WHITE PAPER

THE INTERNET OF RELEVANT THINGS

ACHIEVING STRATEGIC GOALS BY BRIDGING BUSINESS OBJECTIVES WITH IOT CONTEXT & DATA

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

THE PROFESSOR AND THE WOODSMAN

Some years ago the head of the Industrial Engineering Department of Yale University stated, "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."[1] 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."[2] 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 Internet of Things (IoT) projects. Whether it's the allure – or misunderstanding – of the IoT concept, fear of being left behind by competitors, or pressure to do something new, companies frequently rush head first into IoT projects without clearly defining objectives, value propositions, or the suitability of tools. The result is a high rate of failure for IoT projects, and disillusionment among customers.[3]

Part of the problem is that the phrase, Internet of Things, is misleading and deceptive. Originally intended to describe an ecosystem of interconnected machines, the turn of phrase has been taken literally to mean connecting all devices to the Internet. The overarching objective of IoT is not to network every device in an enterprise, much less connect every device to the Internet. IoT devices are vessels for context and data, and only relevant information – and devices – need to be tapped.

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 Gartner calls "business moments" – transient, customer-related opportunities that can be dynamically exploited.[4] A business moment is the point of convergence between the enterprise's strategic goals and relevant IoT context and data (Figure 1) that when properly exploited will positively change a customer's behavior, attitude, and/or sentiment.

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

And so we return full circle to the professor and the woodsman. The first order of business in any IoT 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 IoT architecture is the tool by which relevant IoT context and data are extracted and exploited to reorient customer behavior, attitudes, and actions in favor of the strategic goals.

Business goals and objectives inform the IoT architecture and relevant devices to tap, not the other way around. IoT solutions selected for eye candy appeal or hype alone will go wanting.

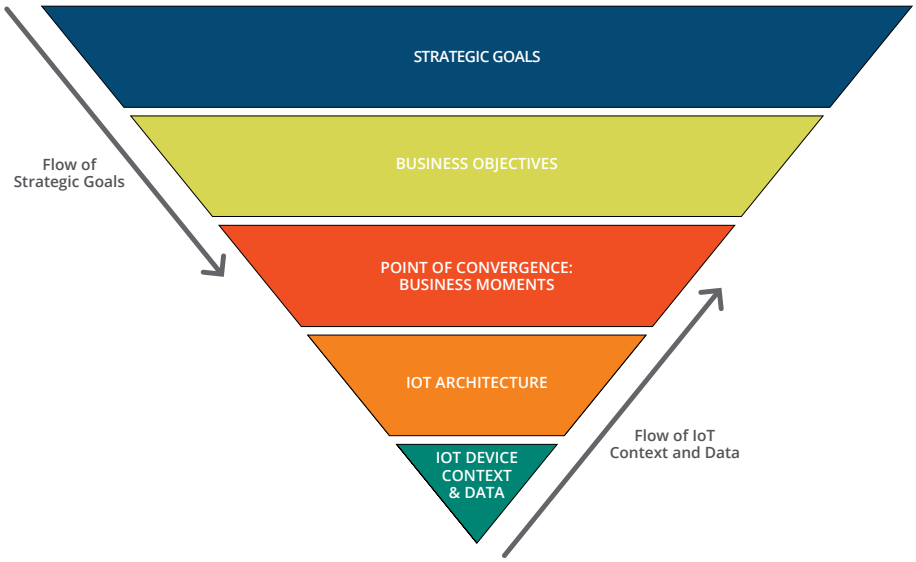


Figure 1: IoT Strategic Hierarchy

BUILDING A BRIDGE

Bridging between business goals and the IoT architecture needed to achieve them can be very challenging without a framework to guide the process. Stakeholders from different business units may have to surrender individual agendas to align with corporate objectives. New levels of collaboration will be needed across management, product, engineering, IT, and operations organizations.[5] Projects and technologies may have to be scrapped in favor of more relevant alternatives. And long-standing vendor relationships may have to be sidelined to onboard new suppliers with more pertinent solutions.

The IoT Value Cycle (Figure 2) provides such a framework by deconstructing business objectives into four primary elements: visibility, security, innovation, and profitability. The first two are associated with IoT infrastructure that extracts context and data relevant to business goals and objectives. The latter two define the business moments that leverage those context and data. Successfully aligning stakeholders with the definition and implementation of these four elements ensures that IoT solutions address the target business moments, and satisfy the business objectives guiding them.

Visibility answers the question "Am I fully connected?," and is achieved by interfacing with all devices, machines, and other sources of relevant process, business, and customer related context and data. The infrastructure by which this is implemented will vary by application. An automotive application may require cellular telematics, a supervisory control and data acquisition system may need a LAN and mesh wireless, while an off shore oil platform might require Class 1 Division 1 explosion-proof Wi-Fi infrastructure.

Regardless of the physical location of relevant devices, we need to ensure that we're seeing and using only trustworthy data from trusted sources. Accordingly, IoT data must be protected and governed, both in-motion and at-rest, throughout their lifecycles. Devices, operating systems, BIOSs, and infrastructure must be protected against tampering, both externally and by insiders. The people who install and service IoT solutions – and the tools they use – must also be securely managed. Application and system assurance is needed to ensure non-stop functionality, and appropriate governance over data usage has to be enforced at all times. Trust is a fleeting commodity because the cybersecurity landscape is constantly evolving. The question "Am I fully protected?" must therefore be asked repeatedly throughout the life of an IoT project to ensure that the latest safeguards are always in place.

Figure 2: Internet of Things Value Cycle

Visibility and security inform the IoT architecture needed to reach into data sources, assert trust, and govern the lifecycle of extracted information. As such they define the second layer of the IoT Strategic Hierarchy.

The base of the IoT Strategic Hierarchy is where we have to align accessibility and trust with relevant context and data contained within, and generated by, IoT devices. Needlessly tapping into every device without regard for relevance is expensive from many perspectives: device cost rises when connectivity is added, extending visibility and security requires labor and capital, extracted data need to be processed and stored, and resources are consumed separating wheat from chaff.

The guidelines that determine relevancy, and help us target specific IoT devices, fall to the Profitability and Productivity elements. Profitability is achieved by increasing revenue and/or decreasing costs by better serving customers, catering products and services to their preferences, and positively changing behavior and attitudes towards the business. The question "Am I fully innovating?" addresses how to deliver service excellence, engage with customers, differentiate competitively, simplify interactions, enhance loyalty, validate product performance, and monetize services.

Productivity, the fourth and final element in the IoT Value Cycle, focuses on empowering human and capital assets to work as efficiently as possible. This can be achieved by maximizing uptime, minimizing downtime, simplifying sales and support processes, more efficiently managing customers and staff, optimizing asset handling and process throughput, and becoming more responsive to requests and changes. The question "Am I fully exploiting knowledge?" addresses how IoT context and data can be exploited to improve efficiency.

The instantiation of visibility, security, profitability, and productivity will be unique to each customer – there is no such thing as a one-size-fits-all IoT solution, even within a specific vertical. Slight differences in the goals and objectives of an enterprise can reshape the solution needed to achieve them. While it's informative to see what competitors are doing, their solutions may not be relevant if your target goals, objectives, and business moments don't match theirs. Blindly following a competitor's lead may not be a prudent course of action.

You can bridge objectives and architecture by overlying the IoT Value Cycle on the IoT Strategic Hierarchy (Figure 3). The Profitability and Productivity elements identify relevant sources of context and data, while the Visibility and Security elements inform the architecture and the infrastructure needed to tap those sources.

The best way to visualize bridging is by example. In later sections we'll consider scenarios from different vertical markets, starting with retail, but first a cautionary discussion about security.

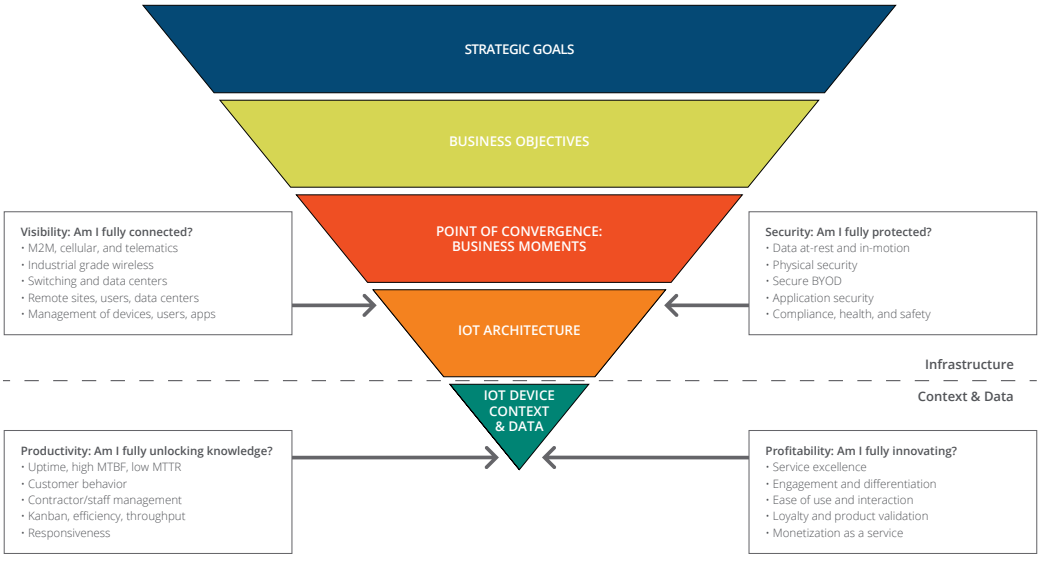


Figure 3: Bridging Business Objectives With Architecture And IoT Context/Data

SECURITY FROM THE OUTSIDE IN AND INSIDE OUT

IoT network penetrations and data breaches have become almost commonplace in every industry – nuclear, retail, healthcare, consumer. The reason is simple enough – most IoT devices and implementations are untrustworthy due to poor or no security. The engineers who design IoT devices are typically trained on process reliability and application-specific architectures. These fall under the auspices of operations technology (OT), the goal of which is to make products work reliably for as long as possible. Cybersecurity expertise, on the other hand, sits with information technology (IT) engineers. If OT and IT don't closely collaborate on IoT product and system design, untrustworthy solutions can result.

Relying on IoT information and processes that are at risk of being manipulated, intentionally or otherwise, is imprudent. The integrity and trustworthiness of the information we use must be beyond reproach, and that requires asserting trust from end-to-end – starting with IoT devices and extending to the applications that consume them. The way to achieve that is by incorporating security features into new IoT devices, and enveloping legacy devices within a protective bubble, creating a 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.

Aruba's IoT security framework is called Connect-and-Protect, and it includes the following protective mechanisms:

- Authenticating source/destination devices and monitoring traffic patterns including sensor iputs and buses;
- Encrypting data packets using commercial and, where applicable, government encryption standards;
- Enveloping the packets inside a secure tunnel to ensure they go only to their intended destination;
- Fingerprinting IoT 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.

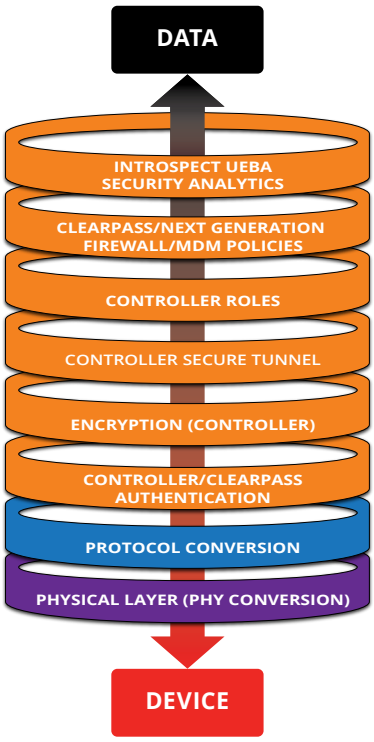


Figure 4: Connect-and-Protect IoT Security Mechanisms

Of particular note is the role played by Aruba's ClearPass Policy Manager in IoT device profiling, identity, and posture. Profiling fingerprints and classifies IoT devices as they attempt to connect to differentiate between device types and to detect impersonators. Identity tags IoT devices with a role that determines when and how they connect – including location, time of day, day of week, and current security posture – to provide more granular role based access control. Posture is a health check to determine known vulnerabilities, active ports, operating system version, and SNMP security among other features; posture needs to be routinely verified to ensure compliance, and trusted devices may be denied access if the posture is sub-standard.

ClearPass uses profiling, identity, and posture to identify IoT devices as trusted, untrusted, or unknown, and then takes action accordingly. Profiling data will flag if a device changes its mode of operation or masquerades as another IoT device, in response to which ClearPass will automatically modify the device's authorization privileges. For example, if a Programmable Logic Controller tries to masquerade as a Windows PC, network access will be immediately denied.

Policies are only as effective as the information used to build them, and the enforcement tools available to protect them. Applying a systems approach to security helps identify IoT threat vectors and the security technologies needed for remediation.

The end game of IoT is to enable business transformation by exploiting the rich sources of data locked inside of IoT devices. With the right security measures designed in from the ground up, trust can be asserted throughout the IoT solution. Attention can then be refocused on bridging strategic goals using the trustworthy IoT architecture. Let's turn now to examples of how that bridging process works.

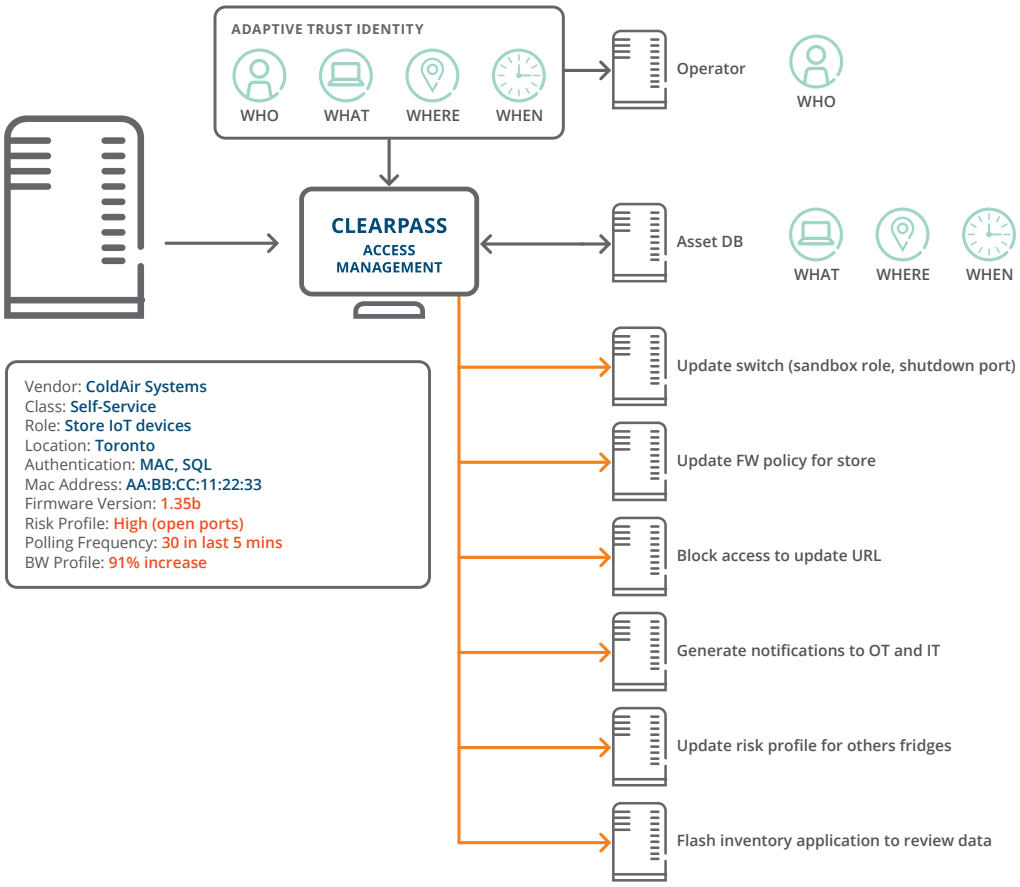


Figure 5: ClearPass IoT Device Security Violation Workflow

GOING VERTICAL: RETAIL

For the coming year a national big-box retailer needs to increase basket size by 10%, and cut store abandonment rate in half, to reach their target revenue number. These goals dictate a more engaging customer experience, and that has several objectives. First, customers need to be presented with, and easily find, products relevant to them, at price points within their spending range, so they don't abandon the store out of frustration. Second, customers that showroom – looking at merchandise but buying on-line after price checking – need to be convinced to buy in-store, and that requires active intervention in some form. Finally, customers who can't find items they want need to be quickly served so they don't quit the store, requiring careful management of the customer-to-associate ratio.

Since customers, associates, and inventory are mobile, IoT location-based services – working in concert with backend CRM, point of sale, and inventory applications – are the most promising tools to use. Location services address one or more of the following questions:

- "Where am I?"
- "Where are they?"
- "Where is it?"

For this retail application we have to achieve the following business objectives:

- Identify existing customers that enter the store so the retailer can analyze past buying and Web behavior to push real-time offers that will be of interest on the current trip;
- Allow customers to run inventory lookups on their smartphones and receive turn-by-turn instructions to in-stock or substitute items, using a pathway that maximizes upsell opportunities to increase basket size;
- Provide freely available Wi-Fi over which customers can surf the Web, and thru which the retailer can see what applications customers are using and where they use them. For example, in response to showrooming activity the retailer will update electronic signage and send push messages about Internet price matching. Store associates will also be notified so they can help convert the customer to an in-store purchase;
- Monitor the location and ratio of customers to associates so that no parts of the store are underserved.

With the business objectives identified we now move to the selection of appropriate IoT tools. The table below shows the range of Aruba's IoT location-based service options. Solution selection starts at the top with the high level question to be answered, and ends at the bottom with a specific IoT tool recommendation.

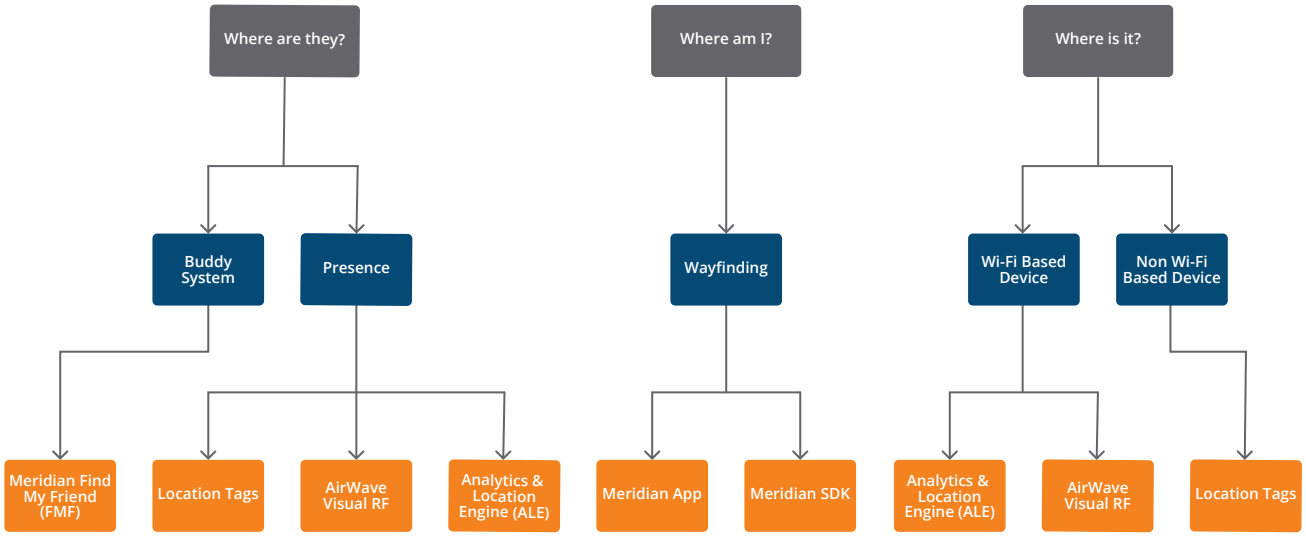


Figure 6: Location-Based Service Options

Four different types of location tools will be required to achieve the identified business objectives:

- Wayfinding: an app that helps customers self-navigate a site with indoor GPS-like services, alerts when they cross a geofenced boundary, and provides push messaging direct to the customer;
- Presence: determines when and which customers are present, what they're doing on-line, and when they cross geofenced boundaries;
- Buddy System: finds where associates are located throughout the store;
- Non-Wi-Fi Based Asset Tracking: identifies the location of assets, pallets, and merchandise.

The highest degree of customer engagement comes from direct interaction that changes behavior in real time, i.e., an application that runs on the customer's own smartphone or tablet, and thru which wayfinding, push messaging, and geofencing can be delivered right to the customer. Aruba's Meridian service provides all three essential services in a single app. The solution delivers an indoor GPS-like wayfinding experience, guiding guests with turn-by-turn instructions and real-time position on a map. Meridian's Find A Friend feature enables store managers to directly observe the location of store associates. Geofences can trigger actions and applications along the way.

Meridian can be interfaced with customer relationship management (CRM), point of sale (PoS), and other backend applications, as well as business rules engines to implement complex Boolean condition processing. A push messaging feature delivers instantaneous feedback, offers, and updates. If the retailer already has its own app then the Meridian SDK can deliver these same services to their app instead.

Moving from wayfinding to showrooming detection is not simple as it requires knowing when a customer hits an on-line shopping service, such as Amazon. Aruba's Analytics & Location Engine (ALE) calculates the x/y position of everyone in the store with a Wi-Fi enabled device who opted in, and monitors url surfing behavior conducted over the Wi-Fi network. Used in conjunction with a backend analytics engine, ALE can help retailers identify showrooming and convert more opportunities to in-store sales.

ALE's x/y monitoring can also be used with backend or cloud applications to monitor customer-to-associate ratios. When the ratio falls below a minimum acceptable level both the associates and store manager can be notified. ALE's location processing has an additional side benefit: it can monitor walk-by versus walk-in traffic, letting the retailer know what percentage of foot traffic is coming into their store.

Figure 5 shows how the retailer's strategic goals flow down into business moments, and how those moments are serviced by IoT infrastructure and device data tailored to the task. This example demonstrates how to move from a high level goal to a specific set of IoT tools that deliver successful business moments.

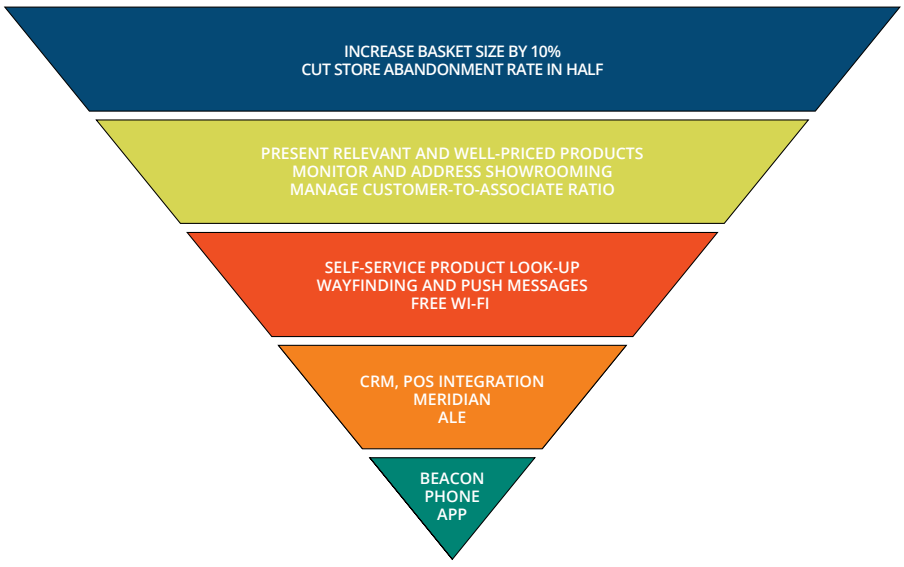


Figure 7: Aligning IoT Infrastructure with the Retailer's Strategic Goals

IoT projects go sideways when goals and tools are misaligned. For example, passively tracking customer location using presence analytics alone offers a backward-facing view of customer behavior – you know where the customer went but you can't change buying behavior in real-time. Many presence analytics projects launched because they were easy to deploy on existing Wi-Fi infrastructure, only to subsequently crash and burn because there was no way to convert presence analytics into sales. The lesson is clear: ensure that the IoT solution and business goals are tightly aligned prior to embarking on an IoT project.

GOING VERTICAL: HEALTHCARE

Let's turn now to a healthcare example that leverages some of the location-based services from the retail example. In the coming fiscal year a managed care organization with dozens of hospitals and clinics wants to increase billable visits by 10% without increasing its real estate footprint, hiring, or overtime pay. Patient and staff satisfaction surveys show that reducing the duration of appointments is inviable because physician-patient face time is already bordering on being unacceptably brief. The same surveys show frustration by both patients and staff about missed appointment times. Patients are upset because the large facilities are difficult to navigate, site maps aren't easily interpreted by non-English speakers and elderly patients, and the available clinic rooms change during the day but appointment reminders aren't updated. Staff and physicians are upset because morning appointments often go unfilled due to no- or late-shows, while afternoon appointments back up past the end of the shift so (now angry) patients have to be rescheduled for another day.

Achieving the corporate goal will require a more efficient way for English and non-English speaking patients to navigate the facilities so that every available appointment slot can be filled on time, avoiding end-of-day back-ups. In the context of "Where am I?," "Where are they?," and "Where is it?" location services, the target objectives include:

- Pushing a message to each patient, in their preferred language, on arrival at the clinic about the time of their appointment and exact office number;
- Pushing an updated message should there be a change in the appointment location or time;
- Providing turn-by-turn instructions and arrival time for the next appointment that takes into account the entrance or garage thru which the patient enters the facility;
- Providing the same push messaging and wayfinding features to visiting or temporary physicians and staff so they can easily navigate to their next appointments;
- Allowing staff to track the location of patients as they navigate the facility so they can reach out by phone if the patient is late.

Three different tool categories are needed to achieve these objectives:

- A wayfinding app that helps patients, staff, and physicians self-navigate the site, with instructions in the language of their choice;
- Geofencing that triggers when a patient enters the site and interacts with the appointment scheduling system to push a greeting message with the location and time of the user's next appointment;
- Personnel Tracking so staff can locate patients and visiting physicians who are late for appointments.

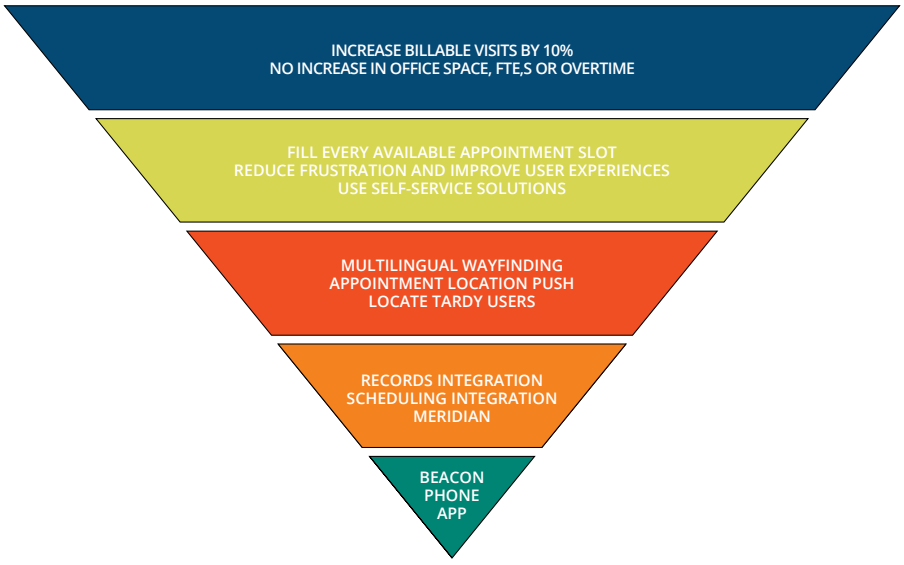


Figure 8: Aligning IoT Infrastructure With The Healthcare Organization's Strategic Goals

Aruba's Meridian Service described earlier works over both cellular and Wi-Fi, so services can be delivered in garages and outside areas that lack cellular and/or Wi-Fi coverage. Since Meridian is Wi-Fi network independent, it can function over both Aruba and non-Aruba Wi-Fi systems.

This solution requires integration with patient record, accounting, and staff personnel systems. While that requires heavy lifting at the time of implementation, once completed it can serve as a platform for a host of additional added value services in the future, e.g., time and motion optimization, site real estate utilization, and parking lot full/available notifications.

On the other hand, losing site of the goals could point us to vendors with suboptimal solutions. For example, using location services to generate e-mail or text messages wouldn't be as engaging, and might not be received in a timely manner, compared with a real-time wayfinding app. Multi-lingual map support might require more up-front configuration but it ensures that patients, or their helpers, can select the language best suited to them. And updating staff in real-time can help them better plan schedules, or find wayward patients, with minimal wasted effort.

GOING VERTICAL: OIL & GAS

We'll now turn to an industrial IoT example that leverages both location-based services and edge analytics. In the coming fiscal year an oil and gas company with 25,000 jack pumps and 15,000 contractors wants to reduce pump down time by 10%, decrease contractor costs by 10% without lowering well production, and lower spare parts shrinkage by 25% without impacting productivity. The company has attempted, unsuccessfully, to align pump service schedules with theoretical pump failure rates. As a result pump outages are not uncommon which, in turn, reduces production revenue. Additionally, lost, misplaced, or stolen pump spare parts and pipes are driving up costs and impacting the timely repair of equipment; it's unclear who is removing the inventory, and if theft or improper records are to blame. Finally, manually reconciling invoices for contractor services against actual time on site is a challenge – there are simply too many contractors and not enough accounting staff.

Achieving the corporate goals requires a way to monitor pumps in real-time and predict failures based on observations of anomalous behavior. The pumps are instrumented with sensors and actuators that feed local closed-loop controls, but the data are not otherwise mined for insights. With so many pumps in service, and wide-area cellular network costs a variable expense, forwarding all pump data for remote analysis would be too expensive. Instead, running analytics locally on the jack pumps and notifying a monitoring center only when anomalous behavior is detected would be much more economical. The monitoring center could request supplemental sensor data if needed, provided it was archived at the pump site. The center could also analyze historical operating data against the pump manufacturers' databases to determine how best to address the anomaly.

Tracking when contractors arrive and leave jack pumps and logistics yards, and sharing those data with the company's accounting applications, will enable direct comparison of billed versus actual hours on site. The solution requires an automated method of reporting so no additional labor costs are incurred due to manual processes. It also requires a contractual change mandating full participation by all contractors if they wish to be paid for services.

The same tracking solution used to monitor contractors at the pump sites can also be used at logistics yards. Sharing location data with the access control and closed circuit televisions systems (CCTV) would tie contractor identity with a site visit, and simplify identification of suspects should inventory go missing.

The business objectives for the oil and gas company include:

- Enabling the jack pumps to process analog and digital data generated by the jack pump control systems and report anomalies;
- Deploying a remote monitoring center to manage the wide-area data collection system, perform meta analytics on pump data, and tie into a predictive analytics application leveraging historic failure data;
- Mandating that all contractors be equipped with a location services app to report when they arrive at and depart a pump site or logistics yard. Since the contractors are independent agents, for privacy reasons the applications must only be triggered by arrivals and departures at the oil company's facilities; always-on GPS tracking is an unacceptable solution.

Several different tool categories are needed to achieve these objectives:

- Gateways that acquire sensor and actuator data from the jack pumps, run analytics applications to process the data, and provide a wide-area network to communicate the results to a remote monitoring station;
- A remote monitoring system that manages the wide-area network, runs its own analytics on aggregated data, and interfaces with other data repositories such as service histories and manufacturer data bases;
- Geofences that trigger an app on the contractors' smart phones or tablets when they enter or leave pump and logistics sites;
- Interfaces to access control and video surveillance applications through which contractor identification data and time/date can be exchanged whenever a contractor enters or exits a site. If a contractor lacks permission to access a facility then the access control system will deny access.

At a high level predictive fault detection requires a few basic building blocks that can be mixed to address different implementation requirements: the IoT Intelligent IoT Device, the Access Device, Communications Media, an IoT Controller, the IoT Business and Analytics Application, and System Management Tools.

The Intelligent IoT Device is a machine, in this case a jack pump, that generates analog, digital, and/or control network data into which the enterprise wants visibility. The access device interfaces with the IoT device, ingests the data, and then takes local action and/or conveys the data to the IoT controller at a remote monitoring site.

There are two forms of access devices: Gateways and Converged IoT Systems. A Gateway converts data streams from IoT devices into a secure format that is compatible with the network in use. Gateways are used when an IoT device lacks the ability to securely communicate with a network (LAN, cellular, Wi-Fi), is unable to run a local VPN client for secure remote access, or has serial, analog, or proprietary inputs/outputs (I/O) that are incompatible with the wide area network.

Figure 10: Aruba Edgeline Gateway Access Device

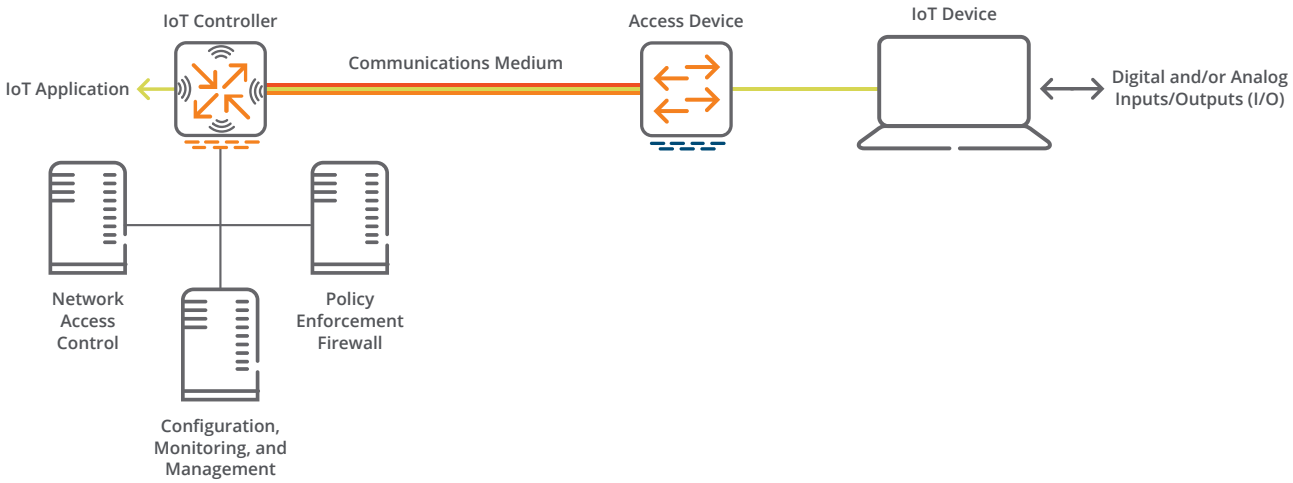


Figure 9: Predictive Fault Monitoring Building Blocks

A Converged IoT Device has I/O interfaces and compute power to locally process data from IoT devices. This solution is used to reduce process latency, lower the volume and cost of wide area data communication traffic, process and store local IoT activity, and/or send a remote data center a summary of local IoT activity. Converged IoT Devices accomplish these tasks by locally running machine learning and data analytics engines, and the devices are characterized by their powerful compute engines, ability to ingest analog/digital sensor data and control bus traffic, and remote management capabilities.

Figure 11: Aruba Converged IoT System Access Devices

In the case of the oil and gas company, a Converged IoT System is the most appropriate access device since local insights are needed to minimize wide area network expenses. The system will use cellular telephony as the communications medium to simplify deployment time and because cellular systems are typically resilient in the event of a single tower outage.

Cellular costs will be addressed by using Hewlett Packard Enterprise's Mobile Virtual Network Operator (MVNO) service which has pre-negotiated favorable subscription rates for low bandwidth IoT applications such as machine monitoring applications. Pre-processing IoT data on-site using a Converged IoT System with analytics software will significantly reduce both the volume and cost of cellular communications.

Aruba's VIA VPN will encrypt and tunnel data between the jack pumps and the monitoring center. VIA supports AES 256+ bit key encryption and provides network-level peer authentication, data origin authentication, data integrity, and replay protection. For government IoT applications, VIA is also available with Suite B elliptic curve encryption to protect releasable information up to Top Secret classification.

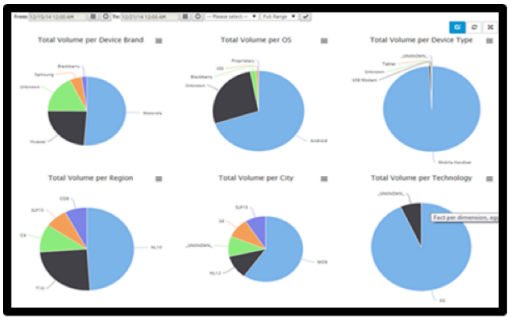
The VIA VPN will terminate at the IoT controller at the oil and gas company's data center. The controller manages network encryption and authentication, and interfaces with firewall, network access control, and policy management applications that enforce application-layer security, packet prioritization, and access rules. Controller software instances can be used in lieu of hardware controllers for private and public cloud applications.

Figure 12: Aruba Controller

Analytics applications will run both at the Converged IoT Systems and in the monitoring systems. The analytics application will consume IoT data and use mathematics, statistics, machine learning, and/or predictive modeling to flag anomalous behavior and predict failures by mining data pools from the pump vendor, internal service records, and even other company sites. Example applications include HPE Vertica, SAP HANA, GE Predix, and Schneider Wonderware.

Jack pump sites will be monitored using HPE's Universal IoT Platform (UIoT) application, a powerful application suite that includes a range of specialized services for IoT device monitoring. These services include:

- APIs through which data can be consumed by client applications;
- Digital services through which new applications, micro services, and algorithms can be quickly introduced;
- Data acquisition from Aruba Gateways and Converged IoT Platforms, as well as IoT protocols via open source message brokering;
- Management of cellular infrastructure;
- Robust predictive analytics with pre-built algorithms and ready to use templates;
- Alignment with oneM2M or equivalent data structure standard and built-in protocol libraries for commonly used control protocols;
- Message queuing through open standard messaging bus including both device and subscription management.



FEATURES	CORE BASELINE	OPTION	MODULE
Managing devices and services	Yes		DSM
Uplink and downlink data acquisition	Yes		NIP
Data acquisition and validation	Yes		DAV
APIs exposure	Yes		SGF PRM
Advanced dashboard	Yes		Console
Relational database	Yes		EDB
Dashboard designer		Yes	Console designer
Analytic columnar database		Yes	Vertica
Alarms handling and correlation		Yes	TeMIP/UCA
Micro service design and execution		Yes	SIS

Figure 13: UIoT IoT Device Monitoring System

UIoT aligns IoT device support with the oneM2M industry standard, and supports a wide variety of IoT applications and processes. New applications can be rapidly instantiated on a large scale, including device discovery, configuration and control of IoT traffic (outside of traditional voice and data traffic) on the same private or hybrid cloud platform.

As with the Meridian platform, UIoT can service as the foundation for a variety of added-value services beyond those required to meet the current strategic goals. UIoT supports ground mobile telematics applications, interfaces with LoRa and Sigfox long-range wireless systems, and has a broad range of APIs to interface with other monitoring, reporting, and auditing applications.

Contractor location services can be provided by Aruba's Meridian geofencing and push messaging services. Jack pumps and logistics sites equipped with Aruba BLE Beacons will have geofences established at the boundaries to the pump service and storage areas. The size of the geofence will be tailored to each location. When a contactors' smart phone or tablet crosses into or out from the geofence, a notification will be pushed to the accounting app noted the identity, time, and location of the geofence trigger. The contractor can also be pushed a message confirming that Meridian correctly recorded the activity. By insisting that contractors use the Meridian app in order to be paid for services rendered, the oil and gas company can ensure a high rate of compliance.

Meridian includes APIs thru which location-related data can be shared with other applications, such as accounting, access control, and video surveillance workflows. This capability enables the same Beacons and app to be used at the jack pumps and to trigger security systems at the logistics facilities so pick-ups and deliveries can be correlated with card access and video surveillance data. If inventory shrinkage is associated with contractor activity, contractor identification will be an essential component of the security record.

This example demonstrates how the oil and gas company can move from high level goals targeting pump up-time, contractor cost management, and shrinkage reduction to a specific set of analytics, reporting, and location-based service IoT tools that address these goals.

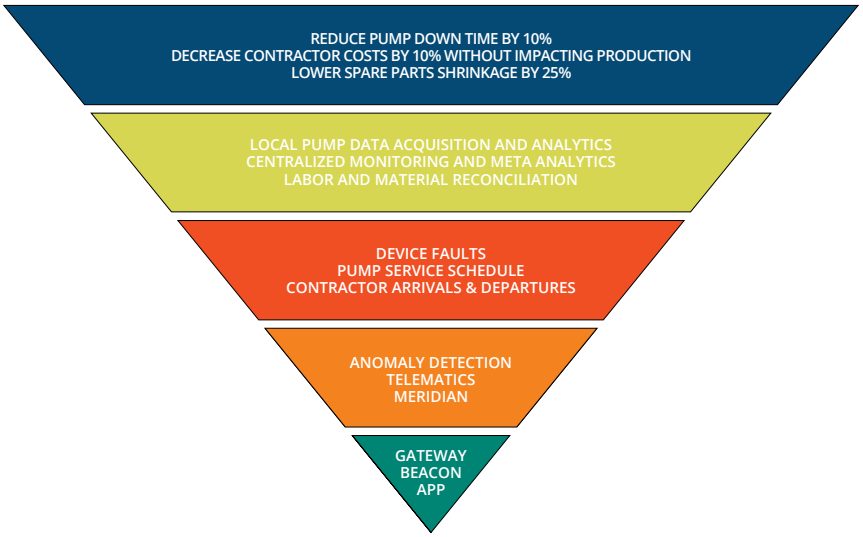


Figure 14: Aligning IoT Infrastructure With The Oil and Gas Company's Strategic Goals

THE FIRST STEP OF THE IoT TRANSFORMATION JOURNEY

IoT tools should be both scalable and extensible so they can serve as a platform to address future business goals. In all three cases discussed above, the Aruba and UIoT solutions are both massively scalable and extensible to serve a broad range of use cases.

The technical challenges associated with bridging between business goals and the IoT architecture may be more easily overcome than the political hurdles needed to achieve alignment within an organization. Existing agendas and projects in process may catalyze different interpretations of the strategic goals or business objectives, challenging other groups to align with their interpretation. Stakeholders from different business units may vie for control of projects and agendas, threatening to withhold support or funding if their particular vision isn't implemented.

Achieving new levels of collaboration needed across management, product, engineering, IT, and operations organizations may necessitate the intervention of a neutral third party. To this end HPE's Technical Services Consulting organization has crafted an IoT workshop to help define a unified vision for IoT projects, build alignment with key stakeholders, and Identify strategic objectives and quick wins. For more information please see https://www.hpe.com/h20195/v2/GetPDF.aspx/4AA6-7269ENW.pdf.

CONCLUSION

The overarching objective of IoT is to converge the enterprise's strategic goals with relevant IoT context and data to deliver successful business moments. A successful business moment has to be carefully orchestrated to dynamically exploit transient customer-related opportunities, and IoT context and data have a critical role to play in positively changing a customer's behavior, attitude, and/or sentiment towards the enterprise.

The chain that stretches from relevant IoT context and data via IoT architecture has to be well executed. This white paper has shown how to bridge between the elements of the IoT Hierarchy, extracting relevant context and data from IoT devices and then implementing an appropriate architecture to make use of them. Careful preparation, objective definition, and tool selection will pay big dividends if they are accompanied by organizational alignment on the goals and objectives. Once that's in place even the most challenging business goals can be achieved.

REFERENCES

1. William H. Markle, "The Manufacturing Manager's Skills" in *The Manufacturing Man and His Job* by Robert E. Finley and Henry R. Ziobro, American Management Association, Inc., New York 1966
2. C. R. Jaccard, "Objectives and Philosophy of Public Affairs Education" in *Increasing Understanding of Public Problems and Policies: A Group Study of Four Topics in the Farm Foundation*, Chicago, Illinois 1956
3. Alfonso Velosa, W. Roy Schulte, Benoit J. Lheureux, *Hype Cycle for the Internet of Things*, 2016, Gartner, 14 July 2016
4. A business moment is a transient set of context-sensitive interactions between people, business, and things that yield a negotiated result as opposed to a predetermined result, i.e., a personalized, targeted offer from a retailer based on location, time, and CRM data. See Frank Buytendijk, *Digital Connectivism Tenet 4: We Do Not Differentiate Between People and Things*, Gartner, 1 November 2016
5. Dale Kutnick and Saul Brand, *Exploit Enterprise Architecture to Guide IoT Deployments at Scale*, Gartner, 15 December 2016