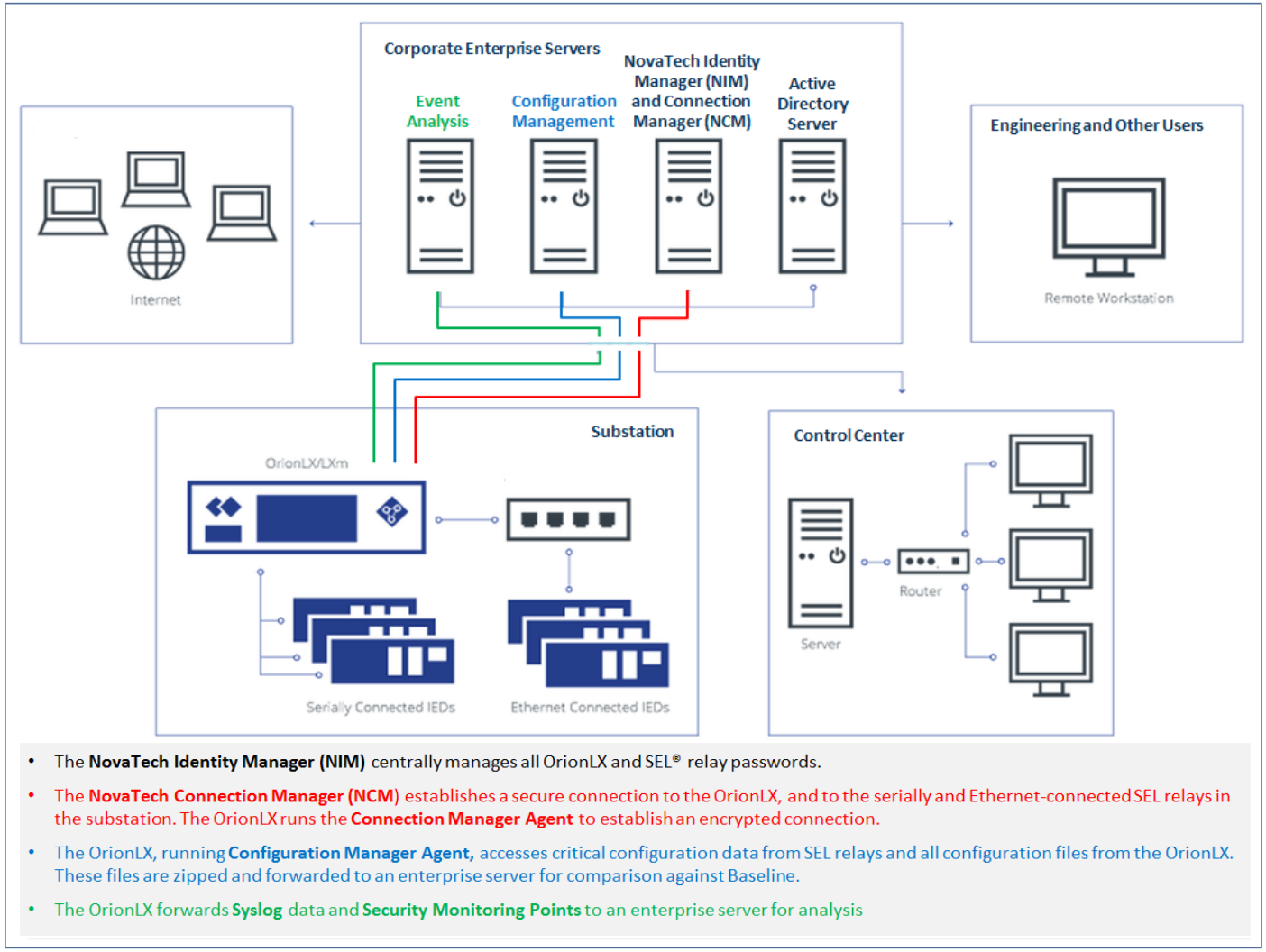
NovaTech NERC CIP Compliance Document and Product Description
Updated June 2015

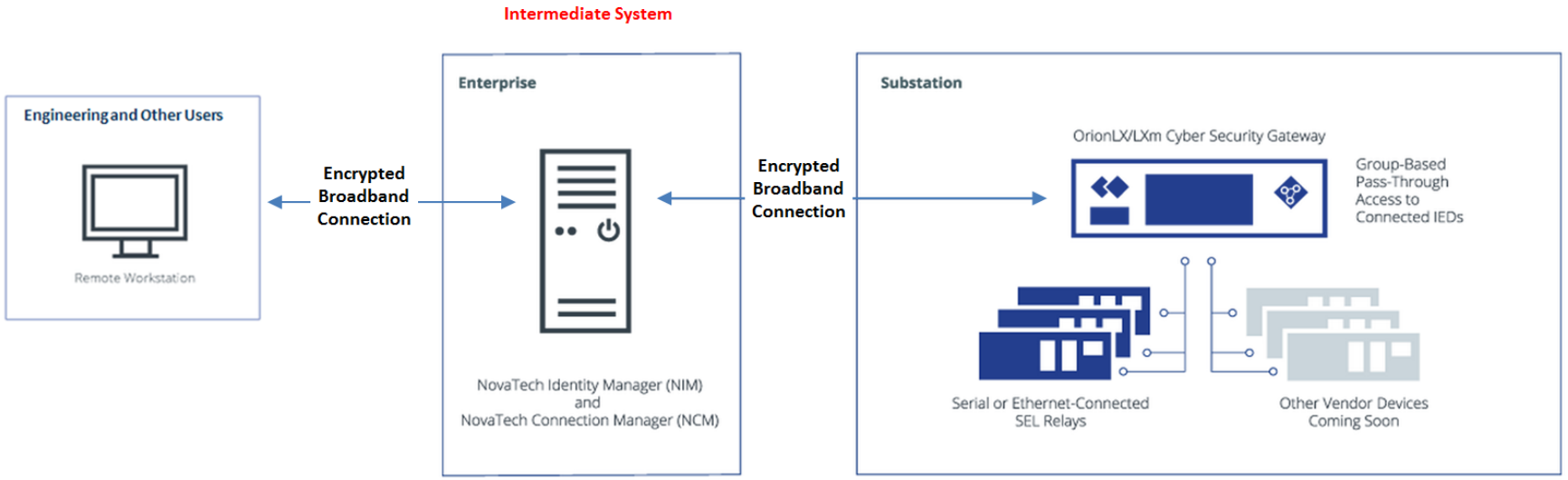
This document describes the NovaTech Products for NERC CIP compliance and how they address the latest requirements of NERC CIP Version 5.

NovaTech produces both enterprise products for NERC CIP compliance and in-substation OrionLX products for NERC CIP compliance. The two enterprise products are the NovaTech Identity Manager ("NIM") and the NovaTech Connection Manager ("NCM"). The OrionLX products are the Connection Manager Agent, Configuration Manager Agent, Syslog, and Security Monitoring Points. The diagram below summarizes where each of these NovaTech products are located in the utility power system and how they are interconnected:



Compliance Table

The NovaTech products for NERC CIP compliance address portions of the requirements of Version 5 of CIP-005, CIP-007, CIP-008, CIP-009, CIP-010 and CIP-011. Compliance for each area is summarized below. More detail on User Password Management and IED (Host) Password Management is provided at the end of this document.

Standard	Req't	Language
CIP-005	R1 (1.2)	All External Routable Connectivity must be through an identified Electronic Access Point (EAP). **NovaTech Response:** The OrionLX serves as the Cyber Asset interface on an Electronic Security Perimeter that allows routable communication between Cyber Assets outside an Electronic Security Perimeter and Cyber Assets inside an Electronic Security Perimeter.
CIP-005	R1 (1.3)	Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default. **NovaTech Response:** The OrionLX provides both a firewall and a list of authorized users, each with permissions related to their role, to restrict access to protected Cyber Systems. The OrionLX uses netfilter/iptables supporting stateless and stateful packet filtering for both inbound and outbound traffic. Connection tracking is provided by (ip_conntrack, nf_conntrack). The OrionLX firewall can be configured through a web-based GUI, or configured at the command line.
CIP-005	R1 (1.5)	Have one or more methods for detecting known or suspected malicious communications for both inbound and outbound communications. **NovaTech Response:** The OrionLX monitors unsuccessful login attempts and logs the user name, media and protocol interface (e.g. keyboard access, SSH attempt, etc).
CIP-005	R2 (2.1)	Utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset. **NovaTech Response:** NovaTech offers two enterprise products to serve as the Intermediate System. These are the NovaTech Identity Manager ("NIM") and the NovaTech Connection Manager ("NCM"). All connections from connected Cyber Assets to substation Cyber Assets must go through this Intermediate System. 

CIP-005	R2 (2.2)	For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System. **NovaTech Response:** All communication to and from the NovaTech Intermediate System is encrypted using 128-bit techniques.
CIP-005	R2 (2.3)	Require multi-factor authentication for all Interactive Remote Access sessions. **NovaTech Response:** The utility's existing multi-factor authentication system is used to access utility enterprise systems, including the NovaTech Intermediate System.

CIP-007	R1 (1.1)	Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.
		NovaTech Response:
		The OrionLX by default has non-secure FTP, telnet, and HTTP ports disabled. The OrionLX supports a firewall that can be used as a compensating measure to "block" any open ports that are not used and that cannot be disabled. Using the command ngc –s will list all of the OrionLX services. The OrionLX supports the "netstat" command from the root command line. By adding the options to the command the OrionLX will list the Listening TCP and UDP ports. This command will allow the Responsible Entity to monitor what Ports are open and Listening on the OrionLX without having to use external port scanning software which can cause operational issues with equipment. See example capture below:
		`# netstat -ltu`
		`Active Internet connections (only servers)`
		`Proto Recv-Q Send-Q Local Address Foreign Address State`
		`tcp 0 0 (null):22 (null):* LISTEN`
		`tcp 0 0 :::22 :::* LISTEN`
		`tcp 0 0 :::443 :::* LISTEN`
		`udp 0 0 (null):ntp (null):*`
		`udp 0 0 localhost:ntp (null):*`
		`udp 0 0 (null):ntp (null):*`
		Using the command LSOF (List Open Files) provides additional data, See example capture below:
		`# lsof -i -n -P`
		`COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME`
		`syslog-ng 639 root 29u IPv4 1216 0t0 UDP 172.16.123.12:36614->172.16.3.68:514`
		`ntpd 671 root 20u IPv4 1281 0t0 UDP *:123`
		`ntpd 671 root 22u IPv4 1285 0t0 UDP 127.0.0.1:123`
		`ntpd 671 root 23u IPv4 1286 0t0 UDP 172.16.123.12:123`
		`sshd 700 root 3u IPv4 1385 0t0 TCP *:22 (LISTEN)`
		`sshd 700 root 4u IPv6 1389 0t0 TCP *:22 (LISTEN)`
		`apache2 29020 root 5u IPv6 225748 0t0 TCP *:443 (LISTEN)`
		`apache2 29021 http 5u IPv6 225748 0t0 TCP *:443 (LISTEN)`
		`sshd 29022 root 3u IPv4 225760 0t0 TCP 172.16.123.12:22->172.16.3.22:56613 (ESTABLISHED)`
		`sshd 29024 novatech 3u IPv4 225760 0t0 TCP 172.16.123.12:22->172.16.3.22:56613 (ESTABLISHED)`
		`apache2 29033 http 5u IPv6 225748 0t0 TCP *:443 (LISTEN)`
		`apache2 29033 http 22u IPv6 227781 0t0 TCP 172.16.123.12:443->172.16.3.22:56645 (ESTABLISHED)`
		`apache2 29033 http 24u IPv6 227782 0t0 TCP 172.16.123.12:443->172.16.3.22:56646 (ESTABLISHED)`
		`apache2 29033 http 25u IPv6 227783 0t0 TCP 172.16.123.12:443->172.16.3.22:56647 (ESTABLISHED)`
		`apache2 29033 http 26u IPv6 227784 0t0 TCP 172.16.123.12:443->172.16.3.22:56648 (ESTABLISHED)`
		`apache2 29033 http 28u IPv6 227458 0t0 TCP 172.16.123.12:443->172.16.3.22:56644 (ESTABLISHED)`
		`apache2 29033 http 31u IPv6 225963 0t0 TCP 172.16.123.12:443->172.16.3.22:56638 (ESTABLISHED)`

CIP-007	R1 (1.2)	Protect against the use of unnecessary physical input/output ports used for network connectivity, console commands, or removable media. **NovaTech Response:** This requirement does not apply to NovaTech Orion-based in-substation systems or to the NovaTech enterprise-based Intermediate System. It only applies to High Impact BES Cyber Systems and Medium Impact BES Cyber Systems at Control Centers. The OrionLX does make possible the physical removal of unused Ethernet ports and serial ports (modular cards). Unused USB ports are not removable.

CIP-007 R2 (2.1) A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.

CIP-007 R2 (2.2) At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.

CIP-007 R2 (2.3) For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions:

- Apply the applicable patches; or
- Create a dated mitigation plan; or
- Revise an existing mitigation plan.

Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.

CIP-007 R2 (2.4) For each mitigation plan created or revised in Part 2.3, implement the plan within the timeframe specified in the plan, unless a revision to the plan or an extension to the timeframe specified in Part 2.3 is approved by the CIP Senior Manager or delegate.

NovaTech Response for 2.1, 2.2, 2.3 and 2.4:

NovaTech monitors multiple sources for any vulnerabilities in the packages that run on the OrionLX platform. NovaTech releases updates for the OrionLX (including the O/S, the "OrionLX executive", and third party packages) on an as needed basis; historically these have averaged three per year for the past five years. These patches (bundled for convenience into "distros") do not always contain updates that will affect security, nor must they mandatorily be installed. Currently the updates are posted on the NovaTech Users Support website along with release notes. Notification of updates can also be emailed to users if they request this service.

CIP-007 R3 (3.1) Deploy method(s) to deter, detect, or prevent malicious code.

CIP-007 R3 (3.2) Mitigate the threat of detected malicious code.

NovaTech Response for 3.1 and 3.2:

All software packages that run on the OrionLX must be digitally signed files. Unsigned files will not install or corrupt the system. Furthermore, only authorized users (as determined by predefined "permissions" associated with individual users) are able to load packages. Any package that is not signed will not run and will be logged in the OrionLX syslog. The capture below shows the log for a successful file load and an unsuccessful file load:

Successful update (correct digital signature)

2014-07-18 14:21:50.936	audispd	INFO	node=orionlx.novatech.novatech-llc.com type=SERVICE_START msg=audit(1405711310.917:278): user pid=1 uid=0 auid=4294967295 ses=4294967295 msg=' comm="upgrade" exe="/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'
2014-07-18 14:21:50.340	systemd	INFO	Reloading.
2014-07-18 14:10:19.095	systemd	INFO	Starting Upgrade...
2014-07-18 14:10:18.851	Packaging	INFO	Installing package: nt-orion-selmaster

Failed update (incorrect digital signature)

2014-07-18 14:22:13.122	audispd	INFO	node=orionlx.novatech.novatech-llc.com type=SERVICE_START msg=audit(1405711332.990:281): user pid=1 uid=0 auid=4294967295 ses=4294967295 msg=' comm="upgrade" exe="/lib/systemd/systemd" hostname=? addr=? terminal=? res=failed'
2014-07-18 14:22:13.098	systemd	NOTICE	Unit upgrade.service entered failed state.
2014-07-18 14:22:12.998	systemd	NOTICE	upgrade.service: main process exited, code=exited, status=1/FAILURE
2014-07-18 14:21:59.127	systemd	INFO	Starting Upgrade...
2014-07-18 14:21:58.928	Packaging	INFO	Installing package: nt-orion-logicpak

CIP-007 R3 (3.3) For those methods identified in Part 3.1 that use signatures or patterns, have a process for the update of the signatures or patterns. The process must address testing and installing the signatures or patterns.

NovaTech Response:

NovaTech does not employ a technique that uses signatures or patterns to check for malware. Reason: Updating these signatures or patterns is required too often to be practical for OrionLX devices in remote, unattended substations. In addition, the process of updating the signatures or patterns introduces risk factors, particularly if done from a remote location.

CIP-007 R4 (4.1) Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events:
4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; and 4.1.3. Detected malicious code.

NovaTech Response:

OrionLX Syslog:

i. The OrionLX creates a "syslog" of all system alarms and events. These time-stamped logs, which can be sorted and filtered, contain the raw data required for NERC reporting, including:
    1. Who attempted access
    2. What they attempted to do
    3. Connect and disconnect information
    4. Packages running on Orion
    5. Passthrough attempts to IEDs
    6. Connection details

ii. The OrionLX "System Logger" function can be configured to make user-selected points available in syslog, including circuit breaker position and other events and alarms in Orion database not automatically logged to syslog.

iii. An automatic transfer of logged events can be set up between the OrionLX (the syslog client) and a remote syslog server, through webpage entries on the "Settings" page. Transfer of logged events to two or more remote servers is also possible.

OrionLX System Monitoring Points:

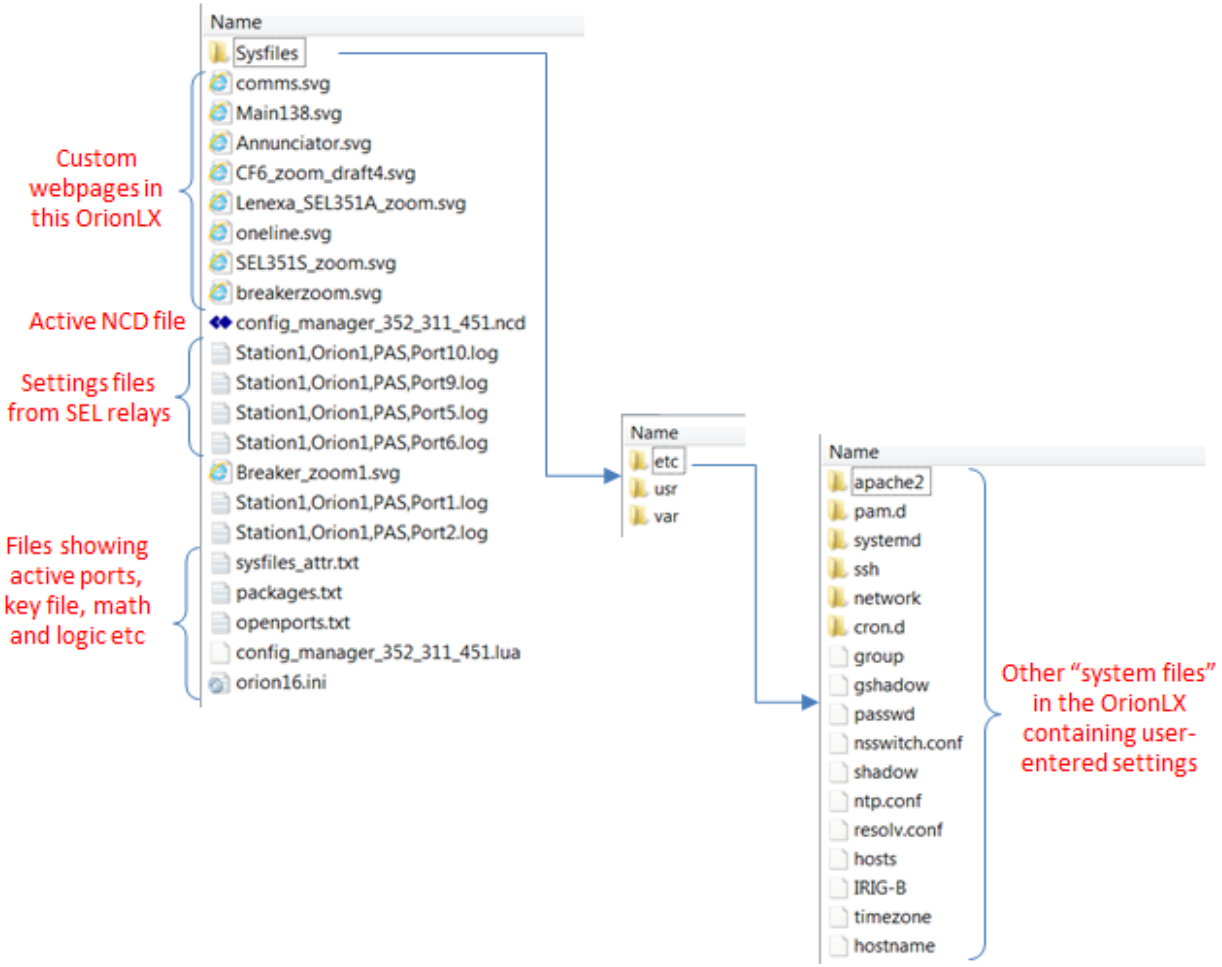
Security Monitoring Points indicating who is connected and how they are connected can be brought out of the OrionLX. These points can be mapped to SCADA or to an alarm log.

1. SSH session status
2. telnet session status
3. HTTP and HTTPS session status
4. Login TTY (serial port) session status
5. FTP session status
6. GDM (keyboard and mouse) session status
7. PPP session status
8. IEC 61131-3 session status
9. "Passthrough" session status
10. Root session status
11. Local or remote session status
12. Name of user logged in
13. How many users logged in
14. Known user login failure indication and name
15. Unknown user login failure indication and name
16. User lockout indication and name

CIP-007	R4 (4.2)	Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per CyberAsset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging. **NovaTech Response:** The OrionLX will only accept digitally signed files, and syslog will log an error if an attempt is made to load an unsigned file. Please see response at R3 (3.1 and 3.2) above for more detail. In addition, the OrionLX Configuration Manager Agent includes an option to calculate a checksum on the .zip file that contains all of the configurations in the OrionLX and the settings in SEL relays. If any of the constituent configuration files or executable code has been modifued, this checksum will change. The checksum can be forwarded to enterprise systems for comparison. To detect failure of event logging, the OrionLX can create a login event using logic, and then monitor whether the event was logged.
CIP-007	R5 (5.1)	Have a method(s) to enforce authentication of interactive user access, where technically feasible. **NovaTech Response:** The NovaTech Identity Manager (NIM) enforces all users to be centrally authenticated before they can interact with any OrionLX or SEL Cyber Assets. GE Cyber Assets planned for addition in 2015. The OrionLX supports remote authentication via LDAP and Kerberos. If remote, centralized authentication will not be implemented, the OrionLX can be configured with a password policy to force the use of strong passwords.
CIP-007	R5 (5.2)	Identify and inventory all known enabled default or other generic account types, either by system, by groups of systems, by location, or by system type(s).
CIP-007	R5 (5.3)	Identify individuals who have authorized access to shared accounts.
CIP-007	R5 (5.4)	Change known default passwords, per Cyber Asset capability **NovaTech Response to 5.2, 5.3 and 5.4:** The OrionLX comes standard with two default user accounts. One of these accounts is the "root" account. The root account cannot be removed, but the password can be changed. The root account is also only accessible to a user with a specific access permission ("wheel"), and can be configured for only local access. The second default user account is the "novatech" account. The novatech account should be deleted once the customer creates a new user.
CIP-007	R5 (5.5)	For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, non- alphanumeric) or the maximum complexity supported by the Cyber Asset.numeric **NovaTech Response:** These requirements are supported by the NovaTech Identity Manager (NIM). If remote, centralized authentication will not be implemented, the OrionLX can be configured with a password policy to force the use of strong passwords.
CIP-007	R5 (5.6)	Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months. **NovaTech Response:** These requirements are supported by the NovaTech Identity Manager (NIM). If remote, centralized authentication will not be implemented, the changing of the OrionLX password would be a procedural requirement for the Utility.

CIP-007	R5 (5.7)	Where technically feasible, either: •Limit the number of unsuccessful authentication attempts; or •Generate alerts after a threshold of unsuccessful authentication attempts. **NovaTech Response:** Only required at High Impact BES Cyber Systems and Mediaum Impact at Control Centers, but these requirements are supported by both the NovaTech Identity Manager (NIM) and the OrionLX. User Password Policy configuration parameters include how many attempts are permitted before the user is locked out, plus how long the user should be locked out. If remote, centralized authentication will not be implemented, The OrionLX can locally enforce incorrect login attempt rules, and generate a log entry for each unsuccessful attempt when the user is locked out. The OrionLX also has a lockout feature that temporarily locks out the user account after each unsuccessful login attempt to help prevent a brute force attack.
CIP-008	R1 (1.1)	One or more processes to identify, classify, and respond to Cyber Security Incidents. **NovaTech Response:** Logs are created by the NovaTech Identity Manager (NIM), the NovaTech Connectioin Manager (NCM) and by the OrionLX (syslog). These logs include time-stamped entries detailing user login, connection attempst, users actions, and any system modification. These logs can be forwarded to an incident and event management system such as the Tripwire(R) Log Center. In addition, the Security Monitoring Points generated by the OrionLX provided notification of login attempts, type of login and user name. These points can be mapped to SCADA or processed in OrionLX alarm management systems.
CIP-009	R1 (1.3)	One or more processes for the backup and storage of information required to recover BES Cyber System functionality.
CIP-009	R1 (1.5)	One or more processes to preserve data, per Cyber Asset capability, for determining the cause of a Cyber Security Incident that triggers activation of the recovery plan(s). Data preservation should not impede or restrict recovery. **NovaTech Response for 1.3 and 1.5:** The OrionLX Configuration Manager Agent retrieves and zips all configuration files from the OrionLX (points mapping configuration, math and logic, HMI screens, firewall settings, etc) plus settings from SEL relays. This zipped file is transfered via secure SFTP to one or more secure storage locations of user choice. If the OrionLX or SEL relay was compromised or destoyed, the files in storage could be loaded into replacement units to restore operation.
CIP-010	R1 (1.1)	Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and 1.1.5. Any security patches applied. **NovaTech Response:** The .zip file described in the response for 1.3 and 1.5 above, or the standard OrionLX sysfiles.zip file, contain all of the data described above. These files make up the baseline configuration for OrionLXs and SEL relays, and are transfered to an enterprise configuration management system for archival, such as the PAS Cyber Integrity system or the Tripwire File Integrity Manager.

CIP-010 R1 (1.1) (cont.) Below are captures showing some of the files that are retrieved, zipped and forwarded to an enterprise server for analysis:



CIP-010 R1 (1.2) Authorize and document changes that deviate from the existing baseline configuration.

CIP-010 R1 (1.3) For a change that deviates from the existing baseline configuration, update the baseline configuration as necessary within 30 calendar days of completing the change.

CIP-010 R1 (1.4) For a change that deviates from the existing baseline configuration:

1.4.1. Prior to the change, determine required cyber security controls in CIP-005 and CIP-007 that could be impacted by the change;

1.4.2. Following the change, verify that required cyber security controls determined in 1.4.1 are not adversely affected; and

1.4.3. Document the results of the verification.

NovaTech Response:

The OrionLX in the substation retrieves configuration files from protected cyber assets, zips them and transfers them to an enterprise configuration management system where the tasks in 1.2, 1.3 and 1.4 above can be performed. The "Tripwire Enterprise" product can process the zip file forwarded from the OrionLX.

CIP-011	R1 (1.2)	Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.
CIP-011	R2 (2.1)	Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.
CIP-011	R2 (2.2)	Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media. **NovaTech Response for 2.1 and 2.2:** The OrionLX can be manually reflashed to revert back to "default" (all of settings as the unit left the factory). This will erase all user-entered data.

Summary of User Password Management Features in the NovaTech Identity Manager (NIM)

1. Provides centralized authentication of users
2. Can be configured to set up a Trust with an Active Directory authentication system
3. Supports Role-based Authentication; each user (or group of users) can have their own privileges
   Examples:
   a. *Technician Group:* Permitted to view relay settings but not change settings, view HMI but not control critical devices, only acknowledge non-critical alarms, attach using SSH but not HTTPS, etc.
   b. *Manager Group:* Same privileges as Technician group but additional privileges to change settings, control critical devices, acknowledge critical alarms
   c. *IT Group:* Permitted to change IP addresses, firewall settings, etc. but not permitted to have access to "non-IT" settings or controls
4. Supports creation of strong password rules that meet IT industry standards
   a. Rules can vary for different User Groups; "Manager Group" may require stronger password construction, or more frequent password changing than "General Group".
5. Complete logging of all changes

Summary of IED (Host) Password Management Features in the NovaTech Identity Manager (NIM)

1. Provides centralized administration of IED passwords
2. Currently designed for management of SEL relay passwords. Other IEDs will be added in future development phases.
3. SEL relays can be placed into groups for simplified administration.
   a. For example: "Transmission Relays", "Distribution Relays", "Critical Relay Assets", "Non-critical relay Assets", etc.
4. Rules can be created for specific IED password construction.
   a. For example, the password construction rules for an SEL-421 are different than the rules for an SEL-501.
   b. Enables SEL relays to be secured with the strongest passwords possible
5. Complete activity logging provided
6. SEL relay Password Change Modes:
   a. *Normal Password Change Mode*
      i. Select specific SEL relay, or SEL relay group, to be changed.
      ii. View password policies for the SEL relays in the selected group (different relays in the group may have different password policies).
      iii. Enter in new passwords, or have system generate random passwords.
      iv. Send passwords to relays in the selected group.
      v. All actions logged

Summary of IED (Host) Password Management Features in the NovaTech Identity Manager (NIM) - Continued

b. *Maintenance Mode*
   i. This mode is for crews in substation performing upgrades and reconfigurations.
   ii. Passwords for substation IEDs are temporarily changed to a "maintenance" password.
   iii. Maintenance password is well known.

c. *Emergency Mode (or "Password Checkout" Mode)*
   i. Generally only used if the broadband connection to the substation has been lost.
   ii. Administrator can view passwords and divulge to utility people in substation.
   iii. All administrator actions logged.

d. *Local Password Caching in the security gateway*
   i. Caching for accessing OrionLX and accessing SEL relays when the connection to the enterprise server is not available
   ii. Caching incudes settings for:
      1. Enable / disable caching
      2. How long caching is enabled after connection to the remote server is lost

NovaTech, LLC 13555 West 107th Street Lenexa, KS 66215 Phone (913) 451-1880
www.novatechweb.com
orion.support@novatechweb.com