Chapter 9 - Manufacturing

Overview

An Introduction to Connected Manufacturing

An Architecture for the Converged Factory

Industrial Automation Control Protocols

Connected Factory Security

Edge Computing in the Connected Factory

An Introduction to Connected Manufacturing

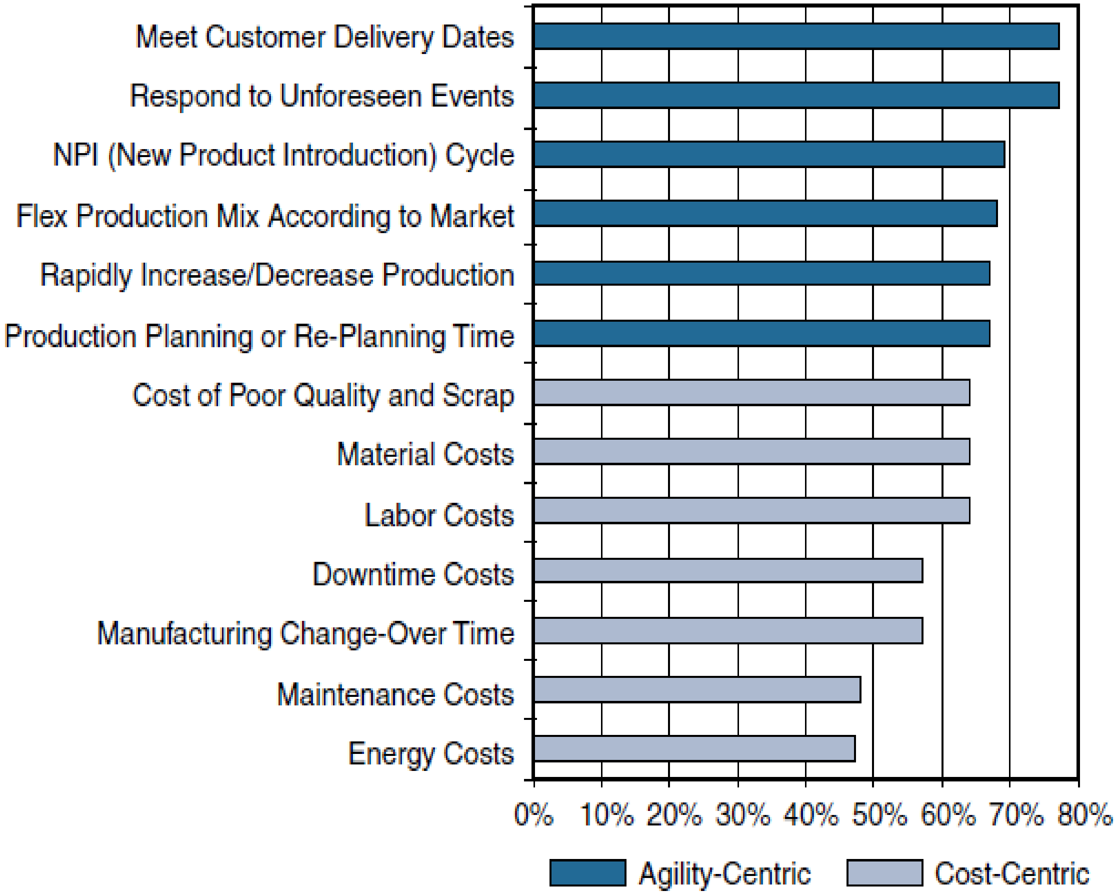


Figure 9-1 Shifting Focus from Cost to Agility

Source: SCM World /Cisco, Smart Manufacturing and the Internet of Things 2015 Survey of 418 Manufacturing Business Line and Executives and Plant Managers Across 17 Vertical Industries.

It is estimated that nearly 75% of US plants are more than 20 years old. Factories around the world are facing a similar challenge: Their aging assets not only slow innovation but also cost billions in unplanned downtime.

By some estimates, there are 60 million machines in factories throughout the world. Of them, 90% are not connected, and the vast majority of the machines are more than 15 years old

IoT-related technologies

- **Data-driven manufacturing:**- Manufacturers are also exploring ways to use data generated from the machines to support rapid retooling when market fluctuations or other needs occur.
- **OT and IT convergence**: IP networking is enabling closer integration between machines and factories and the line between factory and enterprise networks is becoming less distinct

- **Improved technology with lower costs**: The convergence of compute, switching, routing, and security has the potential to drive down the cost of connecting machines.

- **Machine builder OEMs focused on new priorities**: Original equipment manufacturers (OEMs) are facing disruption by new cloud-based providers that intend to provide Machines as a Service (MaaS). This offers remote connectivity and monitoring of the machines.

  - Manufacturers are looking toward near 100% uptime and zero-touch deployments.

  - They are also exploring ways to control support costs through remote connectivity and monitoring

An Architecture for the Connected Factory

Network security in the factory was typically limited to an industrial DMZ, leaving the machines mostly unprotected

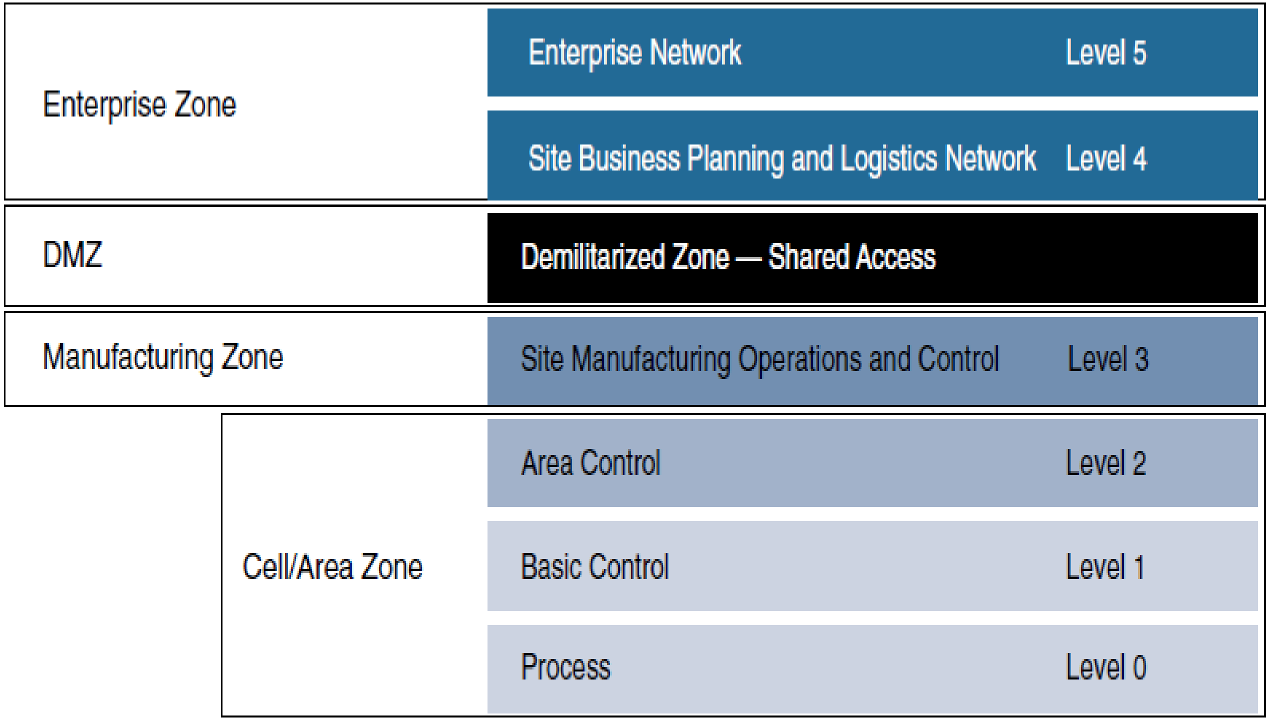
Factories rarely deployed network-level security systems that included identity policies and secure remote access tools that allowed plant-level data to be securely extended to the cloud.

Companies are beginning to tie together their industrial automation and control systems (IACS) with IT applications and analytics tools to provide control and analytics capabilities that are driving operational and business benefits.

Industrial Automation and Control Systems Reference Model

Manufacturing environments heavily rely on different communication technologies which are vendor-specific.

IACS is built on hierarchical Purdue model that provides logical framework to describe network and security



Enterprise Zone	Enterprise Network	Level 5
	Site Business Planning and Logistics Network	Level 4
DMZ	Demilitarized Zone — Shared Access	
Manufacturing Zone	Site Manufacturing Operations and Control	Level 3
Cell/Area Zone	Area Control	Level 2
	Basic Control	Level 1
	Process	Level 0

Figure 9-3 *The ISA99 / IEC-62443 IACS Logical Framework, Based on the Purdue Model for Control Hierarchy*

- The IACS logical framework identifies functional zones and levels of the manufacturing plant and defines operations at each level.
  - **Safety Zone**:The safety system׳s function in this zone is to provide an

    IACS shutdown (a ״stop״ button) in case of an emergency. You can think of this as a hardwired fail-safe used to protect personnel and equipment if a dangerous event occurs.
  - **Manufacturing zone**: It supports secure plant operations and functioning of the IACS applications, there is a secure separation of the manufacturing zone and the enterprise zone (Levels 4 and 5).
  - **Cell/area zone**: It has three levels of activity;
    - Level 0: Process: It consists of Sensors and Actuators performing activities such as moving a robot, spraying, driving a motor or welding
    - Level 1: Basic Control: This is where controller that direct manufacturing live.
    - Level 2: Area Supervisory Control: includes functions within the cell/area zone that require runtime supervision and operation

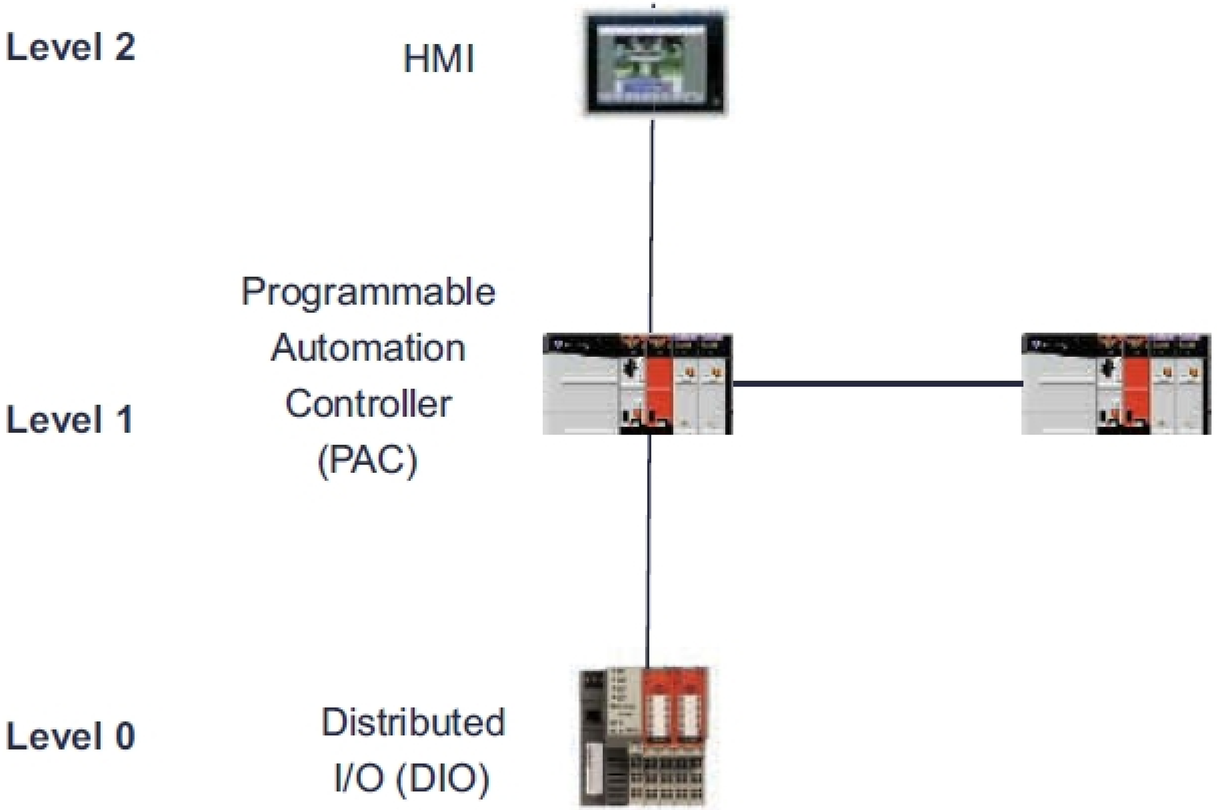


Figure 9-4 *IACS Controller Traffic Flow*

- **Level 3: Site level**: The functions and applications at level 3 include SCADA Systems, file servers, control room workstations, scheduling systems, and reporting.
- **Demilitarized Zone** – DMZ: This is the security critical to plant operations as it protects the machines at the lower level from malicious activity that may occur in the traditional enterprise network.
- **Enterprise Zone**: Level 4 and 5 in the enterprise zone relate to traditional IT or enterprise networking functions, including file services, internet connectivity and email systems.

The CPwE Reference Model

- The Converged Plantwide Ethernet reference model was developed by the cisco to address the need of Ethernet and TCP/IP communication protocols.
- The CpwE solution is designed to enable the convergence of IACS applications with enterprise IP system
- CPwE Ethernet networks come in various topologies, including redundant star, bus/star, and ring.
- The distribution switches between the cell/area and industrial zones form a demarcation point
- The distribution switches touch the same Ethernet segment as the access switches in the cell/area, they are also considered cell/area infrastructure devices and are typically required to be ruggedized devices
- The industrial zone is analogous to Level 3 of the IACS reference model and is also very similar to a traditional campus network.
- The industrial zone provides network connectivity through routed distribution switches to multiple cell/area zones as required.
- The industrial zone also supports IP routing capabilities for IACS devices that require Level 3 application support

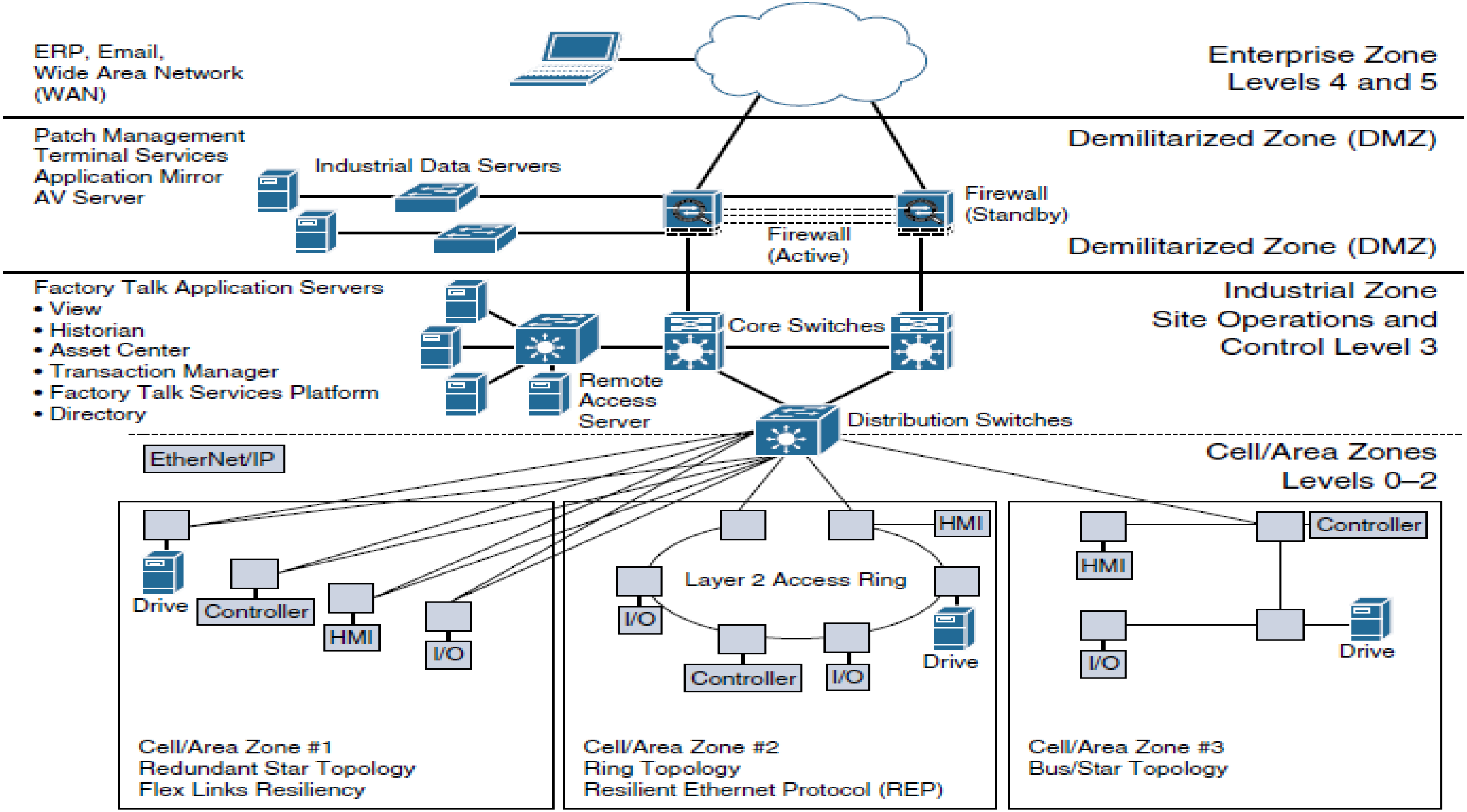


Figure 9-5 *A High-Level View of the CPwE Architecture with Three Different Cell/Area Zone Ethernet Topologies*

CPwE Resilient Network Design

- Due to sensitive controller and application requirements in IACS networks, network resiliency between IACS devices is a mandatory requirement within cell/area zones.
- Resilient IACS networks need to support the following capabilities:
  - **Availability**:A fully redundant physical path in the IACS Ethernet network topology should be chosen.
  - **Predictable performance**:Reliability and real time traffic requirements of IACS applications is a requirement for successful CpwE deployments.
  - **Fast network re-convergence:**Typical IACS application interruption tolerance limits are on the order of less than 100 ms, with minimal jitter.
  - **Industrial Protocol**: CPwE IACS devices and networking equipment need to support industrial application protocol requirements.

Communication pattern that requires network resiliency

- Controller to HMI
- Controller to controller
- Controller to input/output (I/O; the sensor and controller modules for machines)
- Controller to variable frequent drives (VFDs; adjustable electromechanical drives to control a motor)
- Controller to motor control centers (MCCs; used in factories to control a large number of motors from one central controller)

Having the ability to quickly bring new machines online and connect them to the Ethernet network has yielded much greater flexibility and has significantly reduced new model and new product introduction, thus improving the overall time to market.

- **Resilient Ethernet Protocol**
  - In the CPwE reference architecture, Resilient Ethernet Protocol (REP) is used in the cell/ area zone to achieve high-speed protection of ring topologies
  - REP controls a group of ports connected to an Ethernet segment to ensure that no bridging loops exist and that the Ethernet segment is able to respond to topology changes.
  - Another key advantage of REP is that it is not limited to a small number of devices on a single Ethernet segment.
  - REP has no fixed upper limit on the number of nodes per segment, thus supporting large ring topologies unlike STP which limited to seven devices per segment
  - For each REP segment, one switch is designated as a master node that controls the overall ring

- A REP segment is a chain of ports on an Ethernet segment configured with a segment ID.
- When all ports in the ring segment are active, one port is identified as the alternate port, meaning it is in the blocking state, thus preventing the ring from becoming a Layer 2
- If any other port in the REP segment fails, the alternate port is signaled to change state into the forwarding state, repairing the broken Ethernet ring segment and allowing communications to continue

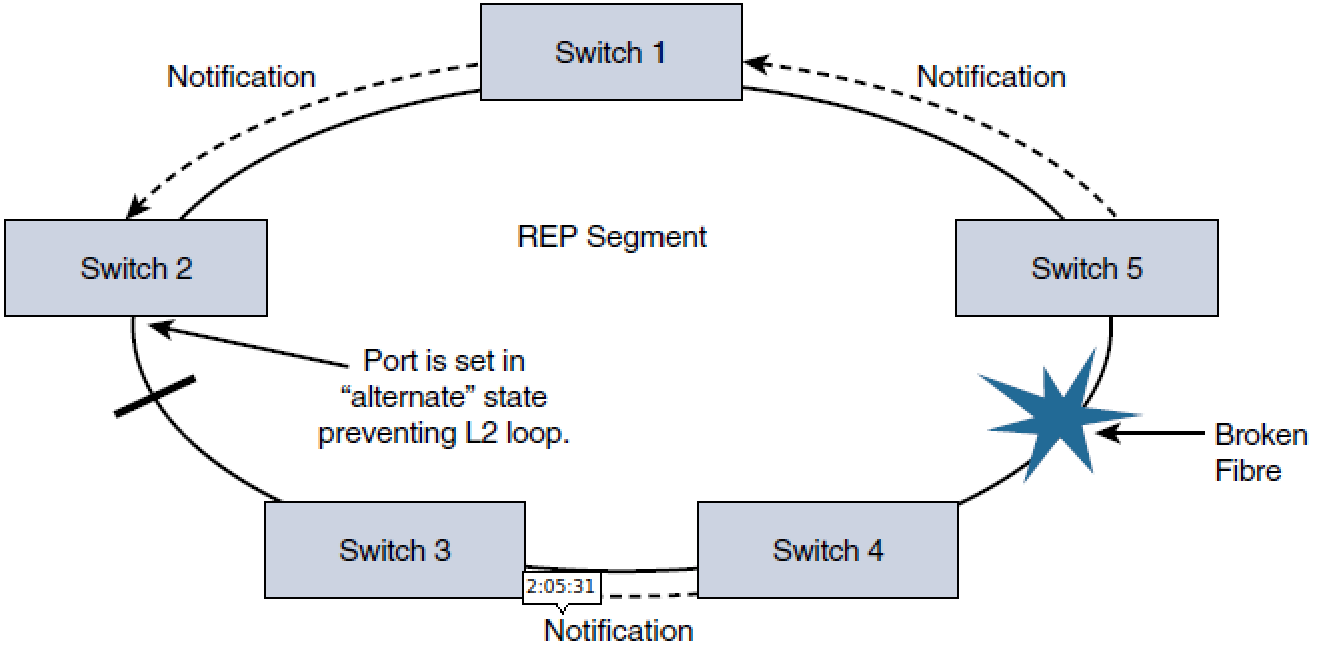


Figure 9-6 *REP Notification When a Topology Change Occurs*

- **Business value of Resiliency of Converged Networks**
  - It increases the number of devices being connected to the plant floor
  - Devices such as sensors, and actuators that collect data are used as tool to help understand the complex processes.
  - A resilient network design allows a single device to be taken out of service without impacting the rest of the cell/area network.
  - REP based architecture support systems that connect people, processes, and data to real-time applications, even during a network disruption.

CPwE Wireless

- While deploying CpwE, wired Ethernet access switches are used often but plantwide architectures are increasingly adapting the use of Wi-Fi for IACS applications with similar requirements like QoS with minimal latency and jitter.
- CpwE wireless networks are used in;
  - Managing machines
  - Handheld devices
  - Automated Guided Vehicles (AGVs)
  - Avoiding costs involved in physical wiring of the network

- **CPwE Wireless Network Architecture**

While deploying a network a thought of the following is taken into account

- Bandwidth
- QoS handling
- Thoroughput
- Reliability
- Security

Latency is impacted by how many stations are associated to AP.

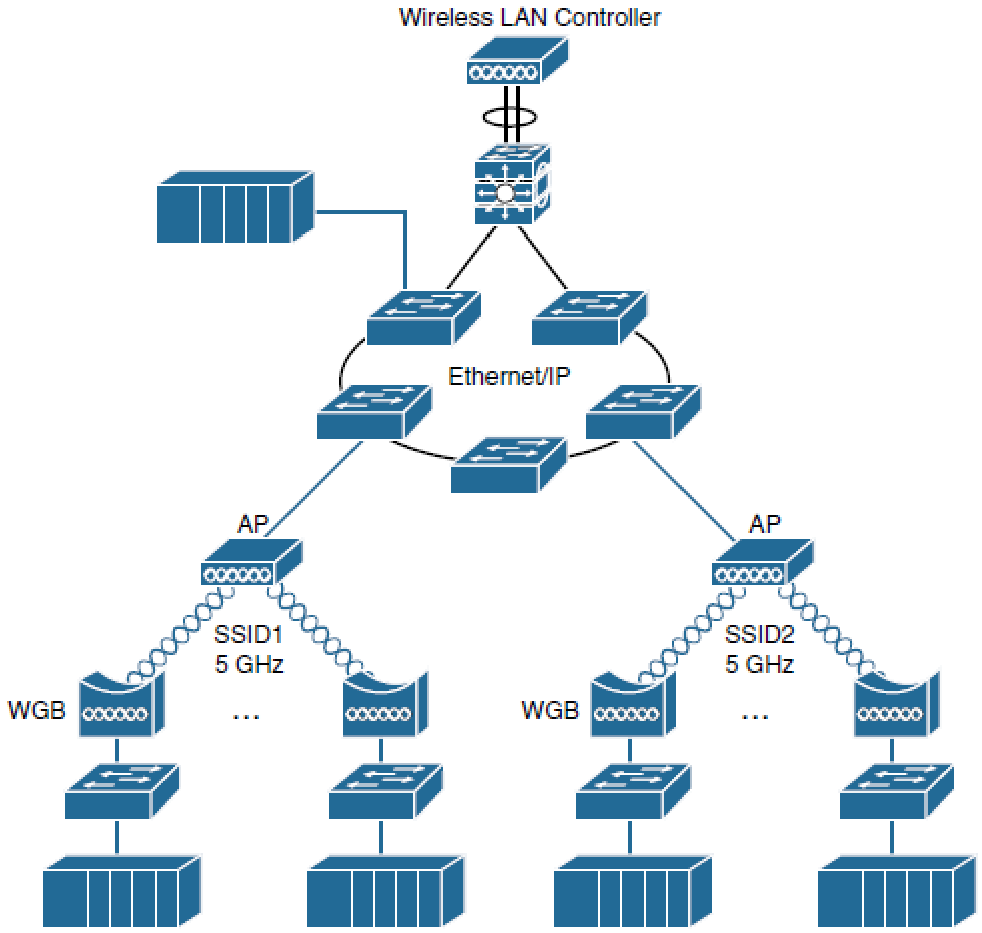


Figure 9-8 *A Factory Wireless LAN Architecture*

- **Use cases of Wi-Fi usage in Manufacturing Environments**.
  - **Fixed-position devices**: Commonly in Original equipment manufacturer (OEM) machine or skid that needs to be integrated into a production line over a wireless link.
  - **Nomadic devices**:Nomadic equipment stays in place while operating and then moves to a new location in the shutdown state
  - **Operational relocation devices**: The machinery that uses wireless as a replacement for wired solutions, such as inductive rails and slip rings

- **Real Time Location System – RTLS**

Wi-Fi–based location tracking systems typically include active battery-powered Wi-Fi radio frequency identification (RFID) tags that are attached to machines, skids, vehicles, or other devices that have a measure of mobility within the plant.

Advantages of using RTLS;

=> By using RTLS and a graphical location visualization tool, it is possible for assembly workers, shift supervisors, and plant managers to view the location of plant materials and assets through tablets and smart phones.

=> Using RTLS also allows plant managers to monitor how quickly employees are completing their respective stages in the production process.

=> IT helps factory managers better understand how to increase efficiency and lower costs associated with inventory.

Industrial Automation Control Protocols

Industrial automation application systems use a unique set of protocols for control, motion, synchronization, and safety.

We discuss the three protocols that are more adopted by the manufacturing market

These include;

1. EtherNet/IP
2. PROFINET
3. Modbus/TCP

- **1. EtherNet/IP and CIP**

EtherNet/IP is an open standard for industrial automation systems that was developed by Rockwell Automation and is now managed by the Open DeviceNet Vendors Association(ODVA).

‶**IP**″ stands for ‶Industrial Protocol,″ not ‶Internet Protocol.″ and they are specifically used to handle industrial automation applications, such as those for control, safety, motion, and configuration

The EtherNet/IP adapts the the Common Industrial Protocol

Capability types of CIP communications

- Explicit messaging: This involves configuration, diagnostics and data collection and it is based on TCP unicast messaging.
- Implicit messaging: This involves real-time I/O data, functional safety data, motion control data and often UDP multicast

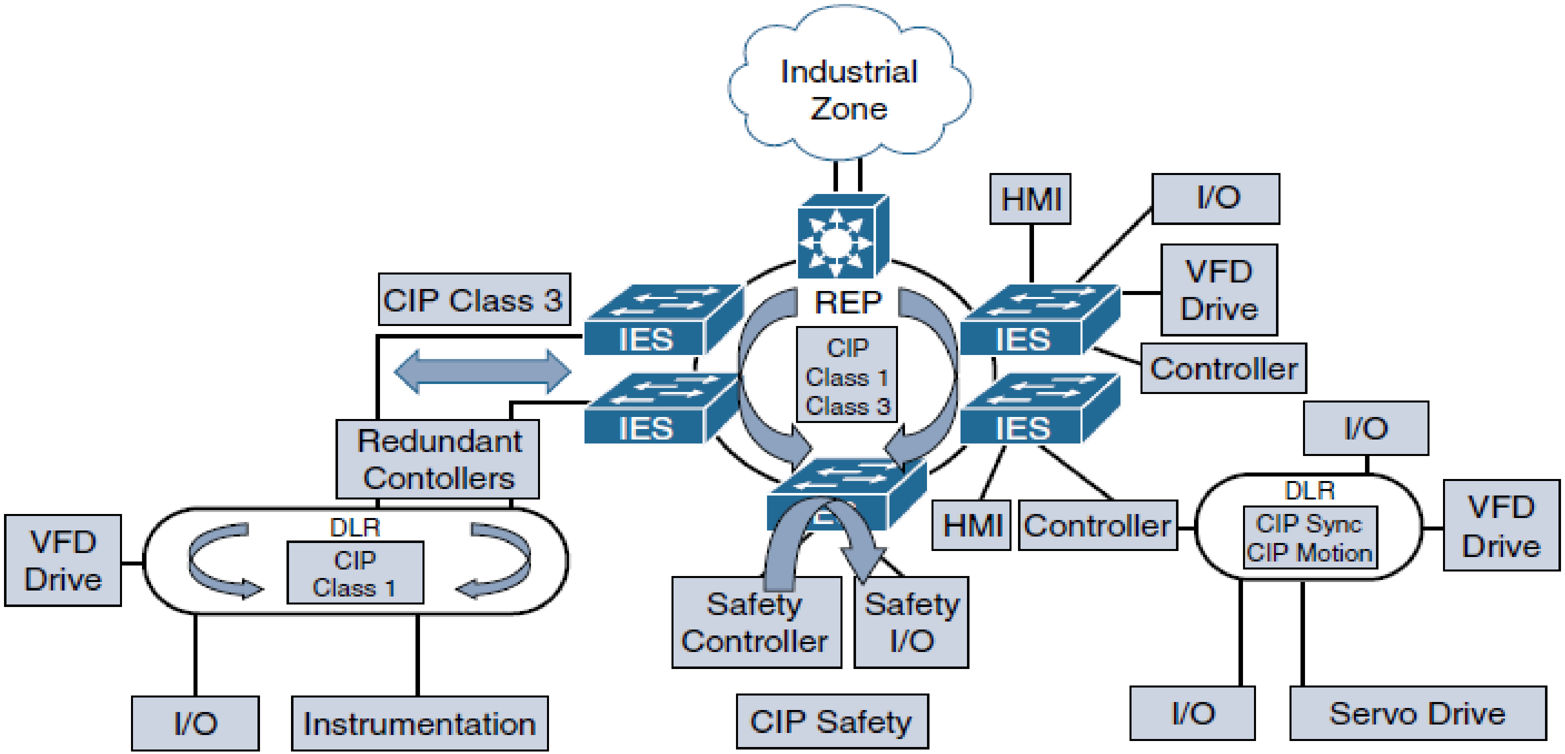


Figure 9-9 A Factory Network Based on EtherNet/IP

- REP is used as a resiliency mechanism between the industrial Ethernet switches (IESs) to pass CIP Class 1 (real-time Ethernet) and Class 3 (TCP) messages.
- EtherNet/IP also specifies a redundancy protocol known as Device Level Ring (DLR),which is used when the system requires continuous operation and is able to achieve high-speed re-convergence in the case of a ring break.

The CPwE reference architecture for industrial applications discussed earlier is largely based on EtherNet/IP and CIP.

- PROFINET
  - PROFINET (Process Field Net) is a widely used industrial technology for the exchange of data between controllers and devices.
  - One of the key advantages of PROFINET is that it exchanges messages in a deterministic manner over high-speed Ethernet links.
  - It uses UDP over TCP thus enabling sending and receiving of data directly to the application layer which introduces waiting variable.
  - PROFINET networks are designed to support real-time PROFINET communications with minimal latency, while supporting network resiliency at the manufacturing plant floor.

Benefits of a well designed PROFINET Architecture

- It reduces the risk of production downtime through the use of a resilient network architecture capable of network convergence based on the IEC 62439-2 standard.
- It improves plant uptime through validated reference architectures, with a focus on application availability.
- It enriches critical information access from machines and applications through better managed network resources.
- It enhances single-pane management compliance, using industry standard general system description (GSD) files and supervisor applications of PROFINET-compliant devices.

- The PROFINET architecture

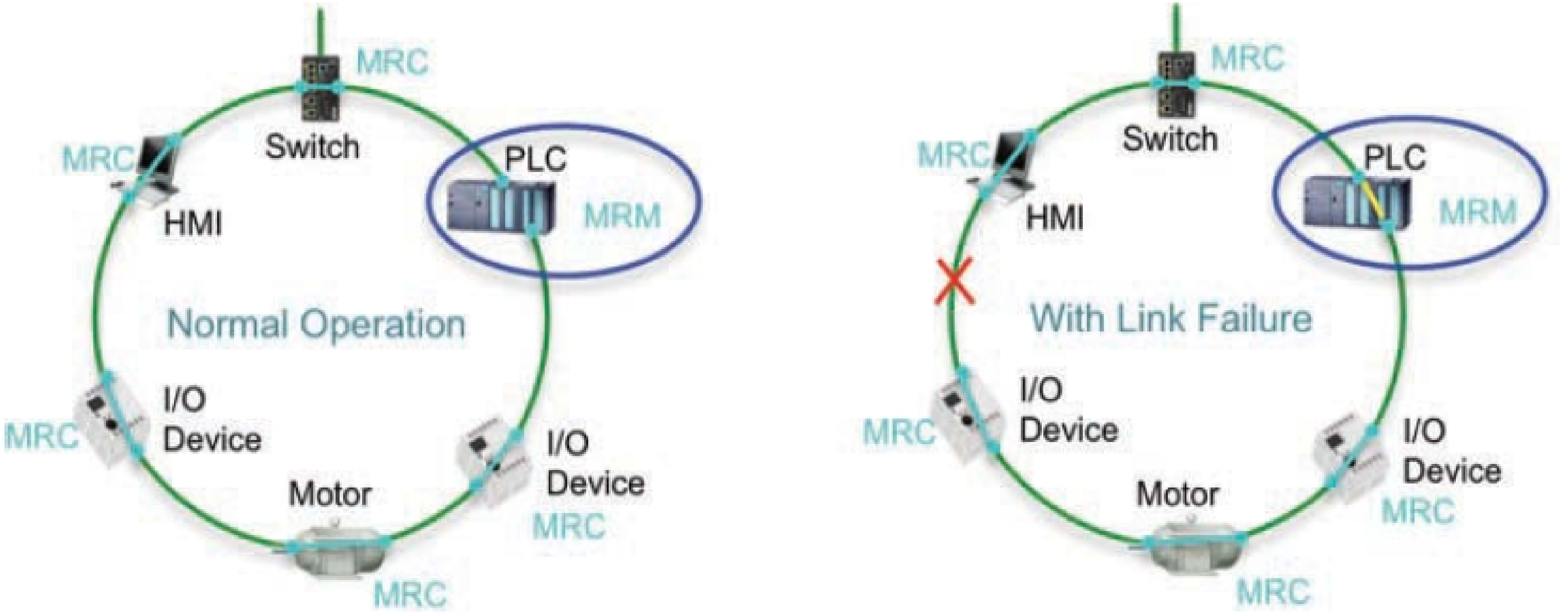


Figure 9-10 *PROFINET MRP Operation*

- The architecture consists of the following

■ Industrial automation devices: These include robots, sensors, actuators, and drives.

■ HMIs: HMIs provide visual status reports and control of the industrial automation devices.

■ Controllers: Examples include PLCs and distributed I/O devices.

The PROFINET architecture is similar to CpwE architecture as both include support for network resiliency, automation and use of the Purdue model

It is designed in a way that Disruptions in the control network—even short ones lasting just milliseconds—can create significant impacts on the functioning of a production facility.

Much as with CPwE, the cell/area zone in PROFITNET is the primary zone where most of the industrial automation activities are performed

- **Media Redundancy Protocol (MRP)**
  - Determinism in industrial automation ensures that Ethernet frames are sent and arrive when required.

While the PROFINET device is responsible for scheduling

and transmitting the Ethernet frame, the network´s main impact on a system´s determinism is based on the following performance characteristics:

■ Latency: The average amount of time a message takes to be transmitted and processed from originating node to destination node

■ Jitter: The amount of variance in the latency

■ Packet Loss: The number of packets, usually expressed as a percentage, lost in a transmission from one device to another

Industrial automation networks must adhere to the following requirements for real-time

Applications:

- Machine and process cycle times: This includes the frequency with which the industrial automation application moves from one operation to the next.
- Request packet interval (RPI) or I/O update time: This is the frequency at which input and outputs are sent and received.
- Packet-loss tolerance: This is the number of consecutive

MRP is an industry protocol defined in the IEC 62439-2 standard

MRP allows rings of industrial Ethernet switches to overcome a single segment failure with recovery times similar to those of REP

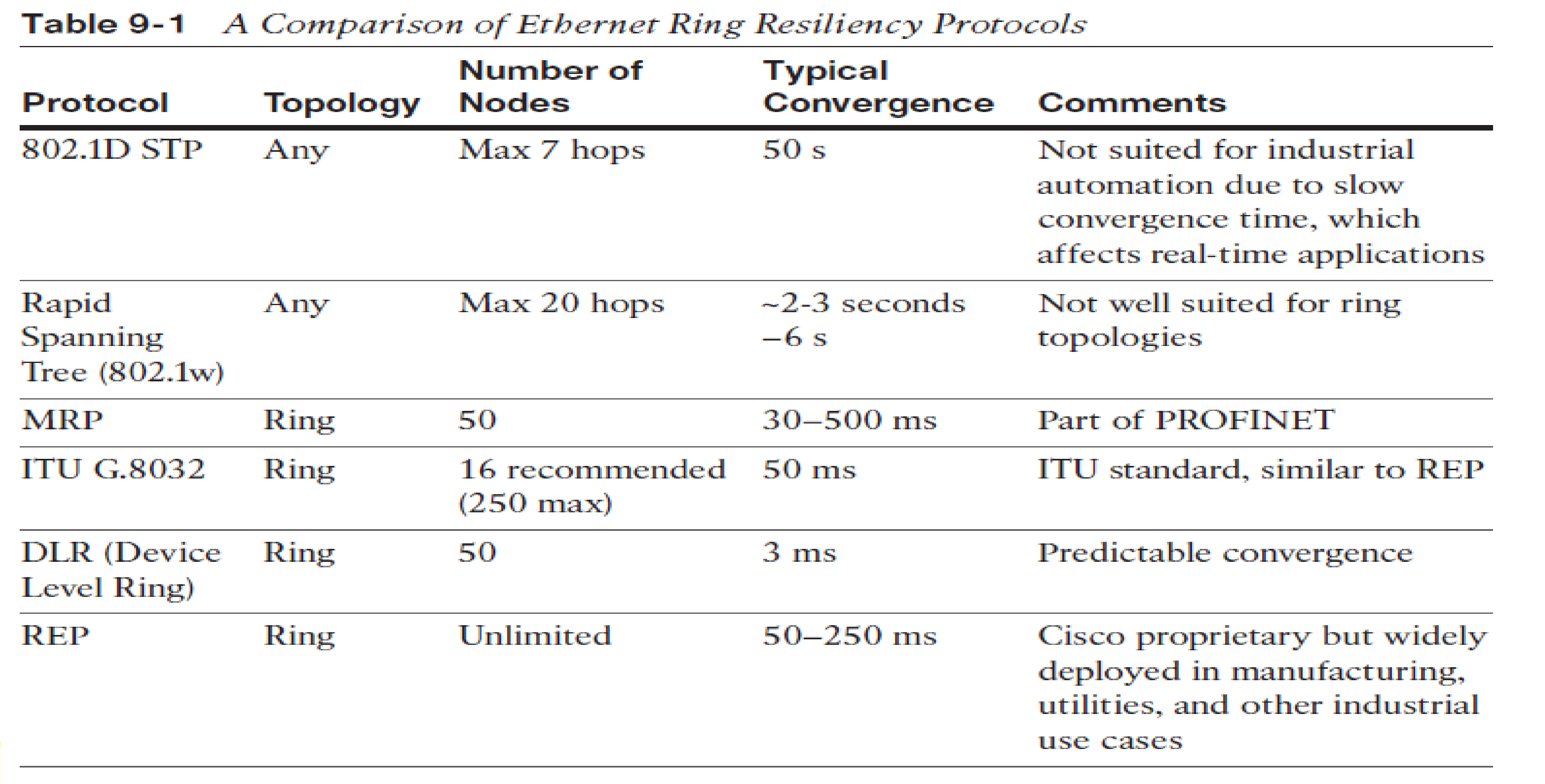


Table 9-1 *A Comparison of Ethernet Ring Resiliency Protocols*

Protocol	Topology	Number of Nodes	Typical Convergence	Comments
802.1D STP	Any	Max 7 hops	50 s	Not suited for industrial automation due to slow convergence time, which affects real-time applications
Rapid Spanning Tree (802.1w)	Any	Max 20 hops	~2-3 seconds –6 s	Not well suited for ring topologies
MRP	Ring	50	30–500 ms	Part of PROFINET
ITU G.8032	Ring	16 recommended (250 max)	50 ms	ITU standard, similar to REP
DLR (Device Level Ring)	Ring	50	3 ms	Predictable convergence
REP	Ring	Unlimited	50–250 ms	Cisco proprietary but widely deployed in manufacturing, utilities, and other industrial use cases

- ## 3. Modbus/TCP

Modbus is popular due to the fact that the protocol is an open published standard and is well established throughout the world.

The Modbus master/slave configuration is well suited to the connection-oriented nature of TCP, but this mode of communication tends to introduce extra latency and is generally not as flexible as either EtherNet/IP or PROFINET.

Connected Factory Security:-

Often the solution to a cyber attack on manufacturing plant is disconnecting it from IT enterprise network

More threats can come from the computers in the plant that have been accessed by the contractors and employees with unfettered access.

A Holistic Approach to Industrial Security

- In most cases, holistic factory security requires that different stakeholders work together, including control system engineers, IT network engineers, and the IT security architects.
- Responsibilities for these different stakeholders include the following:
  - Control Systems Engineers
    - IACS device hardening (that is, physical and electronic)
    - Infrastructure device hardening (for example, port security)
    - Network segmentation
    - IACS application authentication, authorization, and accounting (forexample, AAA)

- Control Systems Engineers in collaboration with IT network engineers
    - Zone-based policy firewalls at the IACS application
    - Operating system hardening
    - Network device hardening (for example, access control, resiliency)
    - Wireless LAN access control policies
- IT security architects in collaboration with control systems engineers
    - Identity services (wired and wireless)
    - Directory services
    - Remote access servers
    - Plant firewalls
    - Industrial demilitarized zone (IDMZ) design best practices

- **The three aspects of factory security in an Industrial Security Framework:**
  - The Network Address Translation in the factory
  - The Industrial DMZ
  - Factory Security Identity Services

a). The NATs

- Network Address Translation (NAT) enables the reuse of IP addressing without introducing duplicate IP address errors into your IACS application architecture.
- Technology and Business drivers are the aspects for the implementation of NATs in an industry.
- NAT is a networking technology that enables control system engineers to build IACS applications that reuse IP addresses,

b). The Industrial DMZ

- This is a standard in which business system networks are segmented from the plant networks to deal with penetration threats from the enterprise zones
- The IDMZ is a buffer that enforces data security policies between a trusted network(industrial zone) and an untrusted network (enterprise zone).
- IDMZ assets act as a broker between the IACS, and use the following methods to broke data;

  ■A reverse proxy server

  ■ An application mirror, which is similar to a proxy server—essentially a facsimile of the actual application running outside the protected data center

  ■ Remote desktop services (such as Microsoft RDP)

- **Factory Security Identity Services**

Network identity services provide an additional layer of network access and control by identifying the type of computer, operating system, and user that is accessing the network.

It is important to note that the security architecture likely needs to support both wired and wireless access methods by plant personnel and contractors.

This is achieved by deploying a centralized identity services system that is capable of establishing a trust boundary on all network access points.

Benefits of Factory Security Identity Services

- A comprehensive centralized policy for network access in both the manufacturing and enterprise zones
- Streamlined device onboarding
- Policy-driven rules and access control policies
- Guest portal services for contractors and guests

Edge Computing in the Connected Factory

- Machines at the factory produce massive data, PCs are deployed to collect this data.
- The collection of this large volume of data has led to maintenance and security challenges at the factory due to hardware breakdowns and OS upgrades.
- To address the above dilema, machine-embedded and near-machine edge compute devices that include switching, routing, and security features in a single ruggedized form factor to connect machines and the edge compute services.

Connected Machines and Edge Computing

There has to be away to connect the hardware devices to a software interoperable in several manufacturing communication protocols.

The protocols are based on XML or HTTP.

New developments in edge computing platforms combine switching, NAT, routing, and security features into a single ruggedized edge appliance which is more cost effective

Because the data can be sourced from disparate resources, it is anticipated that they will increasingly deliver web services using RESTful APIs that can be consumed in a connected machine´s web portal for end-user manufacturers.

This helps to reduce costs for standardizing data on the plant