SECURE NETWORK REFRESH: PCN Switches

Product Information Note

A large number of Process Control Network (PCN) switches located in layers 1, 2, 3, and 3.5, have reached their end-of-life and are no longer supported by the manufacturer. For many of these switches, both the hardware and software are obsolete, some as early as 2009.

Additionally, these switches represent an era of equipment where the focus was solely on connectivity, with no eye to security. Installation configurations often did not invoke even rudimentary security measures. Operating software did not include security features commonly implemented in today’s industrial control environment. Also potentially missing are the corresponding upstream router and firewall configurations for optimum protection. As a result, critical security elements that protect the network from takeover are not in place.

Secure Network Refresh PCN Switches: Features

- A basic cyber security walk-through
- New switches that provide:
  - Encryption support for configurations and secure access
  - Increased switch processing capacity to support advanced features such as encryption and port mirroring
  - Higher speed interfaces to avoid network oversubscription (10/100/1000Mbps)
  - Improved network packet buffering to help prevent dropped packets and frame errors
- Replacement, configuration, and testing of new switches including:
  - Configuration for both connectivity and security
  - Verification of Fault Tolerant Ethernet (FTE) status
  - Installation of most current version of Honeywell validated IOS supporting encryption
  - Switch configuration for support of Network Time Protocol (NTP) if an NTP server is present
  - Simple Network Management Protocol (SNMP) configuration of the new switches including appropriate trap reporting
  - Setup and fine tuning of Secure Shell (SSH) configurations
  - Verification of router configuration for secure communications to newly installed switches

Plus, switch configuration is implemented by Honeywell Cyber Security personnel to ensure optimum protection and inclusion of important security safeguards. All designed to improve the security and communications of the switch portion of the PCN network.

PCN Switches: Key Security Elements

<table>
<thead>
<tr>
<th>SECURITY ELEMENT</th>
<th>PROTECTION ADVANTAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internetwork Operating System (IOS) Encryption (k9)</td>
<td>Updated operating system to support payload and configuration encryption using SSH (AES/3DES)</td>
</tr>
<tr>
<td>SSH Enabled</td>
<td>SSH encryption provides security for switch configuration. Using passwords and keys, configuration and configuration communications are encrypted. Prior switch IOS versions used Telnet which had no security measures. Telnet communications, including passwords and configurations, were in the clear and left the switch vulnerable to take over</td>
</tr>
<tr>
<td>SNMP v3 Support</td>
<td>SNMP v3 provides improved secure SNMP communications between network devices by using both authentication and encryption</td>
</tr>
<tr>
<td>Port Mirroring Capability</td>
<td>Processing power needed to support Port Mirroring, used for deep packet look up in order to detect malware and intrusions</td>
</tr>
</tbody>
</table>
Secure Network Refresh

Many old or obsolete PCN switches, routers, and firewalls do not meet today’s cyber security standards. As a result, this equipment presents a considerable vulnerability to the security of the network and process operations. Additionally, out of support equipment is often not repairable and raises the potential of longer downtimes in the event of a failure. This older equipment needs to be replaced with new hardware, current software, and updated configurations to support today’s security measures.

Secure Network Refresh provides:

- Targeted PCN security upgrades providing equipment improvements, software enhancements, and strengthened cyber security configurations
- Elimination of obsolete equipment and vulnerable operating systems
- Equipment architecture engineered for today’s industrial plant performance and cyber security protection
- Improved cyber security maturity rankings for equipment, security processes, and security practices
- New equipment installation and updated configurations performed by Honeywell’s Industrial Cyber Security personnel

Complete Cyber Security Solutions

Honeywell Industrial Cyber Security is the leading provider of cyber security solutions that help protect the availability, safety and reliability of industrial facilities and helps securely deploy IIoT technologies. Leveraging our industry-leading process control and cyber security experience, expertise and technology, Honeywell delivers complete, proven solutions designed for the specific needs of process control environments and critical infrastructure sectors.

In addition to the Secure Network Refresh PCN Switches, our portfolio includes Managed Industrial Cyber Security Services and the Honeywell Industrial Cyber Security Risk Manager solution which proactively monitors, measures and manages industrial cyber security risk. We also offer consulting and remediation services including security assessments and audits, architecture and design, network security, endpoint protection, situational awareness, and response and recovery. These solutions are enabled by innovative technology and delivered by a global team of cyber security experts.

For More Information

Learn more about Honeywell Industrial Cyber Security Solutions, visit www.becybersecure.com or contact your Honeywell Account Manager.

Honeywell Process Solutions

1250 West Sam Houston Parkway South
Houston, TX 77042

Honeywell House, Arlington Business Park
Bracknell, Berkshire, England RG12 1EB UK

Shanghai City Centre, 100 Zunyi Road
Shanghai, China 200051

www.honeywellprocess.com

PIN-16-14-ENG
August 2016
© 2016 Honeywell International Inc.