



WHITE PAPER

Secure and Reliable Utility Telecom Networks

**Strengthening Underlying Telecom Infrastructure in Today's
Risk-Sensitive Environment**

An Industry under the Microscope

In the aftermath of 9/11 and other international terrorist attacks, high-profile power blackouts in the U.S. and abroad, and simulated cyber attacks on critical infrastructure (e.g., the U.S. Department of Homeland Security's Aurora experiment and the large-scale, multinational Cyber Storm I & II exercises), the focus on utility infrastructure security and reliability in the U.S. and other countries has never been greater.

At the U.S. federal level, critical infrastructure protection is a primary objective within the National Cyber Security Division of the Department of Homeland Security, and the Department of Energy is using the National SCADA Test Bed to conduct vulnerability assessments. The Federal Energy Regulatory Commission (FERC) is also quite attuned to utility reliability, particularly within the electric power industry. FERC activities include reliability workshops, blackout task force initiatives, and power reliability policy initiatives.

At the industry level, the North American Electric Reliability Corporation (NERC) works closely with FERC and government entities in Canada to ensure the reliability of the bulk power grid in North America. With renewed emphasis on addressing cyber security and critical infrastructure protection, ongoing NERC initiatives include monitoring and enforcing mandatory standards compliance among utility operators (e.g., the CIP-002 through CIP-009 standards), streamlining the standards setting and review processes, long-term reliability assessments, and technical initiatives focused on improving system protection relay systems to slow or limit the spread of power outages. NERC and FERC have also established Violation Severity Levels to help determine monetary penalties for violations of mandatory electric reliability standards – penalties that can quickly escalate to millions of dollars per instance.

At a time when public utilities' vulnerabilities are making headlines and drawing the critical attention of the U.S. Congress, the energy sector faces greater scrutiny and, potentially, further regulation to ensure its resistance to sabotage and natural disasters. Similar efforts are underway outside of North America, such as the European Programme for Critical Infrastructure Protection.

While the scope of these initiatives goes well beyond telecom-related issues, they serve as a reminder of the intense scrutiny being applied to any area of utility operations, including telecom, which may harbor a weak link in terms of reliability and security. Reliability and security are not identical concepts, of course, but they are related: steps taken to improve one often improve the other, and vice versa.

In the context of utility telecom networks, security and reliability issues appear at essentially all major layers of the networking model. From application-layer viruses, "back-door" user log-ins, and firewall breaches, to potentially harmed physical communications links, utilities face a variety of exposures both old and new. This paper focuses on ways to strengthen security and reliability at Layer 1 – the province of leased lines and the transport equipment that shuttles data, voice, SCADA, and other traffic between points in a utility telecom network.

Interrelated Challenges

In a telecom transport network, security and reliability are related to system complexity and operational expense issues. Today, the energy sector's communications infrastructure represents a multi-vendor, multi-technology mix of subsystems with widely differing requirements and constraints, operating across a multitude of paths and communications technologies. Such complexity increases the number of potential failure points, lengthens troubleshooting procedures, inflates sparing requirements, strains management personnel and applications, and accelerates parts obsolescence problems.

As a result, operational costs are skyrocketing. Utilities must wrestle with managing, supporting, and tracking numerous concurrent communications technologies while improving the security and reliability of their networks – a challenge in the best of times and even more daunting in an environment of strained capital and operating budgets, smaller staffs, and greater oversight.

A case in point: Last-generation remote terminal units typically connect to an operations center over separate, dedicated communications facilities. To prevent an isolated event from causing catastrophic failure within the power grid, the power and utility industry has, over time, deployed any of several different technologies to ensure redundancy and security (e.g., differential relays, pilot relays, transfer trips). The end result is that utilities have inherited a staggering variety of widely differing communications technologies, representing diverse complexity and technological sophistication. Further, many such technologies were developed specifically to compensate for an unreliable communications infrastructure, making potential upgrade and replacement strategies even trickier.

Figure 1 illustrates the interdependencies of these challenges: complexity, security and reliability, and operational cost. For example, increased system complexity increases (a) reliability and security risks (e.g., by increasing the number of points of failure and points of vulnerability to hostile incursion) and (b) operational expense, replacing action with reaction.

Reducing complexity can improve reliability and lower operating costs. One attractive tactic is to consolidate multiple communication links (e.g., SCADA, telemetry, telephony) onto fewer facilities. This enables redundancy, simplifies network management, accelerates problem detection, and reduces recurring costs. Perhaps the greatest challenge in communications facility consolidation lies in continuing to meet the requirements of diverse energy sector applications. Any link(s) with consolidated traffic must maintain at least the current level of reliability, or operators risk incurring the stiff regulatory penalties imposed for power grid events and faults.

Multiple Layers of Protection

It is good strategy to implement one or more Layer 1 protection methods to achieve greater transport network security and reliability. These techniques are transparent to any higher-level protection schemes, yet they serve to strengthen all of them by enabling a more robust telecom foundation.

Hardware Protection

To conserve precious rack space in power substations and hub stations, utilities often deploy telecom equipment that combines multiple circuit interfaces onto a single card or module. This means, for example, that a single module failure affects several T1/E1 circuits (and all associated DS0s within them).

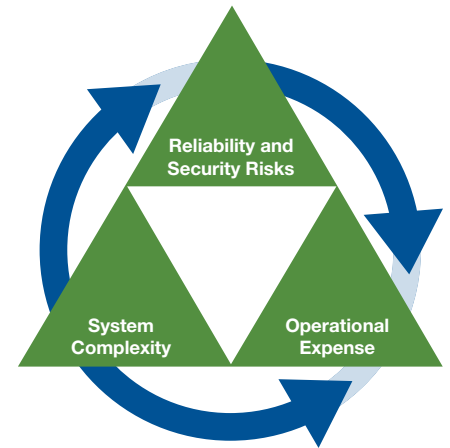
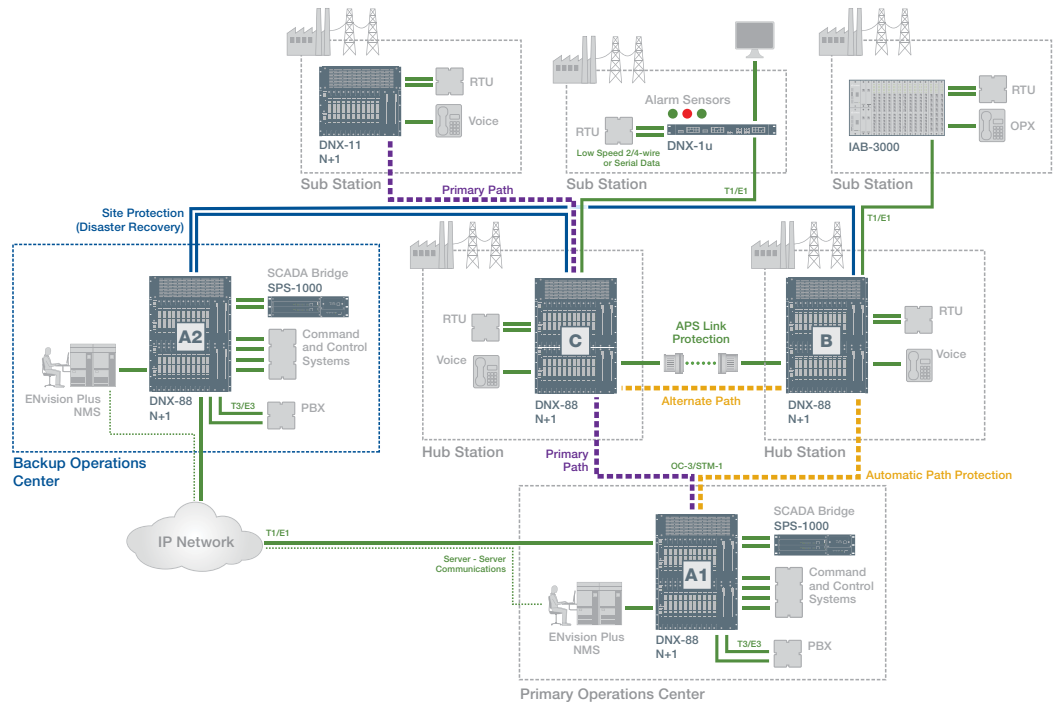


Figure 1: Utility network operators face interrelated trade-offs

Figure 2: A multi-layered protection architecture for utility telecom networks



To counteract this risk, some system designs offer a module protection feature. The chassis monitors the status of modules and, in the event of a failure, transfers all circuits associated with the failure to another module within the chassis.

Since a multiple-module failure is unlikely, such systems generally support 1: N redundancy, where a single module functions as standby for several primary modules. If one of the primaries fails, the system loads the failed module’s configuration onto the standby module and brings the standby online.

Hardware protection requires that the system remain adequately operational to (a) detect the failed module, (b) copy the configuration of the failed module to the standby module, (c) activate the standby module, and (d) switch connections to the standby module.

In Figure 2, hardware protection is represented by N+1 protection switches added to cross-connect platforms (e.g., DNX-11, DNX-88).

Link Protection

Utilities can also employ link protection, which triggers rerouting to another link when a single T1 or E1 fails. There are currently two ways to provide link protection:

- **1+1 Protection** – The most common mechanism allocates twice the number of required circuits, sending identical traffic down a back-up link for use in the event the primary link fails. Although arguably the most reliable form of protection switching, 1+1 also imposes the highest cost, by requiring a back-up facility for each protected link.
- **1:1 Protection** – A more efficient alternative, 1-for-1 is sometimes called traffic bumping or traffic preemption. When a protected link fails, the network element (e.g., cross-connect) transfers affected circuits onto another facility already in use, preempting lower-priority traffic on that link. This allows operators to specify traffic priorities for preemption, ensuring preferential access to available circuits for higher priority traffic.

Figure 2 shows link protection (automatic protection switching, or APS) as a back-up microwave facility between hub stations B and C.

Path Protection

One method of responding to localized failures is path protection. For purposes of this discussion, a path is essentially a route connecting two end points in a network, with or without intermediate nodes. Each pair of nodes along a path is connected via one or more communication links. As a system-level network configuration, path protection identifies ingress and egress points, but not specific paths and hops. This approach, long a staple of Layer 2 and higher packet switching and virtual circuit technologies, is now finding its way into Layer 1 physical layer (transmission) products.

In Figure 2, path protection is represented by the alternate path (A1 – B – C) activated when the primary path fails (A1 – C).

Site Protection

If utilities are to maintain high levels of availability, they must be able to respond to catastrophic site failures. In the event of a total site failure (e.g., lightning, fire, explosion, geological disaster), equipment and network management technologies available today can enable automated bulk moves of circuits from a failed site to a back-up (disaster recovery) site. This level of site protection requires an appropriately meshed network of communication links, and a high degree of centralized connection topology and system state awareness in network nodes and management systems. With these in place, it is possible to automatically and swiftly move hundreds or even thousands of network connections.

In Figure 2, site protection can automatically move traffic to the back-up operations site (A2) via the orange back-up links connected at hub stations B and C.

Role of the Network Management System

Path and site protection mechanisms require a management system with centralized knowledge of the state of the network, topology awareness, and the intelligence to make automatic rerouting decisions upon the occurrence of operator-defined events. Some systems offer this degree of sophistication and can truly be considered intelligent network management systems (NMS); others are better suited to traditional element management tasks, such as device configuration (i.e., EMS tasks).

Figure 2 depicts a topology-aware NMS in a redundant, active/standby configuration, deployed at both operations centers, to enable the definition and operation of path protection and site protection.

Evolving the Legacy Infrastructure

Utility networks built and expanded over decades use many interdependent technologies and applications. The challenge lies in how to add capabilities that improve security and reliability, while preserving elements of the legacy environment that are – at least for now – absolutely essential for continued operations.

Fortunately, network transport solutions exist for doing exactly that. They respect the installed base of multi-generational communications infrastructure by being *both* circuit friendly and packet friendly, yet simplify the network and add security and reliability that benefit every network-based application.

Equipment and Communication

Link Consolidation

Many of the redundancy and reliability approaches described above presume the availability of back-up links, devices, and paths. If a utility were to maintain separate communication facilities for all of the various elements in the network and then add redundancy/protection measures to each, the cost would be prohibitive.

In contrast, simply by cross-connecting and consolidating links where possible, utilities can realize the benefits of developing one set of reliable, redundant systems rather than many. This empowers network operators to select technologies and products providing the best combination of protection mechanisms – including hardware, link, path, and site protection – with functional integration that enables true consolidation. A few of today's digital access cross-connect switch (DACS) designs fulfill this requirement and offer additional features worth considering.

Rapid Trunk Conditioning

Designed specifically for utility telecom networks, rapid trunk conditioning allows a DACS to initiate T1/E1 trunk conditioning in less than 5 milliseconds (ms). Why is this important? Many power relay systems (e.g., transfer trip relays) rely upon audible spectrum tone generation for signaling. The presence (or absence) of audio tones at certain frequencies indicates the status of an element in the power grid. When the transfer relay activates, it signals a switchover within the power grid.

A challenge arises when a dedicated point-to-point link is replaced by DACS functionality. Telcordia standards specify that a DACS should “hide” a link failure for 2-3 seconds to prevent link bouncing. While this works for general telephony purposes, it can mean big problems for utilities. Power grid relays are sensitive to even very brief signal loss (often less than 100 ms). Rapid trunk conditioning enables the transfer trip application to respond appropriately, sensing a failure only of the communications medium and not a failure of the main power grid itself.

Remote Management

The best available products offer more comprehensive remote management technology compared to legacy telecom equipment. In fact, current-generation cross-connects usually include many optional remote management facilities – such as remote test access functions, terminal servers, dry-contact alarm fixtures, SNMP trap generation, and IP routing – for complete site management and monitoring. For instance, if a remote device fails and self-heals, the DACS should provide a mechanism to alert the operations center of the failure and initiate replacement procedures.

In contrast, typical infrastructure at utility substations and hub stations is woefully inadequate for remote diagnostics and configuration. With the current aging technology in place, it would be impossible to properly diagnose many catastrophic failures without on-site troubleshooting and repair. Replacing legacy equipment with feature-rich DACS platforms can translate to immediate network simplification and significant reductions in network downtime.

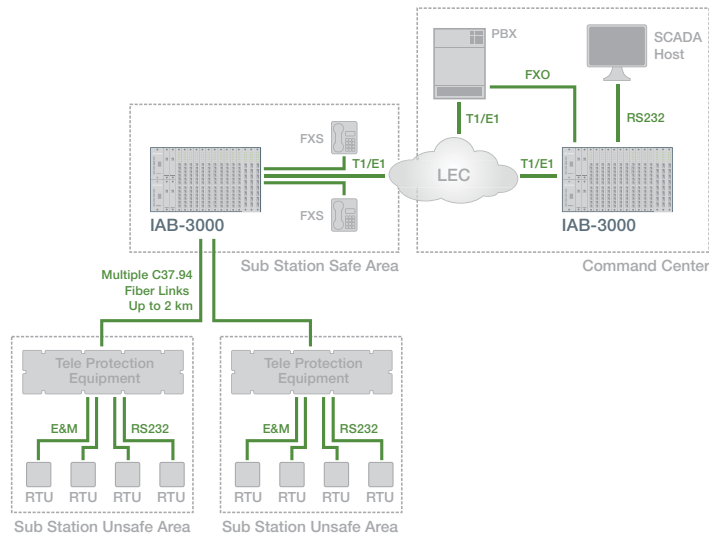


Figure 3: IEEE C37.94 optical technologies improve reliability of substation communications

Modem Data Bridging Capabilities

Poll-able SCADA systems using modem data bridging technologies are essential to utility operations and a source of concern in terms of potential reliability and security exposures. They are also at risk of being discontinued by vendors, even though they are critical elements of the legacy telecom infrastructure.

Some utility telecom solutions include modem data bridging functionality incorporated into the various Layer 1 protection methods discussed above. This approach ensures the continuation of important legacy applications while improving the security and reliability of SCADA infrastructure.

Avoiding Intra-Substation Link Dangers

In the high-voltage environments of electric utility plants, teleprotection equipment is used on communication links to quickly isolate faults and protect the network from failure and damage.

Historically, copper interfaces between the teleprotection equipment and multiplexers transferred critical information to the command center. These high-speed, low-energy signal interfaces are vulnerable to intra-substation electromagnetic and radiofrequency interference (EMI and RFI), signal ground loops, and ground potential rise (GPR) – all of which considerably reduce communications reliability during electrical faults.

Optical fibers do not have ground paths and are immune to noise interference, so optical data links provide a superior interface for intra-substation communications between teleprotection equipment and multiplexers. Replacing copper interfaces with optical fiber ensures isolation from dangerous GPR, prevents induced electrical noise, and eliminates the signal ground loops and data errors common to electrical connections.

The IEEE C37.94 Optical Interface Standard

The IEEE C37.94 standard defines the communication link between teleprotection equipment and digital multiplexers, via multimode optical fiber, as an interface that supports synchronous data at the rate of $N \times 64$ kilobits per second, where $N = 1, 2, \dots, 12$, up to 2 km distance. Many electric utilities are deploying C37.94-compliant solutions to achieve safer and more reliable data communication links in high-voltage substation environments.

Cost Considerations

A detailed discussion of cost implications is outside the scope of this paper. However, today's communications equipment solutions make it possible to take strong steps toward increasing network reliability and security while also reducing costs in key areas. Potential cost benefits include:

Reduction in Communications Facility Costs

Collapsing multiple T1/E1 or microwave links onto fewer facilities for SCADA, telephony, telemetry, and other data applications produces immediate and ongoing savings.

Equipment Consolidation

Collapsing channel bank(s), CSU/DSUs, routers, terminal servers, alarm panels, DSX patch panels, and BERT/loopback testers into a multiservice, multi-function DACS reduces overall equipment and sparing costs while minimizing rack space requirements, power consumption, and cooling loads.

Simplified Network Management and Troubleshooting

Consolidating equipment and communications facilities generally reduces the costs and time associated with system provisioning and maintenance, and problem determination and resolution. And today's best-in-class transport equipment goes a step further by providing remote test access features, telemetry functions, and other tools that help network operators remotely troubleshoot problems located within a substation.

An Ongoing Challenge

Utility network operators continue to own responsibility for enhancing network reliability and security in an environment that presents significant system complexity and cost containment challenges. Intelligent bandwidth management solutions can help in this effort, particularly within the telecom transport network. These solutions make it possible for utility operators to incorporate important layers of protection into their networks, consolidate generations of legacy equipment using a more manageable and secure architecture, add new capabilities, and realize overall cost-of-ownership savings. The approaches outlined in this paper represent solid steps toward upgrading the underlying infrastructure in ways that enhance reliability and security for all layers of the utility telecom network.

North American Electric Reliability Corporation (NERC)	www.nerc.com
U.S. Federal Energy Regulatory Commission (FERC)	www.ferc.gov
U.S. Department of Homeland Security (DHS)	www.dhs.gov
U.S. DHS National Cyber Security Division (NCSD)	www.dhs.gov/xabout/structure/editorial_0839.shtm
U.S. DHS National Infrastructure Protection Plan (NIPP)	www.dhs.gov/xprevprot/programs/editorial_0827.shtm
U.S. DHS Project LOGIIC	www.cyber.st.dhs.gov/logiic.html
U.S. Department of Energy (DOE)	www.doe.gov
U.S. DOE National SCADA Test Bed (NSTB)	www.oe.energy.gov/nstb.htm
The Center for SCADA Security	www.sandia.gov/scada/home.htm
Public Safety Canada – CIP Information	www.publicsafety.gc.ca/prg/em/cip-eng.aspx
European Programme for Critical Infrastructure Protection	www.libertysecurity.org/article718.html
Utilities Telecom Council	www.utc.org
Power Systems Engineering Research Center	www.pserc.wisc.edu/Resources.htm
The Critical Infrastructure Institute	www.ci-institute.org/

Sycamore Networks, Inc. • 220 Mill Road • Chelmsford, MA 01824-4144, USA • Phone: 978-250-2900 • Fax: 978-256-3434 • www.sycamorenet.com

Sycamore Networks, Inc. (NASDAQ: SCMR) is a leading provider of intelligent bandwidth management solutions for fixed line and mobile network operators worldwide. From multiservice access networks to the optical core, Sycamore products enable network operators to lower overall network costs, increase operational efficiencies, and rapidly deploy new revenue-generating services.

Sycamore assumes no responsibility for the accuracy of the information presented, which is subject to change without notice. Sycamore and Sycamore Networks are trademarks or registered trademarks of Sycamore Networks, Inc. in the United States and/or other countries. Copyright © 2009 Sycamore Networks, Inc. All Rights Reserved

