Application Note AN2009-07

Cybersecurity With the SEL-1102 Computing Platform and N-Dimension Solutions™

John Harrell

INTRODUCTION

Cybersecurity solutions are an essential element for protecting systems that operate critical infrastructure. Utilities are finding that these solutions provide an effective means to reduce electronic vulnerabilities in critical communications systems. National and international research firms have identified threats and documented specific cases of real cyberattacks. In some cases, it cost hundreds of thousands of dollars to repair the damage.

To secure devices used in environmentally challenging substations or other remote field sites from potential cybersecurity attacks, a hardware platform needs to be hardened to the same standards as the protective relays that are being secured. The hardware platform needs to comply with the following standards: IEEE 1613, IEEE 37.90, and IEC 60255. The tough SEL-1102 computer satisfies these standards with its flexible design that can be implemented in a multitude of applications. Specifically, the SEL-1102 should be used as the hardware platform for cybersecurity appliances, such as the n-Platform 340S Unified Threat Management System from N-Dimension Solutions.

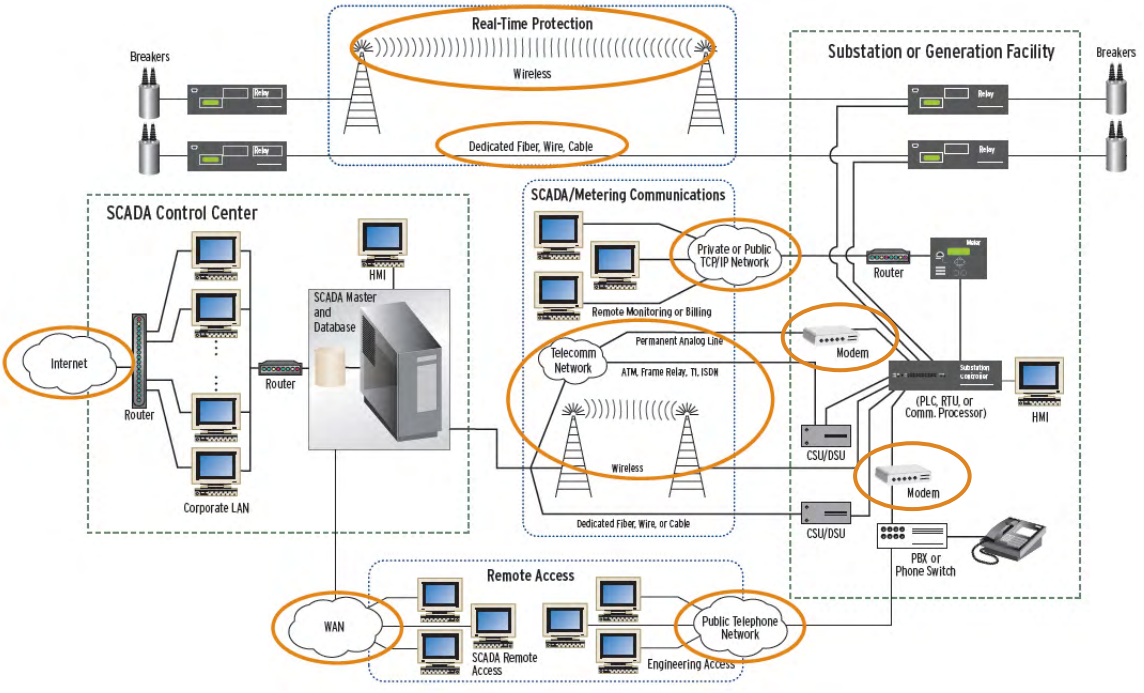

Figure 1 Typical Network Access Points to Consider Securing

SEL Tough Computer Hardware Platform Features

The SEL-1102 is the hardware platform of choice for tough cybersecurity solutions. Designed for reliability in harsh environments, SEL-1102 tough computer makes use of error-correcting memory and other technologies to achieve over ten times the mean time between failures (MTBF) of other typical industrial computers. This removes the need to constantly reboot and replace cybersecurity hardware platforms in the field.

Cybersecurity Solution

The n-Platform 340S is designed to work with the SEL-1102 hardware platform (see Figure 2), and together they facilitate the securing of environmentally challenging substations (see Figure 3) or other remote field sites from potential cybersecurity attacks. This appliance provides a comprehensive portfolio of network and security features that enable a critical infrastructure organization to implement strong security protection for critical control systems and networks, monitor those systems and networks for security vulnerabilities and potential intrusions, collect comprehensive log information about security-related actions and events, generate security reports, and facilitate North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) compliance reporting.

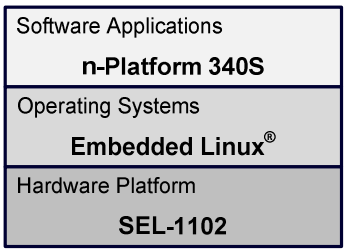

Figure 2 Hardware Software Stack Complete With Cybersecurity Solution

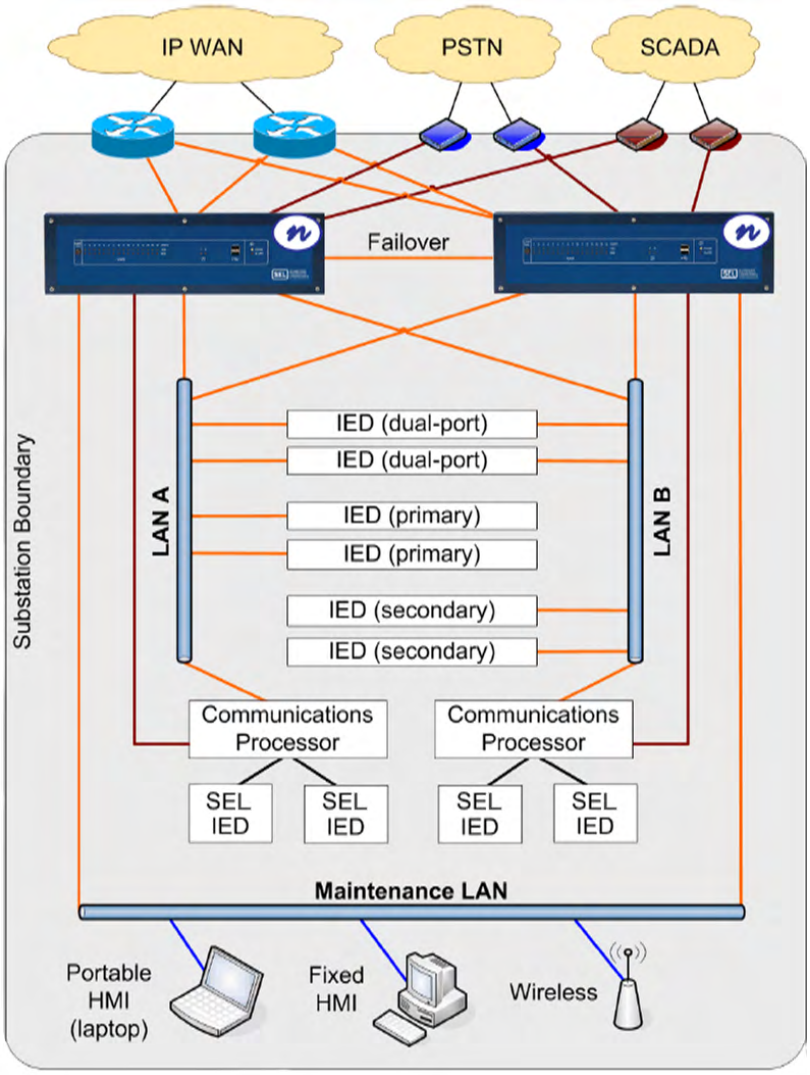

Figure 3 Substation Boundary Protected With n-Platform 340S

Gateway Mode Features

The gateway mode in the n-Platform 340S protects connections between networks, such as between the substation and the control center. The gateway mode features include the following:

- Routing
- Firewall
- Antivirus
- Proxy filter
- Network device control
- Virtual private network (VPN), including site to site, remote access, and serial SCADA (supervisory control and data acquisition)
- Lightweight Directory Access Protocol (LDAP) server for secure, centralized engineering access control of substations enabled with Internet Protocol (IP) or accessible via dial up (in development)

Surveillance Mode Features

The surveillance mode in the n-Platform 340S monitors network traffic and checks for any abnormalities that may cause instability of the interconnected infrastructure, such as indicators of potential cybersecurity attacks. The surveillance mode features include the following:

- SCADA intrusion detection system (IDS)
- Vulnerability scan
- Port scan
- Availability monitor
- Performance monitor

Administrative Features

Whether running in gateway mode or surveillance mode, the n-Platform 340S offers the following administrative features:

- Syslog and Simple Network Management Protocol (SNMP) for NERC CIP compliance reporting
- SCADA integration for security system status monitoring
- Domain Name System (DNS) server
- Dynamic Host Configuration Protocol (DHCP) server
- Network Time Protocol (NTP) server
- LDAP and Microsoft® Active Directory® service integration for administrative and VPN access
- Configuration via easy-to-use, browser-based GUI (graphical user interface)

LAN2009-07

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com