WHITE PAPER

aruba
a Hewlett Packard
Enterprise company

Designing hyper-aware industrial facilities

Secure infrastructure and partner solutions for chemical, defense, food & beverage, logistics, manufacturing, petrochemical, pharma, transportation, and utility applications

TABLE OF CONTENTS

TABLE OF CONTENTS

EXECUTIVE OVERVIEW

At its core, the Internet of Things (IoT) is an amalgamation of machines in the physical world, logical representations of the physical phenomena acted upon by those machines (voltage, temperature, flow, speed), contextual data generated by networks connecting the machines (identity, location, applications in use), and business applications that analyze, mine, share, and respond to those data. In Industrial IoT (IIoT) systems the machines and applications are tailored to factories, process operations, material handling, transportation, utility services, and logistics.

By securely interfacing IIoT devices, and generating contextual information, Aruba's networks enable industrial control and business applications to become hyper-aware of their operating environments. Aruba's unified infrastructure, zero-trust security, and AI-powered software - used in conjunction with solutions from key technology partners - enable industrial facilities to successfully deploy and exploit IIoT solutions. The richer the set of available data and context, the greater the opportunities to optimize operations, implement predictive maintenance, optimize inventory, bolster health and safety, and maximize human productivity.

Solutions from Aruba and its technology partners are applicable across a broad range of vertical markets - chemical and petrochemical, food & beverage, logistics, manufacturing, pharmaceutical, utility, water, and wastewater. Use cases and partners discussed in this white paper include:

- **Operations Optimization**
  - Building A Contextually Adaptive Plant (ZF Openmatics)
  - Securing Control Networks That Can't Protect Themselves (Claroty, Microsoft CyberX, Nozomi, and Tenable Indegy)
  - Connecting And Protecting Remote Sites (VIA, RAPs, SD-Branch)
  - Running Profinet IO Over Shared Wireless Infrastructure (Profinet IO over Aruba APs)
  - Redundant Intra-Site Wireless Video And Data Links (Aruba 5/60GHz Access Point)
  - Intercepting Quality-Impacting IIoT Issues In The Switching Fabric (Aruba NAE Python scripting)
  - Bridging IT/OT Plant-Wide For Uniform Visibility & Security (Siemens)
  - Automating Plant Network Access For Service Personnel And Contractors (Aruba, Envoy)
  - Securely Sharing Plant Wireless Networks Without Losing Control (Aruba MultiZone)
- **Predictive Maintenance**
  - Migrating From Break/Fix to Predictive Maintenance (ABB)
- **Inventory Optimization**
  - Increasing Inventory Turns By Reducing Picking Time (Zebra)
- **Improved Maintenance**
  - Plant Monitoring And Digital Twin Enablement (EnOcean and Microsoft)
  - Seamless 5G To Wi-Fi Roaming Without Distributed Antenna Systems (AirPass)
  - Reducing Mean Time To Repair With Real-Time Location Services (Aruba APs and Meridian)
- **Health and Safety Monitoring**
  - Physical Distance Monitoring And Contact Tracing (AiRISTA Flow, AisleLabs, CohuHD, CXapp, Kiana, Patrocinium, SkyFii)
  - Real-Time Personnel And Asset Safety Monitoring (Mobilaris)
  - Context-Aware, Real-Time Integrated Emergency Response And Notification (Meridian and Patrocinium)
  - Air Quality Monitoring (IP video)
  - Gunshot Detection (AmberBox)

INTRODUCTION

What is a cognizant industrial site, and why is the Industrial Internet of Things (IIoT) relevant to it? A hyper-aware industrial site is instrumented such that applications are cognizant of the contextual status of the environment, machines, occupants, inventory, service needs, security, and safety. IIoT is collectively the eyes and ears of a cognizant plant, and generates logical representations of physical data, i.e., temperature, flow, current consumption, and speed, among many others. IIoT data are supplemented by contextual information generated by a plant's data network, i.e., identity, location, and applications in use.

The combination of data and context enables applications to be cognizant, and plants to become smart enough to adapt to the environment, machines, and workers. The richer the set of data and context, the more adaptive the site can become. Some plants have only limited cognizance, while others are fully instrumented and hyper-aware.

IIoT is characterized by devices and systems that are ruggedly designed and constructed, capable of operating in environmentally uncontrolled environments with high mean time between failures, operated using a wide range of wired and wireless physical layers and communication protocols, often deployed in firewalled silos without access to the Internet, and capable of deterministic operation in closed-loop control applications. The category cuts across many industries including automotive, bottling, chemical, food processing, gas, manufacturing, material handling, mining and resource extraction, oil, paper, petrochemical, pharmaceutical, power generation, power distribution, pulp, transportation, water, and waste water. Many defense applications fall into the industrial category but impose additional security and performance requirements.

The diversity of the category means there is no such thing as a one size fits all IIoT solution. Each vertical imposes its own certification, safety, regulatory, performance, EMI, and/or construction requirements.

According to McKinsey1 the total economic impact of IIoT in worksites and factories in 2025 will be $1.3T-$4.6T. The top identified areas include operations optimization, predictive maintenance, inventory optimization, health and safety, and human productivity monitoring:

- Operations optimization is expected to increase worksite productivity by 5-10%, and lower costs by 5-12%;
- Predictive and improved maintenance are expected to yield 3-5% productivity gains and lower costs by 10-40%;
- Inventory optimization is expected to lower costs by 20-50%;
- Health and Safety are expected to reduce costs by 10-20%; and
- Human Productivity Monitoring is expected to yield a 5-10% increase in productivity.

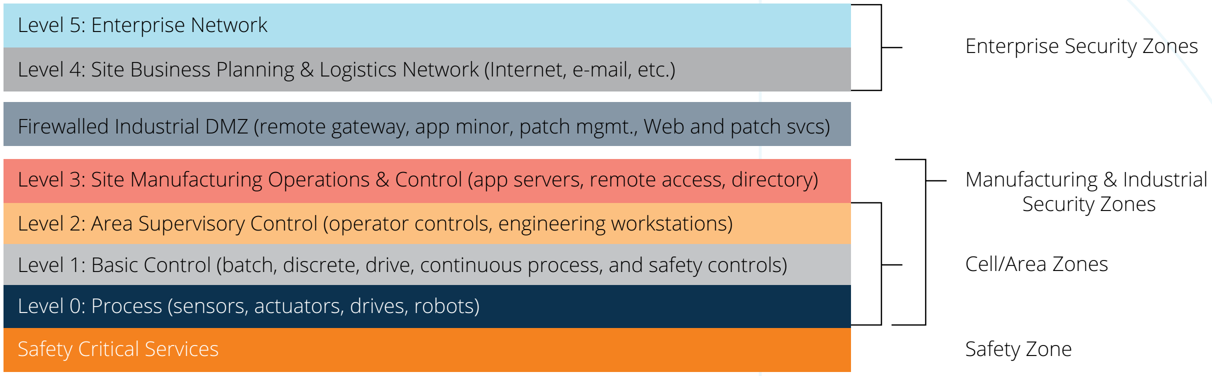
Before looking at specific use cases, it's useful to look at the environment within which IIoT systems have to be implemented. The Purdue Model is instructive for this purpose because it distinguishes between edge, plant, and enterprise networks. The more recent Industrie 4.0 and Industrial Internet Consortium reference architectures build up from the Purdue Model, offering greater deployment flexibility and inter-vendor interoperability. That said, the Purdue Model is sufficient for the purpose of explaining the stratification between networks and Zones, and the challenges that need to be overcome to deliver uniform IIoT security and visibility. Those learnings apply equally well to the other architectures, which the reader is encouraged to explore.

THE PURDUE MODEL

The Purdue Model is a commonly used framework for industrial control systems because it shows the interconnections and interdependencies of the components of a typical IIoT system. Developed in the 1990s by Theodore J. Williams and members of the Industry-Purdue University Consortium for Computer Integrated Manufacturing, the Purdue Model uses a five layer structure akin to the seven layer ISO IT model. The diagram below shows the five level model and associated security Zones. Zones are typically firewalled from each other.

The Enterprise Zone - Levels 4 and 5 - defines business systems (like ERP) networks. Levels 5 is corporate-wide and collects reports from all lower level control systems and monitors demand, production, and inventory. Level 4 includes all plant–related IT systems associated with logistics and business planning. It distributes data from Level 5 business systems to the infrastructure that runs the plant, also called Operational Technology (OT) systems. Level 4 includes file, data base, and application servers, and supervisory systems. The OT, or manufacturing, Zones include Level 3 site operations, Level 2 area supervisory control, Level 1 basic control, Level 0 process services, and a safety level.

The DMZ separates and protects OT systems from the IT systems above them, and securely brokers necessary data exchanges. The DMZ includes proxy servers, firewalls, domain controllers, and database replication servers. In theory this isolation is supposed prevent direct attacks originating from IT systems, and acts like a circuit breaker to isolate OT systems during an attack. That myth was disproved when Stuxnet jumped the gap on a thumb drive.



Level 5: Enterprise Network

Level 4: Site Business Planning & Logistics Network (Internet, e-mail, etc.)

Firewalled Industrial DMZ (remote gateway, app minor, patch mgmt., Web and patch svcs)

Level 3: Site Manufacturing Operations & Control (app servers, remote access, directory)

Level 2: Area Supervisory Control (operator controls, engineering workstations)

Level 1: Basic Control (batch, discrete, drive, continuous process, and safety controls)

Level 0: Process (sensors, actuators, drives, robots)

Safety Critical Services

Enterprise Security Zones

Manufacturing & Industrial Security Zones

Cell/Area Zones

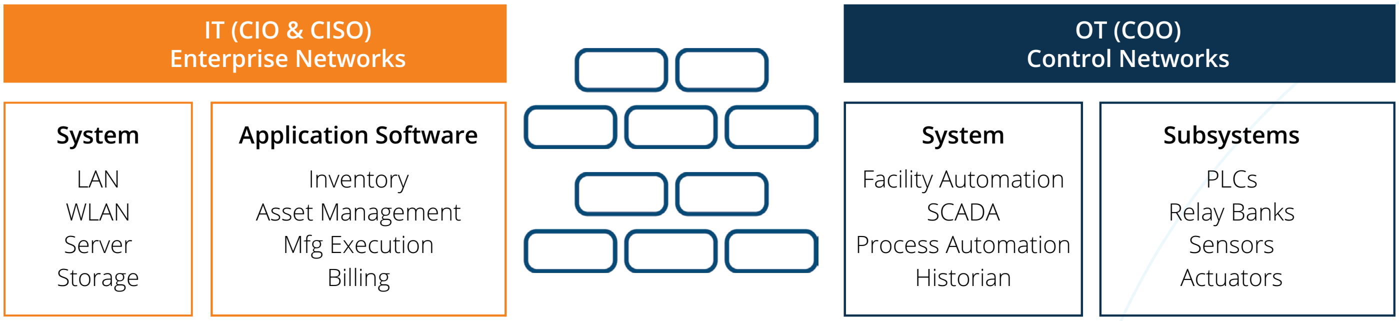
Safety Zone

Figure 1: Classic Purdue Model

Level 3 is where plant-wide monitoring and control systems reside, including operator human machine interfaces (HMIs). HMIs are used to monitor alarms, take equipment readings, log events, and check operational status. This is also the level at which OT data from sensors and actuators are relegated to the shadows, abstracted within summary data passed up to business applications. Level 3 includes domain controllers, HMI servers, and database and application servers.

Level 2 monitors subsystems including machines, programmable logic controllers (PLCs), HMI displays, emergency stop and call buttons, and limit monitors. Level 1 is the basic machine level and includes PLCs, motor and variable speed drivers, proportional-integral-derivative (PID) loops, and supervisory equipment. Sensors, pumps, motors, valves, and other actuators, operating discretely or connected to PLCs, reside at Level 0. Level 0 is called the process level because it is where the actual processes of manufacturing reside, and where high-speed, robust, faultless operation is expected. The Safety Level, at the bottom of the model, is for emergency start-stop systems that run at all times, regardless of the status of the Zones above them.

The security challenges involved with protecting Layer 1 and below are unique. Many different physical layers and non-TCP/IP protocols are used in these layers, and standard IT monitoring and security systems don't function in these environments. Low-level device data are filtered by PLCs and other IIoT equipment, and not directly visible to deep packet analytics or security applications located in higher layers.



IT (CIO & CISO)
Enterprise Networks

System
LAN
WLAN
Server
Storage

Application Software
Inventory
Asset Management
Mfg Execution
Billing

OT (COO)
Control Networks

System
Facility Automation
SCADA
Process Automation
Historian

Subsystems
PLCs
Relay Banks
Sensors
Actuators

Figure 2: The IT/OT Divide

OT protocols were designed for high speed and high reliability, not high security. Some, like Control Area Network (CAN) bus, have no security at all. Protecting the configuration of Layer 1 devices, like PLCs, is just as important as protecting the data they consume and generate. An unauthorized reconfiguration can cause significant damage to equipment and processes.

To overcome these issues Aruba has partnered with OT security partners that make specialized probes and systems to monitor OT protocols and devices. OT security systems can detect abnormal or unauthorized communication activity and equipment reconfiguration, and exchange security policy and device status with Aruba's ClearPass Policy Manager for remediation. Working in concert, Aruba and its OT security partners can flag out-of-normal activity, and alert higher level systems, so the impact on business processes can be immediately understood and responses implemented in accordance with OT guidelines.

OT data traversing the network switch fabric has business value but historically has not been accessible to applications at higher layers. For example, a vision system camera that scans products for defects, and relays images to a PLC, is typically not manually observed. Degraded performance can have ramifications for quality control and work in process, but may go unnoticed until it becomes a serious problem. Monitoring video packets as they traverse the switch fabric, then triggering an alert when they degrade - a feature available in the Aruba CX switch operating system - can help organizations migrate from break/fix to predictive maintenance.

Other data within the Zones are generated by the networks themselves. Identity, location, and applications-in-use are examples of rich contextual information generated by networks. These data are critical for many business, security, and safety applications. Identity is used to establish access policies and launch micro-segmented secure tunnels. Aruba's real-time location services can be used for asset tracking, geofencing hazardous locations, guiding service personnel to machines in need of service, auditing contractor activities, and worker safety in a muster event. Knowledge about applications in use informs the enforcement of quality of service for better application experiences.

The use and benefits of context transcends consumption in any one Zone: data often need to be simultaneously shared across many Zones without filtering. And therein lies one of the limitations with the Purdue Model.

THE META ZONE

The Purdue Model was defined before the advent of contextually-generated information and cloud IIoT services. The model divides IIoT into Levels, each for a different subsystem, and the Levels are then further grouped into Zones representing enterprise, manufacturing, cell/area, and safety systems. Connections between Zones are highly managed, and the level of security and visibility falls as you proceed to lower zones. The Safety zone, for example, may be autonomous from all other Zones, and have no security whatsoever. Air gapping has historically been used to separate the IT Zones 4 and 5 from lower OT Zones, a security practice that had proven highly ineffective.

As result of egregious IIoT security breaches, customers now want uniform security across the entire Purdue model using a zero trust framework. Such a framework has to accommodate the way and places work is done today, versus in the 1990s when the Purdue Model was created. That means respecting that devices and applications may reside on-premise, in data centers, and in private/public clouds. And that attacks could originate from anywhere inside and outside the four walls of a plant, including being carried across an air gap – unintentionally or maliciously – in maintenance tools, software updates, and thumb drives.

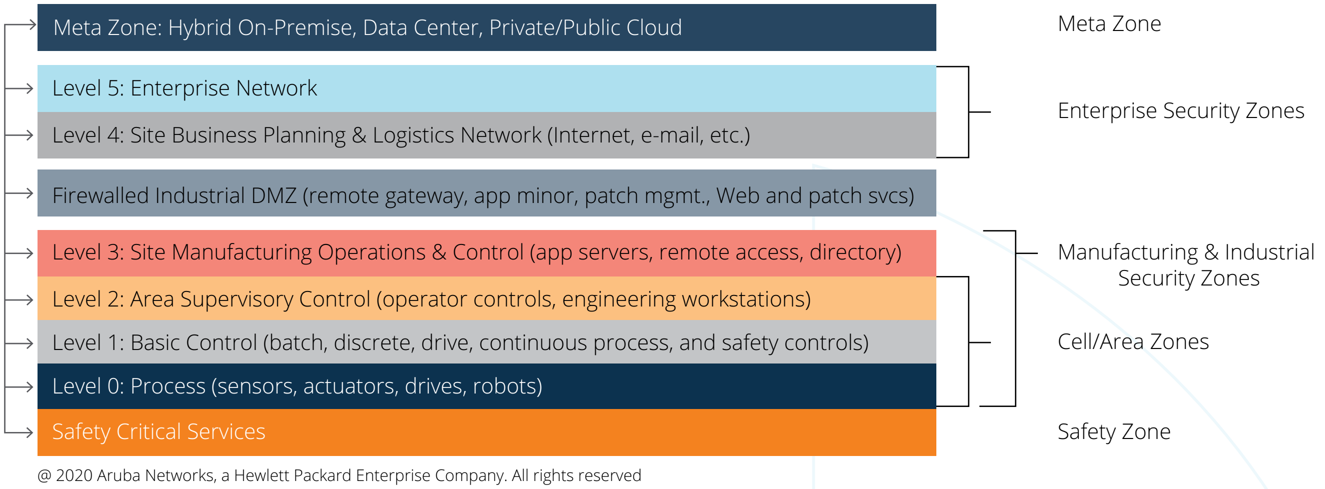

Meta Zone: Hybrid On-Premise, Data Center, Private/Public Cloud
Level 5: Enterprise Network
Level 4: Site Business Planning & Logistics Network (Internet, e-mail, etc.)
Firewalled Industrial DMZ (remote gateway, app minor, patch mgmt., Web and patch svcs)
Level 3: Site Manufacturing Operations & Control (app servers, remote access, directory)
Level 2: Area Supervisory Control (operator controls, engineering workstations)
Level 1: Basic Control (batch, discrete, drive, continuous process, and safety controls)
Level 0: Process (sensors, actuators, drives, robots)
Safety Critical Services
Meta Zone
Enterprise Security Zones
Manufacturing & Industrial Security Zones
Cell/Area Zones
Safety Zone
@ 2020 Aruba Networks, a Hewlett Packard Enterprise Company. All rights reserved

Figure 3: The Meta Zone

Customers also want uniform end-to-end visibility of operational and contextual data in real-time, from the Safety Zone and Zone 0 all the way to the CEO suite. That degree of visibility requires a new “Meta Zone,” sitting above Zones 4 and 5, that can reached directly into any Zone. Digital transformation in a hybrid world requires tapping data from across the enterprise, say from a hybrid cloud that encompasses on-premise, data centers, and/or private/ public clouds.

Direct access to data from lower Zones offers the possibility of real-time insights and digital twin updates without losing context from devices hidden in the shadows behind gateways, PLCs, and other proxies. A true bird’s eye view allows mining of seemingly disparate events, which when taken collectively impact could business continuity, predict pending failures, and help optimize material planning and personnel management.

Provided that comprehensive cybersecurity is applied to protect the Meta Zone, its data and connections, this super-Purdue Model has several advantages:

- It allows the Meta Zone to reach directly into any Zone for visibility and security data, allowing faster response to performance degradation and security breaches in lower Zones that might not be propagated up due to filtering between Zones:
- It avoids a single point of failure between Zones from obfuscating activity in lower Zones; and
- It addresses systems and architectures that were not anticipated when the Purdue Model was originally created.

The hierarchical Purdue Model works well for process operations, but not for uniform visibility and security. Nor does the model accommodate cloud architectures in which data need to flow unfiltered from lower Zones directly to business logic.

IIoT SECURITY

IIoT stands out as a category because in no other industry is the impact of a security breach so impactful or the defenses so poor. The ‘Achilles heel’ of IIoT is security: IIoT devices are fundamentally untrustworthy. The reason is simple: the engineers who design, install, and maintain these devices are typically trained on process reliability and application-specific architectures, and their objective is to make products work reliably for as long as possible. Cybersecurity expertise sits with information technology (IT) engineers. Adhering strictly to a zero trust framework, IIoT devices should not be allowed on a network unless and until trust can be asserted to the same standard as it is with IT devices.

Addressing the shortcomings of IIoT device security isn’t a trivial task. The diversity of installed legacy devices is vast; many have been in service for decades and predate the advent of both modern cybersecurity and the Internet. Replacing legacy devices is often technically and economically unviable, not to mention the disruption that upgrades would cause to on-going operations. Many new IIoT devices also lack sound cybersecurity features, and many CISOs will not permit either IIoT devices or gateways on corporate networks, making it challenging to bridge the IT/OT divide.

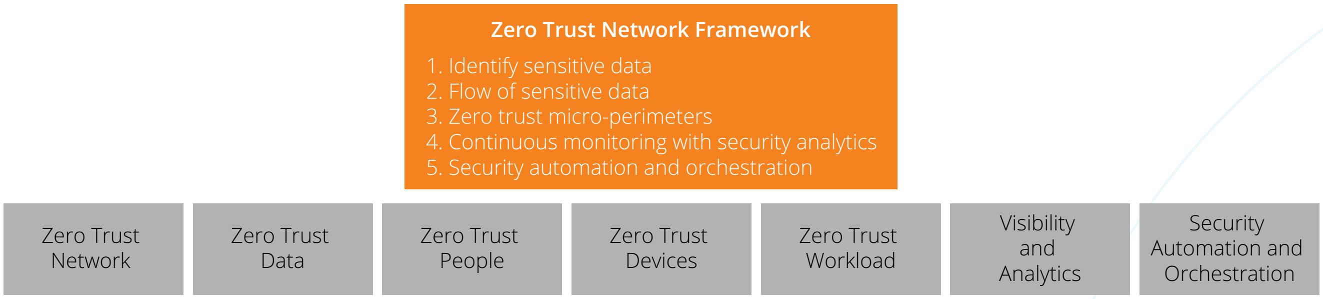

Zero Trust Network Framework
1. Identify sensitive data
2. Flow of sensitive data
3. Zero trust micro-perimeters
4. Continuous monitoring with security analytics
5. Security automation and orchestration
Zero Trust Network
Zero Trust Data
Zero Trust People
Zero Trust Devices
Zero Trust Workload
Visibility and Analytics
Security Automation and Orchestration

Figure 4: Zero Trust Framework

The goal should be to create a zero trust defensive framework in which no device or user is trusted until proven otherwise. The framework should leverage contextual information from a multitude of sources to scrutinize user and device security posture before and after they connect. Doing so helps overcome the limitations of fixed security perimeters tied to physical boundaries, which break down in the face of mobile IIoT devices and during plant changeovers, adds, moves, and changes.

IIoT security framework should include layered protective mechanisms in accordance with a zero trust framework:

- Authenticating source/destination devices and monitoring traffic patterns;
- Encrypting data packets using commercial and, where applicable, government encryption standards;
- Micro-segmenting traffic inside secure tunnels to ensure devices communicate only with their intended applications;
- Fingerprinting IIoT devices to determine if they are trusted, untrusted or unknown, and then applying appropriate roles and context-based policies that control access and network services;
- Inspecting north-south traffic with application firewalls and malware detection systems to monitor and manage behavior;
- Leveraging enterprise mobility management (EMM), mobile application management (MAM) and mobile device management (MDM) systems to monitor behavior and protect other devices in the event of a policy breach; and
- Relying on AI-based analytics to continuously look for anomalous behavior even after trust has been asserted.

Legacy IIoT devices can be identified as known or unknown upon connecting to the network using their MAC address in an external or internal database. The profiling data should flag if a device changes its mode of operation or masquerades as another IIoT device – a common issue with MAC-based authentication - and then automatically modify the device's authorization privileges. For example, if a Windows tablet PC tries to masquerade as a programmable logic controller (PLC), network access should be immediately denied.

Mitigating IIoT security risks requires a blended approach that includes methods taken from mobile, cloud, automation, and physical security. The sheer breadth of IIoT solutions mandates an array of embedded trust, device identity, secure credential, and real-time visibility solutions. New and unfamiliar cybersecurity risks include: IIoT solutions can change the state of a digital environment, in addition to generating data, and this variability of state requires a new view of cybersecurity; IIoT environments include unattended endpoints - in lights-out factories and remote sites - that can be both physically probed and logically attacked; and machine-to-machine (M2M) authentication works in newer IIoT devices but not in many legacy devices, creating trust gaps between generations of devices and gateways.

The industrial control market is very conservative, and the rate of technological change has been significantly slower than the consumer product industry. As a consequence, today's plants require security expertise outside the realm of traditional automation companies. Cybersecurity has to underpin all IIoT solutions but is not a core skill for most industrial suppliers. Indeed, cyber security, location-based services, and analytics, all foundations elements of IIoT, are the province of IT.

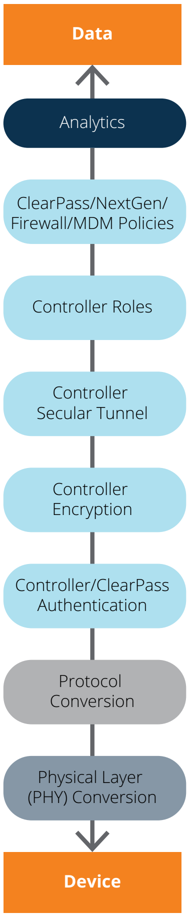

Data
Analytics
ClearPass/NextGen/ Firewall/MDM Policies
Controller Roles
Controller Secular Tunnel
Controller Encryption
Controller/ClearPass Authentication
Protocol Conversion
Physical Layer (PHY) Conversion
Device

Figure 5: IIoT Protection Mechanisms

Bridging the IT/OT divide is paramount to the successful implementation of a zero trust framework. Aruba's policy enforcement firewall and encryption, working in concert with secure tunneling and the ClearPass Policy Manager, can protect IIoT systems and secure the network edge. However, policies are only as effective as the information used to build them, and that must be based on a deep understanding of the processes and procedures underpinning the industrial enterprise. Applying a collaborative systems approach to the problem will help identify the IIoT threat vectors and the security technologies needed for remediation.

Transforming untrusted IIoT devices into trusted data will allow the strategic business goals of cognitively aware plants to be realized without incurring unacceptable risk. Let's now examine how to align a company's strategic goals with the implementation of cognitively aware plants.

BUSINESS TRANSFORMATION ENABLED

Some years ago the head of the Industrial Engineering Department of Yale University said, "If I had only one hour to solve a problem, I would spend up to two-thirds of that hour attempting to define what the problem is."2 In the same vein, a woodsman was once asked, "What would you do if you had just five minutes to chop down a tree?" He answered, "I would spend the first two and a half minutes sharpening my axe." 3 Regardless of your industry or task, it's important to be prepared, carefully defining your objectives and selecting the tools needed to achieve them.

Sadly, this lesson is often overlooked when it comes to IIoT projects. Whether it's the allure - or misunderstanding - of the IIoT concept, fear of being left behind by competitors, or pressure to do something new, companies frequently rush head first into IIoT projects without clearly defining objectives, value propositions, or the suitability of tools. The result is a high rate of failure, and disillusionment among customers.

Originally intended to describe an ecosystem of interconnected machines, the phrase "Industrial Internet of Things" has been taken literally to mean connecting all devices to the Internet. The overarching objective of IIoT is not to connect every device to the Internet. IIoT devices are vessels for context and data, and the objective is to tap only relevant information and devices.

How does one determine what is or is not relevant information? Relevance is established by a chain that stretches from the enterprise's strategic goals, to business objectives designed to achieve those goals, to what Gartner4 calls "business moments" – transient, customer-related opportunities that can be dynamically exploited. A business moment is the point of convergence between the owner's strategic goals and relevant IIoT context and data that when properly exploited will positively change reliability, performance, and/or safety.

Business moments must be carefully orchestrated, even if they appear spontaneous. Success hinges on a second chain that stretches from relevant IIoT context and data thru the IIoT architecture that accesses and conveys them to a target business moment. If the chain is poorly executed, say because the IIoT architecture can't extract relevant information, then the business moment may pass without result, or could even trigger negative results to the detriment of the strategic goals.

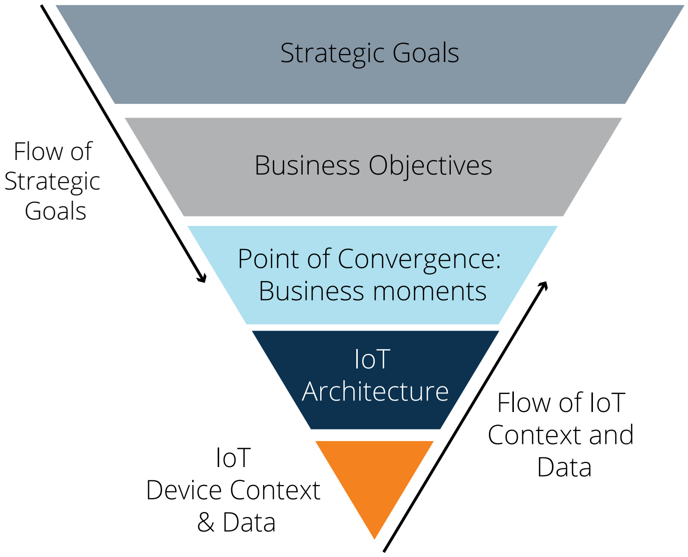

Strategic Goals
Business Objectives
Point of Convergence: Business moments
IoT Architecture
Flow of Strategic Goals
Flow of IoT Context and Data
IoT Device Context & Data

Figure 6: IIoT Strategic Hierarchy

And so we return full circle to the professor and the woodsman. The first order of business in any IIoT project is to identify the strategic business goals to be achieved. Those should flow down into a series of specific objectives that rely on successfully delivered business moments. The IIoT architecture is the tool by which relevant context and data can be successfully extracted and exploited in favor of the strategic goals.

Business goals and objectives inform IIoT architecture, not the other way around. Where does one start this process? The first order of business is to identify the customer's strategic goals and the associated business objectives that must be met. Is the objective to optimize production yields with better workflows and raw goods management? Migrate from break/fix to predictive maintenance? Enhance personal safety with social distancing and thermographic monitoring? The answer(s) will impact the business moments that need to be delivered, and what constitutes relevant data and context.

This document presents IIoT use cases that are relevant to a broad range of chemical, food & beverage, logistics, manufacturing, petrochemical, pharmaceutical, and utility applications. Government and defense-related applications that require Common Criteria, FIPS-140-2, and high security validations are included. Most of the use cases include at least one Aruba technology partner whose solution, used in concert with Aruba infrastructure, helps address strategic business challenges.

BUILDING A CONTEXTUALLY-ADAPTIVE PLANT

Factory asset tracking systems feed real-time inventory and work-in-process data to analytics engines to more efficiently manage production lines. If inventory delivery is delayed production lines can be slowed instead of stopped, reducing expensive scrap, rework, and re-start expenses. The result is a contextually adaptive factory that automatically balances the speed of production with the availability of parts.

Asset tags are an important building block of an adaptive factory. Attached to, or inserted into, items to be tracked, asset tags broadcast an ID number over wireless to identify the specific asset and, optionally, send telemetry data such as temperature or shock level. RF asset tracking infrastructure picks up the ID number and telemetry, and relays them to the factory management systems.

Dedicated tag RF infrastructure is expensive to deploy, adds a new failure domain that can impact the system mean time between failure (MTBF) rate, and presents an attack surface that CISOs would like to avoid. Since workflows, revenue, profit margins, and network security are all at risk, operations teams typically prefer asset tag data to be collected and managed thru a factory's existing wireless infrastructure.

With their built-in IIoT radios, Aruba access points are control network platforms that can support a broad range of IIoT devices, including BLE-based asset tags.

ZF | OPENMATICS

ZF OPENMATICS, a division of ZF Aftermarket - the second largest product and solution supplier in the global automobile spare part market worldwide - is a major supplier of ruggedized deTAGtive BLE asset tags (TAGs). TAGs have industrial ratings up to IP69K, and are resistant to compressed water, rough treatment, and harsh weather conditions.

Figure 7: ZF Openmatics TAG

Used together with the Openmatics DeTAGtive® mobile app and cloud-based deTAGtive logistics portal, TAGs help track the location of power trains, engines, and other industrial goods through logistics chains and manufacturing floors.

ZF OPENMATICS and Aruba have partnered to deliver asset tracking solutions that can be economically, reliably, and securely deployed over a site's Aruba wireless network by leveraging access points' internal BLE radios. In fact, the deTAGtive solution is used throughout ZF's own production facilities in conjunction with the installed Aruba Wi-Fi infrastructure.

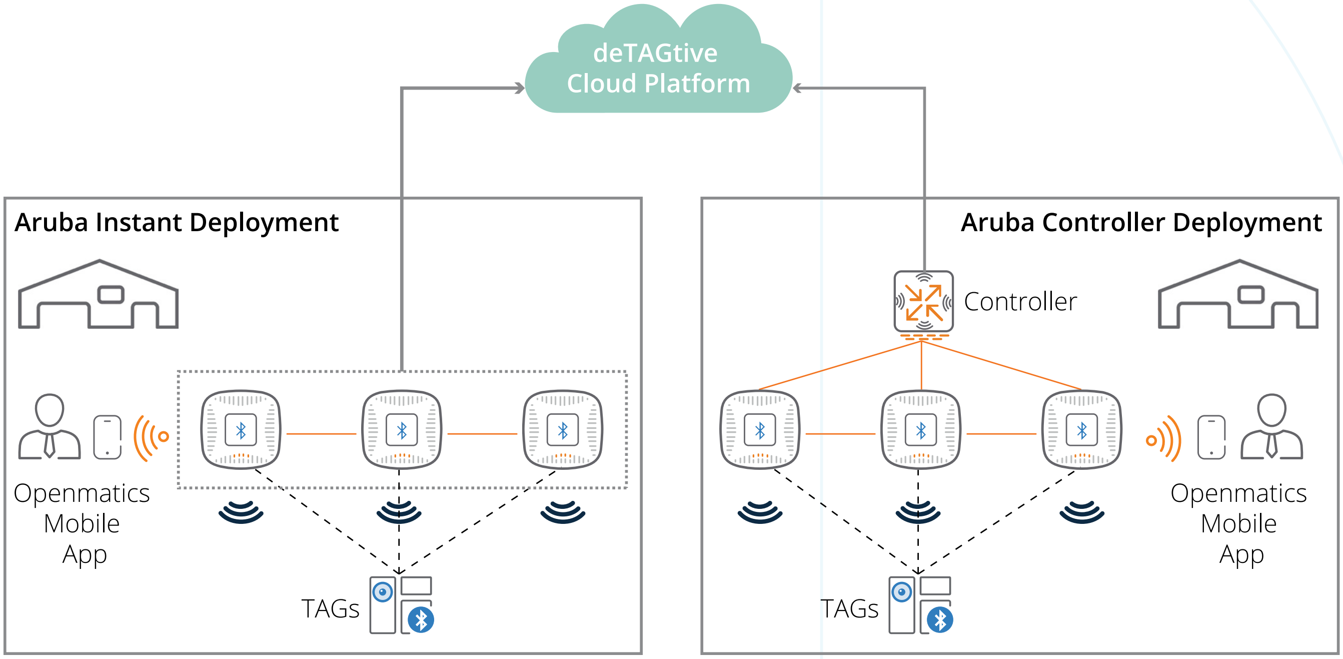


Figure 8: Aruba and ZF Openmatics Joint Solution

Aruba access points serve as secure communications platforms between TAGs and the deTAGtive portal. Dynamic segmentation is maintained through the Aruba switch fabric, helping to protect the asset tracking system against attack, and the network against infected devices. Dynamic segmentation automatically establishes the correct secure connections with access points regardless of the switch port to which they're connected. This feature greatly simplifies system deployment, and reduces the chances of miswiring during plant updates.Aruba access points serve as secure communications platforms between TAGs and the deTAGtive portal. Dynamic segmentation is maintained through the Aruba switch fabric, helping to protect the asset tracking system against attack, and the network against infected devices. Dynamic segmentation automatically establishes the correct secure connections with access points regardless of the switch port to which they're connected. This feature greatly simplifies system deployment, and reduces the chances of miswiring during plant updates.

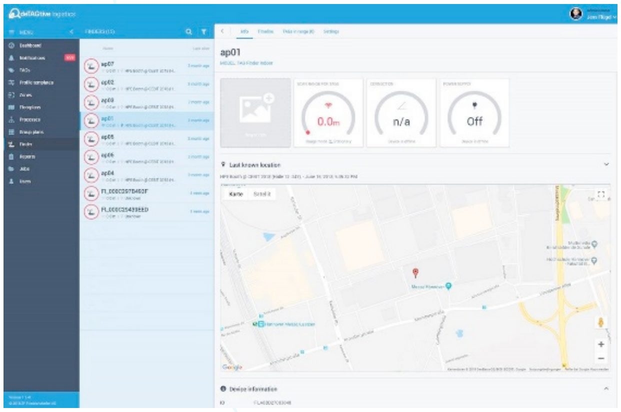


Figure 9: ZF Openmatics Dashboard

Once deployed, the system updates the cloud-based deTAGtive application about asset location. These data can then be shared with ERP systems using open APIs to further automate production management.

Key business benefits include:

- Enabling real-time location monitoring across the entire plant without significant investments in new infrastructure;
- Updating cloud-based applications without impacting workflows;
- Sharing location data and asset status via open APIs to optimize time-and-motion, maintenance, and asset storage processes; and
- Protecting factory workflow information with end-to-end security.

The joint solution is an ideal way to optimize workflow based on the availability of component parts, and can be used in industrial and manufacturing applications of any size.

SECURING CONTROL NETWORKS THAT CAN'T PROTECT THEMSELVES

Industrial and manufacturing customers typically have large deployments of Operational Technology (OT) sensors, actuators, programmable logic controllers, and human machine interfaces that run factories and plants. Historically OT systems were air gapped from the rest of the building systems because operations teams wanted full responsibility for uptime and management, and to protect them from attack. That approach proved ineffective in the face of modern cyber threats, like the Stuxnet virus, that cross air gaps. Even inter-Zone firewalls in the Purdue model are insufficient in the face of many modern cyber threats. That has turned a spotlight on the security of OT systems, and a pivot away from air gaps to active OT monitoring.

The objective of active OT monitoring is to provide uniform visibility and security policies across the OT control buses, programmable logic controllers, SCADA remote terminal units, and related devices. OT systems use unique physical layers (PHY) and protocols, so specialized tools are needed to monitor them and share data with Aruba's ClearPass Policy Manager.

Inserting eyes and ears into an OT network, and enabling security system based in the Meta Zone to reach directly into the Safety Zone and Zones 0 and 1, requires tight alignment with the operating modes of OT infrastructure. In addition to understanding the OT physical layers and protocols, the monitoring system needs to have a library of devices types, know correct and abnormal operating modes, and do no harm in both normal operating and failure modes.

Aruba has partnered with best-in-class OT security companies to help bridge the IT and OT security divide. These partners couple deep knowledge of industrial control systems and machine learning-based threat analytics with a bi-directional link to ClearPass Policy Manager. The solution identifies OT devices, finds vulnerabilities, detects threats, and responds in a manner appropriate to the customer's needs, i.e., alert only, remediate thru ClearPass access control, or alert and remediate.

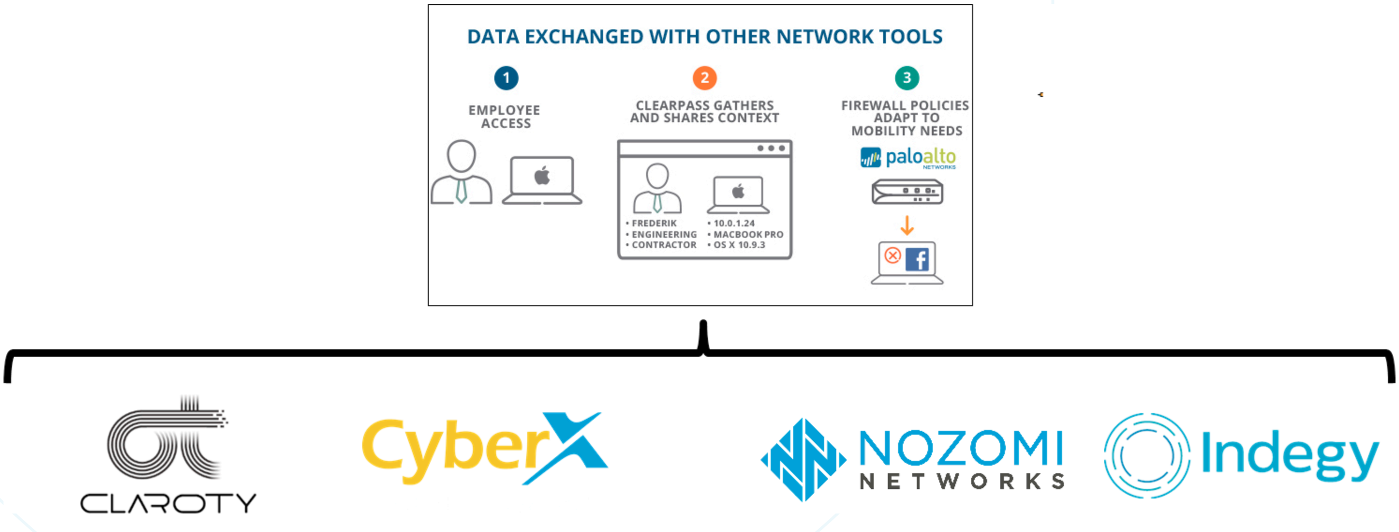


Figure 10: OT Security System Integration With Aruba ClearPass

ClearPass Policy Manager uses device profiling, role-based access control, and real-time policy enforcement to identify, on-board, and control devices. OT security partners enhance these services by discovering OT devices, flagging risks and abnormalities, and enforcing security postures.

The joint solution allows IT administrators to centrally manage connected devices and enforce policies governing what those devices can do: OT retains control of their devices, IT obtains uniform visibility and security policies across the entire enterprise, and the end user avoids costly downtime, safety incidents, and loss of intellectual property.

When an OT device connects to the network it is discovered by the OT security system, which synchronizes with ClearPass Policy Manager to give it a comprehensive view of all IT and OT devices. The supplied context can be used by Aruba to dynamically segment OT communications – a foundational element of a zero trust framework – ensuring that devices only communicate with appropriate applications.

These features enable OT managers to:

- Gain insight into network devices across IT and OT networks;
- Utilize contextual data to deploy seamless edge security; and
- Ensure that only devices compliant with the latest updates are allowed on the network.

OT security partners currently include Claroty, Microsoft CyberX, Nozomi, and Tenable Indegy. Additional partner integrations are anticipated in the near future.

CONNECTING AND PROTECTING REMOTE IIoT SITES

Industry analysts have long opined that the rise of smart machines, cognitive technologies, and algorithmic business models could render obsolete the competitive advantage of offshoring. Hyper-automation, it is argued, will be more influential than labor arbitrage in driving profitability and enhancing productivity. Smart machines will accomplish this by classifying content, finding patterns, and extrapolating generalizations from those patterns.

Labor arbitrage aside, there is no denying the central role of IIoT on the journey to run businesses more efficiently, productively, and profitably. The underpinnings of IIoT are the sensors, actuators, and related control systems that for decades have been running plants and infrastructure.

Large, geographically-distributed industrial companies and utilities have sites spread across broad areas, and depending on the remote site it could be unattended for large parts of the day. Remote sites are particularly at risk of break-ins and cyber attacks because of the vulnerability of IIoT devices running inside them, and the complexity of setting up and managing secure remote access solutions.

Virtual private network (VPN) access has historically been essential for security and vexing to set up: the labor savings that come from centralized VPN management are often offset by the complexity of system configuration and modifications. Additionally, VPNs don't protect endpoints or data at rest, and need to be supplemented with firewalls, intrusion protection systems, and other endpoint defenses. These solutions can be difficult to integrate with IIoT devices, and confusing for users because the remote access methods – like VPN authentication – differ from those used at corporate facilities.

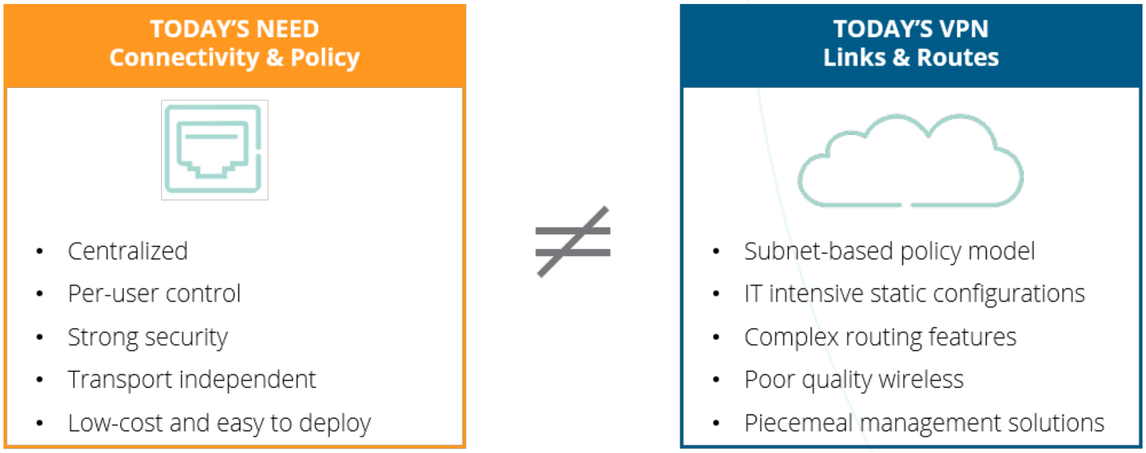


Figure 11: Limitations Of Traditional VPNs

Aruba addresses these issues by simplifying remote site access and connectivity to IIoT devices. Solutions are tailored to the type and number of IIoT devices on site.

If the remote site uses a standalone IIoT controller running Linux, Windows, iOS, MacOS, or Android operating systems, Aruba's VIA VPN Client application can be used. VIA can also be used by field engineers and contractors with ruggedized laptops or tablets. VIA scans and selects the best Ethernet or broadband connection from the IIoT device to the main building network. Unlike traditional VPN clients, VIA offers a zero-touch experience and automatically connects to an Aruba VPN concentrator controller on which it has been allow-listed.

High security government or defense-related sites can run the VIA Suite B VPN client. The client is a hybrid IPsec/SSL VPN. When used in conjunction with an Aruba VPN concentrator controller running the Aruba OS Advanced Cryptography (ACR) module, ACR supports elliptic curve cryptography validated for classified information.

VIA sets up a secure, encrypted tunnel to an Aruba VPN concentrator controller at the main site or data center. The controller runs the Aruba Operating System (AOS) and terminates the VPN tunnels, manages identity assignment, centralizes encryption, and runs Aruba's unique role-based firewall. Every IIoT device and field engineering laptop/tablet is assigned a unique identity by the role-based firewall to regulate how and when the device connects to and uses the network. Identity follows the devices, regardless of how or where they connect to the VPN network.

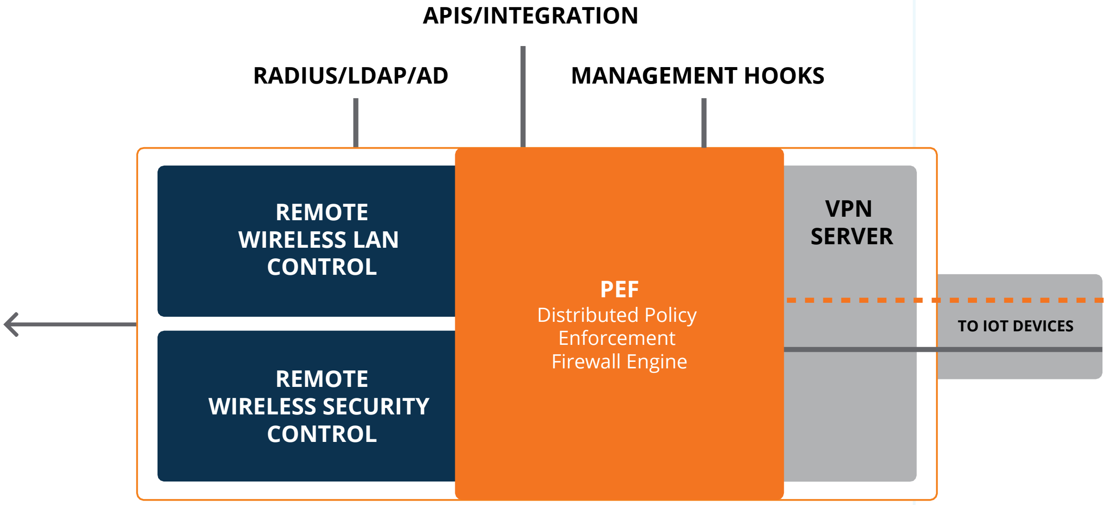

APIS/INTEGRATION
RADIUS/LDAP/AD
MANAGEMENT HOOKS
REMOTE WIRELESS LAN CONTROL
REMOTE WIRELESS SECURITY CONTROL
PEF
Distributed Policy Enforcement Firewall Engine
VPN SERVER
TO IOT DEVICES

Figure 12: Aruba VPN Concentrator Controller

IIoT device MAC addresses can be spoofed, so the identity of headless devices needs to be supplemented by the controller with strong authentication protocols (like 802.1x) and role-based contextual data. These data include location, time of day, day of week, and current security posture, which are used to provide more granular role based access control.

A role is applied during the authentication process, before the device has network access, using Active Directory, RADIUS, LDAP, or comparable data. Unlike simple Access Control Lists (ACLs), Aruba's stateful role-based firewall will actually track upper-layer flows to ensure that unauthorized traffic can't bypass access control. For example, a packet claiming to be part of an established Telnet session would be blocked unless there was an actual established Telnet session underway.

Many remote sites – such as SCADA applications - have multiple IIoT devices, devices that cannot run a VIA client, and/or need a secure local Ethernet and/or Wi-Fi network. In these instance a Remote Access Point (RAP) can be used to provide secure remote connectivity to Ethernet or Wi-Fi based IoT devices using a broadband WAN and/or cellular connection. Like VIA, a RAP uses a zero-touch mechanisms to set up a secure, encrypted tunnel with an Aruba VPN concentrator controller at the plant or data center. Suite B support is available on TAA-compliant RAPs. Unlike VIA, RAPs include local Ethernet ports, Wi-Fi access, and the option to plug-in a cellular modem for primary or redundant back-up wide area communications.

A side benefit of role-based access is that controls are available to optimize the bandwidth utilization of Wi-Fi enabled devices. Since Wi-Fi is a shared medium, significant benefits accrue from limiting the maximum amount of bandwidth consumption for some devices, and guaranteeing a minimum bandwidth level for others. These mechanisms help limit the impact of denial of service attacks while allowing critical IIoT devices to continue operating.

IIoT devices and field engineering laptops/tablets are authenticated, and data encrypted, without any client software or manual intervention. The result is high security connectivity with remote sites and field engineers that is easily configured, requires no user training, and delivers a plug-and-play monitoring experience.

An example remote monitoring application is shown below. In this case the objective is to remotely supervise a chiller that has I/O information of value to plant operations. The chiller has an available Ethernet port but lacks modern security features or VPN support. The Ethernet port is connected to a RAP, which establishes a secure IPsec tunnel via Internet broadband with a cellular back-up. Chiller I/O data are streamed thru the tunnel to the plant management application. RAP updates are pushed automatically from time to time, and no manual or local intervention is required.

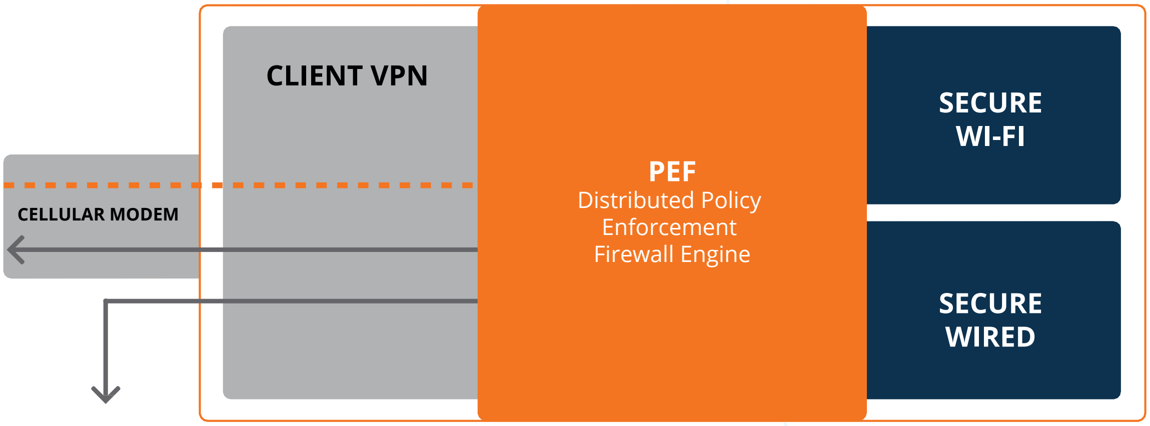


Figure 13: Aruba Remote Access Point

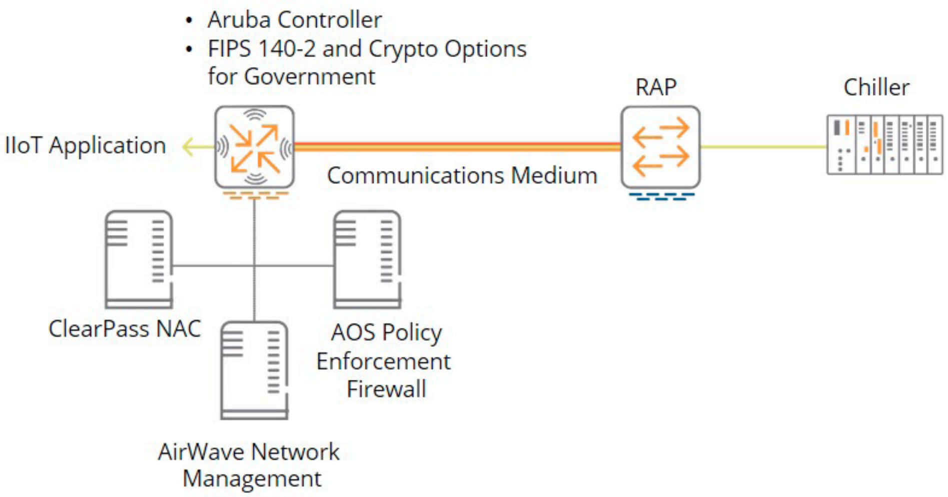

• Aruba Controller
• FIPS 140-2 and Crypto Options for Government
RAP
Chiller
IIoT Application
Communications Medium
ClearPass NAC
AOS Policy Enforcement Firewall
AirWave Network Management

Figure 14: Remote Chiller Monitoring

For sites than need secure, high-bandwidth connectivity with back-up communication paths with service level agreements, a software defined wide area network (WAN) may be appropriate. Traditional WAN infrastructure is complex, and on a large scale can require hundreds of routers, firewalls, and network security systems. Provisioning and maintaining Multiprotocol Label Switching (MPLS) and other dedicated WAN links is time consuming, and can require expensive on-site configuration and maintenance. Direct Internet Access (DIA) services are less expensive than MPLS, however, best path selection for applications requires probing paths and mapping flows.

Aruba's SD Branch solution addresses these issues by providing a central point for configuring routing and access control policies, and a simple means of pushing those policies to remote sites. There is no on-premise management equipment to update or maintain. WAN management is orchestrated through the Aruba Central cloud, from which it's easy to distribute routes and build secure, scalable VPN tunnels on demand. Aruba Central can monitor where traffic enters and exits a remote site, regardless of uplink type, making it easy to manage WAN environments using public WAN connections.

To ensure uniform security, access policies dynamically follow IIoT devices (such as replacement parts) and field engineering tools (like ruggedized laptops and tablets) as they move between sites. High availability active/active and active/standby modes deliver full redundancy for sites that need it.

SD-WAN Gateways located at remote sites are designed to support multiple broadband, MPLS, or cellular links. Policy-based routing ensures that traffic can be routed across multiple private or public WAN uplinks based in the traffic type, link health, device profile, user role, and destination. Traffic can be routed over the best available uplink based on factors such as throughout, latency, jitter, and packet loss.

Regardless of whether you need to monitor a single remote IIoT device, small sites with multiple IIoT devices, or a critical site requiring fault-tolerant WAN links, Aruba has you covered.

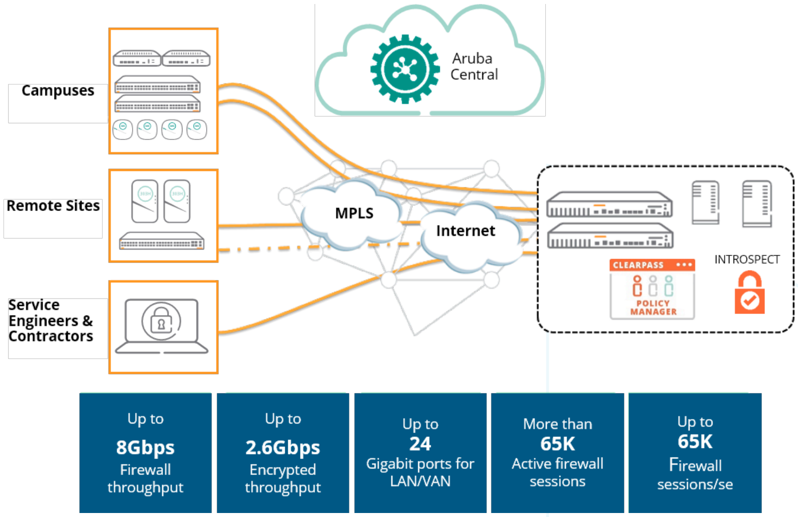

Aruba Central
Campuses
Remote Sites
Service Engineers & Contractors
MPLS
Internet
CLEARPASS
POLICY MANAGER
INTROSPECT
Up to 8Gbps Firewall throughput
Up to 2.6Gbps Encrypted throughput
Up to 24 Gigabit ports for LAN/VAN
More than 65K Active firewall sessions
Up to 65K Firewall sessions/se

Figure 15: Aruba Remote SCADA Site Connectivity

RUNNING PROFINET IO OVER SHARED WIRELESS INFRASTRUCTURE

Profinet IO is a commonly used, open IIoT control networking solution for data exchange between programmable logic controllers (PLCs). Profinet IO uses TCP/IP for parameterization, configuration and on-demand read/write operations, and can be transported over Wi-Fi so long as the wireless infrastructure can address the latency, fast roaming, bandwidth reservation, and redundancy requirements of the Profinet application. Typical Profinet IO deployment scenarios include dedicated point-to-point (P-to-P), point-to-multipoint (P-to-MP), and site networks for roaming.

Many IIoT vendors make dedicated P-to-P and P-to-MP wireless networks for Profinet IO, however, these systems aren't optimized be used for other plant services like voice and video, and lack the uniform security and inform visibility built into Aruba wireless infrastructure.

Aruba's AI-based wireless infrastructure can address Profinet's latency, fast roaming, and redundancy requirements, while Aruba's Policy Enforcement Firewall can ensure adequate bandwidth reservation.

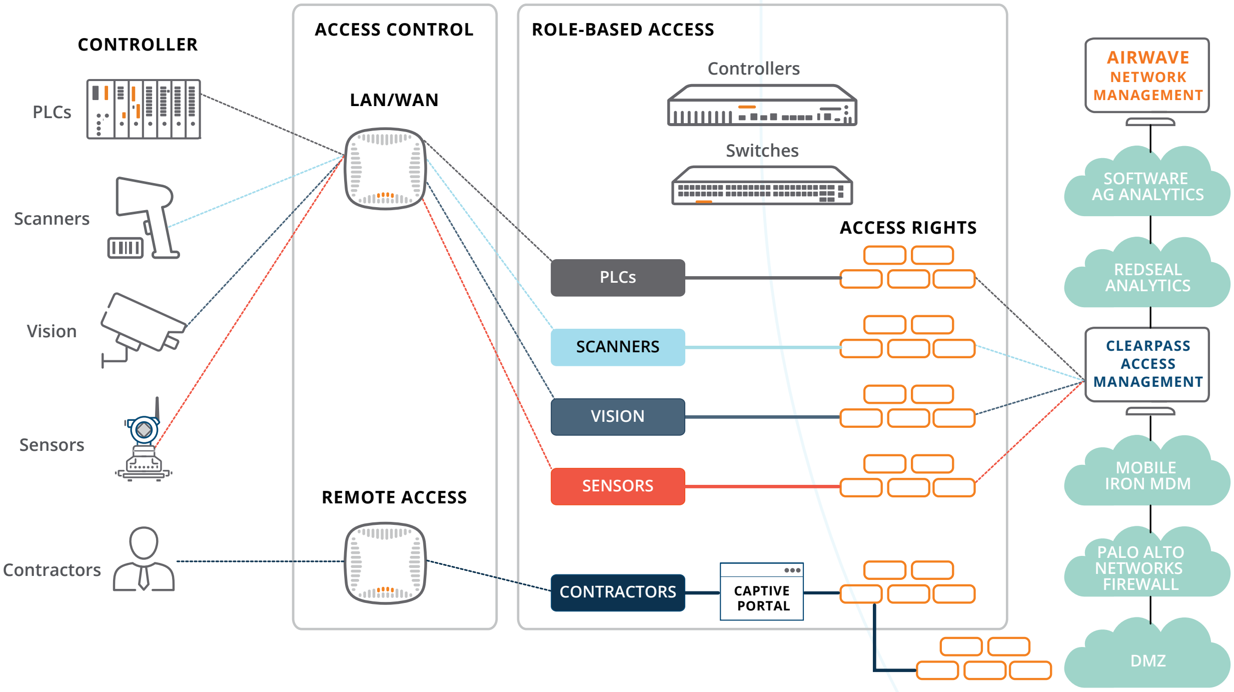


Figure 16: Using Aruba's AI And Policy Enforcement Firewall Services To Connect And Protect Profinet IO

More specifically, the default configuration should be set to forward ethertype 0x8892 traffic, and depending on the Profinet client type and age additional adjustments to default configurations may be required. Many IIoT deployments still use aging 802.11g or 802.11n devices. When high retries, drops, or problems with CSD are observed, it's rarely possible to adjust older client devices to remedy the issue. Instead, the access point should be set to 802.11g or 802.11n, as appropriate. For Profinet applications that access points are typically set to one 20MHz wide, non-DFS 5GHz channel with adaptive radio management disabled. Profinet IO relies on broadcast to match devices and servers, so flooding is essential and there can be no transmit latency.

Running Profinet IO on a wireless network requires attention to Ethernet switch settings, too. Upstream switches may need to handle a VLAN tag of "0" and re-mark frames to ensure end-to-end Quality of Service over the wired network to and from the access point.

Using Aruba's secure infrastructure for Profinet IO avoids the expense and complexity of parallel network infrastructure. The simpler design, with fewer parts, also boosts overall system MTBF.

REDUNDANT INTRA-SITE WIRELESS VIDEO AND DATA LINKS

Inter-building IIoT data, outdoor surveillance video, remote gate control, and supervisory control and data acquisition systems often require outdoor data links. The choice between wired or wireless data links typically comes down to cost. If a wired network requires reaching across a parking lot or gully to surveillance cameras or an out building, it can easily take days of work to trench and repair asphalt or concrete. If there is hazardous buried material in the path, pipelines to cross, or the right of way is unavailable, the challenges continue to mount.

Wireless data links are easier to deploy than buried cables, however, the cost of a point-to-point high-speed microwave link can make it prohibitive for short-haul links under 400 meters. Less expensive links represent a single point of failure because they typically don't offer redundancy and can be impacted by nearby cellular networks. Additionally, in areas subject to high winds, even the slightest movement of the mounting brackets can throw an antenna out of alignment and require a service call.

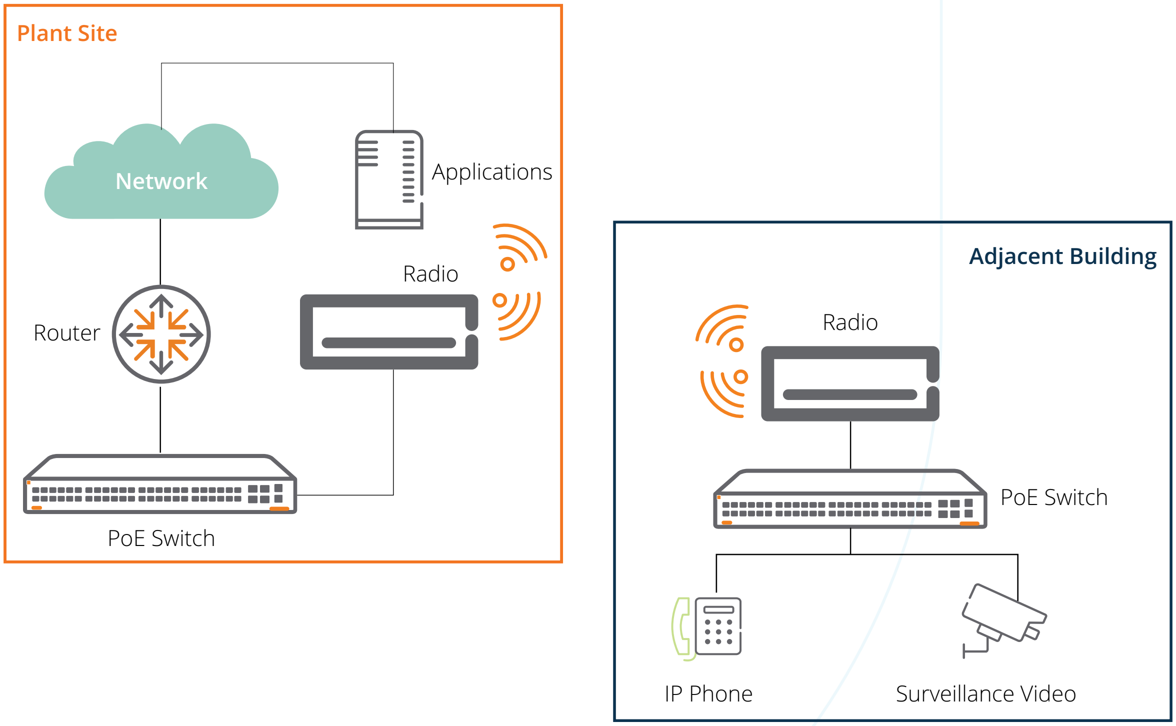


Figure 17: Point-To-Point Extension of a Plant Network to an Adjacent Building

Aruba's AP-387 is a high-speed, dual-radio, point-to-point link that addresses the shortcomings of today's point-to-point links. Incorporating a 60GHz millimeter wave radio with electrically steerable antenna array, the AP-387 provides automatic fallback to a 5GHz radio in the event that rain or snow attenuate the 60GHz signal. Redundant radios ensure that the link is always optimized, offering an aggregate peak rate of 3.37Gbps and a fallback rate of 867Mbps. Advanced cellular coexistence minimizes interference from cellular networks, distributed antenna systems, and commercial small cells, and femtocell equipment.

The auto-adjusting 60GHz antennas can dramatically reduce labor costs throughout the life of the site. The 60GHz radios will intelligently link with alignment ±45 degrees azimuth, and ±17 degrees elevation; the 5GHz radio fixed sector antennas cover the same alignment zone. This eliminates the need for precision alignment, or high-cost skilled labor, during installation. Just point one radio in the general direction of the other, even if they are separated by as much as 20 stories of elevation, and the radios will link up.

Weighing just 1.2kg each, the radios can be commissioned by a single installer. The AP-387 includes an integrated BLE radio for hands-free set-up.

Extending plant-critical communications to other buildings and on-site locations shouldn't compromise reliability or your budget. The AP-387 can provide a redundant, point-to-point link up to 400 meters. With an aggregate peak rate of 3.37Gbps it can support a very broad range of IIoT, telephony, streaming video, and physical security applications.

INTERCEPTING QUALITY-IMPACTING IIOT ISSUES IN THE SWITCHING FABRIC

Lights-out manufacturing depends on IIoT automation and robotics to eliminate human participation in the manufacturing process to boost productivity and lower costs. Without human workers plants can be more densely designed, climate-control can be tailored to machines efficiency instead of human comfort, and shift change slowdowns are a thing of the past. Humans instead are relegated to service roles.

The challenge is that with full automation comes a dependency on rapid error detection and correction. Take, for example, a computer vision system in which a networked camera monitoring product defects streams data to a network-connected programmable logic controller. In this machine-to-machine application, if the video stream starts going astray there is no human present to detect the degradation on a monitor. The same is true of other networked processes in a lights-out factory.

A lights-out factory may be an extreme case but it drives home the point that an automated supervisory system is important for both operations optimization and preventive maintenance. Since the only commonly-shared element among all machine-to-machine applications is the plant Ethernet network, it makes sense to look first at a solution that runs within the switching fabric.

Figure 18: Aruba AP-387 High-Speed Outdoor Point-To-Point Link

Figure 19: Aruba CX 8400 High-Availability Switch

Aruba's CX switch operating system uses a database-centric design and a programmatic interface to the entire database schema. All internal states, protocols, and statistics are expressed in the database, providing visibility into everything that happens on the network. With a database-driven operating system, any factor can be monitored and performance compared over time.

Aruba's Network Analytics Engine (NAE) uses Python scripts to define which switch resources to monitor and, optionally, rules for actions to take when certain conditions are true. CX is database-driven, and any factor can be monitored over time and acted upon. Python scripts typically target IIoT performance, security, and scale.

In the example above, the vision system camera data flow could be monitored with an NAE script, and an automated notification sent to service personnel if degradation is detected in the data stream or switching fabric itself. Proactively addressing a vision system problem prior to failure can save the expense of a line shut-down and restart, as well as the cost of reworking finished goods that escaped detection.

BRIDGING IT/OT PLANT-WIDE FOR UNIFORM VISIBILITY & SECURITY

The proliferation of connected IIoT devices has moved in lock step with initiatives to optimize operations, boost efficiency, better manage inventory, and enhance safety. Powered by insights from data analytics applications, and fueled by device data and contextual information like location and identity, these initiatives have generated an almost insatiable demand for high-availability, connected devices.

A connected device is only useful when it's operating properly, and the data it generates are trustworthy. These requirements demand data visibility and cybersecurity spanning from I/O to CEO, from the Safety Zone to the Meta Zone. It is here that a trust divide typically surfaces between IT networks that interconnect the enterprise, and OT networks that runs plants and factories.

OT is a broad field ranging from pre-Internet legacy systems to modern Industrie 4.0 digital technology. A challenge common across industries is that the OT infrastructure running plants, and the IT networks running enterprises, are not tightly coupled. This creates gaps in data and device visibility, application assurance, and security that can delay the resolution of network problems, impact user experiences, and mask vulnerable attack surfaces.

Bridging the gaps requires expertise that cuts across traditional OT and IT boundaries, making I/O-to-CEO visibility and security a real challenge. It also requires a deep understanding of how CIOs and COOs prioritize network operations. For CIOs cybersecurity and trustworthy data are top priorities, and device and network outages are tolerated during security and operating system vulnerability updates. COOs prioritize plant availability and manufacturing output targets. Security updates and OS patches are anathema to both and must be very carefully implemented so as not to disrupt operations.

Even the meaning of the word "trust" differs between CIOs and COOs. In the IT world, trust is associated with the provenance and security of data and devices. In the OT, world trust is equated with the reliability and resilience of systems that are often in place for decades. IT systems are frequently patched and updated, resulting in device or network outages, no matter how brief, that would be unacceptable in the OT world.

What do CIOs and COOs have in common? Both want uniform visibility into, and security of, OT traffic and device behavior, with IT policy management supervision of crossover traffic.

Bridging the IT and OT divide requires a recognition that both definitions of trust, and both modes of operations, are important to achieving enterprise-wide data visibility and cybersecurity. One without the other would put an enterprise at risk financially and operationally.

SIEMENS
Ingenuity for life

Siemens and Aruba have partnered to realize that vision. Siemens brings over 30 years of experience in the fields of OT communication technology, with services and infrastructure that can be customized and scaled to meet the needs of a wide range of industrial and manufacturing customers.

Siemens' OT solutions include Scalance, Ruggedcom, Simatic, and MindSphere brands. Products include Industrial Ethernet switches and wireless, modems, routers, WAN radios, security appliances, and the cloud-based MindSphere IoT operating system. Ruggedcom products work in harsh environmental and electromagnetic conditions, while Simatic location and RFID systems can track mobile robots, transport systems, and work in process.

Aruba's solution platform is built around core connectivity, security, location, compute, and management building blocks, which together form its architecture for building zero trust IIoT solutions. Interconnections with Siemens' products and services deliver unique value in bridging the OT/IT divide.

Aruba knows well how to satisfy CIOs, and has extended its solution set to address COO' concerns about availability and output:

- Hitless updates allows Aruba to keep deployments current with operating system updates and security patches without bringing down an entire network;
- Dynamic segmentation, a foundational element of a zero trust framework, identifies IIoT devices and securely tunnels IIoT data to target applications. The solution is automatic and immune from the types of miswiring errors common with VLANs;
- Aruba's MultiZone feature allows a common IT infrastructure to be managed by IT, while the OT teams manage access rights to up to five independently operating Zones (for the factory, contractors, machine-as-a-service, and other entities). The solution is available in FIPS 140-2 and Common Criteria validated versions for defense-related IIoT applications.

More specifically with regard to integrated Aruba/Siemens deployments, Aruba's ClearPass automatically identifies, profiles, on-boards, and assigns appropriate security policies to IP-based Siemens devices, as well as mobile and fixed IIoT devices. ClearPass' RADIUS server enables Siemens devices to obtain AAA services from the IT infrastructure, providing one common source of control. Adds, moves, and changes are faster, lowering lifecycle costs and reducing the mean time to repair systems. ClearPass also interfaces with other security infrastructure – next gen firewalls, MDM, SIEM, EMS, OT monitoring – to provide comprehensive security, including quarantining if permitted under OT rules.

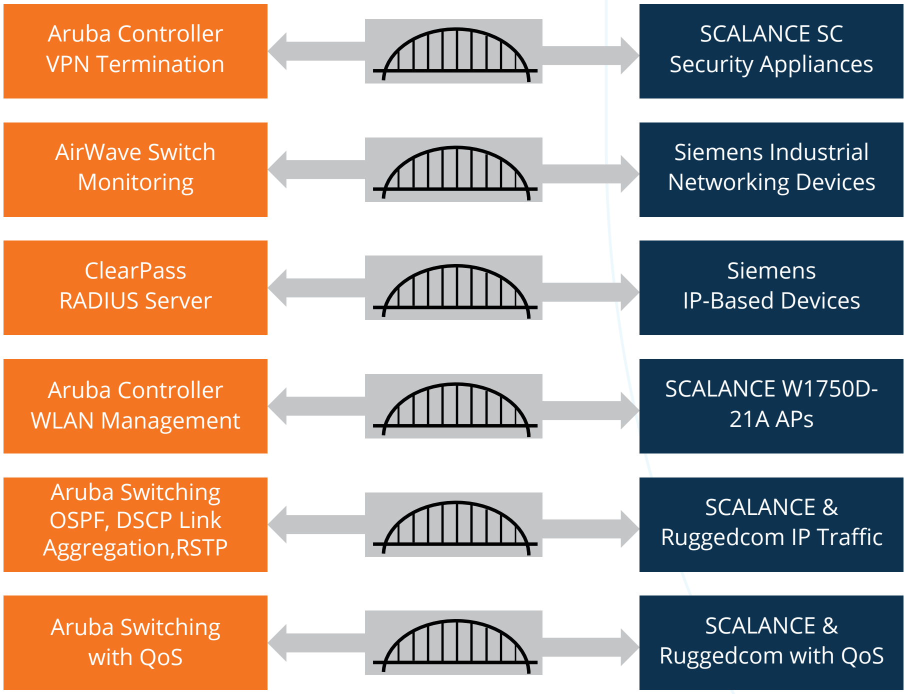

Aruba Controller VPN Termination
SCALANCE SC Security Appliances
AirWave Switch Monitoring
Siemens Industrial Networking Devices
ClearPass RADIUS Server
Siemens IP-Based Devices
Aruba Controller WLAN Management
SCALANCE W1750D-21A APs
Aruba Switching OSPF, DSCP Link Aggregation,RSTP
SCALANCE & Ruggedcom IP Traffic
Aruba Switching with QoS
SCALANCE & Ruggedcom with QoS

Figure 20: Bridging the IT/OT Divide

Aruba's AirWave network management solution offers single pane of glass visibility into wireless and L2/3 switch operations, zero touch device provisioning, intrusion detection, and trouble ticket management. By pulling data from every element of the Aruba infrastructure, these tools deliver fine grained visibility and predictive insights into systems of any size. AirWave is capable of monitoring select Siemens industrial network devices, delivering a homogeneous view of a heterogeneous network that is more intuitive to operate and manage.

Siemens and Aruba have also taken the guess work out of IT/OT deployments by validating interoperable operation across products, and documenting reference designs, for Aruba, SCALANCE, and Ruggedcom products. Every deployment will have unique aspects, so for illustrative purposes the diagram below shows a typical joint deployment scenario.

Key benefits of integrated Aruba-Siemens deployments include:

- Integrated plant-wide IT and OT architecture provides visibility and cybersecurity from I/O-to-CEO;
- Dynamic segmentation provides common enforcement options for devices connected to Aruba switches;
- Common AAA services simplifies security management; and
- Single pane of visibility through the AirWave console.

Working in concert, Aruba and Siemens bridge the IT/OT gap, satisfying both COOs and CIOs by ensuring plant and network availability, reliability, and security.

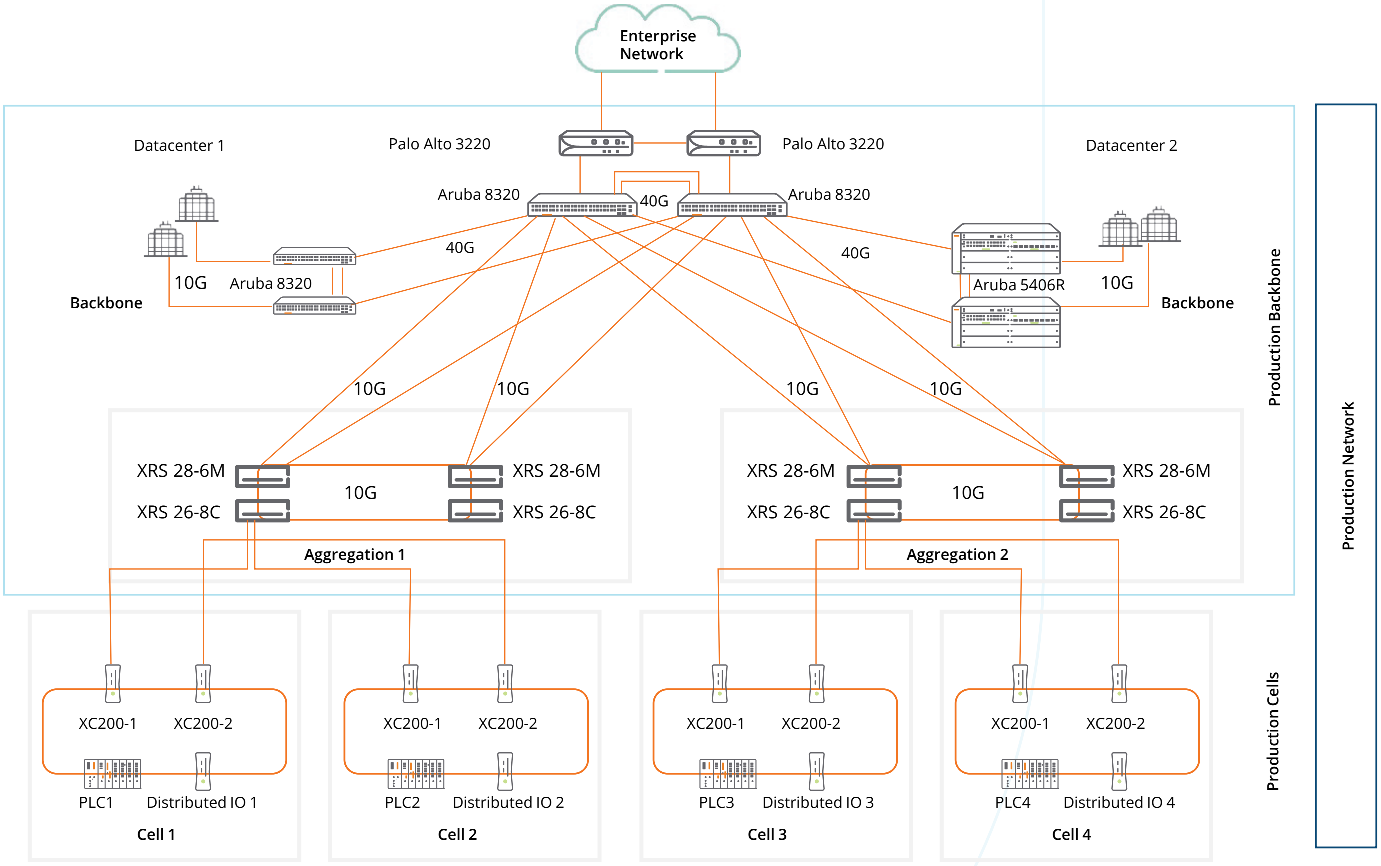


Figure 21: Typical Joint Deployment Scenario

AUTOMATING PLANT NETWORK ACCESS FOR SERVICE PERSONNEL AND CONTRACTORS

Enhancing human productivity necessitates making devices and the environments in which they work more cognizant of, and automatically adaptive to, the needs of employees, service personnel, and contractors. On-boarding service personnel and contractors onto plant networks has historically been challenging because of network security concerns. In some cases, access is simply refused, forcing visitors to use cellular networks that by-pass plant IT security and can't take advantage of on-site applications and servers. The trick is to both simplify guest access so it doesn't create an administrative burden, and implement security policies that tightly control what guests can do and access while on the network.

Aruba and its technology partners have a proven solution by which service personnel and contractors can be automatically badged and enrolled on the plant Wi-Fi network, guided to their hoteling space or destination using wayfinding, and enable personally-owned devices to securely connect to projection screens and other network resources in designated areas.

Key solution components include Aruba Wi-Fi 6 Access Points, ClearPass Guest Access, ClearPass Policy Manager, Envoy's visitor management solution, WPA3 Enhanced Open, and an Access Code captive portal. Performance of the offered services are monitored using the Aruba User Experience Insight (UXI) solution to ensure that service level agreements are satisfied and application performance meets plant guidelines.

Aruba 500 Series Wi-Fi 6 Access Points are recommended because of their Wi-Fi performance and integrated IoT radios for sensing and control. ArubaOS 8.4 or newer code running on a Mobility Conductor/Mobility Controller, Aruba Instant, and/or Central are supported. A comprehensive validated reference design is available for controller-based deployments.

ClearPass 6.7.2 or newer is required. ClearPass runs on hardware appliances with pre-installed software or as a Virtual Machine under VMware (ESXi 5.5, 6.0, 6.5 or higher), Microsoft Hyper-V Server (2012 R2 or 2016 R2), Hyper-V on Microsoft Windows Server (2012 R2 or 2016 R2), and KVM (CentOS 7.5).

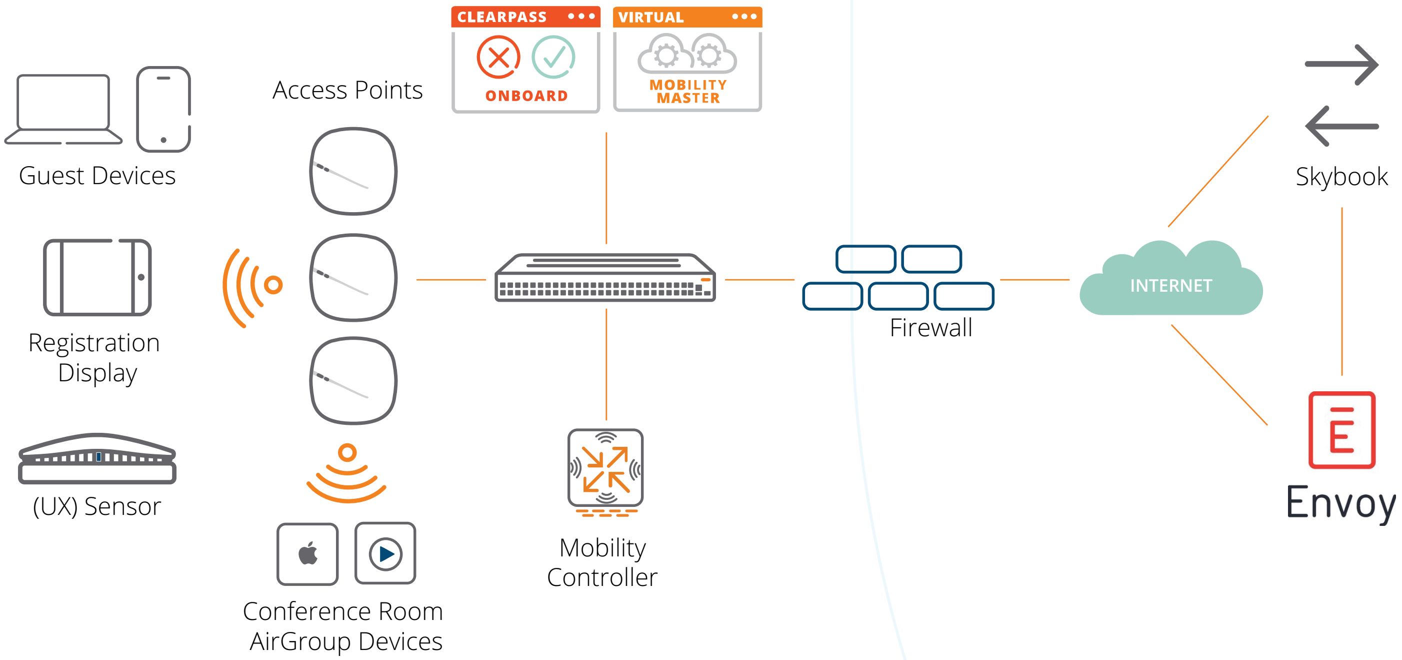


Figure 22: Automated Service Personnel And Contractor Access Solution

Envoy

Envoy Visitors is a guest management platform that streamlines sign-in. When service personnel and contractors arrive on site, Envoy makes it easy for them to register, presents relevant non-disclosure and health/safety forms for completion, and notifies hosts of the guest's arrival via e-mail or SMS. Simultaneously, ClearPass dynamically provisions temporary Wi-Fi access credentials for their service tools and sends an individualized security code for Wi-Fi access via e-mail or SMS.

Envoy leverages ClearPass' microservice extensions running in a container independent of the ClearPass operating system. ClearPass extensions are used to interact with external systems, including advanced two-factor authentication services and IIoT firewalls.

The joint Aruba/Envoy solution automates the entire onboarding process, minimizing the need for manual assistance, and ensuring that security standards are enforced throughout the visit. Never again will service personnel and contractors need to circumvent IT security just to obtain reliable connectivity.

SECURELY SHARING PLANT WIRELESS NETWORKS WITHOUT LOSING CONTROL

Plant wireless network access is typically tightly controlled out of concern that critical services and devices, such as Profinet IO communications and automated guided vehicle control, could be negatively impacted by wireless users. However, growing demands for mobile device wireless access to enhance worker efficiency, productivity and safety increase pressure to open up plant networks and avoid the cost and RF interference of parallel networks. Both IT and Operations are struggling to find a mutually acceptable solution.

Several years ago the US Department of Defense (DOD) encountered a very similar situation. There was pressure to use one common network to support secret (SIPR) and non-secret (NIPR) traffic. These distinct traffic flows were managed by different groups, each of which needed total control over who access to the traffic they manages. Security was paramount, and there could be no sharing of data across groups or unauthorized network access within a group.

Aruba solved the issue by developing MultiZone, a networking solution that allows each of up to five groups to define authentication, access, operation, and management rules applicable to, and enforced within, their unique "Zone." One Aruba controller is assigned to the Primary Zone, managed by IT, which handles access points and RF settings, and directs access points to authenticate to Data Zone controllers. Separate Data Zone controllers handle authentication, access, operation, and management rules for the SIPR and NIPR groups. MultiZone supports up to five Data Zones

The multi-tenancy design of MultiZone is ideal for IIoT applications. Separate Data Zones can be allocated to the groups managing, say, real-time controls, machine-as-a-service, corporate services, contractors, and auditors, Each

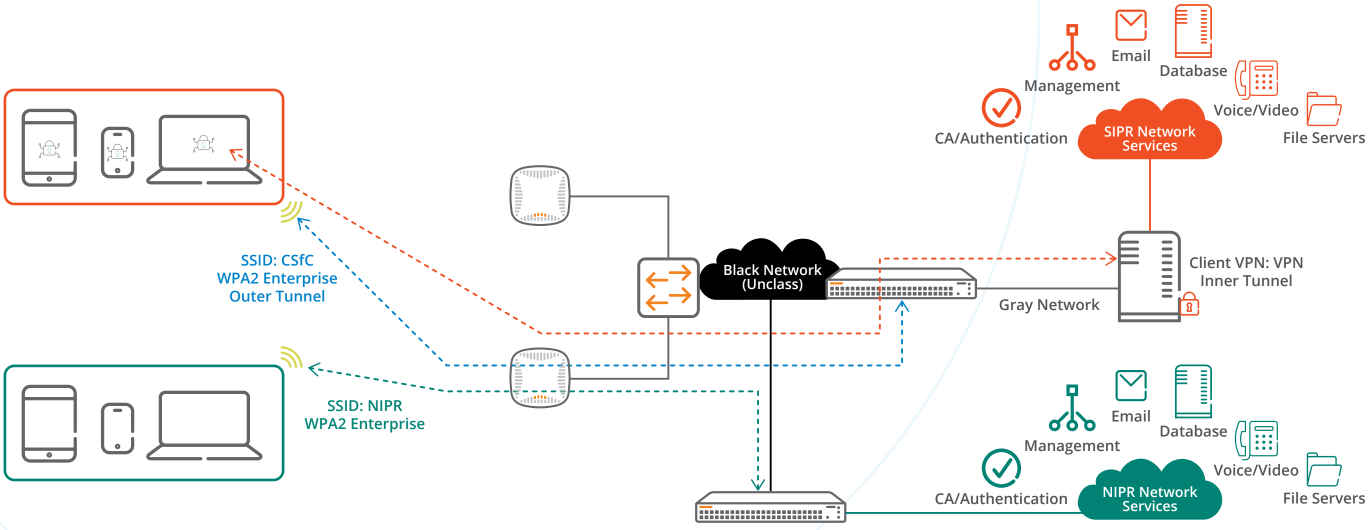


Figure 23: Aruba Multizone Solution

group separately controls who and what is allowed access into their Data Zone, including Internet and VPN connectivity to remote services. Defense-related plants can use MultiZone in conjunction Aruba's commercial solutions for classified applications, including elliptic curve encryption and other FIPS 140-2 and Common Criteria related services.

In a MultiZone system IT manages the overall infrastructure through the Primary Zone but cannot access Data Zone traffic. Uniform visibility and security can be achieved while simultaneously respecting the access control rights of Data Zone owners.

MIGRATING FROM BREAK/FIX TO PREDICTIVE MAINTENANCE

Up-time and defect-free processes are prime objectives of operations groups, whose charge is to keep plant and equipment running non-stop. Addressing maintenance proactively to minimize downtime, and maximize the utilization and performance of assets, can reduce maintenance costs by up to 40%.

Predictive maintenance is an essential tool in this quest. By instrumenting equipment, monitoring for degradation, and identifying potential problems in advance of failure, predictive maintenance can provide visibility into the performance of assets, ensure high availability, and maximize the returns on often substantial capital investments.

The challenge is that identifying the source of possible failures is not always a simple task. Sensor networks and gateways have traditionally been expensive to deploy, and can have vulnerable attack surfaces that keep CISOs awake at night. COOs, in turn, fret whether innovative AI predictive maintenance solutions require resources beyond the means of operations teams.

Spending on predictive maintenance is expected to hit $12.9 billion in the next two years. Juggling the high cost asset performance management solutions, and its security risks, against the benefits of lower downtime and fewer disruptions is a challenging calculus.

An optimal solution is to leverage secure, robust IT infrastructure that is already deployed in a plant to capture machine status from IIoT sensors. A dual-use IT/IIoT network is more economical to deploy and can eliminate gateways and the security threat they pose.

ABB

ABB is a technology leader in industrial digital transformation of electrification, automation, motion, and robotics. Thru its ABB Ability™ digital platform, ABB drives improvements in productivity, reliability, and efficiency.

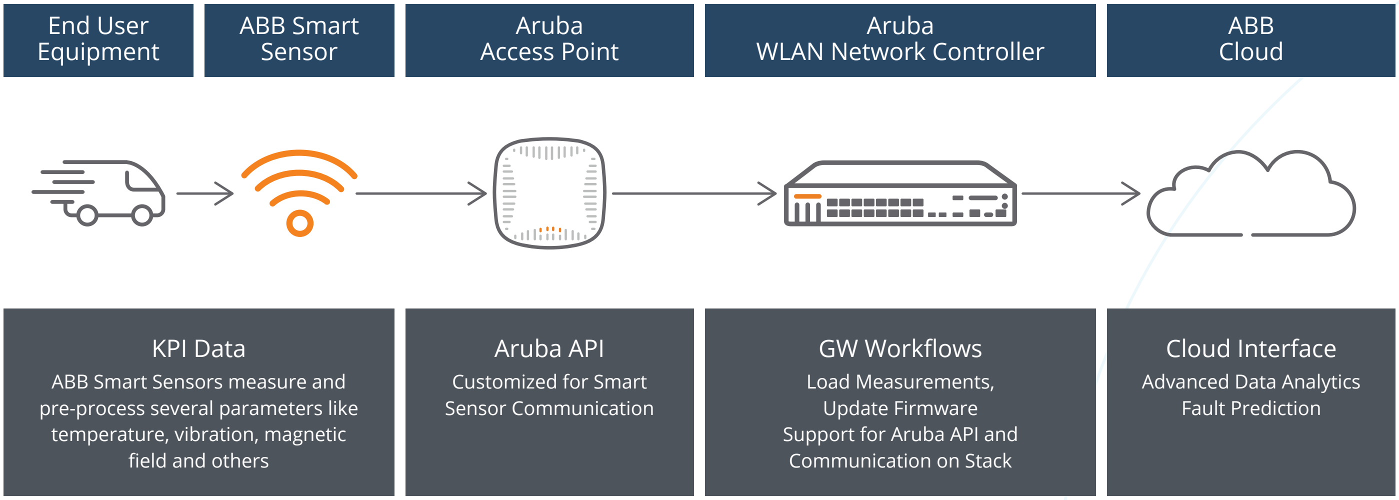
The ABB Ability Smart Sensor is a battery-powered, multi-sensor device that monitors rotating machinery like motor drives, valves, and pumps for abnormal behavior indicative of pending failure. Status is communicated over a secure Bluetooth link, and analyzed by ABB's advanced algorithms. Operations engineers are automatically notified of out-of-normal conditions well before failure, allowing repairs to be performed before processes are impacted.

The Smart Sensor helps customers migrate from break/fix to predictive maintenance, a digital transformation that reduces downtime, enhances asset utilization, and optimizes scheduling of field engineers. All of which ultimately boost efficiency and profitability.

ABB and Aruba have partnered to enable Aruba Wi-Fi 5 and Wi-Fi 6 multi-radio access points to securely collect and forward ABB Ability™ Smart Sensor data to the ABB Ability™ Condition Monitoring application. Using Aruba zero trust infrastructure as a data collection platform provides uniform security and visibility across both IT and IIoT domains. It eliminates the costs and security risks and costs associated with large fleets of gateways. Since gateways filter raw data streams that can be rich in visibility data, removing them has the added benefit of improving visibility all the way down to individual sensors.

The Aruba-ABB solution works with brownfield and greenfield deployments of any Aruba 802.11ac and 802.11ax access points equipped with a BLE radio and AOS 8.6 or later. This means that predictive maintenance monitoring can be retrofitted to existing Aruba WLAN deployments without adding additional IT gear or gateways.

The joint ABB-Aruba solution delivers the operational visibility and robustness demanded by COOs, without the expense of a dedicated wired sensor system. Wireless communication allows Ability Smart Sensor to be deployed anywhere without expensive conduit or enclosures. These savings extend throughout the life cycle of a plants since adds, moves, and changes are easy and inexpensive.



End User Equipment

ABB Smart Sensor

Aruba Access Point

Aruba WLAN Network Controller

ABB Cloud

KPI Data
ABB Smart Sensors measure and pre-process several parameters like temperature, vibration, magnetic field and others

Aruba API
Customized for Smart Sensor Communication

GW Workflows
Load Measurements, Update Firmware
Support for Aruba API and Communication on Stack

Cloud Interface
Advanced Data Analytics
Fault Prediction

Figure 24: Aruba and ABB Integration Overview

The intersection between OT and IT has historically been a point of friction, but not so with the ABB-Aruba joint solution. Both companies are respected leaders in IIoT and IT, respectively, and the joint integration allows data to flow reliably and securely between systems. Visibility and robust design address the uptime concerns of COOs, while I/O-to-application security and policy management check the box for CISOs. And the cost savings will cheer CFOs.

INCREASING INVENTORY TURNS BY REDUCING PICKING TIME

IIoT is the digital raceway that transports data and context to mining engines that alchemize them into insights to better manage inventory, optimize operations, and improve user experiences. Information sources used in this calculus include discrete and process automation systems, ERP, and Kanban scheduling, among others. The veracity of these sources impacts the value of the insights, so validating the quality and provenance of information fed into the engines is paramount.

Locating, harvesting, and conveying relevant, trustworthy IIoT data and context is easier said than done. Data must be captured with fidelity over networks that reach wherever IIoT devices and supporting personnel are working or roaming. Data input is often hit or miss, and voice communications with workers unreliable, especially when roaming. Locating inventory, work in process, and people can be difficult.

Optimizing secure Wi-Fi 6 infrastructure to deliver toll-quality voice and uninterrupted data to mobile IIoT devices operating in plant settings – many with high levels of multi-path and electrical noise - is a challenge. Yet Wi-Fi is the only way to economically deliver voice and data in these environments, most of which don't have good cellular macrocell coverage. Private 5G will be an order of magnitude more expensive to deploy and manage than Wi-Fi 6 because of the density of millimeter wave radios required to deliver high speed communications. The high cost of distributed antenna systems rules them out as well. As with other use cases, a dual-use IT/IIoT network is the best choice provided that quality of service and fast roaming can be reliably delivered to roaming IIoT devices

ZEBRA

Zebra Technologies is the market leader in automatic information and data capture (AIDC), ruggedized mobile computer, and mobile industrial printing systems. Zebra is heralded for its ability to capture data quickly and reliably on the first pass, and brings great depth of vertical expertise in the manufacturing and logistics markets.

Zebra Technologies and Aruba have partnered to address the roaming voice picking and data capture requirements of industrial customers. This has been accomplished through a combination of technology integration, automated application detection using deep packet inspection, and validated implementation reference designs.

Aruba's deep packet inspection engine, supported by voice heuristics and intelligent Quality of Service tagging, brings toll-quality audio to Zebra's Workforce Connect application and the voice-enabled Zebra devices that use it. Combined with Aruba's AI-based network optimization, mobile users in manufacturing cells and on forklifts obtain more legible voice, fewer drop-offs, and higher speed connections over larger areas.

Aruba's ClearPass Access Manager can automatically profile, identify, on-board, and assign the appropriate security policies to mobile and fixed Zebra devices. Employees can be productive faster without compromising network security.,

Security experts recommend that IIoT devices be dynamically segmented to protect against breaches, while IT departments can avoid VLAN explosion as the number of fixed barcode scanners, wired printers, and other wired IIoT devices continues to rise. ClearPass works with Aruba switches to dynamically segment Zebra devices, providing a common enforcement option for both wired and wireless Zebra devices. As a simpler alternative to VLANs, this technology separates L3 network traffic and sends targeted Zebra traffic to a specific service, e.g., a firewall zone. This allows wired Zebra printers and computers to connect to any available switch port, making the network simpler to set-up and prevents security breaches related to cabling during model changeovers and adds/moves/changes.

Zebra application performance can be validated using Aruba's User Experience Insight (UXI) solution. UXI uses synthetic transactions and AI to identify application bottlenecks by monitoring critical cloud, on-premise, and hybrid applications. UXI works with both wired and wireless Zebra IIoT devices, and a cellular option allows rapid deployment in trouble spots.

Working together, Aruba and Zebra have made mobile data input, mobile voice and picking communications, and mobile printing reliable and secure in harsh industrial, manufacturing, and logistics applications. The Aruba infrastructure on which the joint solution is based can do double duty for other IIoT applications - like telemetry monitoring and asset tracking – ensuring that customers get the greatest value from their capital investment.

PLANT MONITORING AND DIGITAL TWIN ENABLEMENT

Situational awareness is essential for efficient plant maintenance. IIoT devices are the eyes and ears of plant status, and are given voice by the secure connectivity infrastructure through which they talk with monitoring applications. The better instrumented the plant facilities, the more comprehensive the insights that can be made across time and space, including projections of future issues

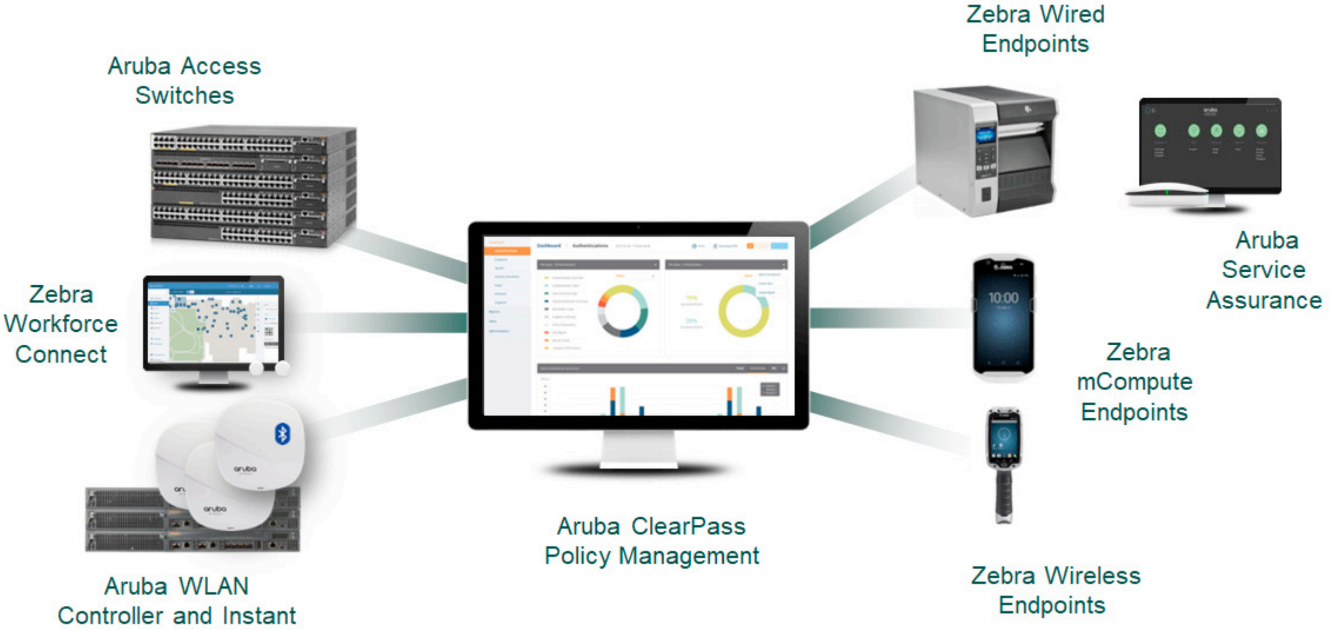


Figure 25: Aruba and Zebra Integration Overview

that impact up-time. Plant monitoring encompasses a wide variety of IIoT telemetry including power quality, power consumption, leak detection, air and fluid quality, enthalpy, refrigeration, lighting, temperature, and humidity.

Digital twin modeling combines IIoT monitoring data with artificial intelligence, historical data, domain knowledge expertise, and graph modeling to establish and analyze relationships between and among plant devices and systems. By creating real-time simulation models in the digital world that change and learn in lock-step with the plant systems, digital twins can identify sub-optimized processes, recommend operational enhancements, assess complex systems that would be too difficult for a human to track, and monitor the remaining useful life of machines for contingency mitigation.

The benefits of plant monitoring and digital twin modeling hinge on the availability of timely access to relevant IIoT data. Securely and economically interfacing IIoT monitoring devices across a plant can be challenging. The breadth of telemetry to be gathered, interfacing with legacy IIoT devices that use non-interoperable protocols, securing the data path, and importantly the cost of deployment – initially and during plant changeovers – can be daunting and expensive.

Wired monitoring systems require dedicated cabling, which is expensive to deploy and labor intensive to maintain across adds, moves, and changes. Wireless IIoT devices are more economical to deploy but the cost of battery maintenance can be prohibitive.

As plants deploy next-generation Wi-Fi 6 wireless networks for staff mobility, asset tracking, and production operations, that same secure IT infrastructure can be leveraged for plant monitoring and digital twin applications. Advanced access points that have built-in IIoT radios, and support for external USB adapters, can serve as IIoT data gathering platforms.

The remaining hurdle is to eliminate batteries wherever possible. Energy harvesting technology derives, captures, and stores power from external sources, e.g., kinetic and visible light. Miniaturized energy harvesting power sources, embedded inside IIoT sensors, can solve this problem and allow IIoT plant monitoring sensors to be placed wherever needed with no wires or maintenance.

enocean® enocean®alliance

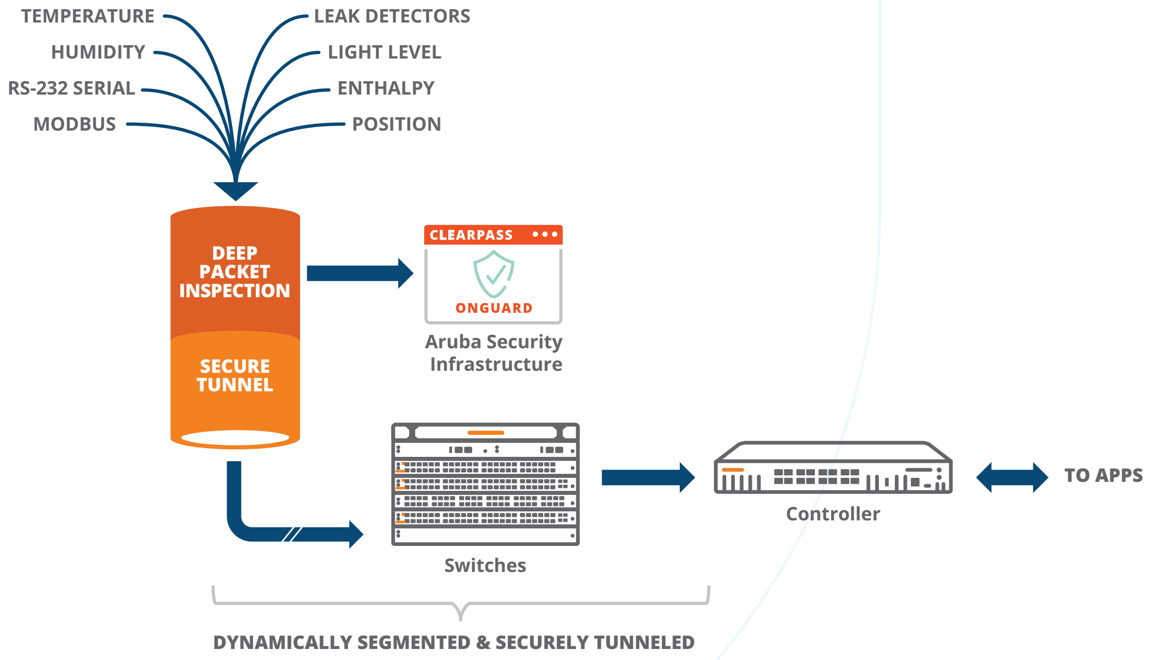


Figure 26: Aruba Access Points Are IoT Platforms For EnOcean Device Data

EnOcean, a venture-funded spin-off of Siemens AG, is the creator of the ISO/IEC 14543-3-10/11 energy harvesting 800/900MHz wireless standard. More than 400 EnOcean Alliance vendors build facility monitoring and control systems using this standard. Sensors require no batteries for power, and no wires to communicate, making them economical to deploy and maintenance-free.

RS-232, RS-485, ModBus, LONWORKS, BACnet, KNX, and DALI control systems and devices are supported via locally powered, EnOcean-enabled gateways. These gateways extend the reach of monitoring and digital twin applications into legacy infrastructure, yielding deeper visibility and insights without incurring the cost of ripping-and-replacing installed devices.

EnOcean and Aruba have partnered to allow Aruba Wi-Fi 5 and Wi-Fi 6 access points equipped with EnOcean 800/900MHz USB adapters, and using Aruba OS version 8.7 or later, to communicate bi-directionally with ISO/IEC 14543-3-10/11 compatible devices. With literally thousands of such devices and gateways from which to choose, virtually any facility monitoring application can be accommodated. The joint solution can be retrofitted to existing Aruba deployments, extending the value of sunk capital investments.

Aruba access points stream EnOcean telemetry data in real time via protobuf to monitoring applications over a secure Web socket connection. Applications can be on-premise, or in a public or private cloud. The EnOcean Alliance includes software application vendors as well as device vendors, and ensures interoperability between both.

The wide range of available ISO/IEC 14543-3-10/11 compatible devices, combined with the security and extensibility of Aruba infrastructure, delivers an extraordinarily flexible and economical way to monitor plants. The solution can even be extended into carpeted spaces should remote site monitoring and control be needed.

Azure IoT Hub

Customers that want digital twin modeling and telemetry monitoring can simply point Aruba’s Web socket connection to Microsoft’s Azure IoT Hub – on-premise or in the Azure cloud. Azure IoT Hub will extract the telemetry data from the protobuf stream, and make it available to the Azure Digital Twins IoT service.

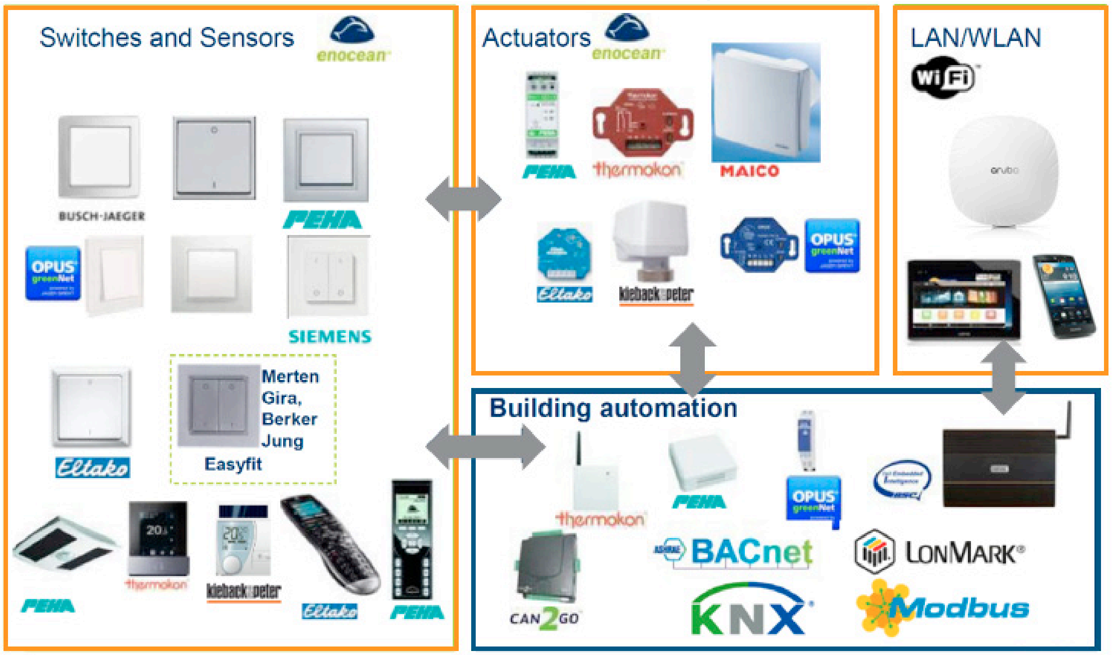


Figure 27: EnOcean Ecosystem

The Azure Digital Twins service creates spatial intelligence graphs to model relationships and interactions. Thru the service users can build reusable, highly scalable, spatially-aware digital models based on their physical plants, and use them to identify optimize processes and remedy issues.

SEAMLESS 5G TO WI-FI ROAMING WITHOUT DISTRIBUTED ANTENNA SYSTEMS

If you can't connect with people and machines inside a plant, then you can't extract or share information. The prevalence of low-emission glass, energy-efficient construction materials, and evolving building codes have made indoor wireless coverage from outdoor cellular networks a recurring challenge. This results in inconsistent experiences for mobile users and devices as they roam in and out of sites. These problems are compounded with high-speed 5G, which operates at higher frequencies that do not penetrate indoors as far as 3G or 4G cellular.

For decades, indoor cellular issues have been addressed by deploying distributed antenna systems (DAS). This expensive infrastructure operates as extended antennas for one or more cellular carriers. More recently, indoor small cell (also called "femtocell") networks have been deployed by individual mobile network operators (MNOs). Unlike DAS, a separate layer of equipment is required for each MNO. Both DAS and small cells are complex, very costly, and are rarely cost effective for facilities with less than 200,000 ft2 (20,000 m2).

Over 150 MNOs in nearly 50 countries have embraced Wi-Fi Calling. This service leverages the existing Wi-Fi network, which when properly designed provides pervasive coverage throughout a sites. 5G includes support for Wi-Fi 6 integration as a radio access network (RAN), so site owners do not need to choose between 5G and Wi-Fi 6: Wi-Fi Calling and other services can be performed over both. For this reason, wireless LANs are the premier and most economical onramps for indoor cellular devices.

Aruba Air Pass is the industry's first seamless cellular roaming solution designed to unify enterprise and mobile network experiences. The service enables 5G initiatives - including service engineer, contractor, and IIoT device on-boarding and roaming - to be accomplished with enterprise-class security over Wi-Fi 6 without the high cost of a DAS or issues with inconsistent cellular connectivity.

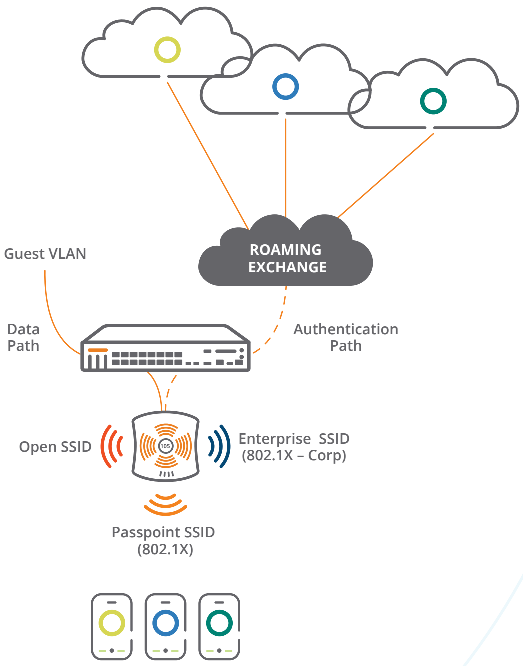


Figure 28: Aruba AirPass System Architecture

Air Pass uses pre-negotiated agreements with MNOs that support the Wi-Fi CERTIFIED Passpoint standard to automatically gain network access using cellular SIM credentials for authentication. No captive portals, user names, or passwords are required. Aruba ClearPass provide high security network access control so that public and private resources remain secure and separate. Mobile subscribers, and Passpoint-capable IIoT devices, can then roam between the cellular and Wi-Fi networks in compliance with IT security standards.

Air Pass is managed by Aruba Central, a massively scalable cloud-based network operations, assurance, and security platform. Aruba Central simplifies the deployment, management, and orchestration of wireless, wired, and SD-WAN environments. This includes delivering 5G and Wi-Fi 6 to the network and customer edge, complete with built-in and third-party services.

Mobile users and IIoT devices are increasingly accessing cloud services and other bandwidth-intensive applications like digital twin management and augmented/virtual reality. Air Pass leverages Air Slice for SLA-grade application assurance by dynamically allocating radio resources such as time, frequency, and spatial streams to specified users, devices, and applications.

Reliably connecting people and IIoT devices inside a plant is essential for context-aware engagement, safety, and security. Air Pass marks an end to a dependence on expensive DAS systems. It also overcomes connectivity, security, and convenience issues associated with indoor cellular coverage gaps, insecure open wireless networks, manually hunting for Wi-Fi networks, and the inconvenience of navigating captive portals. Secure connectivity is assured regardless of where people and IIoT devices work or roam.

REDUCING MEAN TIME TO REPAIR WITH REAL-TIME LOCATION SERVICES

Many industrial and manufacturing enterprises today retain siloed repositories of IIoT device data. Even though these data are rich with insights if properly mined, the justification for isolation is that these data are needed for process monitoring and which, if exposed, could be attacked or impacted by IT actions such as system updates, reboots, or maintenance.

The downside of confining data is that it deprives the Meta Zone of valuable insights that could be gleaned from larger data sets, i.e., combining IIoT data with supply chain, inventory management, predictive maintenance, and other sources. Sharing contextual data – location, users, devices, and applications that originate from IoT devices and the personnel who use and manage them – can significantly enhance business insights.

Application	Role of Location-Based Services
Human productivity optimization	Guide occupants to meetings and places of interest Improve time and motion paths Validate contractor activity
Predictive maintenance	Wayfinding to guide service personnel
Inventory optimization	Quickly find raw materials and work in progress
Health and safety	Guide occupants to muster points Social distance monitoring

Table 1: location-based services by application

With proper data life cycle governance these sources can be safely and securely shared, and that's when the real benefits of IIoT can be reaped. Limiting access to these data would deny us valuable insights about trends in time and motion, maintenance services, and energy consumption.

From among the many types of available contextual data, location data are particularly insightful. Location data can guide us unescorted through facilities, improving our experience without encumbering others to assist us. They can help us keep track of people wherever they work or roam. And they can track capital assets so they can be quickly located and repaired.

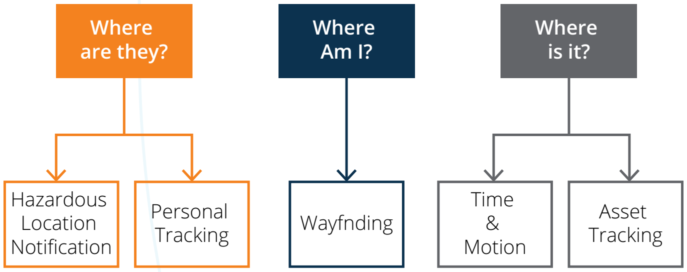


Figure 29: Aruba Location Services And Target Applications

Plants, logistics yards, and campuses are often very large and difficult to navigate. If someone is delayed or lost traversing the facility the consequences can range in severity from lost revenue or time to loss of life. Engineers, contractors, and public safety officers can all benefit when a self-navigation solution – "wayfinding" – delivers them to their destinations quickly and unassisted.

Additionally, the contextual data generated along the way can be mined for business-relevant information. Examples include notification of hazardous areas that require safety gear, flagging occupied areas in the event of a muster event, and tracking contractor time spent on site versus what was billed.

Aruba's Meridian platform is a mobile application platform that provides self-guided wayfinding, geofencing, and push messaging services for a broad range of IIoT applications. The system consists of the following components:

- Location Beacons - standalone or integrated into Aruba access points;
- Meridian Application (App) for tablets and phones; and
- Meridian cloud service.

Beacons use Bluetooth Low Energy (BLE) to broadcast an anchor location that is picked up by the Meridian App and shared with the cloud service to assist with locationing. Beacons are built into Aruba Wi-Fi 5 and Wi-Fi 6 access points, including Class 1 Division 2/ATEX Zone 2 models qualified for HazLoc environments. Standalone battery- and USB-powered beacons are also available.

Fig 30: AP-530 Wi-Fi 6 Access Point With 802.11ax, BLE, And 802.15.4 Radios

Fig 31: AP-375EX Access Point For Hazardous Areas Like Propane Storage And Fuel Refilling

Radio-transparent enclosures are available from Bartec and Stahl for using Meridian in Class 1 Division 1/ATEX Zone 1 hazardous environments.

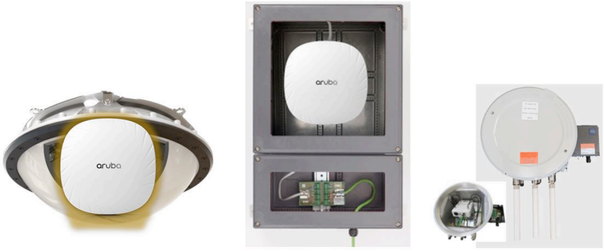


Fig 32: Bartec (left) and Stahl (center and right) Radio-Transparent Enclosures

Typical IIoT wayfinding applications include guiding service personnel to machines in need to repair, guiding employees to muster points, and allowing visitors self-service access to large facilities. Self-guided wayfinding directs users to a point of interest, and offers a simple way to pinpoint their current location, search for points of interest, and access turn-by-turn directions, inside or outside. A glowing dot shows the user's location on a map, and tracks their progress along the route. Users can retrieve turn-by-turn directions from their current location without entering a starting point, an important time saver in emergencies that require mustering to safe areas.

Wayfinding also enables contractors to navigate sites without assistance, conserving operational and administrative resources from acting as guides. Upon nearing a target destination, a logical geofence can be triggered and push a contextually-relevant message or notify a relevant application, i.e., retrieve machine service records. The power of Meridian comes from the context it applies to user engagement, the precision of its geofencing, and the flexibility with which it can interact with other systems.

Reducing mean time to repair (MTTR) is a prime example of the value Meridian brings to IIoT applications. Imagine that the bearing on a motor drive starts to wear unevenly, and resonates in out-of-normal frequencies. The multi-axis accelerometer in an ABB Ability Smart Sensor affixed to the motor drive can pick up the anomalous signals and relay an alert via an Aruba Ex access point to the ABB Ability monitoring application.

An engineer can be dispatched preemptively to repair the bearing before it fails. Instead of leaving it to the engineer to navigate the plant on his or her own, however, the Meridian

App triggers a geofence when the engineer enters the plant – notifying the Finance Department when work commences - and then guides the engineer using turn-by-turn navigation to the failing motor drive.

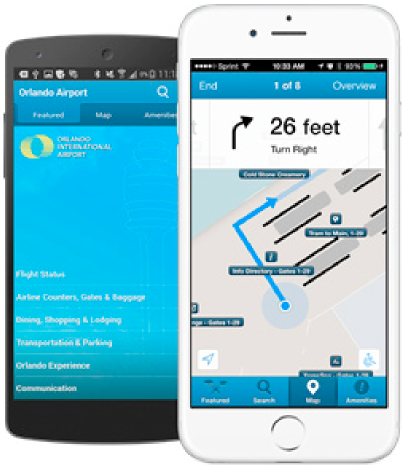


Fig 33: Meridian Turn-By-Turn Wayfinding

As the engineer approaches the machine another geofence is triggered, recalling the service record for that drive and again notifying Finance that repair work has commenced. Once the repair has been effected the engineer is guided to back to his/her truck and a third geofence notifies Finance that the work has been completed.

In large sites, wayfinding can reduce the mean time to repair by tens of minutes per incident, making engineers more efficient and reducing the risk of equipment failing while awaiting the arrival of service personnel. Equally important, the same location services can reconcile service charges and labor allocations, a complex tasks at sites with many contractors and/or service engineers.

PHYSICAL DISTANCE MONITORING AND CONTACT TRACING

Workplace safety extends beyond physical and environmental hazards. Today, physical distance monitoring and contact tracing are essential for back-to-work and stay-healthy-at-work initiatives. Whether mandated by local regulations or company policies, maintaining safe distances from other workers and infection control tracing are top of mind for operations teams. While there is no single physical distance monitoring and contact tracing application that will work for all enterprises, real-time location services and identity stores have an essential role to play in every workplace infection control solution.

Aruba has teamed with multiple technology partners to deliver a broad range of health monitoring solutions. The solutions fall into four categories:

- Physical distancing enforced by wearable tags or wristbands for situations in which a personally-owned device is not suitable;
- Application-based physical distancing solutions that run on personally-owned or company issued devices;
- Presence detection systems that pick-up Wi-Fi signals from personally-owned or company issued devices, but do not require an application; and
- Thermographic and facial recognition systems that monitor the temperature of individuals' heads, and can process dozens of people simultaneously.

AiRISTA FLOW

The AiRISTA Flow Social Distancing and Contact Tracing Solution uses a wireless tag worn by employees to help enforce guidelines for social distancing and automate contact tracing. The tags communicate with each other autonomously, without supervisory control, and trigger when they are closer than 2 meters apart. The user is signaled haptically and the devices forward the incident via Aruba access points to the AiRISTA Flow cloud-based software system.

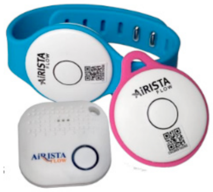
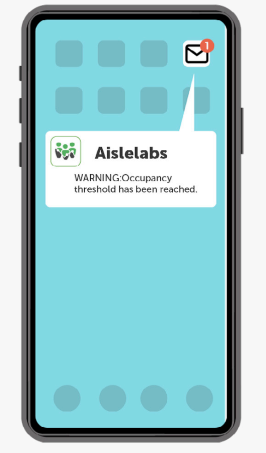


Fig 34: AiRISTA Flow BLE Proximity Tags With Haptic Feedback

Aislelabs

Aislelabs provides a real-time footfall and occupancy monitoring to promote social distancing in large sites without the need to download an app or obtain opt-in approval. The solution uses personally-owned, Wi-Fi enabled smart phones or tablets, together with existing Aruba Wi-Fi infrastructure, to anonymously log the movement of people and area occupancy in an auditable database. Violation alerting is triggered based on programmable thresholds.



Aislelabs

WARNING:Occupancy threshold has been reached.

Fig 35: AisleLabs COVID-19 Social Distancing Solution

CohuHD's Thermographic System is an intelligent thermal imaging, radiometric detection, optical imaging, and facial recognition solution. The system automatically and simultaneously identifies the faces of more than thirty people within one second, reads forehead temperatures, and alerts when a reading is above normal. All measurements are recorded together with location for trend analysis. If a high temperature reading is detected the system can respond automatically using voice synthesis, triggered relay outputs, and access control interfaces. The camera uses a US Department of Commerce compliant SoC.

The CxApp Touchless Application leverages Meridian BLE Beacons strategically placed around the workplace, and the Meridian cloud service for location data. The mobile app sends notifications based on crowded times, vacant times, and total employees per square foot, all based on real-time occupancy within the environment.

Kiana Analytics' Rapid Containment Application uses real-time location data, collected by existing Aruba access points from Wi-Fi enabled mobile phones and tablets, to identify the presence and movement of people. The application analyzes social transmission vectors, including locations and contact trees, to help mitigate spreading of communicable diseases.

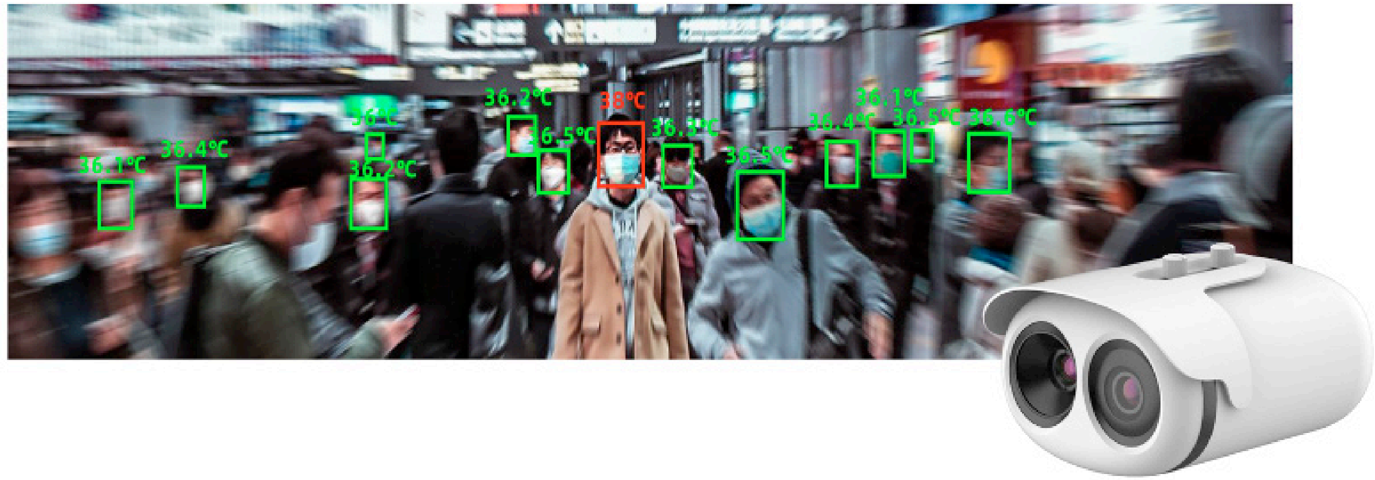


Figure 36: CohuHD Non-Contact Thermographic And Facial Recognition Camera

Patrocinium™

The Patrocinium Safe Return Application leverages Meridian BLE Beacons, the Meridian cloud service for location data, and Patrocinium's ArcInsight analytics package. The application runs on personally-owned or corporate-issued smartphones and tablets, and automatically detects when other personnel are too close. The location and identity of the individuals are sent to the analytics application via Aruba Wi-Fi for contact tracing.

skyfii iO

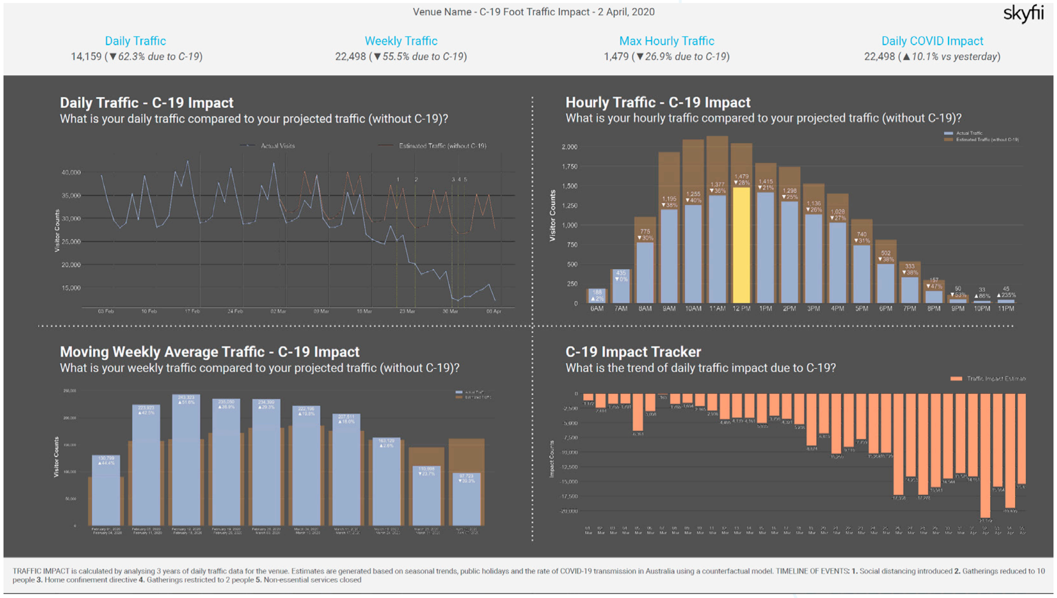
OccupancyNow is an automated occupancy and social distancing management toolkit from SkyFii. The cloud-based solution uses real-time location data from existing Aruba infrastructure to maintain safe occupancy and social distancing guidelines, automatically alert staff when occupancy counts reach a set threshold, and facilitate contact tracing via with Skyfii's analytics and communication tools. OccupancyNow also helps track whether routine cleaning and sanitization procedures are being performed.

REAL-TIME PERSONNEL AND ASSET SAFETY MONITORING

Many IIoT applications involve work in locations that are hazardous by virtual of the environment, type of equipment that's used, or both. For example, in 1874 Mr. Cadwallader Washburn, a Wisconsin businessman from La Crosse, Wisconsin built the seven story A Mill flour mill in Washburn, Minnesota. The largest industrial building in the city, the A Mill employed 200 workers and was powered by Mississippi River water diverted through a canal running through the lower floor. At 7PM on 2 May 1878, an hour after the start of the night shift, the mill burst into a ball of flames accompanied by a series of explosions. An eyewitness described seeing brilliant flashes and blown out windows, starting with the basement floor and progressing upwards to the roof. The source of the disaster: flour dust.

Dust explosions caused by flour, sugar, and dried milk have a long history. The first recorded explosion was 14 December 1785 at Giacomelli's Bakery Warehouse in Turin, Italy. Flour dust generated during normal handling operations allegedly contacted a worker's lamp. It's not unusual to drive by farms of flour silos and see one or more missing or twisted silos, testaments to the ongoing challenge presented by explosive dust.

Other industries have to contend with their own explosion hazards: methane in mining; acetylene in shipyards; metal filings in machine works; hydrocarbon vapors in refineries; and gunpowder in ammunition depots.



Venue Name - C-19 Foot Traffic Impact - 2 April, 2020

skyfii

Daily Traffic	Weekly Traffic	Max Hourly Traffic	Daily COVID Impact
14,159 (▼62.3% due to C-19)	22,498 (▼55.5% due to C-19)	1,479 (▼26.9% due to C-19)	22,498 (▲10.1% vs yesterday)

Daily Traffic - C-19 Impact
What is your daily traffic compared to your projected traffic (without C-19)?

Hourly Traffic - C-19 Impact
What is your hourly traffic compared to your projected traffic (without C-19)?

Moving Weekly Average Traffic - C-19 Impact
What is your weekly traffic compared to your projected traffic (without C-19)?

C-19 Impact Tracker
What is the trend of daily traffic impact due to C-19?

TRAFFIC IMPACT is calculated by analysing 3 years of daily traffic data for the venue. Estimates are generated based on seasonal trends, public holidays and the rate of COVID-19 transmission in Australia using a counterfactual model. TIMELINE OF EVENTS: **1.** Social distancing introduced **2.** Gatherings reduced to 10 people **3.** Home confinement directive **4.** Gatherings restricted to 2 people **5.** Non-essential services closed

Figure 37: SkyFii OccupancyNow Dashboard

A potentially explosive atmosphere exists when air gas, vapor, mist, flyings, or dust - alone or in combination- are present under circumstances in which it or they can ignite under specified operating conditions. Places with potentially explosive atmospheres are called "hazardous" or "classified" areas or locations. Multiple local and international regulations are in place to mitigate the risk posted by operating networks and IIoT devices in potentially explosive atmospheres. Increasingly these regulations are becoming harmonized under a framework developed by the International Electrotechnical Commission (IEC) and European and US standards.

Environment aside, many industries use machinery that presents its own hazards to humans. Subsurface and surface mining equipment, drilling rigs, gantry cranes, and high pressure compressors also pose hazards to those who work around them. Accordingly, location-based safety systems are mandated in these industries. These systems have to be designed to operate safely in the target environments, which could be explosive, large in scale, and occupied by people working in close proximity to dangerous machinery.

MOBILARIS

Mobilaris Group is a leading location-based intelligence and decision support solution company focused on mining and industrial safety solutions. Mobilaris Mining Intelligence™ helps mining operations digitalize subsurface operations with double digit productivity increases. The mining suite delivers real-time 3D situational awareness by tracking the location of people and assets, and with automated ventilation, geofencing, and vehicular navigation systems. The Mobilaris Tunneling Intelligence™ extends the benefits to tunneling projects with real-time positioning, sensor data, dispatch, analytics, and 3D tunnel visualization tools.

The Mobilaris Industrial Intelligence™ suite tracks the location of workers, vehicles, and hazardous areas, and integrates these data with video surveillance, access control, business, and production systems. The objective is to help avoid dangerous situations, but if one does flare up to keep personnel and assets out of harm's way.

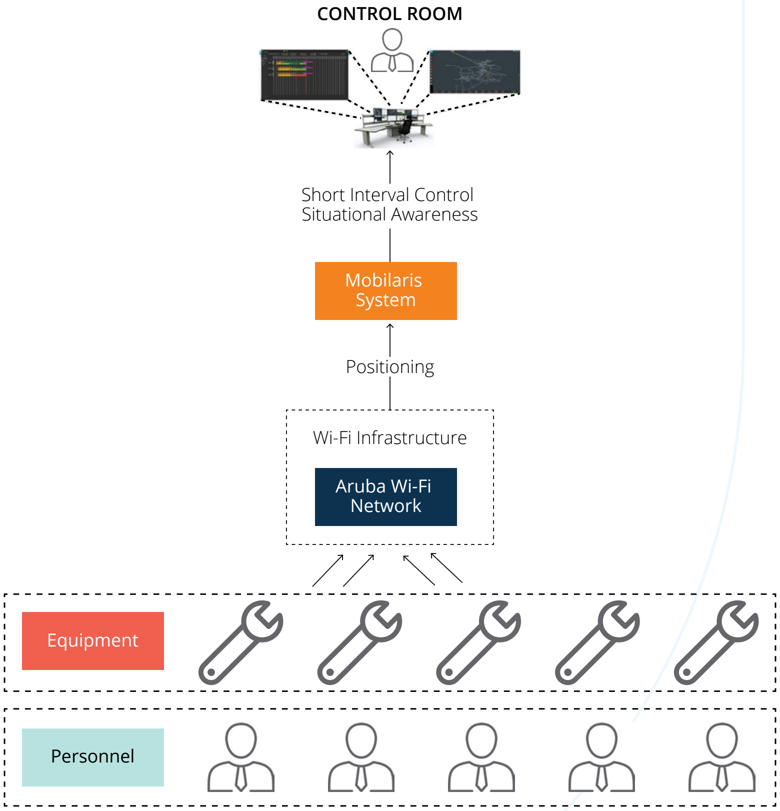


Figure 38: Mobilaris Worker & Asset Tracking System For Surface And Sub-Surface Industrial Applications

Mobilaris and Aruba have partnered to enhance worker safety and asset tracking in industrial sites and mines. Real-time location data, gathered by Aruba access points from tags on workers and equipment, are relayed over a secure tunnel from Aruba controllers to the Mobilaris system, and then on to workforce safety situation awareness applications.

Access to real-time information about personnel location enables those in evacuation zones to be instantly notified of the situation, and told how and where to muster. Status information is visualized on a 3D site map supplemented by safety status lists, allowing rescue personnel to focus on the most critical locations and tasks. Mobilaris has demonstrated that real-time situational awareness can reduce evacuation time by fifty percent.

Worksite safety is also monitored using real-time location data. If a worker moves too close to a dangerous machine, overhead crane, vehicle or hazardous area, they are instantly notified via vibrating tag, flashing light, or blinking safety vest so an accident can be averted. The more workers and contractors employed at the site, the greater the need for automated notifications.

The Mobilaris system provides real-time safety information on machines, areas, vehicles, equipment, muster locations, rescue showers, and other critical data. By making these data available to everyone at the site, both employees and temporary visitors can be protected. Since the solution uses existing Aruba infrastructure, it is economical to deploy and can do double-duty for other IIoT, voice, video, and data applications.

CONTEXT-AWARE, REAL-TIME INTEGRATED EMERGENCY RESPONSE AND NOTIFICATION

Plant security teams have an obligation to protect the wellbeing of people who work in, visit, or travel through their facilities. Posted evacuation plans and audio/visual alarms are often considered sufficient for this purpose, but in reality they aren't. During an incident people need context-relevant information pushed to them to keep them safe under highly fluid circumstances.

Moreover, first responders need the ability to communicate in real-time with those in imminent danger, who need assistance exiting the facility, or who are in safe areas but don't know it. Active communication can often make the difference between a well-managed incident and a nightmare scenario.

Patrocinium, in partnership with Aruba, addresses integrated emergency response and notification by combining Meridian indoor location services with an innovative mobile app. The solution informs people of incidents and what actions should take based on danger in or near their specific location. Communication occurs in real time with tenants, visitors, and staff, and unique 4D graphics enables first responders to see where people are situated within buildings.

All that is required for 4D support is a Meridian subscription and Aruba Beacons, standalone or embedded within Wi-Fi access points, throughout the facility. Patrocinium's app leverages Meridian's maps and indoor location, in addition to GPS, to provide a new level of visibility. Unlike GPS-only

Figure 39: Meridian-Based Patrocinium Emergency Response Platform

based location services that cannot differentiate between floors, and may be unusable indoors, Aruba's BLE indoor location incorporates that critical 4th dimension

Generic crisis management and emergency notification tools that use text, e-mail, social media, and audio/visual alarms to alert people of danger fall short because they can't isolate those in danger from other occupants, or provide real-time situational awareness.

Working together, the Patrocinium Platform and Meridian location services fill this critical gap. Doing away with lists and opt-in workflows. Patrocinium instead uses patented software to automatically notify occupants when they are within a danger zone geofence without first signing up for alerts. To protect user privacy, Patrocinium's geofencing technology only visualizes individuals' locations when they are in or near danger, or need assistance.

This event-triggered process generates an immediate, personalized flow of information to anyone at risk of being affected by an incident. Occupants are shown their location, relevant pushed updates, perimeters, and muster zones. If help is needed it's one button-push away. In essence, users become sensors for the security team.

Key benefits include:

- Situational awareness indoors so users can see their location relative to incidents, fire extinguishers, exits, and other safety-related data;
- Wayfinding guides users to stairwells, exits, and designated outdoor muster areas;
- A4D picture with longitude, latitude, floor number, and time gives first responders more details than they could obtain from just GPS;
- Exact location is presented when a user declares themselves safe/unsafe via the mobile app;
- Easily integrates into existing branded mobile apps - a dedicated app is not required;
- Responders can send specific information to targeted recipients; and
- Incident recording ensures that all relevant data are saved for digital auditing and reporting.

Patrocinium and Aruba have created an event-triggered process that generates an immediate, personalized flow of information to those affected by an incident. Employees, visitors, service engineers, and contractors can all benefit from the real-time situation awareness enabled by the system.

VAPING DETECTION AND AIR QUALITY MONITORING

In 2016 the U.S. Food and Drug Administration (FDA) mandated that electronic cigarettes (e-cigarette) products be regulated as tobacco products, and subsequently banned the sale of these products to minors. That same year a World Health Organization (WHO) report recommended that e-cigarettes be banned in indoor areas and wherever smoking is prohibited. Since then governments worldwide have enacted laws that prohibit e-cigarette usage (vaping) everywhere that smoking is banned.

The challenge has been how best to enforce no-vaping rules since the vapors can be difficult to detect. E-cigarette vapor contains ammonia, and the first vaping detection sensors simply detected when a preset level of ammonia was present and triggered an alarm. The problem is that many products contain ammonia, resulting in a high false alarm rate.

An alternate solution is to use two different sensors to detect ammonia and other chemicals present in e-cigarette vapors. Dual-trigger sensors have a much lower false alarm rate, and raise confidence that a vaping alert is valid.

IPVideo Corporation

IP Video is a New York-based developer of smart building physical security sensors. Their HALO IIoT Smart Sensor is a multi-function security and environmental monitoring devices that hosts chemical sensors, audio detection, and a voice synthesizer.

Figure 40: HALO Smart Sensor Powered by Aruba Switches and Pass-Thru PoE Access Points

IP Video and Aruba have collaborated to enable plants to combat vaping through automated sensing and response. Powered by Aruba PoE pass-thru access points and PoE switches, HALO detects vaping and THC using dual-triggers to reduce false alarms. HALO incorporates multiple sensors so it can serve additional roles, too. On-board sensors can detect particulates, carbon dioxide, carbon monoxide, volatile organic compounds (VOCs), oxidizing agents, and ethanol. These features make HALO well suited to air quality monitoring applications. Audio monitoring enables HALO to detect gunshots and cries for help, while a voice synthesizer lets HALO respond to occupants with context-appropriate messages, i.e., in response to a verbal request for "help" HALO can respond that "help is on the way." Voice detection and response are processed locally, not in the cloud, to ensure that privacy is maintained.

The joint solution is ideal for enforcing no-vaping rules, and monitoring for other signs of danger.

GUNSHOT DETECTION

One of the most dangerous situations faced by first responders is a live shooter inside a plant. Without knowing the location of, and weapons used by, the shooter, first responders imperil themselves when they come on the scene. Situational awareness can save lives and speed apprehension of the perpetrator.

Emerging technologies for public safety sit at the cutting edge of the detection and mitigation of threatening situations, with gunshot detection being an essential element in that toolbox. Despite claims about sophisticated machine learning algorithms, older generation gunshot detection systems based on acoustic sensor arrays were notoriously prone to false alarms.

The most current generation of gunshot detection relies on multiple sensing mechanisms – muzzle flash, impulse, and pattern matching – to validate the presence, type, and even barrel length of discharged firearms. The result is fewer false alarms and more efficient routing of first responders to active shooter-involved incidents.

Installing a dedicated network to support gunshot detectors is not economically viable, and many CISOs will not permit such overlay networks. Additionally, battery-operated sensors on dedicated wireless networks, like LoRa, present cybersecurity risks by bypassing standard IT security monitoring tools. There are also maintenance issues associated with battery replacement.

Aruba's Wi-Fi 6 access points overcome these issues by providing a USB port that supplies power and data communications for gunshot detectors. Standard Aruba security mechanisms help protect against malicious or unintentional security breaches.

AMBERBOX Gunshot Detection

AmberBox, a leading provider of next-generation gunshot detectors, and Aruba have partnered to ensure that first responders can be reliably notified when an active incident is in process. Applications include both plants and corporate offices

Figure 41: Amberbox Gunshot Detector

The joint solution works with Aruba Wi-Fi 6 (802.11ax) or Wi-Fi 5 (802.11ac) access points already deployed on-site, avoiding the need for a separate overlay network. AmberBox sensors interface with the access points' USB ports, which provide both power and data access. Sensor spacing matches access point spacing required for voice applications. AmberBox sensors do not interfere with the access point's ability to deliver high performance voice, video, location, and telemetry.

The sensors use acoustic and infrared data to recognize when firearms are discharged. Within roughly 3.6 seconds, the sensor identifies the actual gunshot signature and relays an alert using the USB port. Access points use secure tunnels to relay data to the AmberBox monitoring application. Automatic alerts can then be sent to law enforcement via the AmberBox cloud-based e911-certified platform, with additional notifications to plants security or other responding parties. A conference call line is automatically established to share information and coordinate efficiently.

AmberBox can also immediately activate building security systems while alerting personnel with SMS, e-mail and call notification. Real-time shooter location tracking can be viewed through the Web or a mobile response platform.

Dynamic segmentation of IIoT traffic is maintained throughout the Aruba infrastructure, protecting the rest of the network against compromised devices. Aruba switches automatically set-up secure connections with Aruba access points without the need for separate VLANs, regardless of the switch port into which they're connected. This feature simplifies the initial deployment of the access points, and minimizes opportunities for miswiring during adds, moves, and changes over the life of the deployment.

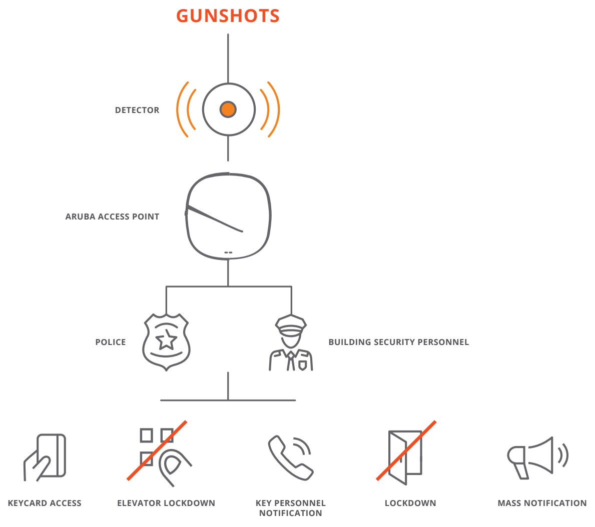


figure 1.0_081519_amberbox-psoa

Figure 42: AmberBox Gunshot Detection And Notification System

Key benefits of a jointly deployed solution include:

- Gunshot detectors can be placed where needed without new cabling or PoE injectors;
- No maintenance required, unlike with battery operated systems;
- Uses existing Aruba access points and leverages Aruba security mechanisms; and
- Supplements security solutions from Aruba and other partners including occupant safety monitoring, video surveillance, door locking controls, and wayfinding solutions.

Jointly deployed with AmberBox sensors, Aruba access points dramatically improve situational awareness so first responders know what they're facing on arrival.

SUMMARY

The digital transformation of IIoT is focused on delivering meaningful business value across all facets of local and remote operations. By enabling uniform visibility and uniform security from I/O to CEO, and accommodating the different operating modes of both IT and OT, Aruba is able to address the needs of CIOs, COOs, and CISOs at a price-point that checks the box for CFOs.

Working in concert with key technology partners, Aruba's unified infrastructure, zero-trust security, and AI powered solutions help bridge the IT/OT divide and boost efficiency, productivity, reliability, safety, security, and profitability.

Please contact us for more information on how we can help your plants make the digital transformation to hyper awareness.

a Hewlett Packard
Enterprise company

WP_IndustrialFacilities+NR_102020

Contact Us Share