Five Future Challenges for Industrial Ethernet Switches

Executive summary

The benefits of IP convergence, such as enhanced efficiency, improved manageability and lower cost of ownership, have long been the driving force behind the growth in the number of industrial Ethernet deployments for supervisory and control level applications. According to studies conducted by IMS Research, the global number of industrial Ethernet nodes at supervisory and control levels will continue to grow at an average rate of 15% from 2010 to 2015. However, the number of field level nodes for industrial Ethernet will grow at an average rate of approximately 36%.

These projections confirm steady industry wide acceptance of industrial Ethernet technology, but also pose hidden threats to industrial network availability resulting from inherent challenges found in field level environments. This paper will discuss how future industrial Ethernet networks can introduce new challenges for industrial switch reliability, bandwidth availability, switch security, switch manageability and network redundancy.

Switches must resist field level environmental impact

If industrial Ethernet technology is increasingly deployed at remote field locations, industrial Ethernet switch reliability will need to be robust enough to handle harsh field site conditions, these can include high voltage transients, severe shock and vibration and extremely high temperatures.

High voltage transients can result from ESD, surge, burst, EFT, and even lightning strikes. Industrial switches should be capable of withstanding high voltage transients with high electromagnetic protection.

Electrostatic discharge (ESD)

ESD is the sudden transfer of static electricity between two objects with different electrical potentials. For example, factory workers wearing rubber boots and gloves can easily accumulate high levels of static electricity. Physical contact with switch devices can discharge several kilovolts (kV) of static electricity and permanently damage internal circuitry.

Surge/burst/electrical fast transients (EFT)

Switching disturbances and short circuits can inject high level voltage spikes to cause serious damage to electronic devices. Industrial high powered equipment/machinery can require large amounts of energy to switch on and turn off components such as motors and hydraulic systems. This switching can abruptly generate high quantities of power flow, disrupting the steady voltage flow in an electrical system, which can be severe enough to instantly damage, or gradually degrade, device system circuitry.

Electrical field emissions (radiated)

Not to be confused with conducted electromagnetic emissions, electrical field emissions can affect almost every device. Electromagnetic radiation can be emitted by one device to generate RF currents in surrounding devices, causing electromagnetic disturbances and even possibly damaging a device. RF shielding, such as metallic device housings, can effectively repel electrical field emissions.

Shock and vibration can disconnect wires for communication or power. Long term exposure to shock and vibration can eventually result in electrical shorts, broken solder joints, loose PCB components, PCB delamination and cracked device housings. Shock and vibration can also disable a switch by shaking loose wires for power, data, and redundancy. Remote field locations with moving heavy machinery or nearby vehicular traffic will require industrial switches with robust shock and vibration resistance.

Extreme temperatures can quickly deteriorate internal circuitry. Extreme outdoor temperatures can reach below freezing at night, and rise to an excess of 50°C (122°F) during the day. Temperatures inside roadside cabinets can in some instances reach extreme temperatures of over 60°C (140°F). Thermal stress/cycling will cause PCBs to expand and contract, which can also cause broken solder joints and PCB delamination. Remote field locations will probably not have air conditioning, high temperature tolerance with optimal heat dissipation is necessary to prolong the lifetime of the switch.

Bandwidth availability must be highly scalable

As remote field applications converge onto one single network, especially for video and other bandwidth hungry applications, bandwidth and network availability will be critical factors to consider during network design. While a 100 megabit network will generally be enough for a network of 10 to 15 cameras (each using roughly 3 Mbps of bandwidth @ 720p resolution), a large scale surveillance network with more than 30 cameras will likely require a gigabit backbone for video transmission. Industrial switches should be capable of gigabit speeds to prevent network congestion and provide optional fibre interfaces to allow long distance data transmission from field sites back to the control room.

Network redundancy must provide millisecond level recovery

Network redundancy will also be crucial in maintaining high network availability. RSTP is acceptable in an enterprise network where a few seconds of network delay is tolerable. But in an industrial control network, one second of network interruption can severely impact production process and even jeopardise the safety of onsite personnel. Many proprietary ring technologies for redundancy will claim sub 50 millisecond recovery times. However, as the number of switches increases, recovery time can take up to hundreds of milliseconds. Turbo Ring is a field proven redundancy technology that has been proven to provide sub 20 millisecond network recovery, even when tested with a ring of 250 switches. As field level applications are aggregated onto the network, network redundancy becomes even more critical in ensuring network resilience.

Industrial networks must be secure to protect highly critical systems

Security vulnerabilities and loopholes of most industrial networks are, unfortunately, discovered only after a security breach has occurred. Existing systems were previously isolated and inaccessible via a remote connection. However, the integration of these existing systems with information technology data networks will undoubtedly present inherent network risks and vulnerabilities. With the rapid growth of industrial Ethernet nodes deployed at field level, possible sensitive/confidential information will need to be protected with network level authentication, such as with VPN (virtual private network) and firewalls, to prevent unauthorised access to a network.

Switch level security measures, such as Radius and TACACS+ for user access authentication, IEEE 802.1X for port based access, and HTTPS, SSH, SNMPv3 for data

encryption, are vital in preventing unauthorised access to ensure a healthy network state. Role based account management is also an important security measure, which can be used to grant switch access to different authorised users using multi level access permissions.

Switch manageability must be designed for easy operation

Switch manageability is an important aspect of maintaining large scale networks. Operators and engineers will also need tools to efficiently manage switches from onsite and central control locations. Whether for initial installation, configuration backups, firmware updates, or configuration rollbacks, an efficient solution to quickly accomplish these tasks will mean a faster time to market and improved system uptime.

During initial installation at onsite locations, manual switch configuration can be a daunting task for large scale networks. Aside from labour costs during initial configuration, possible input errors resulting from manual configuration will require additional time to diagnose and troubleshoot. A mass configuration utility is a must to allow maintenance engineers to minimise the time required to configure network switches. Some network configuration tools now support smart configuration methods to enable network link sequence detection to eliminate the possibility of manual input errors to reduce total cost of ownership.

Without effective network management software for remote switch management, industrial operators are unable to monitor, identify, and react to network issues immediately, which can result in production losses and safety concerns. Typical enterprise network management software, which use complex features and sophisticated user interfaces will have a high learning curve and can be unsuitable for use in industrial environments. An effective industrial network management software tool can auto detect network devices and offer a virtual physical network topology to allow operators to visually monitor, manage, and diagnose network devices and events in real time.

Legacy devices, PLCs, and SCADAs are still widely used in field level applications. In order to effectively converge and manage these existing devices, switches should be enabled with industrial Ethernet protocols, such as Modbus TCP, PROFINET, and EtherNet/IP to offer operators the efficiency of centralised network management with greater network scalability and flexibility. To optimise system performance and improve network manageability, switches should integrate seamlessly with industrial automation networks for centralised SCADA control and monitoring.

Industrial Networks Require Future Proof Switches

To future proof large scale industrial Ethernet networks, industrial operators must seriously consider a few key requirements of industrial Ethernet switches, along with industrial network manageability and maintainability which are shown in the table below:-

Critical considerations of future proof switches

	Critical considerations
Reliability	High level EMS protection Strong shock/vibration resistance Wide temperature tolerance
Bandwidth	Scalable and multiple gigabit Ethernet connections
Redundancy	Millisecond level network recovery
Security	IEEE 802.1X, RADIUS or TACACS+ for access authentication SNMPv3, HTTPS or SSH for secure data transmission Role based account management
Manageability	Mass configuration capability Visualised remote monitoring Industrial protocols interoperability

If we are to achieve the critical factors, industrial switches must be able to resist high level electromagnetic disturbances, severe shock and vibration, as well as extreme temperatures. For scalability and aggregation requirements, especially in high definition video applications, industrial switches will need to have multiple gigabit speed ports. Network redundancy for industrial Ethernet switches should still be able to recover network connectivity in millisecond timeframes, even when hundreds of switches are on the network. Switch security must not be overlooked, access authentication (IEEE 802.1X, RADIUS, or TACACS+) and secure data transmissions (SNMPv3, HTTPS, SSH) are both critical factors to consider to establish role based account management. Lastly, how quickly and efficiently industrial operators are able to respond to resolve network abnormalities to minimise system downtime will ultimately have a direct impact on the total cost of ownership.