

The OrionLX/Orion5rL Automation Platforms are designed with access controls, intrusion protection and security logging to meet or exceed NERC CIP Cyber Security standards for critical cyber assets. The OrionLX/Orion5rL are designed to provide a migration path to upgrade the existing Orion5/Orion5r platforms to meet these new security requirements. Configuration conversions tools are provided to preserve engineering investments. This table summarizes security features on the OrionLX/Orion5rL compared to the Orion5/Orion5r.

Security-Related Feature	OrionLX / Orion5rL	Orion5 / Orion5r
Operating System	Assembled from open Linux modules from www.kernel.org (V2.6.x and above). Kernel specifically tailored for substation automation applications, including: <ul style="list-style-type: none"> - modules for processing IRIG-B - 1ms time-tagging of physical inputs - Real-time preemption (prevention of o/s delays) 	Windows CE
Security-related parameters excluded from Orion NCD configuration?	Yes. OrionLX/Orion5rL IP address, OrionLX/Orion5rL passwords and other security settings all configured online through secure HTTPS (SSL) browser interface.	No. Orion5/Orion5r IP address and Orion5/Orion5r passwords in clear text.
Front Maintenance Port Security	Password required per strength defined below.	No password required.
Ethernet Port Security	Password required per strength defined below. See encrypted protocol support below.	Password required. No encrypted protocol support.
Passwords Strength	Admin-defined number of characters, min types of characters, duration, lockout criteria, etc. See additional details in IEEE 1686 Compliance Table AN-0310-02.	(telnet connections only) <ul style="list-style-type: none"> - up to 25 characters long - case-sensitive - no limitations or requirements on the characters used
User Privileges	Yes, per individual user, including: <ul style="list-style-type: none"> - Viewing privileges - Control privileges - Load / Install privileges - Passthrough privileges - Alarm Acknowledgement privileges <p>Uses pluggable authentication modules (PAM)</p>	No user privileges.
Remote Authentication	LDAP\Kerberos with support for: <ul style="list-style-type: none"> - Identity caching - Password caching - Active directory (with proper configuration - call factory) 	No remote authentication supported.
Firewall	Yes. Uses netfilter/iptables supporting stateless and stateful packet filtering. Connection tracking provided by (ip_conntrack, nf_conntrack). Firewall configuration tool through web browser provided.	Basic firewalling can be set up at command line, but limited to following commands: allow (with inbound and outbound), block, info, flush, commit, enable, disable.



Security Features Comparison

OrionLX/Orion5rL vs. Orion5/Orion5r

Security-Related Feature	OrionLX / Orion5rL	Orion5 / Orion5r																		
Encrypted Protocols – Engineering and Maintenance	SSH	No (only telnet)																		
Encrypted Protocols – Webpages	HTTPS	No (only HTTP)																		
Encrypted Protocols – File Transfer	sFTP	No (only FTP)																		
VPN Support	Yes, using OpenVPN	No																		
Key Management	Yes. Functions supported: <ul style="list-style-type: none"> - Create new keys (hardware based random number generator utilized to create truly random keys. Meets FIPS 140 standard) - Import keys - Export keys 	No																		
Cryptographic Functions	<table style="border: none;"> <tr> <td>Secret Key:</td> <td>Public Key:</td> <td>Hash:</td> </tr> <tr> <td>AES</td> <td>DSA</td> <td>SHA-1</td> </tr> <tr> <td>RC4</td> <td>RSA</td> <td>MD5</td> </tr> <tr> <td>CAST5</td> <td></td> <td></td> </tr> <tr> <td>Blowfish</td> <td></td> <td></td> </tr> <tr> <td>3DES</td> <td></td> <td></td> </tr> </table>	Secret Key:	Public Key:	Hash:	AES	DSA	SHA-1	RC4	RSA	MD5	CAST5			Blowfish			3DES			No
Secret Key:	Public Key:	Hash:																		
AES	DSA	SHA-1																		
RC4	RSA	MD5																		
CAST5																				
Blowfish																				
3DES																				
Package Install	Any firmware loaded to the OrionLX/Orion5rL must be digitally signed in order to load on the OrionLX/Orion5rL CPU.	No digitally signed firmware option																		
Protection against malicious software	All software packages that run on Orion are “signed” files. Unsigned files will not install or corrupt system. Only authorized users (as determined by predefined privileges associated with individual users) are able to load packages.	No digitally signed firmware option																		
Cyber Security Logging	<p>Orion creates syslog files which include:</p> <ul style="list-style-type: none"> - Who attempted access - What they attempted to do - Passthrough attempts to IEDs - Package Installations - Connection details <p>The Orion “System Logger” function can also be configured to make selected points available in syslog, including circuit breaker position and other events and alarms in Orion database not automatically logged to syslog.</p>	No Cyber Security logging																		

Contact:

NovaTech, LLC
 Orion Utility Automation
 13555 West 107th Street
 Lenexa, KS 66215

T: 913.451.1880
 F: 913.451.2845
 E: orion@novatechweb.com
www.novatechweb.com