SEL-751A Feeder Protection Relay



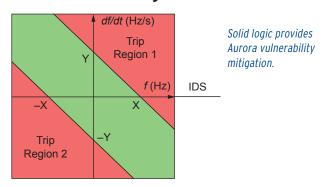


Aurora Vulnerability Mitigation

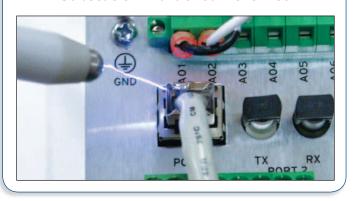


- Meets all NERC Aurora recommendations for hardware mitigation device (HMD)
- 81RF element quickly detects islanding
- Faster than conventional frequency element

Aurora Islanding Detection Scheme



Substation-Hardened Ethernet

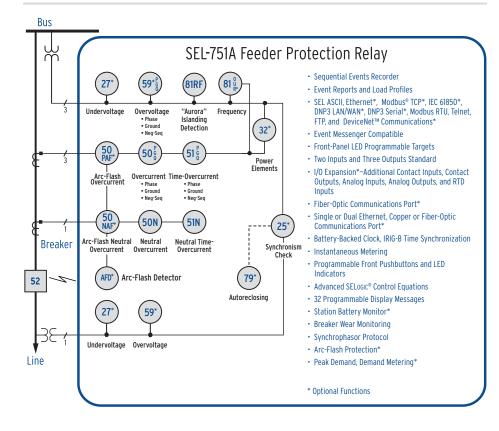


Industry-Leading Quality, Reliability, and Service





Functional Overview



Ordering Options

- Single or dual, copper or fiber-optic Ethernet port(s), Modbus® TCP, DNP3 serial and DNP3 LAN/WAN, FTP, Telnet
- IEC 61850
- DeviceNet™
- EIA-232 or EIA-485 communications
- · Fiber-optic serial port
- Additional EIA-232 or EIA-485 port
- Analog I/O (4 AI/4 AO, 8 AI)
- Digital I/O (4 DI/4 DO, 8 DI, 3 DI/4 DO/1 AO)
- Voltage options, including monitoring package inputs (three-phase voltage input, synchronism-check input, station battery monitor input), aurora islanding detection (81RF element), advanced monitoring and protection, four-channel, fiber-optic AFD inputs and protection
- 10 RTDs
- Conformal coating for chemically harsh and high-moisture environments
- Multishot reclosing
- Configurable labels

Feature Overview

Available with "Aurora" islanding detection (81RF element).

Large 2 x 16 character liquid crystal display.

Use default messages, or program up to 32 custom display labels.

Use default pushbuttons, or program your own pushbutton actions and labels.

Front-panel LEDs can be programmed to indicate custom alarms.





Aurora Attacks

An Aurora event involves intentionally opening a breaker and subsequently closing it out of synchronism to damage generators, motors, and transformers. Out-of-synchronism closing may cause severe stress on the shaft of rotating equipment as well as high currents through transformer windings. The mechanical stress reduces the life of the power apparatus and, in the worst cases, causes their destruction. SEL technology-leading security products mitigate the Aurora attack and lock out malicious hackers.

Aurora Vulnerability

While the likelihood of a successful Aurora attack is low, it is a risk that can and should be evaluated and mitigated. By initiating proper and prudent security measures and protection schemes, the Aurora vulnerability can be minimized. Part of that solution can be an SEL hardware mitigation device (HMD). The SEL HMD provides the fastest detection and response of any isolation device on the market during Real-Time Digital Simulator (RTDS*) testing.

Aurora Mitigation

Evaluate your system for at-risk equipment, and determine access pathways, both physical and electronic. Select the most effective mitigation for the situation. Mitigation should include physical security and monitoring, SEL-encrypted communications links, secure password and login processes, and, if needed installation of an SEL HMD.





