/MMS) packets to pass through. Blocks all other packets.
- Comprehensive logging of all -104/MODBUS/MMS packets. Finger-prints and logs all unauthorized traffic and access attempts.
- Time keeping: Fetches time from NTP Server to maintain millisecond accuracy.

Failsafe – Never itself becomes a point of failure, even in a power down condition.



Applications:

- Utilities: Electric generation, transmission and distribution
- May be installed to Firewall RTU Terminals and server(s) located in Load Dispatch Centres / SCADA Management Centres and Rail Traffic Control.
- Smart Grid Distribution Systems
- Oil & Gas production, pipelines
- Railway Signalling Infrastructure: Rail Traffic Control Room(s)
- All distributed data networks consisting of a central server and multiple edge locations.

Interfaces - Terminal:

- Total Number of Ethernet Interfaces: 2
  - One, 10/100 RJ45 equipment interface for the local (trusted) RTU side
  - One 10/100 RJ45 network interface to the WAN (untrusted) network side
- Auto MDI/X (straight or crossover Ethernet cable correction)
- Management interfaces:
  - Ethernet, RS-232, RS-485, USB

Monitoring and Access Control:

- Password Strength Monitor
- Device Management and Alarm Monitoring
- Command Line Interface – Telnet, SSH
- SNMPv2 Alarm Monitoring
- Alarm condition detection and reporting (traps and SNMP alarm table)
- Syslog

Firewall - Features and Capabilities:

- Protocols supported:
  - IEC 60870-5-104 (IEC 104)
  - MODBUS TCP/IP
  - IEC 61850 MMS
- Lock to user specified MAC addresses.
- Lock to user specified IP address.
- Allows transmission of only -104, MODBUS, MMS packets.
- Port based lock. Allows transmission only on user selected ports. Blocks access on all other ports.
- Deep Packet Inspection. Allows only SCADA (-104/MODBUS/MMS) packets to pass through. Blocks all other packets.
- Per-frame/packet authentication
- Firewall
  - Port (Soft) based
  - MAC based
  - IP Address based
  - IP Domain based
- White-List and Black-List options
  - White-List Exception allowed and blocks all other traffic by default (system default mode)
  - Black-List Exception blocked and allows all other traffic
- Seamless scalability
- Infrastructure neutral: maybe used with SDH, IP/MPLS, MPLS-TP networks
- Transparent to network and applications
- Easy installation and management

Power:

- 15V DC to 60V DC - DIN Rail Mounting
- Power: 1+1 Power Supply Option - 19-inch Rack Mounting
  - 85V DC to 250V DC
  - 100~240V AC, 50/60Hz
- Power Consumption: 15W at maximum load

MTBF:

- Per MIL-HDBK-217F: ≥ 27 years @ 24C
- Per Telcordia SSR 332, Issue 1: ≥ 32 years@ 24C

Firewall and Security:

- Secure Boot
- Firewall Security:
  - Inclusion Policy – Access Control based upon White-List IP addresses, MAC address and IP Domain
  - Exclusion Policy – Access Control based on Black-List
- Resistance to Denial of Service (DoS) Attack
- Encrypted Firmware Updates
- Non-volatile Access Log with capability to "fingerprint" all successful log-in attempts and keep a log of the IP and MAC addresses of all successful logins.
- SNMP trap generation, along with LED and external alarm indication
- Password Protection with password strength monitor
- RADIUS Password Authentication
- SSH (Secure Access Control) with encrypted Password Protection

Environmental (Operational):

- Operating Temperature: -20C to +60C (-4F to 140F) (Fanless, does not require any forced air cooling)
- Maximum Operational Humidity 95% R.H. (Non-condensing)

CE Compliance:

- Immunity as per EN 60255-26
- Low voltage directive as per EN 60255-27

Other Regulatory Compliances:

- RoHS
- Meets CE requirements
- Complies with FCC Part 68 and EMC FCC Part 15
- Telcordia GR-1089 Surge and Power Contact

Physical Dimensions:

DIN Rail Mount Version

- H x W x D: 72.0mm x 190.0mm x 177.0mm
- Weight: 1.5 KG

1U, 19-inch Rack Mount Version

- H x W x D: 44.0mm x 484.0mm x 179.0mm
- Weight: 3.5 KG

High-Security, High-Reliability, Ruggedized RTU Firewall

EMI, EMC, Surge Withstand and other Compliances: Terminal Equipment

EN 50081-2	EN 50082-2	IEC 60068-2-29
IEC 61000-4-6 (Conducted Immunity)	IEC 60068-2-6	IEC 60068-2-2
IEC 60068-2-78	IEC 60068-2-1	IEC 60068-2-14
CISPR 32 / EN55022 Class A (Conducted Emission and Radiated Emission)		
IS 9000 (Part II Sec. 1-4, Part III Sec. 1-5, Part IV, Part 14 Sec. 1-3)		
IEC 60870-2-1	IEC 61000-4-2	IEC 61000-4-5
IEC 61000-4-3 (Radiated Immunity)	IEC 61000-4-4	IEC 61000-4-8
IEC 61000-4-10	IEC 61000-4-11	
Telcordia, GR-1089 Surge and Power Contact		

Ordering Information:

Part #	Description
VCL-2243-DIN	VCL-2243 RTU Firewall IEC 60870-5-104; MODBUS; IEC 61850 MMS Protocol Options* – DIN Rail Mount Version – Power Supply: 15V to 60V DC * Protocol options are required to be ordered separately. * Only one protocol option may be order with each unit.
VCL-2243-C	VCL-2243 RTU Firewall IEC 60870-5-104; MODBUS; IEC 61850 MMS Protocol Options* – 19 Inch Rack Mount Version – **Power Supply Options (add power supply option, as provided below) *Protocol options are required to be ordered separately. *Only one protocol option may be order with each unit.

* Power Supply Options:

Part #	Description
LV DC	15V to 60V DC
HV DC	85V DC to 290V DC
ACV	90V AC~240V AC, 50/60Hz

Revision 1.7 – May 24, 2021

U.K.
Valiant Communications (UK) Ltd
Central House Rear Office,
124 High Street, Hampton Hill,
Middlesex TW12 1NS, United Kingdom
E-mail: gb@valiantcom.com

U.S.A.
Valcomm Technologies Inc.
4000 Ponce de Leon Blvd.,
Suite 470, Coral Gables,
FL 33146, U.S.A.
E-mail: us@valiantcom.com

INDIA
Valiant Communications Limited
71/1, Shivaji Marg,
New Delhi - 110015,
India
E-mail: mail@valiantcom.com