8. Protect Industrial IoT Infrastructure

https://www.insight.tech/content/protect-industrial-iot-infrastructure-with-converged-it-ot-security-gateways

Protect Industrial IoT Infrastructure with Converged IT/OT Security Gateways. (2017, July 13). https://www.insight.tech/content/protect-industrial-iot-infrastructure-with-converged-it-ot-security-gateways

1. **Increasing Connectivity and Cybersecurity Risks in OT Environments**: The paper begins by discussing how Industrial and mission-critical facilities are increasingly being digitized and connected for enhanced efficiency and insights. However, this connectivity exposes traditional Operational Technology (OT) infrastructure like PLCs, RTUs, and SCADA systems to sophisticated cyberattacks.

2. **Inadequacy of Traditional IT Security in OT Contexts**: Max Lee, CTO at Lanner Electronics Inc., points out that traditional IT security is not equipped to protect ICS and SCADA networks, as it's designed for enterprise networks and not for segregated OT environments.

3. **Need for Industrial-Grade Security Measures**: The paper emphasizes the necessity of deploying industrial-grade firewalls in harsh industrial environments to protect critical OT devices like PLCs and RTUs, highlighting the importance of features like surge protection and wide operating temperature ranges.

4. **Integration of IT and OT for IIoT Security**: The paper discusses the need for a mutual understanding of IT and OT requirements in implementing secure Industrial Internet of Things (IIoT) network architectures. This includes connecting OT systems to IT infrastructure for data utilization while addressing security concerns.

5. **Challenges in Connecting Legacy and Modern Systems**: The paper notes the difficulties in integrating legacy industrial devices with modern IT firewalls, due to differences like the lack of serial ports in IT firewalls, creating potential security loopholes.

6. **Converged IT/OT Security Standards and Gateways**: The paper discusses the role of standards like IEC-61850 and the Critical Infrastructure Protection (CIP) standards by NERC in bridging IT and OT security. Vendors like Lanner Electronics are developing IT/OT gateways based on these standards to serve as multilayer network security platforms.

7. **Lanner's IT/OT Security Gateway Solution**: The paper introduces Lanner's LEC-6032 as an example of an IT/OT security gateway. This industrial-grade fanless embedded system, powered by an Intel Atom® E3845 processor, acts as a firewall and UTM device, integrating SCADA, PLCs, and log servers for OT, and protecting ERP, PLM, and mail servers for IT. The processor's features, including virtualization functions and AES-NI

technology, are highlighted for their role in enhancing security and network defense in OT environments.

These key points collectively underscore the critical need for advanced, integrated cybersecurity solutions in the evolving landscape of industrial IoT and the convergence of IT and OT systems.