Bringing Enterprise-Class Security to IP-Based Field Area Communication Networks

Modern field automation systems such as smarter grids, mining management systems, traffic signal management and SCADA systems require two-way information flow. Systems that have traditionally used physically isolated, proprietary networks are evolving toward integrated, open standard, IP-based architectures to facilitate communications. The functionality and integration of wireless IP field automation networks provide substantial value but come with fear of increased exposure to cyber-attacks. This challenge can be met by bringing enterprise-class security to field area networks.

The Evolution of Field Area Communication Networks

Utility, mining and other industries are increasingly using wireless communication networks to monitor and control thousands of automation devices in the field and large outdoor facilities. These field automation networks support diverse applications including advanced metering infrastructure and distribution automation for utilities; telemetry and mining management systems for mining; wellhead monitoring and logging for oil and gas; traffic signal management and video monitoring for transportation; process control for refining and chemicals; and SCADA for a variety of vertical markets.

In the past, utilities and other industrial companies have often used proprietary low-speed wireless communication systems with little security to implement their field automation networks.Increasingly, these industries are turning to secure, open standard IP-based technology to provide field communications.

IP-based wireless field area communication networks provide many advantages. When built using standard technologies such as 802.11 and/or 802.16, they provide high speed and low latency compared to the proprietary networking technologies traditionally deployed in the field, enabling many field automation applications to run on one network. They are very reliable, especially when tools such as mesh routing and TCP with reliable data delivery are employed. IP networks provide interoperable communications for a plethora of diverse endpoints. Unifying communications for many automation applications on one network provides for economical implementation, central management and consistent, end-to-end security policies.

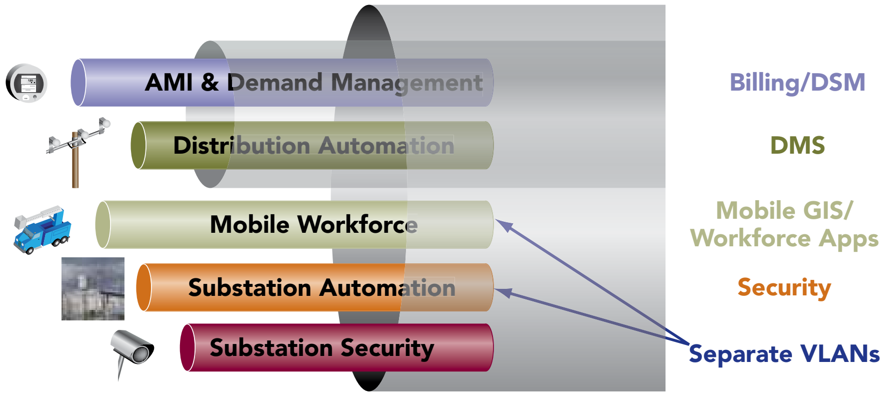
Although the increased functionality and integration of wireless IP field automation networks provide substantial value, they come with fear of increased exposure to cyber-attacks. There is legitimate concern that the tools used by hackers to attack internet sites and enterprise networks could be used to attack IP-based field automation networks. IP networks also face the challenge of securely incorporating legacy field automation devices. These challenges can be met by bringing enterprise-class security to field area communication networks and the systems that manage them.

Bringing Enterprise-Class Security to Field Area Communication Networks

While IP-based field area communication networks present security challenges, they also brings security advantages. Chief among these is that the tools and techniques used to thwart cyber-attacks on IP networks have been honed for years by enterprises and are constantly being updated by the security community to battle emerging threats.

For more than a decade, enterprises have faced the same security challenges that now confront IP-based field area communication networks. As a result, a robust set of tools and techniques that are proven and time-tested have been developed to combat cyber-attacks on enterprise networks. Enterprises with stringent security requirements such as financial firms and the federal government have successfully transitioned to IP while strengthening their security capabilities. Enterprise network security tools that can and should be leveraged in field area communication networks include:

- Internet Protocol Security (IPsec) virtual private networks (VPNs) authenticate the endpoints of a network connection and encrypt data transmission between the endpoints, securing both system access and transmitted data.
- Firewalls permit traffic for only authorized applications, protocols and users to travel over the network while blocking classes of traffic that are not permitted by the forwarding policy. When extended to the edge, firewalls can be used as an effective mechanism for protecting field area assets.
- RADIUS, 802.1x, and 802.11i authentication prevent unauthorized users and devices from accessing the network and enforce strong endpoint authentication.
- AES encryption prevents eavesdropping on management and control traffic as well as data transmission.
- HTTPS-based remote access enables secure device management.
- Virtual local area networks (VLANs) enable traffic from different applications and user groups to be segregated and permit security policies to be tailored to the needs of each application/user group.

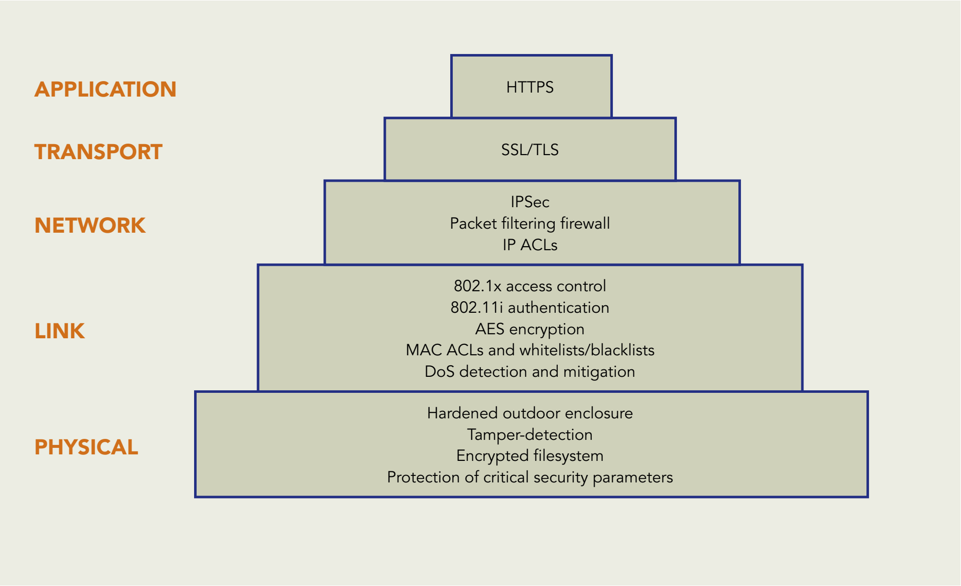


Traffic separation and application-based prioritization

Figure 1: VLANs Enable Multi-Application Security

The capabilities noted above have significant overlap. This is desirable as it permits implementation of a multi-layer security model that provides defense-in-depth. For example, a field area communication network could control access using both firewalls and IPsec VPNs. If an intruder was able to defeat the firewall by, for example, spoofing the IP address of a legitimate user, they still could not access the network because they would lack the credentials required to log in to the VPN. Employing a defense-in-depth strategy can make the amount of resource required to penetrate the network prohibitively high for the would-be attacker.

Another security advantage of IP-based communication network architectures is the existence of a large and active internet and enterprise security community. This community consists of security solution vendors, government-funded organizations (government agencies such as CNSS and outside bodies such as CERT), the security researcher community and others. These groups and individuals discover and publish vulnerabilities, ensuring transparency from vendors of IP-based systems regarding the security of their products. They also provide solutions that correct security weaknesses which can be leveraged by organizations that have deployed IP networks.



APPLICATION	HTTPS
TRANSPORT	SSL/TLS
NETWORK	IPSec Packet filtering firewall IP ACLs
LINK	802.1x access control 802.11i authentication AES encryption MAC ACLs and whitelists/blacklists DoS detection and mitigation
PHYSICAL	Hardened outdoor enclosure Tamper-detection Encrypted filesystem Protection of critical security parameters

Figure 2: Multi-Layer Security Provides Defense in Depth

Extending Secure IP Communications Networks to Legacy Field Automation Endpoints

A common challenge in migrating from proprietary to IP-based field area communication networks is integrating legacy field automation endpoints that don't support IP, Ethernet or standard wireless connections. Not only must legacy endpoints be able to communicate over the IP field area communication network, they must be able do so securely. Stranding legacy field assets, forcing their wholesale replacement or leaving them unsecured simply are not options.

To ensure successful integration, IP field area communication networks must support the physical interfaces used by legacy endpoints, most commonly RS-232 or RS-485 serial, and convert them so they can be carried over standard wireless and Ethernet connections. The networks must also support translation or tunneling mechanisms so that data originally encapsulated in widely used utility and industrial control protocols, including DNP3, Modbus, SEL Mirrored Bits and IEC 61850, can be transported securely across the IP network. Finally, points where legacy devices connect to the IP field area communication networks must be as secure as interfaces to field automation devices that natively run IP.

The Devil is in the (Implementation) Details

Where security is implemented in a field area communication network is just as important as what is secured and how it is secured. For maximum protection, security must be enabled at the edge of the network, in addition to locations closer to the network's core.

Whenever possible, VPN connections should terminate inside field automation endpoints. For field automation assets that don't support VPNs, the best protection is offered when the network infrastructure devices to which they connect can terminate VPN connections at the port where they connect.

Other security functionality, including firewalling, authentication and encryption, should also be implemented in the network infrastructure devices to which field automation assets connect. Enforcing security policies at the edge of the network prevents unauthorized traffic from consuming network capacity and unauthorized users from probing network resources closer to the network core for security vulnerabilities.

Network Management: An Essential Element of Enterprise-Class Security

The wireless network management systems used to monitor and control field area communication networks play an important role in securing them. There are three main requirements for network management with respect to field area communication network security:

- Secure Management: Wireless network management systems and communication between network management systems and network devices in the field must be secured. This can be accomplished using industry standard tools and best practices including role-based authentication with individual user accounts and passwords; encrypting data at rest (e.g., in management server disk, RAM or ROM; field device RAM or ROM) using AES; encrypting management and control information traversing the network using AES; and using secure protocols such as SSH, HTTPS, SNMPv3 and XML/SSL for configuration, troubleshooting and management.
- Consistent Enforcement of Policies: Systems used to manage field area communication networks must ensure complete, consistent, end-to-end application of security policies. They must support over-the-air configuration changes to all network devices in the field; confirm successful upload of new configurations in all network devices before initiating configuration changes; and confirm that the new configuration has been successfully activated after initiating a change. Further, the network management system must allow operators to change security policies dynamically as new applications are added. This includes the ability to create new VLANs, modify firewall rules, and configure access control and authentication mechanisms from a single window that ensures security policies are consistently maintained across the network.
- Audit Trails, Logging and Notification: Field area communication network management systems must provide an audit trail for post-mortem analysis of attempted and successful breaches as well as unauthorized configuration changes and attempts, whether unintended or malicious. This can be accomplished using industry standard Syslog files that contain a time-stamped record of all attempted and successful logins to the network management system and network devices; all attempted and successful configuration changes; and all network alerts, alarms and events. Also, log files must identify the user ID responsible for logins and attempts as well as configuration changes and attempts. By synchronizing time across the network using a standard method such as the Network Time Protocol (NTP), the time stamp information in the log files can be relied on to provide event correlation across the network. In addition to logins and configuration changes, other security-related events – both general network events such as DoS attack detection and wireless network specific events such as evil twin detection – must be logged. Important and serious events must also generate an immediate notification to the network operator via the network management system console, SMS text, page, and/or email.

Considering these requirements when rolling out field area communication network security will ensure that network management is an asset rather than a weak link in the overall security scheme.

Summary

Wireless IP field area communication networks provide substantial value but come with increased exposure to cyber-attacks. The robust, time-tested set of tools and techniques that have been developed to combat cyber-attacks on enterprises can provide cybersecurity for field networks that is comparable to that of the most mission-critical enterprise networks in the world.

While properly securing field area communication networks is necessary to ensure field automation cybersecurity, it is not the only consideration. In addition, where applicable, proper deployment and use of anti-virus and anti-spyware software, intrusion detection systems and role-based authentication with robust passwords as well as strong physical security is required to fully protect valuable field cyber assets.

For more information please contact:

ABB Inc.
Tropos Wireless Research Center
555 Del Rey Avenue
Sunnyvale, CA 94085, USA
Phone: +1 408 331 6800
E-Mail: sales@tropos.com

www.abb.com/tropos