WHITE PAPER

ARCHITECTURE FOR SECURE SCADA AND DISTRIBUTED CONTROL SYSTEM NETWORKS

Comprehensive Network-Based Security for Control Systems

Table of Contents

Table of Figures

Executive Summary

Industrial control systems are an integral part of the critical infrastructures of electric, water, oil/gas, chemicals, pipelines, and transportation. The capabilities of networking these systems provide unprecedented opportunities to improve productivity, reduce impacts on the environment, and help provide energy independence. The Smart Grid is based on these networking capabilities. However, the same networking capabilities that can provide these benefits have also introduced cyber vulnerabilities that have resulted in these systems having been identified as one of the most vulnerable targets for the security of the United States. Consequently, various industry and government efforts have been initiated to address the cyber security of these critical systems.

Introduction

Systems controlling critical infrastructure for generating, transmitting, distributing, storing, and utilizing energy as well as for processes in manufacturing are no longer isolated. The drive towards networked industrial control systems is due to several factors. Integration of geographically distributed assets through centralized control improves agility in responding to supply and demand fluctuations, reduces cost of operations and enables process efficiencies unachievable in the past. For substations and pump-houses located in remote regions, network-based access reduces operational costs by enabling remote monitoring, debugging and maintenance. The ability to perform data gathering and audit-report generation from headquarters is central to keeping overhead costs of regulatory requirements in check. A fundamental need in many industries including power and Oil and Natural Gas (ONG) industries is for instantaneous access to current operational data. This could be the specific gravity of oil flowing in the pipeline at any instant or the amount of power being generated by a hydroelectric power plant. Access to such data in real time enables energy brokers to trade commodities based on the latest production numbers and can save billions of dollars for utilities and ONGs. Electric utilities are also required to provide real-time generation data to Independent Service Operators (ISOs) and other market entities. Many industries are also gravitating towards reducing the cost of physical security using IPTV and voice over IP (VoIP) to remotely monitor premises.

Industrial control systems were created as independent islands of networked devices. Over the past 10 years, such control networks have been rapidly adapted to provide access to and from corporate networks. While the mantra of "from the shop-floor to the boardroom" has created opportunities for process efficiencies and reduced overall costs, many industrial control system networks are now vulnerable to Internet-based threats. Remote access for employees, contractors and vendors is increasingly the norm for industrial control system network management, further exposing these systems to Internet-based exploits.

Industrial control devices are designed with significant consideration for hardening against environmental and physical threats. They are also designed with extensive forensics for physical parameters. However, since these devices were originally created to be deployed in non-networked environments, they have woefully inadequate security against Internet-based threats and few cyber-related forensics. Industrial control system devices typically use non-hardened networking stacks, common operating systems (DOS, Windows NT/2000, and Linux) and applications that are seldom patched after their initial deployment. As a result, such systems can easily fall prey to viruses, worms, and trojans. An assembly line shutdown at a Diamler-Chrysler plant (August 2005) due to the Zotob worm, and the Slammer worm infestation at First Energy's nuclear power plant (January 2003) present clear evidence of such issues.

It is important to realize the distinction between safety and security. While machines are built with several fail-safes to ensure safety, these fail-safes are designed against circumstances that have realistic probabilities of occurrence under normal operation. A cyber attack can skew the probabilities severely or mislead the operator into taking inappropriate actions by presenting false information. Such an attack can cause failures in areas that may never have been construed as practical issues. For example, fatigue failure is typically calibrated based on normal rate of startup and stopping. The same system could fail within a fairly short period of time, if the controller is hacked into and instructed to continuously vary the rotor speed slightly. A video released by the Department of Homeland Security shows a diesel power generator being destroyed as certain safety systems were overridden purely through a network-based attack.

A primary threat to industrial control systems that are connected to the corporate network (or the Internet) is from inside. Inadvertent mistakes, an infected laptop plugged behind the firewall or a disgruntled employee present a significant threat to the continuing operation of such control systems. In January 2000, a disgruntled contractor used a wireless link to break into the SCADA system for Maroochy Shire sewage. The perpetrator was able to intrude 46 times and release millions of gallons of sewage before he was caught by an unrelated traffic stop. The use of wireless continues to grow rapidly in control systems since the cost of cabling in an industrial setting can be as high as $3000 per foot. With wireless capable devices and backdoor (maintenance) accesses through modems, radio and cellular links, the proverbial perimeter has disappeared.

Securing Control Networks

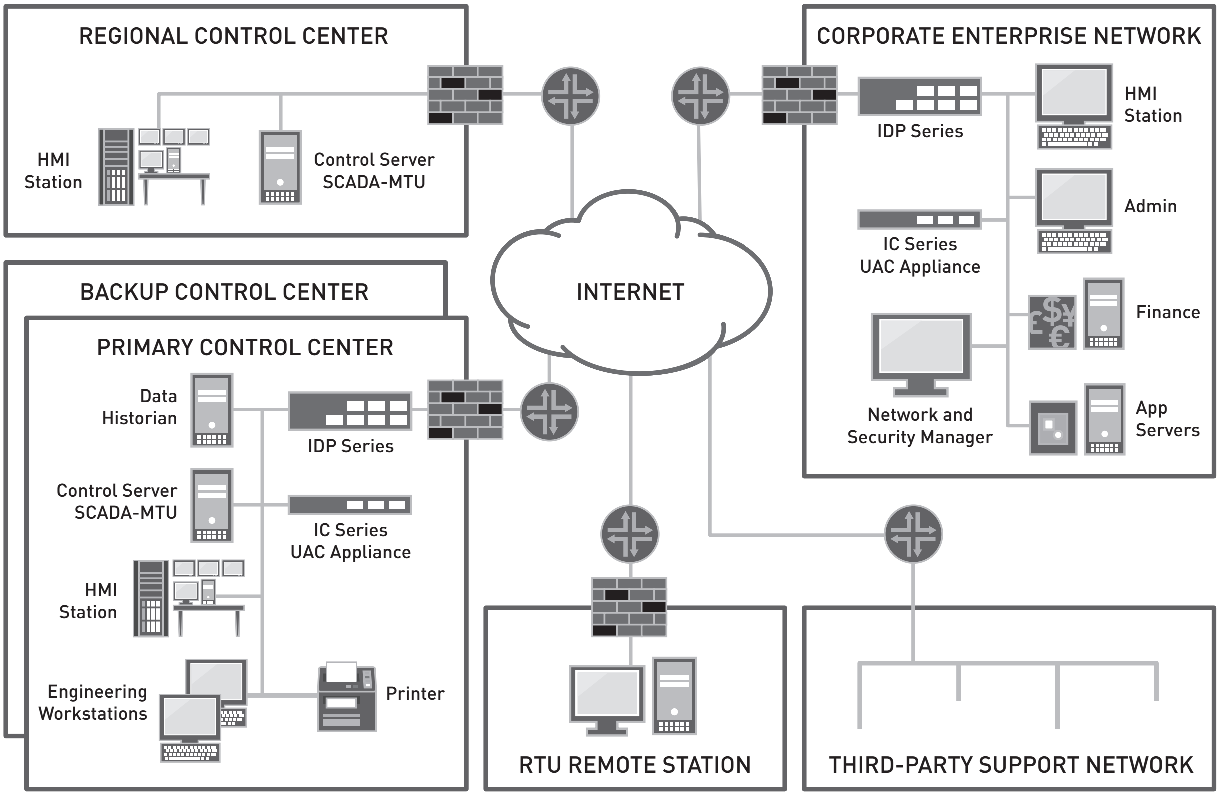

Figure 1: Typical electric SCADA network diagram

To address the security needs of control networks, it is essential to begin with a layered defense-in-depth approach that enables administrators to monitor the network at every level. Primary concerns for a control system network manager include:

- Assuring the integrity of the data
- Securing remote access
- Validating and authenticating every device and user on the control system network

A systematic approach to security begins with reducing the vulnerable surface of the industrial control system network. The first step is the creation of control system-specific policies that detail; which devices, what protocols and which applications may run on the network, who has access to these devices and from where, and what are the types of operations a user (or a role) is allowed to perform. The next step is to identify the appropriate locations to implement the policy. This could be through the appropriate configuration of controls on devices already present on the network, and by adding various network elements. Such network elements are required to create a security perimeter, provide additional enforcement points and segment the network for fault containment. The third step is to monitor the implementation of the policy to ensure these controls are effective, locate any violations and then feedback into the policy any corrections based on observed network behavior. Security is a continuous process and requires diligent monitoring, reviewing and adjusting to be effective. The following sections explain each of these steps and discuss existing technologies that can be used for securing typical control networks such as the one shown in the figure below.

Policy Creation

Policy creation begins with identifying assets that need protection and the requisite level of protection. On a control system network these are real-time servers, data historians, Human-Machine Interfaces (HMI) systems, Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), field devices, and peripherals such as printers and network switches. The primary vector of most concern is the compromise of communication that can alter the operation of field devices. In order to gain a foothold behind a firewall, attackers typically target non-essential appliances that are most vulnerable. Hence any network-enabled device on the control network must be considered critical for security. Since most servers on the control network run standard operating systems and applications, they must be guarded against common cyber threats. Such threats include intentional as well as unintentional Denial of Service (DoS) attacks through packet floods, irregular packets, protocol anomalies, buffer overflows, worms, trojans, and spyware. The policy must also ensure that malicious persons cannot easily tamper with controls they are not authorized to access. The probability of such incidents can be reduced significantly by ensuring access is restricted by user role.

In order to create a comprehensive policy, the network administrator (typically a role performed by a control systems engineer) needs a tool that can collate information from all subnets. Since a majority of the PLCs are vulnerable to active scans from tools like Nessus, passive scanning and identification is the only viable option to discover and identify all devices seen on the network. Juniper Networks® IDP Series Intrusion Detection and Prevention Appliances have a built-in profiler that logs all network activity into tables that provide information about device types, operating systems, protocols, applications and network peers. The profiler can be used to establish a baseline that can track the servers and control devices on the network, as well as the protocols and services those components use to communicate. By immediately locating new components on the network, an administrator can ensure that those components are protected and can track their status. The profiler uses passive fingerprinting to provide an inventory of operating systems and software applications, their versions, and what components use them. As new versions or security updates are announced, an administrator can determine if the network is affected, locate the affected components, and patch as appropriate.

Once devices, networks, applications and users have been identified, Juniper's network management system, Juniper Networks Network and Security Manager, can be used as a centralized management system to create and manage policies across all security devices. Through rule-based policies, an administrator can create policies tailored to the type of devices being protected on a particular subnet or VLAN. Such tailored policies improve efficiency while reducing the number of events an administrator has to address. For example, a Slammer worm attacking a Linux host is not a critical event. NSM also supports dynamic groups of attack objects. An administrator may choose a dynamic group based on operating system or protocol set such as SCADA, and stay up-to-date on protection without having to manually address each vulnerability.

Policy Enforcement

Establishment of a security perimeter, layered defense-in-depth, segmentation, authentication and authorization are essential components of an effective security policy. Industrial control system networks often lend themselves to segmentation by function. The industrial control system network must be segmented to isolate it from other less secure plant or substation networks, the corporate network, and other less secure networks, individual control centers, regional control centers, and possibly remote stations. Firewalls must be deployed to enforce a mutually untrusting policy at these subnet perimeters. Segmentation using subnets and firewalls helps in limiting the extent of damage caused by any cyber event. A firewall alone, however, is not sufficient, as has been shown by actual events and laboratory demonstrations. In order to protect applications, application-aware network devices such as IPS/IDS must be deployed. Since each application represents an attack vector, disallowing non-essential applications such as point to point, instant messaging, and video streaming improves the security posture of the industrial control system network. Such application level restrictions also require network enforcement elements that are application aware. Further, as applications and protocols become port agnostic, application-aware deep inspection devices such as the IDP Series complement and augment the firewall's ability to allow only permissible traffic. For example, while a firewall may open a hole for port 502, the IDP Series can ensure that all non-MODBUS traffic over that port is stopped.

A prerequisite to enforcing an access policy on an industrial control system is to have mechanisms for authentication and authorization. These mechanisms must verify a user's identity, provide access to devices based on that user's role and privilege level, and log all access attempts in order to audit any infringement. Most control system field devices such as RTUs and PLCs fall short on most of these basic security requirements. Industrial control system protocols such as OPC, MODBUS, and DNP currently have very weak authentication mechanisms. Further, such systems seldom provide adequate administration capabilities including granularity with role-based access (identifying specific users). A user has access to perform all operations with no restrictions once authenticated. Due to limited memory, most control devices do not keep or maintain logs of cyber events. This lack of logging has prevented actual cyber incidents from being analyzed and also keep electric utilities from meeting several of the NERC CIP logging and event monitoring requirements.

The policy must provision methods for secure remote access, and role-based access to assets and operations. An important requirement for incident forensics as well as regulatory compliance is the ability to establish the identity of users who made changes to the control systems. Knowing that it was the user named "supervisor" or "shift operator" is not sufficient.

Perimeter Security

Given the need to access control networks from the corporate network or in some cases from the Internet, it is essential to create a strong defense perimeter. A perimeter firewall must create at least three security zones—a secure zone for the control system network elements, a demilitarized zone (DMZ), and an insecure zone. Even if all access to the control network is through the corporate network, the perimeter firewall must treat the corporate network as insecure and have a mutually non-trusting policy. The DMZ contains secure access authentication devices, workstations, and servers that are accessible from the insecure network. Any device in the secure zone should be accessible only through one of the DMZ devices. By ensuring that the devices in DMZ are properly protected and continuously monitored, a control network administrator can significantly reduce the probability of a network-based attack. As previously mentioned, it is key that the perimeter device not only provide security zones and flow-based firewalls, it must also be aware of protocols and applications it is protecting.

Juniper Networks ISG Series Integrated Security Gateways are purpose-built firewall/IPsec VPN security solutions that can be used to secure control system networks. The ISG Series offers robust firewall capabilities, providing the first line of defense from network attacks. Additionally, it can be upgraded with full Intrusion Prevention System (IPS) support to secure the control system network from the latest exploits and attacks. The IPS capability is backed by Juniper's dedicated security team, which develops new attack signatures on a daily basis.

Identity Management and Rogue Device Mitigation

The most likely vector for an intrusion in a control system network is unintentional though inappropriate use. An employee or contractor may plug in his laptop to perform routine tasks without realizing that it has picked up a worm or spyware. The worm may then start scanning the control system network, and cause outages on devices such as PLCs due to unexpected traffic. This scenario is even more likely with the proliferation of wireless access points. Control over access points through authentication of every user and device is essential to ensure security within the perimeter.

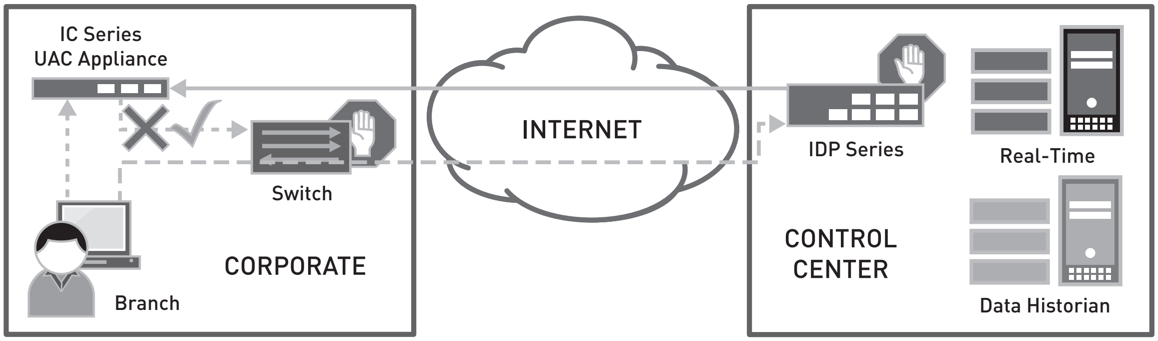

Figure 2: Identity management and rogue device detection and enforcement

Juniper Networks Unified Access Control combines user identity, device security, state and location information for session-specific access policy by user, enforced throughout the network. UAC is an open, standards-based solution built on field-tested, best-in-class security and access control products. With strong authentication supported by UAC, access to the network and resources within the network can be closely controlled. Control over the resources accessible by particular users can hinder the proliferation of worms and other malware, which may have been inadvertently introduced to the network.

One of the primary concerns in augmenting control system networks is to ensure there are minimal devices inline that may reduce the availability of the network. A combination of the IDP Series in sniffer mode and UAC enables the creation of policies that restrict access at the application level, while satisfying the requirement for being completely passive. For example, if a contractor sends a MODBUS write command to change PLC setpoints, the IDP Series can notify the UAC about this event. The UAC can then signal to any 802.1X compliant switch or firewall that the contractor's access must be terminated (or risk being quarantined). Meanwhile, an event is logged for administrators to follow up. The UAC minimizes the need for an administrator to create numerous access control lists (ACLs) across the control system network to provision appropriate level of access for each user. The IDP Series profiler can also provide usage information for every session on the control system network for compliance monitoring and forensics. In addition, the UAC can be deployed locally to the control center with federation of identities enabled from the corporate network to the control network. This allows control systems network administrators to have complete control over the allowed users and their access privileges regardless of their privilege levels on the corporate network without a dual sign-on.

Remote Access

Remote access is enabled for several reasons: a plant operator/engineer may remotely monitor equipment status, an ISO may need to collect current production data, or a vendor may have to diagnose and fix operational problems. In order to minimize the probability of unintentional misuse or tampering, users should be limited only to functions for which they are authorized. For example, a vendor logging in to update a patch must not be able to run any control system commands. If a contractor's laptop contains spyware, or his antivirus is not up to date, that contractor should not be allowed access to the control system network.

Juniper Networks SA Series SSL VPN Appliances are based on the Instant Virtual Extranet (IVE) platform, which uses SSL, the security protocol found in all standard Web browsers. The use of SSL eliminates the need for client-software deployment, changes to internal servers and costly ongoing maintenance and desktop support. Enhanced remote access methods enable the enterprise to provision access by purpose for virtually any resource. The level of access can also be dynamically adjusted to the condition of the remote access device, such as the timestamp of the most recent antivirus definition files.

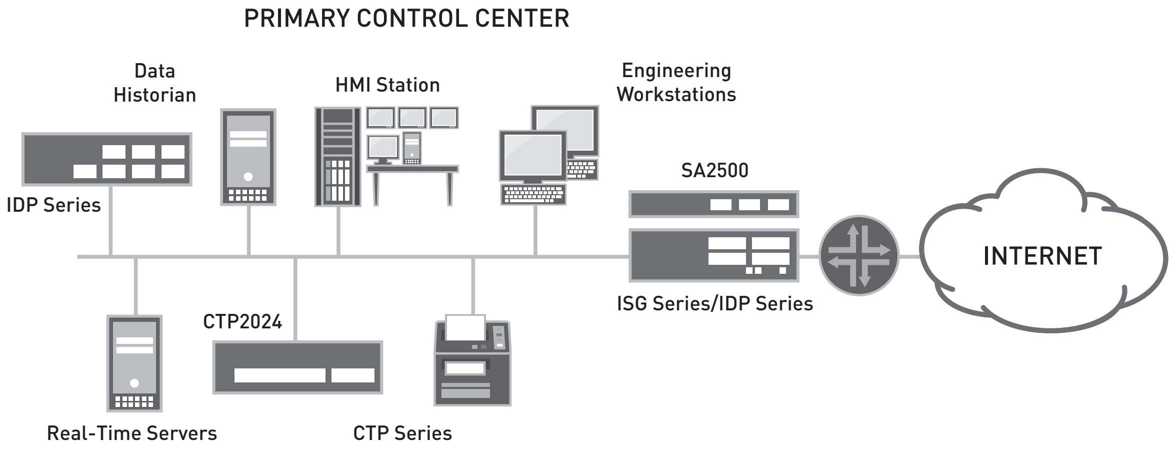

Figure 3: Adding secure remote access to control system networks

100 percent availability is essential for control system networks. This is typically achieved by having redundancy. An IVE device must be placed at the DMZ of each control center to ensure secure access is possible even if some portions of the control system network are inaccessible. Juniper Networks SA Series SSL VPN Appliances also provide coordinated threat control with the IDP Series appliance. As highlighted in the example with UAC, the IDP Series offers extensive layer-7 intelligence, which identifies protocols, applications and specific contexts within applications. This provides fine-grained control over privileges granted to a remote access connection.

Monitoring

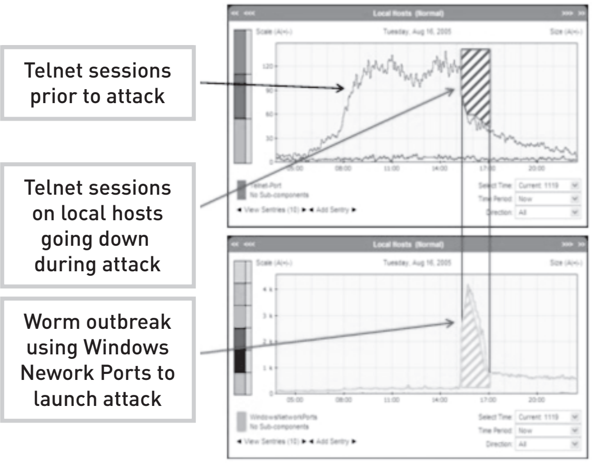

Figure 4: Cyber attack timeline and visibility

Once access policies are defined, firewalls, switches and intrusion prevention devices act as enforcement points as well as monitoring stations for flagging any policy violation. The IDP Series' profiling information combined with user information from the UAC and SA Series provides insight into who is using the network, what applications they are running and where they came from. The IDP Series profiler can provide session context at the granularity of individual control system protocol commands and the values being set. This information can then be used to create a baseline of expected communications. The administrator can establish a policy of acceptable communication and have the management system send an alert on any violations of policy. For example, a point-to-point connection initiated to/from the control system network, or an IRC command being sent to a machine designated as a real-time data collection server, could automatically trigger an alert and notify the control system network administrator of these policy violations. This process can be further automated by using Network Behavior Analysis (NBA) and Security Information Management (SIM) tools such as the Juniper Networks STRM Series Security Threat Response Managers.

STRM Series can keep track of the services running in the SCADA network and alert to any new services being deployed or changes in the behavior of the existing services. Changes to the network or behavior of existing services could indicate an attack has gained access to the equipment or that an employee may be using the systems inappropriately, causing a great deal of risk to the organization. The STRM Series can also monitor for other known attack vectors that may go undetected. These could include a system attempting to connect to known hostile hosts or networks, such as those known to run BOTNET command and control channels. STRM Series also prioritizes and correlates attacks on the SCADA network back to the country of origin, exposing attacks or risks from geographically sensitive areas.

By using the correlation available in the STRM Series, all the devices monitoring the SCADA network, such as IPS, firewalls and antivirus platforms, can be correlated together for a single operational view of the security state of the SCADA network. The STRM Series goes beyond the network and also monitors the application logs from the SCADA system, which may indicate certain attack vectors or even system failures.

The STRM Series, as well as third-party analyzers such SecureView or Arcsight, can provide additional features that add significant value to a complete security solution, including:

- **Historical Data:** Providing precise point-in-time data to support forensics for researching past events. Many solutions support detailed correlation between multiple events, allowing network managers and security professionals to establish the root cause of events.
- **Comprehensive Reporting:** Textual and graphical reports are a vital tool for communicating the status of security-related events to a broad range of personnel, including network managers, facility managers, as well as third parties such as regulatory officials. Third-party reporting solutions provide a framework for establishing consistent, measurable reporting metrics to key constituents.
- **Compliance Management:** With a myriad of ever-changing regulatory requirements, such as those issued by NERC, FERC, and NRC, as well as pending legislation, the ability to correlate implemented policies and controls to specific statements in regulations, best practices, and SLAs is critical. Juniper security solutions can integrate with third-party tools to map these policies and controls to specific compliance criteria, and provide evidence for auditing events.
- **Asset-Based Risk Management:** Knowing the importance—as well as the potential attack vectors—of devices and systems on control networks is an important first step in the process of securing these components. By establishing key criteria related to these assets, such as value, likelihood of specific threats being realized, and the potential consequence of those threats, network managers can establish security controls that are both effective and efficient.

Using Juniper's integrated security solutions coupled with third-party tools, managers of control networks can build a complete, effective, high-performance security system to fully protect SCADA networks against the full spectrum of accidental, intentional, natural, and man-made threats.

Meeting Federal Security Requirements

For the bulk electric industry, the reliability standards focus on physical and virtual systems whose disruption or destruction would impact the reliability of the bulk electric grid. The Nuclear Regulatory Commission has issued a cyber rule affecting all commercial nuclear power plants. Congress is working on additions to the Chemical Facilities Anti-Terrorism Standards (CFATS). Congress, the National Association of Regulatory Utility Commissioners (NARUC) are requiring cyber security standards for the Smart Grid. Lastly, all federal agencies are required to meet the Federal Information Security Management Act (FISMA) with the associated NIST Special Publication (SP) 800-53 control sets. To better regulate and assure adequate security for the nation's electrical grid, the U.S. Federal Energy Regulatory Commission (FERC) has approved the North American Electric Reliability Corporation (NERC) mandatory cyber security regulations for Critical Infrastructure Protection (CIPs) for protecting the national bulk power system, defined as NERC CIP-002 through CIP-009. These reliability standards focus on physical and virtual systems whose disruption or destruction would have a debilitating impact on security, national economic security, and national public health or safety.

The CIP program includes a national structure and a National Infrastructure Assurance Plan. It requires utilities to do the following:

- Identify critical assets to support reliable operation of the electric system
- Assess vulnerabilities to both physical and cyber attacks
- Plan to eliminate significant vulnerabilities
- Develop systems to identify and prevent attempted attacks—alert, contain, and rebuff attacks
- Be able to quickly rebuild essential capabilities as needed
- Provide auditable reports and incident response planning

The NERC CIPs link risk management and infrastructure assurance, providing the capability to eliminate potential vulnerabilities. With these concerns in mind, appropriately applying these mandatory new requirements can help utilities to improve control system security and identify appropriate investments to safeguard facilities now and in the future. It is expected that the Smart Grid may draw from this and NIST SP800-53.

Juniper's network-based security solutions assist utilities to meet NERC CIP requirements with a broad range of functionalities, including:

- Firewalls for stateful inspection, port and traffic awareness, and network transparency
- Juniper Networks IDP Series Intrusion Detection and Prevention Appliances to assess application, protocol, session, and traffic flow awareness; provide multiple detection methods and remediation; and passively profile and identify critical assets
- Juniper Networks Unified Access Control and SA Series SSL VPN Appliances for local and remote authentication and admission by roles and responsibilities
- Forensics analysis tools to provide event correlation, logging, reporting for full visibility
- Centralized, role-based security management

Based on these capabilities, Juniper helps secure SCADA networks by helping utilities accurately analyze the network, create business policies, implement security infrastructures, monitor policy enforcement, and educate employees in security practices.

NERC CIP-002, which focuses on Critical Cyber Asset Identification, requires the initial assessment and evaluation of cyber assets—ranging from control centers, transmission substations, and generation resources to backup systems for restoration, automatic load- shedding systems and facilities, and reliability systems. The IDP Series Profiler and Juniper Networks STRM Series Security Threat Response Managers provide plant managers with real-time network and security visibility—with embedded intelligence and analytics to identify hosts, operating systems, applications, and behavior anomalies.

CIP-003 addresses Security Management Controls, calling for a standardized set of procedures and policies to be put in place to protect the identified assets. Juniper Networks Network and Security Manager supports this initiative by offering a centralized policy management tool for all security devices and the ability to virtualize systems and define roles.

The CIP-005 standard requires the identification and protection of an electronic security perimeter, inside which all cyber assets reside, as well as all access points on the perimeter. To accomplish this goal, utilities must:

- Identify the perimeter's access points and endpoints
- Access point electronic controls
- Monitor and log all access
- Create and maintain compliance documentation
- Assess vulnerabilities

To meet these guidelines, managers need a mechanism that can identify key access points and endpoints; enforce access controls; and monitor and log events to provide complete reporting, visibility, and compliance. The capabilities of IDP Series—combined with the SA Series for secure VLAN access for remote workers, UAC, Juniper Networks SSG Series Secure Services Gateways, ISG Series Integrated Security Gateways, NetScreen Series Security Systems, or SRX Series Services Gateways firewalls—create a solution to address these requirements. Furthermore, the IDP Series logs events for common SCADA protocols, ICCP, MODBUS, and DNP3, and provides about 30 signatures to log events at a granular level—while the STRM Series provides SCADA-specific reports for event analysis and auditing purposes.

CIP-007 focuses on Systems Security Management and defining the methods, processes, and procedures for securing critical and non-critical assets within the security perimeter. To appropriately manage utility security, plants need visibility into ports and protocols; automated defenses against viruses, spam, and phishing; access control enforcement; and event logging and monitoring. Juniper provides multiple layers of defense against potential internal and external attacks—including NSM, SA Series SSL VPN Appliances, IDP Series, the ISG Series, and SRX Series—offering integrated firewall, IPS, and IPsec for secure site-to-site connectivity. All Juniper products are managed and integrated by the NSM centralized management system, providing a more comprehensive threat management solution.

The CIP-008 standard addresses Incident Reporting and Response Planning—and requires high levels of visibility, support for profiling and correlating events, and detailed reporting for auditing purposes. Again, these reporting needs can be addressed by NSM and the STRM Series.

Outside of the scope of Juniper security solutions are CIP-004, which requires training and security awareness for authorized personnel, CIP-006, which discusses implementation of a physical security program for the protection of assets, and CIP-009, which focuses on developing an emergency recovery plan.

Juniper has been an early provider of solutions targeting the security needs of utilities, supporting industrial protocols, and designing functionalities to meet the specific needs of these environments. The company is a member of ISA-SP99 and works in partnership with the Pacific Northwest National Laboratory (PNNL) and the Idaho National Laboratory (INL), the national SCADA infrastructure test beds, with funding from the Department of Energy; and with Sandia National Laboratories on projects for the Department of Homeland Security.

Conclusion

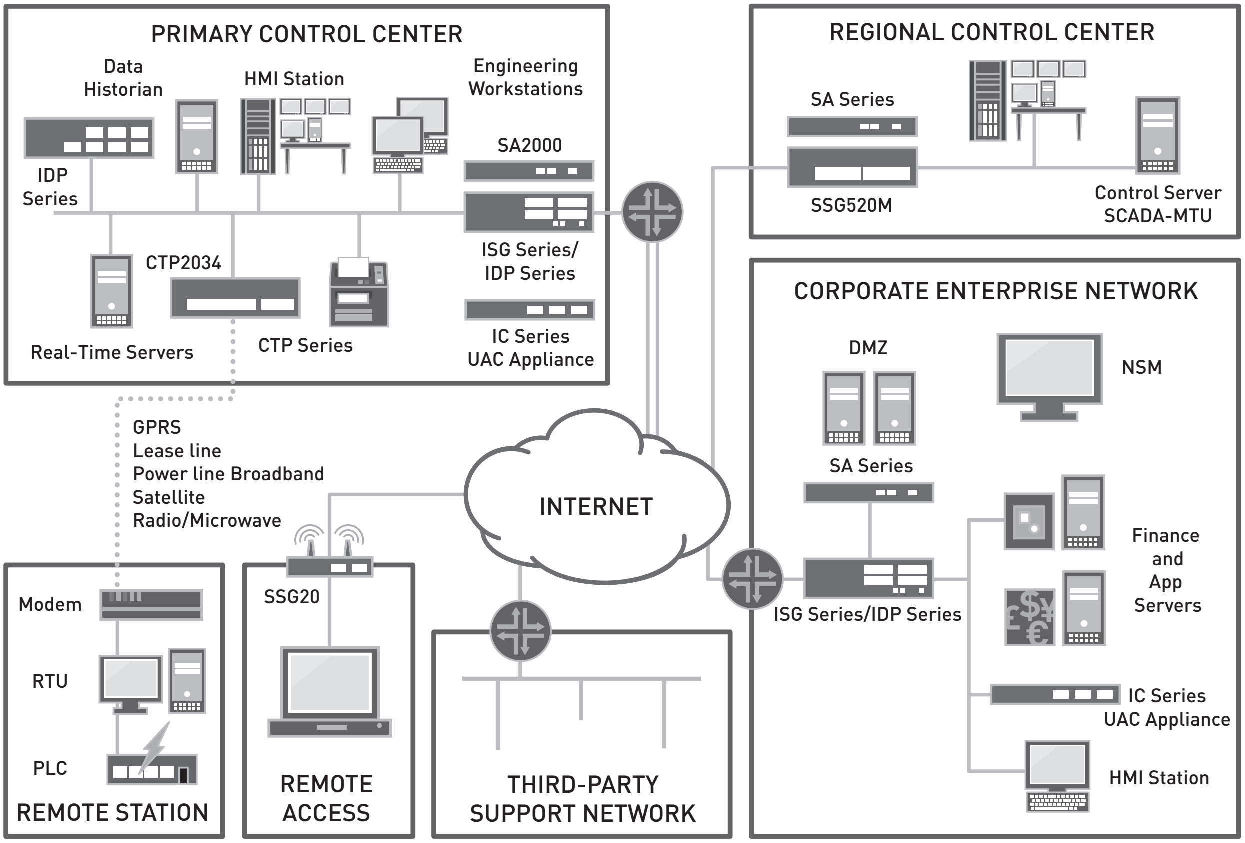

Figure 5: Comprehensive network-based security for control systems

Protection of control system networks is essential for maintaining or improving the reliability of the nation's critical infrastructure. This includes power and energy industries, water, chemical plants, manufacturing facilities, and transportation. It is no secret that the cyber security measures in place for most of these control system networks are inadequate. This has resulted in intentional and unintentional cyber incidents. Cyber events, such as unintentional denial of service attacks have caused loss of property and life. As control system networks are expanded to use the latest networking technologies for improving operations such as the Smart Grid, it is essential to keep in step with the appropriate security methodologies and technologies that ensure continued reliability.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at **www.juniper.net.**

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters
Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters
Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

2000276-004-EN July 2010

Printed on recycled paper