Industrial Network security

Introduction

The purpose of this white paper is to investigate the requirement for security in industrial networks and to discuss common security policies used within organisations. It also aims to highlight the features and benefits of industrial grade security appliances as opposed to commercial grade equipment, including where and why it should be considered over its commercial grade counterparts.

Background

Historically, industrial networks such as process control, industrial automation or SCADA (Supervisory Control and Data Acquisition) systems have commonly been based upon proprietary protocols and operated in isolated environments with no wide area network connection; because of this, industrial networks which protect our critical assets have long been considered secure against the threat of cyber attacks, a problem that has troubled enterprise class networks for decades.

Today, many industrial networks have made the move to open source standards such as TCP/IP in order to increase interoperability and simplify developments, such networks are also more commonly connected to the outside world in order to communicate with remote sites and equipment. Due to the fact that open source protocols are widely understood and available and that wide area network connections offer a gateway for network access from outside intruders, industrial networks have become susceptible to viruses and security breaches.

What are the Risks

Types of cyber attacks include deliberate events such as external hacks, Denial of Service (DoS) attacks, and virus/worm infiltrations, as well as accidental cyber-related incidents. Such intrusions have serious ramifications for industrial control systems and can cause significant damages, risks to personnel safety, and potentially effect manufacturing production levels.

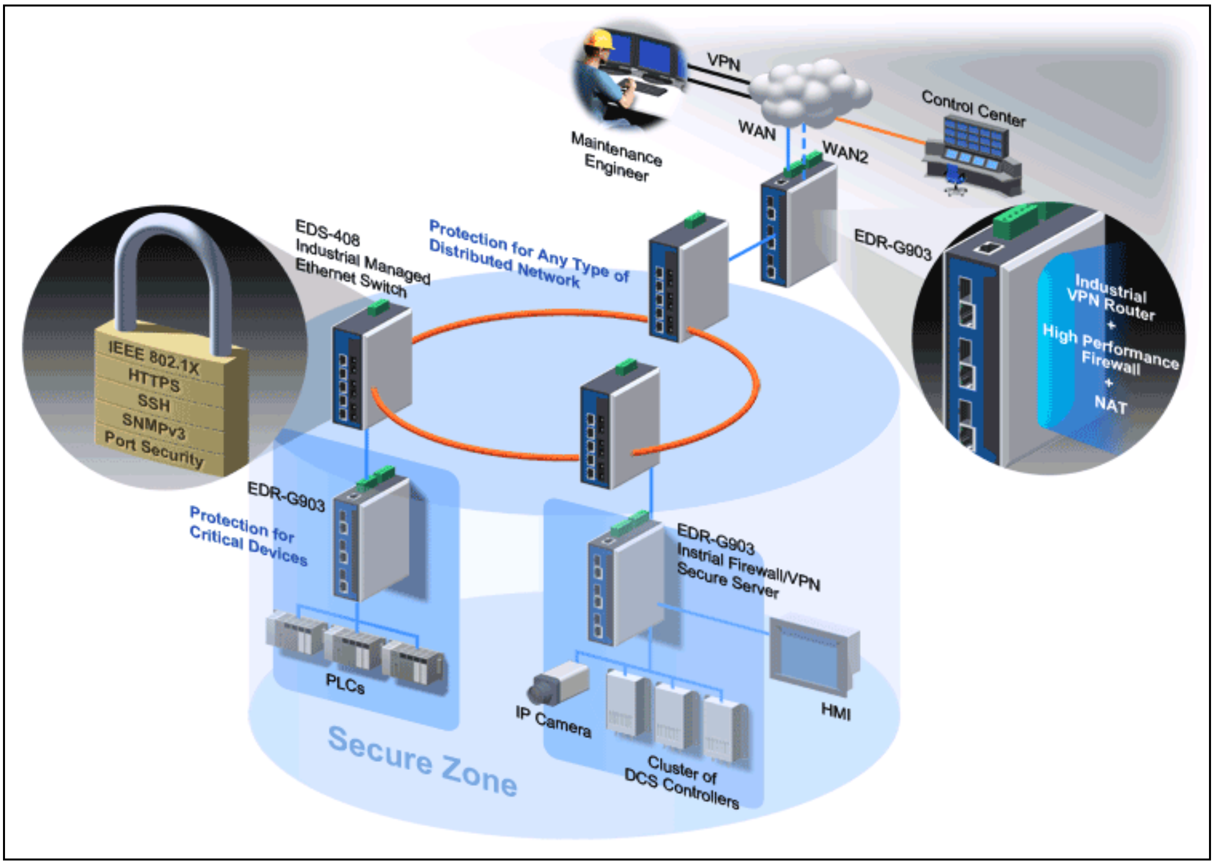
Security Policies within Organisations

In today's industrial network environment, an end to end, layered security approach is required in order to sufficiently reduce industrial network vulnerabilities. To minimise security risks, industrial facilities can adopt a number of precautions, with the overall goal of layering multiple security solutions so that if one fails, another can take up the line of defence. Some of the components involved with implementing an effective security strategy are:

- *Perimeter Firewalls:* Primarily a hardened perimeter must be established, acting as a barrier between two LANs or a WAN connection. This can be achieved with the use of a firewall/router which is configured to carefully control what data passes through and to restrict unauthorized incoming or outgoing network access.
- *Transparent Firewalls:* To introduce greater defence in depth, networks can adopt bridge mode firewalls (or transparent firewalls) to filter traffic between separate

network zones without separating the zones into different subnets, effectively acting like a layer 2 switch with a firewall. This provides inter-network security which prevents potential breaches from spreading further into the overall network, thereby limiting any potential harm.

- *VPNs and VLANs:* Virtual Private Networks and Virtual LANs can be implemented to provide secure, reliable transport of data across unsecure networks and the internet. VPN services implement authentication and encryption of data, creating a safe tunnel for data to pass through when site-to-site and client-to-site communication is required.
- *Physical security:* Protecting premises equipment is crucial in order to safe-guard against direct unauthorised access to sensitive equipment and data. Building access security and locked cabinets is essential.
- *Port access control:* In addition to denying access to the premises, control of port access can be secured, effectively disabling the ports to any un-authorised equipment that attempts to connect.
- *Password protection/Authentication:* Managing the authentication of equipment access should be both strict and prudent, with regular password changes an essential practice.
- *Fibre optic cable:* Light passing through fibre optic cabling is considerably more secure than an electronic signal passing through a copper cable, this is because the magnetic field created by the movement of electrons across a conductor (Ethernet over CAT5/6 cable) can be picked up by specialist equipment and the data can be "tapped" into illegitimately.
- *Employee Training:* Security is only as effective as the practices that are in place. Accidental employee security breaches can be caused in many different ways, such as relaxed password management, user error and unintentional changes to the security policy.


VPN
WAN
WAN2
Maintenance Engineer
Control Center
EDR-G903
Industrial VPN Router + High Performance Firewall + NAT
EDS-408 Industrial Managed Ethernet Switch
Protection for Any Type of Distributed Network
IEEE 802.1X
HTTPS
SSH
SNMPv3
Port Security
EDR-G903
Protection for Critical Devices
EDR-G903 Instrial Firewall/VPN Secure Server
PLCs
IP Camera
HMI
Cluster of DCS Controllers
Secure Zone

A layered secure network with a Moxa EDR-G903 perimeter Router/firewall/VPN and multiple EDR-G903 transparent firewalls protecting mission critical industrial networked equipment.

Equipment Required for Secure Industrial Networks
Routers with firewall protection and VPN support will provide the main crux of the security for a network to perform both perimeter defence and transparent protection in front of the most critical devices. Whereas the perimeter defence will commonly be protected by an enterprise class router/firewall located in an office environment, transparent firewalls are often required to be located in more demanding environments.

Industrial networks require industrial grade equipment in order to cope with higher environmental and application specific demands. Commercial grade equipment is more often than not completely incapable of dealing with such requirements. Some key considerations in the selection are as follows:

- *Wide operating temperature:* Where commercial grade equipment needs to be housed in a temperature controlled environment, specialist industrial grade equipment can reliably operate in temperatures reaching up to -45°C up to 85°C.
- *Metal/rugged enclosure:* Commonly you will find commercial equipment housed in plastic enclosures; this is vulnerable to damage in an industrial environment where there is a greater risk of accidental damage through nearby operations, dust and the harmful ingress of water. Industrial grade equipment employs a hardened design to protect against such possibilities.
- *EMC/EMS tested:* Electromagnetic Compatibility and Electromagnetic Susceptibility testing of industrial grade equipment ensure that there is suitable amount of

protection from outside interference and that the equipment itself will not interfere with any critical equipment in the proximity.

- *Conformal coating:* Extra protection against ingress from water, oil and chemicals can be achieved by coating the electronic circuitry with a special material called conformal coating.
- *Fan-less design:* Although fans are an effective way of keeping internal components cool and thus improving reliability, they do have a limited life cycle and are commonly the first element of a system to fail. Industrial grade equipment is designed with convection cooling techniques in order to remove fans whilst maintaining operation in a wide range of operating temperatures.
- *Wide Voltage input:* Many industrial environments have pre-installed power systems and/or use static power supplies to power equipment. For flexibility, Industrial equipment will often accept common nominal voltage level inputs.
- *High MTBF figures:* Mean Time Before Failure figures offer a means of predicting the elapsed time between inherent failures of a system during operation, high reliability industrial equipment offers superior values because of the level of build quality and the use of high grade components.
- *Extended warranty:* Industrial equipment backs up its reliability claims with a manufacturer warranty of up to 5 years

In Conclusion

A secure Industrial network relies on strength-in-depth strategy, where critical, industrial, network devices are protected by a corporate firewall and a sensible company approach to security policies. In many cases the security solution also includes placing security appliances directly in front of the most critical assets or groups of critical devices. This approach has been a real driving force behind the development of industrial grade security appliances, such as routers and firewalls. This is because of the requirement of locating equipment in demanding environments and the fundamental necessity of guaranteed zero network downtime, a priority for all industrial networks.