

Technical Brief

Distribution Automation System Security

Telemetric System Security

The purpose of this document is to outline the security features of Telemetric wireless communication and control solutions for the electric utility industry. Recognizing the importance of security to distribution automation and control functions, Sensus Telemetric has engineered its hardware, communication systems, and software solutions to provide a high degree of system security.

The holistic security management process for the Telemetric system includes:

- Physical network - including the wireless infrastructure, fiber optic transmission systems, firewalls, routers, switches, and servers
- Link to SCADA/DMS/EMS - via the SCADA-Xchange™ servers and software
- User-level security for PowerVista™ software - enabling commands, monitoring, system and device management

The physical network and SCADA-Xchange security is discussed below in Part One: General System Security. The security aspects related to Telemetric PowerVista application are covered in Part Two: PowerVista Cyber Security.

Guidelines and Standards

As a reference for developing security systems and policies, Sensus Telemetric monitors activity associated with mainstream security standards written specifically for the electric utility industry:

- North American Electric Reliability Corporation (NERC) Cyber Security Standards CIP-002-1 through CIP-009-1 for Critical Infrastructure Protection (CIP)
- NIST Framework and Roadmap for Smart Grid Interoperability Standards
- IEEE Standard 1402-2000; IEEE Guide for Electric Power Substation Physical and Electronic Security

The NERC Cyber Security Standards for Critical Infrastructure Protection CIP-002-1 through CIP-009-1 currently apply only to bulk power control systems. Each utility determines what they consider to be Bulk Power Delivery, sub-Transmission, and Distribution systems. Based upon that, different levels of security standards may be applied. Some large utility security departments have developed different levels of cyber security standards for each. Since NERC audits are only conducted on systems related to Bulk Power Delivery, the standards as practiced by each utility for sub-Transmission and Distribution are

internal standards only and not subject to NERC CIP audits. Sensus Telemetric is not directly subject to CIP as of this date because no customer has applied Telemetric technology to control their Bulk Power Delivery system. Taking that into consideration, we take every effort to align ourselves with current NERC/CIP requirements.

While Telemetric systems do not control Bulk Power Delivery systems, in some customer cases the distribution automation systems are hosted on/with Energy Management Systems that do. Each customer must determine for themselves, and be able to support during a CIP audit, that the CIP defined security perimeter does not encompass the Telemetric system. In the case of one Sensus Telemetric customer that completed a CIP audit, the audit supported the utility's view that the Telemetric system is outside the CIP security periphery and thus not subject to CIP rules.

Part One: General System Security

System Elements

Sensus Telemetric solutions utilize commercial cellular networks and the Sensus private, licensed FlexNet network to provide intelligent, reliable, and secure two-way communications to electric distribution assets and smart grid sensors. Security features are provided at each level of the end-to-end network – from the remote device thru the customer application. The typical data flow diagram is shown in Figure 1, and involves the elements of:

- Telemetric Intelligent Wireless Remote Device
- Wireless cellular communication networks
 - Cell tower Sites
 - Cellular Switching Center(s) (MSC)
 - Cellular Carrier Network Operations Center(s)
- Sensus FlexNet Network (where applicable)
 - Tower Gateway Base Stations (TGB)
 - Regional Network Interface (RNI)
- Telemetric Network Operations Center
- Customer Gateway

The security features of each element will be discussed in greater detail in the following sections.



Telemetric Intelligent Wireless Device Communication over Cellular or Sensus FlexNet Private Networks

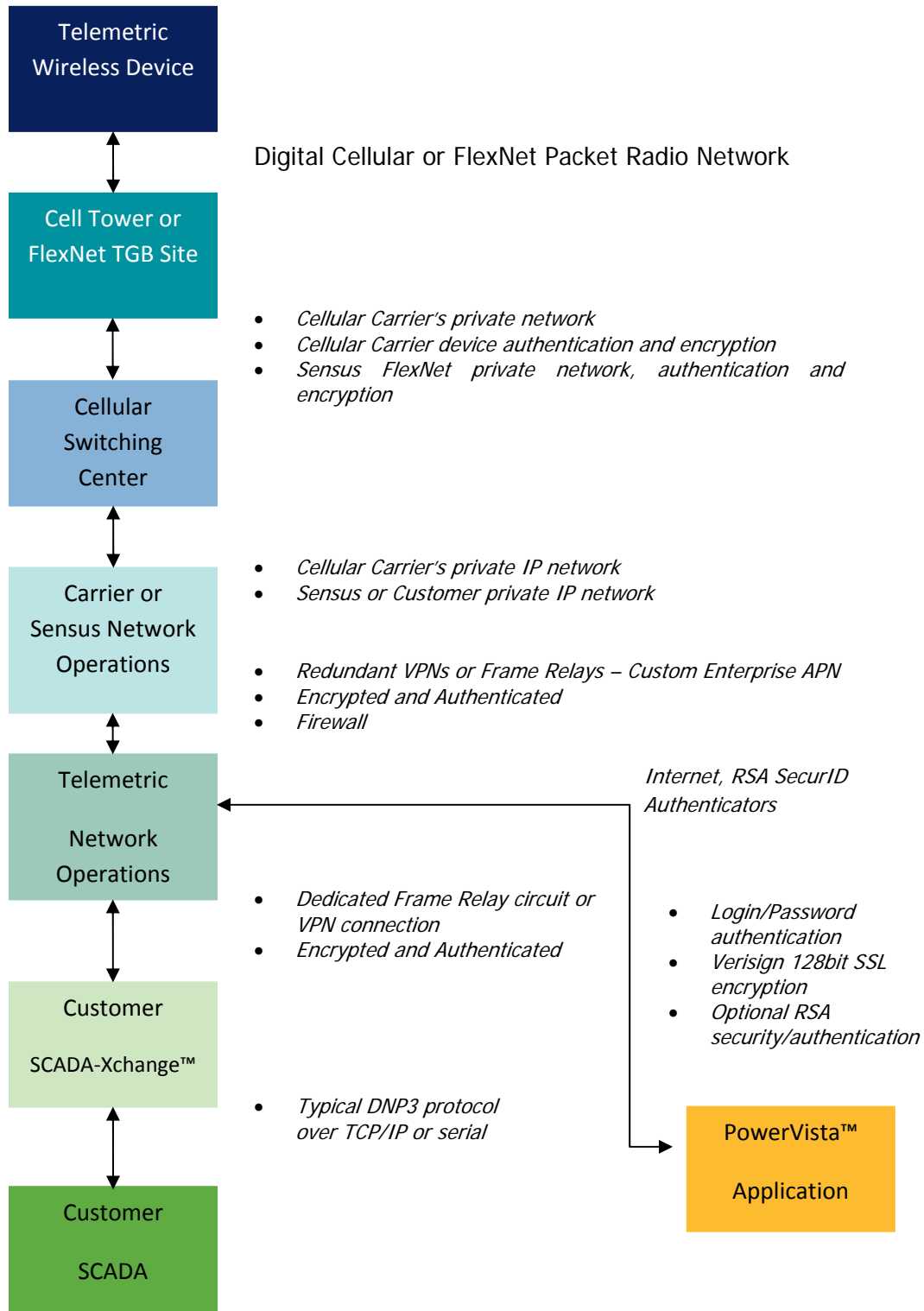


Figure 1

Technical Brief

Distribution Automation System Security

Integrated Radios

All models of Telemetric products are available with digital GSM/GPRS radios, CDMA/1x cellular or Sensus FlexNet private network radios.

GSM is the designation for one type of mobile system technology (Global System for Mobile), which is used by carriers such as AT&T and T-Mobile in the U.S., as well as hundreds of carriers internationally. GPRS and EDGE refer to IP-based data services subsystems that are integral to the GSM system. GSM carriers may additionally provide even higher speed services via "overlay" technologies (e.g. HSDPA, etc.), that enable faster data communications. The overlay technologies are separate systems, though the actual hardware is often combined with state-of-the-art handsets for consumers. Most of the innovation and growth in technology performance is in the overlay technologies, while the carriers utilize the base-level GSM/GPRS system to ensure they have complete geographical coverage for voice and relatively high speed IP anywhere in their serving area.

The second major cellular technology is CDMA/1xRTT used by Verizon, Sprint, and others. CDMA carriers also provide higher speed services such as 1xEV-DO.

Whether GSM or CDMA, Sensus Telemetric utilizes industrial-grade cellular radio modules. They are temperature hardened and provide more robust RF performance than the radios used in consumer handsets, which are designed to provide long battery life. Telemetric radios communicate with AT&T over a Private Enterprise-class Application Program Name (APN) between Telemetric and AT&T data centers. The private nature of this direct connection to AT&T nationwide network allows for a much higher degree of system security than a typical data card or digital modem.

Security Features of Telemetric products with GSM/GPRS technology include:

- **Authentication (Network Layer):** Prior to communications on the network, the AT&T network authenticates the device using a challenge/response authentication algorithm called GSM A3. GSM A3 authenticates the mobile device against the International Mobile Subscriber Identity (IMSI) and secret key stored on the SIM card within the GPRS radio in the Telemetric RTU.
- **Private IP Address Assignment:** When a Telemetric device connects to the network, the AT&T system assigns it a dynamic private IP address from a block of IP addresses dedicated to the Telemetric Custom APN. All peer-to-peer IP functionality is disabled by AT&T for all IP addresses used by the Telemetric Custom APN. Because all private IP data routes to the Telemetric APN, the Telemetric device dynamic IP addresses are not routable or available to the networks outside AT&T or the internet. For example, a Telemetric device on a dynamic IP address cannot be 'pinged' from the internet.
- **Multi-factor Authentication:** The Telemetric NOC stores a database of International Mobile Subscriber Identity (IMSI) Unit ID numbers for all Telemetric devices. The Telemetric NOC uses this database to authenticate all outbound and inbound data transmissions by matching the encrypted International Mobile

Subscriber Identity (IMSI) coming from the Telemetric device with its Unit ID. An unmatched transmission is disregarded.

- **Encryption:** This occurs between the Telemetric device and the carrier's backbone network switch (referred to as a Serving GPRS Support Node or SGSN, a relatively centralized node on the AT&T backbone network). Encryption spans not only the air interface, but a portion of the wire line infrastructure as well as all connections leading to the SGSN (AT&T regional switches). Following authentication of the device, the network and the device derive a bit encryption key. The encryption algorithm for GPRS is referred to as GPRS Encryption Algorithm (GEA). The current version of this algorithm in use is called GEA2. Thus, after device authentication, all data communications are bit encrypted using the GEA2 algorithm. The details of GSM/GPRS authentication and encryption algorithms are not publicly disclosed.

The carrier's SGSN nodes are interconnected via secure, redundant private IP connections to one or more Network Switching Centers. Security of the carrier's network is provided by the private nature of this network.

Security Features of Telemetric products with FlexNet include:

- **Multilayer encryption** combines several encryption keys for even more robust protection. In a FlexNet system, for instance, each device has a *unique key* that was assigned during manufacturing. The regional network interface (RNI) can automatically distribute a *shared key* to all devices on the network. And each device group can be assigned a unique *group key*. The unique device key and/or group key can be used in conjunction with the shared key to encrypt all device-to-RNI traffic. The RNI automatically rotates shared keys.
- **Authentication** establishes or verifies a user or endpoint as authentic, such as through passwords entered by authorized users or digital signatures supplied by devices or computer programs. In the FlexNet system, both ends of the communication are authenticated. Once the identity of a user or device has been validated, **authorization** processes grant access to network resources as permitted. For instance, under a sound security policy of separation of duties, an administrator may have permission to access certain utility network functions or commands but not others.
- A wireless network based on **licensed spectrum** provides intrinsic security advantages. For instance, since this is not a technology that an individual can order through the Internet and plug in at home, it is not a target for casual intruders. Furthermore, by law, only the authorized license holder can access the licensed channel. It is illegal to infringe on this channel either by sending or intercepting transmissions. In the U.S., this protection is enforced by the Federal Communications Commission.



10147 West Emerald Street, Suite 100
Boise, ID 83704 USA
T: 208-658-1292
F: 208-323-5575
www.telemetric.net
telemetricsales@sensus.com

Sensus Confidential

- **Time-windowed commands** add yet another layer of defense to limit the risk of replay attacks and other types of malicious activities. For critical actions, such as configuration changes or firmware updates to remote devices, the system first sends a "notification of action" message to the device. The subsequent "action" message must be received within a designated window of time, and it must contain elements that match those in the notification message, or else the action is rejected.
- **Behavior auditing** monitors activity on the network, looking for suspicious activities or deviations from policy. For example, any attempt to tamper with a secured device or update its firmware would trigger an alarm, alert notifications to appropriate personnel and an audit log entry.

The above mentioned technology-based security tactics must be backed with strong organizational **security policies** as well, such as division of responsibility, physical access control, secure storage of hardcopy information and disaster recovery plans.

AT&T Network Operations Center

Sensus Telemetric maintains an Enterprise-class Private Application Program Name (APN) between Telemetric and AT&T data centers over redundant Virtual Private Networks (VPN). All data communications traffic is passed between AT&T and Telemetric over these secure VPN connections. Sensus Telemetric maintains multiple VPN connections to two separate AT&T network datacenters with automatic BGP failover between nodes for reliability and redundancy.

Telemetric Network Operations Center (NOC)

The Telemetric NOC is located in a secure enterprise class datacenter with a high degree of security and fault-tolerance. Sensus Telemetric's application servers, gateways, and database servers are located in this datacenter behind a CISCO firewall. Physical access to the datacenter is restricted at all times. Application logic within the Telemetric NOC manages the communications with Telemetric devices and routes the data to the customer's application: Telemetric PowerVista™ and SCADA-Xchange™. Customer SCADA or DMS/EMS systems are linked to the system via private networks such as VPN or dedicated frame-relay connections.

Reliability features at the Telemetric NOC include:

- Redundant hot-swappable application servers (PowerVista and SCADA-Xchange servers)
- Redundant database servers (On-site, mirrored)
- All servers include RAID drives and redundant power supplies (PowerVista™/Database/Xchange Servers)
- Load balancer (Foundry Networks)
- Redundant Storage Array
- Redundant firewalls
- External monitoring applications monitor all critical processes at the NOC
- 24 x 7 system status alarm monitoring and personnel on call

- Additional redundancy achieved via utilizing virtualization technologies

Security features for Datacenter physical access:

- 24 X 7 guarded facility
- Biometric (BioScript Biometric Thumbscan) Access - limited to 2 Administrative personnel behind 2 secured doors (access to data center floor limited)
- Once inside the data center, keyed access to locked Telemetric caged containing server racks
- Once inside secured Telemetric cage, keyed access to locked server racks
- CCTV surveillance, with 90 days retained data
- Other Data Center key attributes:
 1. Fire Detection and Suppression - Pre-action dry-pipe fire suppression system with temperature and smoke detectors eliminates false alarms.
 2. Environment (HVAC) - Redundant Liebert systems produce ideal environmental conditions; 78 deg.F (+/-2 degrees), 45%RH (+/- 5%) achieving N+1 standards in a raised-floor semi- clean room environment.
 3. Power - Power backed by a parallel-redundant 500KVA UPS system and one 850KW diesel generator with 96 hours of fuel on-site and guaranteed refueling contracts. All data center power is conditioned and free from utility power fluctuations.

Data Center Electronic Access:

- Our network is built on hardened Cisco routers to ensure maximum security. Our firewalls are managed by security experts, while customer networks are isolated on VLANS.
- Centralized auditing of data center security including:
 1. Modifications to application or OS permissions
 2. Changes to group membership
 3. Changes to user permissions
 4. Password policy changes
 5. User account lockouts
 6. Changes to inventory or asset-related details
- Access to our production environment is limited to 2 Administrative personnel
 1. Our Production network is completely isolated from our business network, with limited access to production to admin only

Production Server Access:

- All access to production is logged. Unique ID's and controls are used for each resource thru the following:
 1. We currently track the following requirements according to CIP: Authentication
 2. Authorization access and control
 3. Confidentiality
 4. Integrity
 5. Availability
 6. Non-Repudiation
 7. Audit and Compliance
 8. Physical
- Monitoring system in place maintains logs, shows availability of systems, and all logs confirm customer transactions.

Technical Brief

Distribution Automation System Security

Application Firewall:

- Protects our web applications and sensitive data against attacks such as SQL Injection, Cross-Site Scripting (XSS), brute force attacks, and prevents data leaks from applications. Additional benefits include:
 1. Accurately monitors and reports Web applications
 2. Automates operations through dynamic profiling
 3. Supports high performance and sub-millisecond latency
 4. Documents security status and compliance
 5. Centralized monitoring of credible attack source data providers

Customer SCADA-Xchange Gateway

Many of Sensus Telemetric's customers achieve a complete end-to-end communication solution by connecting the Telemetric application into their internal SCADA or EMS system. This is achieved in a reliable and secure manner using Telemetric's SCADA-Xchange™ application. SCADA-Xchange is essentially a DNP3.0 proxy server holding all of the most recent data from each individual Telemetric Intelligent Wireless device. SCADA-Xchange responds to DNP3.0 polls, but cannot initiate communications with the SCADA/EMS system, thus providing inherent security and keeping SCADA-Xchange outside the CIP security periphery. SCADA-Xchange is flexible – allowing SCADA to request an immediate poll of the remote device, or to access the most recent reported data. SCADA-Xchange returns requested DNP3.0 data as if it were the actual device, thus providing virtual polling while eliminating constant polling over the airwaves and the very high data services fees that would result.

In a typical SCADA-Xchange setup, the Telemetric NOC is connected to the customer's control center via a secure connection - either by direct frame-relay connection or by Virtual Private Network (VPN) connection. The VPN connection is normally 256bit AES encrypted. Encryption is optional over the dedicated frame relay connection if the customer requires it.

In the case of DNP3.0 protocol communications, the data is either presented as DNP over TCP/IP. Optionally, at the customer firewall, a conversion to DNP3.0 serial can be implemented, depending on the customer application. All traffic comes to Sensus Telemetric as DNP3.0 encapsulated in TCP/IP and is converted to DNP-serial at the customer's location as needed.

Typical security features of this SCADA-Xchange connection include:

- Customer connection to Telemetric NOC is encrypted, either over frame relay (optional) or via 256 bit AES encrypted VPN
- Both the Telemetric NOC and the customer's data center authenticate to each other via password when connected over frame relay. Certificates are utilized for authentication in the case of a VPN connection. There are firewall rules on each end, and each customer has specific DNP Local/Remote addresses.
- Sensus Telemetric maintains a secure firewall at the NOC, and the customer maintains a firewall at their control center interface
- Service typically limited to single IP port combination with Sensus Telemetric side of SCADA-Xchange responding only to DNP3.0 polls



10147 West Emerald Street, Suite 100
 Boise, ID 83704 USA
 T: 208-658-1292
 F: 208-323-5575
www.telemetric.net
telemetricales@sensus.com

Sensus Confidential

Part Two: PowerVista™ Cyber Security

Here we cover both recommendations to utilities on operating procedures as well as Sensus Telemetric features that will enable increased cyber security related to the PowerVista™ application. The following covers three primary areas of cyber security: authentication, authorization, and event reconstruction.

Authentication

Authentication is answering the question “Are you who you say you are?” of a person requesting access. Systems typically verify this with login passwords. The assumption is that if the user knows it, he or she must be who he or she says they are. But it is also possible to gain a password through illegitimate means.

To make fraudulent authentication more difficult the following actions can be considered:

Utility Process Changes to Improve Authentication

- Change passwords on some periodicity – if one is stolen, it’s only valid for a shorter period of time – Admin user can establish this;
- Make it company policy not to leave one’s desk without placing computer in standby;
- Make an IT policy in which a computer requires password login on resumption of standby or after screensaver initialization.

Sensus Telemetric Features for Authentication

- Password logins
- RSA two-factor SecurID Authentication (provided at additional charge). Per RSA, they know of no instance of this authentication method being broken
- Force new password creation by users on some periodicity
- Make the password harder to guess with humans or machines, by requiring “complex” passwords – this can be implemented such that the Telemetric login does not allow creation of short and/or easy to guess passwords through various rules placed in software that forces the user to create a complex password. This functionality is currently available in PowerVista and highly recommended.
- Prohibit multiple simultaneous logins with the same user ID (PowerVista default rule)
- Session timeouts

Authorization

Authorization answers the question of what an individual user should be able to do once access is granted to the system. Authorization measures the potential damage a fraudulent login can perform (and also mitigate damage from accidental improper use of the system – not strictly a security issue). For example, in the military, there is a principle called “need to know”. In certain classes of secure projects or activities, individuals are not authorized to access other than what is needed by them in the performance of their job duties – they are allowed to know only what they “need to know”.

Utility Processes to Improve Authorization Management

- Careful management of authorization levels that keep personnel on a “need to know” basis is a good way to limit damage from improper use of the system. Only provide access and tools to those that need them to do their job and no more.
- It is also advisable to have audits of all existing passwords, RSA key fobs, and access levels on a periodic basis. As personnel change jobs, change duties, or get hired and leave, it is important to ensure there are current and appropriate authorizations.

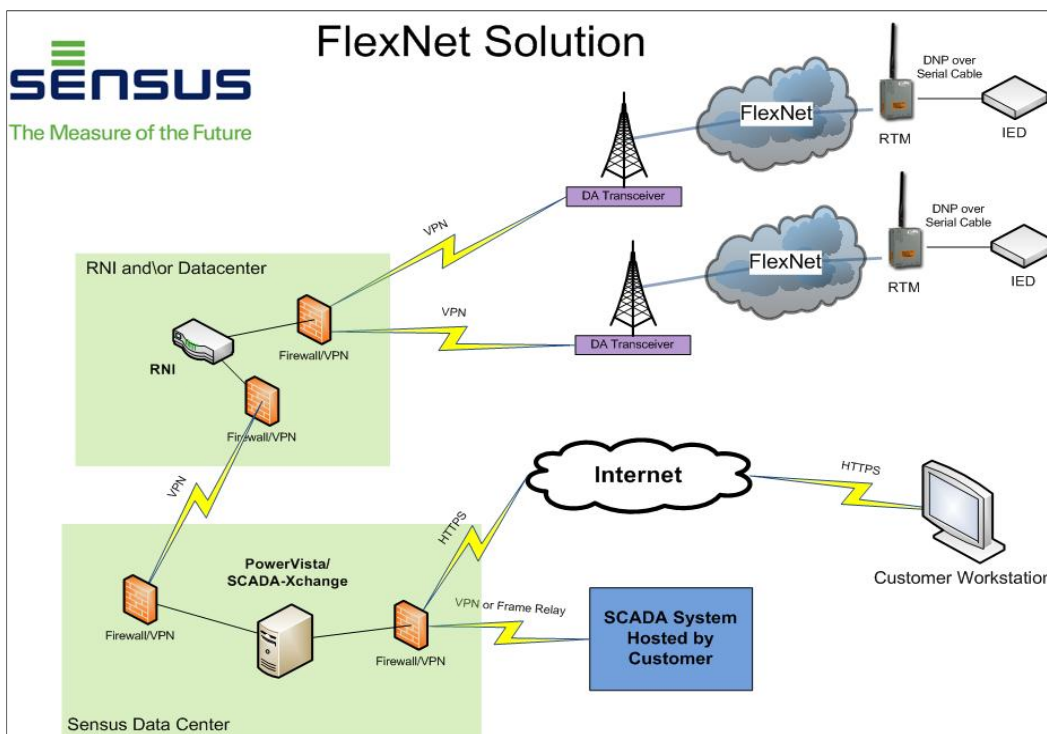
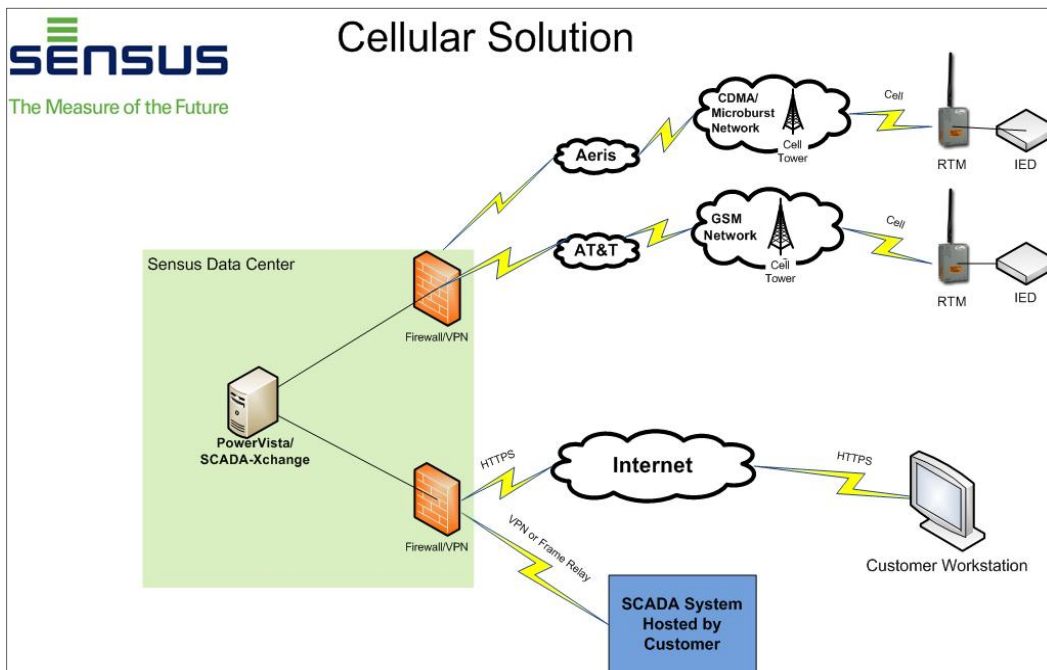
Sensus Telemetric Features for Authorization Management

- Only one Administrator per customer. Administrators can create new users.
- User type assignment – when the administrator creates a new user or edits existing users, they can assign the user a class of authorization from:
 - Sub-Administrator
 - Operators
 - View and report
 - View only
- User group – the Administrator also assigns various groups to each user – the group feature is an important feature for system authorization methods.
- User ID Templates – allows administrators to create and support a role type for multiple users. Allows modifications to template to propagate to all users on that template.

Technical Brief

Distribution Automation System Security

Diagrams depicting our current hosted solution:



Logging and Event Reconstruction

After an undesirable event it is often necessary to assess what went wrong. Was it accidental or intentional? Who or what did it? When? Sensus Telemetric provides utilities the tools for event reconstruction.

Current PowerVista History logs provide:

- Action
- Values
- Time
- User id
- Login attempts logging
- Login attempts time out

These logs are retained and immediately accessible for one year and available through archives after that.

Planned:
SCADA-Xchange™ logging incorporation into PowerVista™ history logging (simplifies research).

Part Three: NERC\CIP Compliance Matrix

CIP 002-1: Critical Cyber Asset Identification

Cyber Assets:

- Our next annual self audit to identify critical assets will take place in June, 2010. These assets will include:
 - Firewalls
 - Load Balancers
 - Database Servers
 - Routers
 - Other Misc. Servers

CIP 003-1: Security Management Controls

Change Control:

- Sensus adheres to strict change control practices:
 - All production changes are scheduled at least 48 hours in advance
 - Changes to critical cyber assets are made during after hour windows approved by management. Currently, these windows are Tuesday thru Thursday, after 6:00pm Mountain Time.
 - Back-out plans, where applicable, are filed with the change plan.
- Change documentation:
 - Change control forms are filled out and kept secure, detailing each change.
 - Automated logs track and log ALL changes. This data is backed up and reviewed regularly.

CIP 004-1: Personnel and Training

Personnel/Training:

- All personnel have undergone background checks.

- Personnel with access to cyber or physical assets undergo yearly training regarding risks, password control, etc.

CIP 005-1: Electronic Perimeter Security

Data Center Electronic Access:

- Our network is built on hardened Cisco routers to ensure maximum security. Our firewalls are managed by security experts, while customer networks are isolated on VLANs.
- Centralized auditing of data center security including:
 - Modifications to application or OS permissions
 - Changes to group membership
 - Changes to user permissions
 - Password policy changes
 - User account lockouts
 - Changes to inventory or asset-related details
- Access limited to 2 Administrative personnel to our production environment
 - Our Production network is completely isolated from our business network, with limited access to production and admin only
- Typical security features of this SCADA-Xchange™ connection include:
 - Customer connection to NOC is encrypted, over private frame relay or via 256 bit AES encrypted VPN.
 - Both the NOC and the customer's data center authenticate to each other via password when connected over frame relay, pre-shared key utilized for authentication in the case of a VPN connection. There are firewall rules on each end and each customer has specific DNP Local/Remote addresses.
 - Sensus Telemetric maintains a secure firewall at the NOC, and the customer maintains a firewall at their control center interface.
- All access to production is logged - unique ID's and controls are used for each resource.

CIP 006-1: Physical Security

Datacenter physical access:

- 24 X 7 guarded facility
- Biometric (BioScript Biometric Thumbscan) Access limited to 2 Administrative personnel behind 2 secured doors (access to data center floor limited)
- Once inside the data center, keyed access to locked caged containing server racks
- Once inside secured cage, keyed access to locked server racks
- CCTV surveillance, with 90 days retained data
- Other Data Center key attributes:
 - Fire Detection and Suppression - Pre-action dry-pipe fire suppression system with temperature and smoke detectors eliminates false alarms.
 - Environment (HVAC) - Redundant Liebert systems produce ideal environmental conditions; 78 deg.F (+/- 2 degrees), 45%RH (+/- 5%) achieving N+1 standards in a raised-floor semi-clean room environment.

Technical Brief

Distribution Automation System Security

- Power - Power backed by a parallel-redundant 500KVA UPS system and one 850KW diesel generator with 96 hours of fuel on-site and guaranteed refueling contracts. All data center power is conditioned and free from utility power fluctuations.

CIP 007-1: Security Management

Vulnerability Assessments:

- a. Sensus runs an external penetration test every 3 months. The results from this test are reviewed by network security management.
- b. Event and Log Management:
 - All firewall and other network equipment (switches, load balancers) traffic is logged. These logs are kept for 90 calendar days and reviewed regularly by network security management.
 - Automated logs track and log ALL changes. This data is backed up and reviewed regularly.
- c. Patch Management:
 - All security patches are immediately reviewed upon release
 - Patches are released into our test environment within 1 week of release
 - Patches are applied once a month, unless a high vulnerability issue is identified whereupon the process is expedited

CIP 008-1: System Incident Response

Cyber Security Incidents:

Sensus maintains a CIRT that responds to any cyber security incident. These are classified and reported as appropriate. When reporting is required, it is reported to ESISAC (Electricity Sector Information Sharing and Analysis Center).

CIP 009-1: System Disaster Recovery

Sensus Maintains a Disaster Recovery Plan:

The disaster recovery plan is tested annually, beginning October, 2010. Our current plan involves bringing up all production systems in a separate Sensus Data Center within 48 hours, while future plans provide complete recovery in as little as 12 hours.



10147 West Emerald Street, Suite 100
Boise, ID 83704 USA
T: 208-658-1292
F: 208-323-5575
www.telemetric.net
telemetricsales@sensus.com

Sensus Confidential

Part Four - Frequently Asked Questions

- What types of network connection are being configured from SCADA Operation Centers to Telemetric's NOC?
 - Site-to-site VPN with authentication and encryption
 - Point to point ATM Frame Relay available at additional cost
- Are VPN connections maintained after reaching your ISPs?
 - Yes, maintained into the 4 walled Telemetric cages to CISCO ASA
- Where are the VPN concentrators located?
 - Inside Telemetric datacenter collocation facility, within the Telemetric 4-walled cage
- How do you secure Frame Relay?
 - Frame Relay terminates into frame interface cards within equipment inside Telemetric 4-walled cage. Frame Relay has inherent security layers and we can offer additional optional encryption.
- Power Vista - Can users remotely control electric distribution equipment of any kind?
 - If desired, control is possible but can also be completely disabled
- Can users download or upgrade software remotely?
 - Yes, to the endpoint modules. The Telemetric RTM firmware is over the air upgradable, so configuration can be changed over the air.
- What application services run over DNP 3?
 - SCADA-Xchange responds as a slave to commands/polling from the DNP master (PG&E RT SCADA). The field device (DNP-RTM) and the associated IED (recloser control) communicate via DNP3.0.
- What types of information are sent by e-mail? Examples?
 - Optional notifications to field or engineering personnel can be setup by using the PowerVista application via email, text or pager. For example, if a recloser locks out, a user can set-up a notification that is sent to a field engineer distribution list and/or pagers.
- Are direct connections from your web servers to application or database servers allowed?
 - ODBC is utilized between the PowerVista application and SQL Server – no other connections are allowed
- Are antivirus, antispysware, intrusion detection enabled for every virtual machine in your virtual infrastructure?
 - Yes, while also being protected by an application firewall. The system is also protected by network intrusion detection which exists at the NOC level and at the router and server level. This security is two way, so it also protects from intrusion via a customer's network.
- Have unused physical devices been disconnected (CD/DVD drives, floppy drives, and USB adapters)?
 - Yes
- Are screen savers turned on?
 - Yes
- Are virtual local area networks being used?
 - Yes
- How, and how often, are security patches applied?
 - Patches are applied by using Microsoft WSUS. Each vulnerability issue is immediately reviewed and patching is done at a minimum once a month. If immediate response vulnerabilities are identified, exceptions are made.
- Are there firewalls set at different layers within your NOC?
 - Yes, there are application firewalls protecting the web application servers and the main firewall is at the VPN concentrator/network level.

Technical Brief

Distribution Automation System Security

Summary

All elements of the Telemetric wireless communication and control solution are designed to provide for a reliable and secure application. Sensus Telemetric has built these systems based upon years of experience delivering secure communication systems for many large utility customers. These systems provide a solid foundation to deliver a system that meets the needs of the customer's application.

Several customers have completed intrusion and risk assessments and concluded that the elements of this system provide strong security relative to distribution automation and control functions. Intrusion assessments are not included in this paper for general distribution. Sensus Telemetric sales representatives and application engineers are available to discuss these details directly with Telemetric customers.

Although this paper provides a general security overview, Sensus Telemetric can discuss any customer-specific security requirements needed for a particular application. For large deployments, Sensus Telemetric Engineering Services can provide customized security solutions to meet the needs of the customer's application. Contact your Sensus Telemetric sales representative to discuss these needs.

Your Input: Sensus Telemetric is pleased to consider comments and/or suggestions to improve security systems for our customers. We welcome your input. Please contact us at telemetricssupport@sensus.com or 208-658-1292 x21 (customer support).



10147 West Emerald Street, Suite 100
Boise, ID 83704 USA
T: 208-658-1292
F: 208-323-5575
www.telemetric.net
telemetricssales@sensus.com

Sensus Confidential