

Remote I/O

Remote I/O panels shall be provided with pushbuttons, indicating lamps and hardwired annunciation system for local control/ operations.

Ethernet Specification

Networking (LAN) components:

Networking (LAN) components including switches, Firewall, fibre optics cable, other cable as required, jack panel with wire manager, patch cord, coupler, rack with all accessories, connectors, port, etc. shall be supplied.

A) The Industrial graded, IEC 61850-3 Std compliant, Managed Ethernet Switches shall meet following minimum requirements:

- i) 48 X Gigabit Ethernet Port
- ii) 24 or 48 x 10/100/1000 Base TX ports (STP)
- iii) SNMP, RMON, VOIP, VLAN, Multi link Trunk support
- iv) Broadcast/multicast storm control
- v) Supervisor Engine redundancy capability
- vi) Redundant Power Supply
- vii) Extra expansion slots for future up gradation.
- viii) Integrated Security features (IPS, ACL, Firewall)
- ix) 10 GB module support for future upgradeability

Expandability/stackability through a dedicated high speed expansion port.

Routable, remotely manageable, configurable.

One intelligent SNMP manageable mini-UPS for 30 minutes backup shall be provided with all accessories and software.

B) Secondary switches shall have the following features:

- i) 24 or 48 X 10/100/1000 Base TX ports (STP)
- ii) 2 or 4 X Gigabit Ethernet Port
- iii) SNMP, RMON, VOIP, VLAN, Multi link Trunk support.
- iv) Support for stacking with high throughput
- v) Broadcast/multicast storm control

C) The Firewall shall meet following minimum requirements:

Firewall appliance shall facilitate multi-vendor, multi-application environment and shall support third-party products on open alliance. It shall support Active-Active configuration.

i) The firewall shall contain following features:

- a) Stateful inspection of packets.
- b) NAT functionality, including dynamic and static NAT translations
- c) Latest version of SNMP

ii) The firewall must send log information to a separate log server via an encrypted connection. Firewall logging must not impact firewall performance.

iii) Remote network access to the firewall shall only be possible through the administration interface.

iv) The firewall administration station must be capable of pushing firewall security policies and configurations to individual or multiple firewalls through a secure, encrypted connection to the firewall administration interfaces.

v) Graphical User Interface (GUI) and a Command Line Interface (CLI) for making changes to the firewall rules set shall be provided. (Access to the firewalls via the GUI or the CLI must be through an secure encrypted channel).

vi) Any changes or commands issued by an authenticated user shall be logged to a database configured on any of the machines in the LAN. The administration station must allow for a hierarchical architecture for rules set administration and viewing of firewall configurations Management.

vii) The firewall must not support any unencrypted means of access to the firewall.

viii) It shall Monitor ALL network traffic-traffic at Firewalls (Internet and external networks), in the DMZ and detect known threat through deep packet inspection.

ix) Detects unknown threats via anomaly scanning.

x) Detect unknown threats via behavior pattern to protect from zero day attacks.

xi) Keeps up-to-date on new threats and vulnerabilities.

D) Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)
Features:

In order to inspect all inbound and outbound network activity and identify suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system on the Station LAN Network, the recommended IDS/IPS shall contain the following combined features. Any feature can be selected depending on whether it is to be configured as IPS or IDS.

i) Able to analyze, detect and report on security related events.

ii) Able to inspect traffic and to drop malicious traffic based on the configuration of security policy.

iii) Able to inspect the content of network packets for unique sequences/signatures.

iv) Able to detect and prevent known types of attacks such as worm or Trojan infections and hacks.

- v) Able to prevent denial of service (DOS) and Distributed Denial of Service attacks.
- vi) Able to prevent abnormal behaviors by monitoring and learning normal network behaviors.
- vii) Keeps up-to-date on new threats and vulnerabilities.
- viii) Shall provide user friendly interface to queries and reports on threats and event data so that security administrators can gain a better understanding of their ability to protect their network.
- ix) Shall provide detailed activity logs for auditing.
- x) Able to detect known threats via deep-packet inspection.
- xi) Able to detect unknown threats via anomaly scanning.
- xii) Able to detect unknown threats via behavior pattern to protect from zero day attacks.

UPS signal IO List

The following minimum hardwire/software signal shall be provided between UPS and PLC. These analog & digital signals shall be updated in HMI MIMICS.

- a. Main I/P 1, 2 alternate I/P voltage, currents.
- b. After line transformer -1&2 voltages
- c. DC O/P VOLTAGE, current and battery charging , discharging currents,
- d. Inverter o/p voltage, current.
- e. Static switch main I/P, alternate i/p voltage.
- f. SCVS O/P VOLTAGE, CURRENT, HZ
- g. UPS-1 & 2 –KVA, KW o/ps
- h. ACDB -1&2 VOLTAGE, CURRENT
- i. UPS-1,2 –POWER FACTOR