FEBRUARY 2018

IOT PLATFORM ARCHITECTURE: AN ENTERPRISE'S PRACTICAL DESIGN GUIDE

EXECUTIVE SUMMARY

Enterprises are looking for practical guidance on deploying Internet of Things (IoT) solutions efficiently and safely. While an IoT solution can drive innovation and operational savings for enterprises, enterprises must properly design their IoT solution components to handle proof-of-concept and large scale deployment. With proper solution design, the anticipated benefits from an IoT solution can be considerable.

One of the most important decisions is the architectural approach chosen for an enterprise's IoT data and device management platform. MachNation has identified 3 design parameters that enterprises must select when choosing their IoT platform architectural model. These design parameters — operational autonomy, data processing depth and integration topology — dictate the levels of control that a platform has on IoT devices, the hierarchical layer where the IoT platform processes data and the geographic proximity of the IoT platform to an enterprise's northbound systems. By properly specifying an IoT platform architecture using these 3 design parameters, enterprises have the opportunity to cost-effectively and safely supply device lifecycle management, support northbound applications and systems and ultimately realize business value from an IoT solution deployment.

This analyst insight article defines the 3 design parameters for IoT platform deployment. By linking these design parameters with use-case examples, MachNation offers practical guidance to enterprises exploring an IoT deployment.

FIGURE 1 Three Design Parameters

OPERATIONAL AUTONOMY
The levels of authority granted to an IoT device to take actions on connected assets or to control data

DATA PROCESSING DEPTH
The hierarchical layer where machine-related data is analyzed and acted upon

INTEGRATION TOPOLOGY
The relative closeness of the IoT platform to a customer's northbound business systems and peer platforms

INTRODUCTION

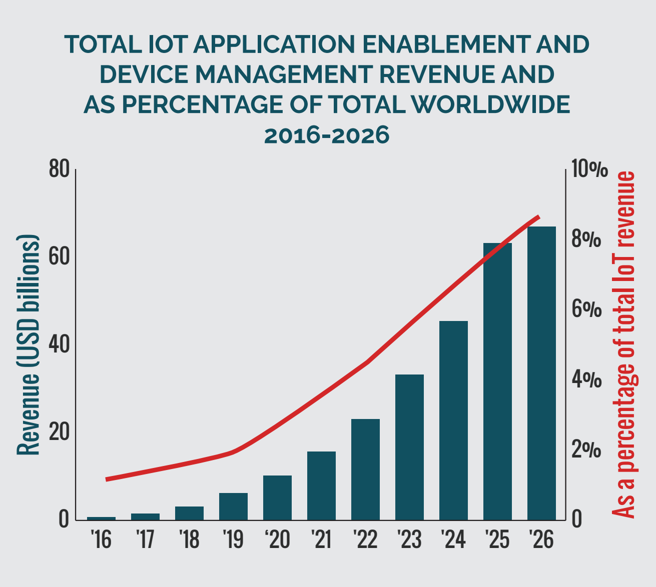
Enterprises in industrial sectors worldwide are looking for ways to deploy IoT solutions efficiently and securely while ensuring long-term manageability. In fact, IoT continues to be one of the ways that businesses evolve their critical business processes and increase productivity while maintaining high levels of safety and security. According to MachNation forecasts, worldwide IoT application enablement revenue will be USD1.7 billion in 2017 growing to USD64.6 billion by 2026 at a compound annual growth rate of 49%.

machnation

CUMULOCITY IoT
BY SOFTWARE AG

Enterprises deploy IoT solutions to address their key business needs. These needs might include reducing ongoing capital spending on equipment, redesigning a business process related to logistics or launching a new set of connectivity-related services for an existing product line. Often, an enterprise will deploy an IoT platform to address one use case and rapidly find additional uses cases that if addressed would positively impact the business. Using its IoT platform to support all of its use cases is a cost effective and simple approach to total IoT solution deployment.

FIGURE 2 IoT AEP Revenue



Once an enterprise chooses to digitize, one of the most important considerations is the architectural approach chosen for an enterprise's IoT data and device management platform. This platform will link together IoT devices and back-end applications. It will provide the foundation for ongoing device lifecycle management. And it will provide a secure way to transport and analyze IoT data.

However, there are always limitations that impact the choice of the IoT platform architectural approach. Limitations include data privacy requirements, various industry-specific regulations, requirements of high-volume data processing and the geo-distribution of assets. For example, remote asset monitoring solutions in the oil and gas industry are constrained by the location of the assets being monitored. Fleet management solutions for shipping companies are constrained by various long-distance mobility requirements. And factory automation solutions for globally distributed manufacturing plants are constrained by the location of back-end operations systems, regulatory issues and high-volume data processing requirements.

Enterprises must consider the limitations of the IoT deployment situation and match these to the architectural design of their IoT AEP platform technology. Picking the right architectural design will allow an enterprise flexibility in deployment, minimize the ongoing platform operational costs and ensure appropriate IoT data and device security.

IOT PLATFORM ARCHITECTURES

MachNation has identified 3 design parameters that enterprises must consider when choosing their IoT platform architectural model. These design parameters — operational autonomy, data processing depth and integration topology — dictate the levels of control that a platform has on IoT devices, the hierarchical layer where the

IoT platform processes data and the geographic proximity of the IoT platform to an enterprise's northbound systems. Having chosen these design parameters, an enterprise will be able to deploy the appropriate IoT platform architecture to support its IoT solutions. Below, MachNation describes the 3 design parameters and then presents several use case examples to illustrate the match between an IoT solution and its 3 design parameters.

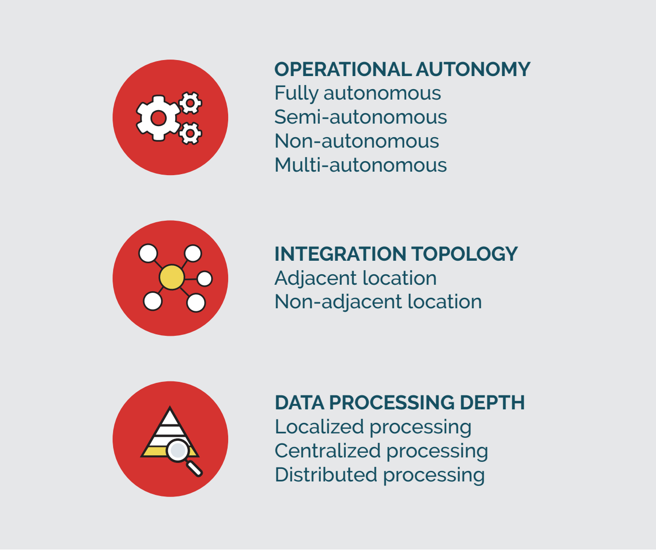
OPERATIONAL AUTONOMY

Operational autonomy is the level of authority granted to an IoT device to take actions on connected assets or to control data.

Operational autonomy is the first IoT platform design parameter. Enterprises choose the level of operational autonomy of IoT devices based on requirements of the device, platform and internal business and technology requirements. Under certain circumstances, an IoT device might function very autonomously using a set of predefined rules that determine the amount of control it can have on connected assets. Under other circumstances, an IoT device might have no autonomy to control a connected asset, thereby requiring control from some other source, platform or application. The autonomy of an IoT device dictates the amount of machine control that the IoT device has on IoT assets: highly autonomous devices have high levels of IoT machine control. In addition, more IoT device autonomy usually requires more processing capabilities on the device which can impact device cost, power consumption, security and other issues. There are 4 levels of operational autonomy.

> Operational autonomy is the level of authority granted to an IoT device to take actions on connected assets or to control data

FIGURE 3 IoT Platform Design Parameters



OPERATIONAL AUTONOMY
Fully autonomous
Semi-autonomous
Non-autonomous
Multi-autonomous

INTEGRATION TOPOLOGY
Adjacent location
Non-adjacent location

DATA PROCESSING DEPTH
Localized processing
Centralized processing
Distributed processing

Fully autonomous control means that authority is granted to the IoT device for various on-device or on-location control functions. IoT solutions that are sensitive to communications latency or have very sensitive data might choose a fully autonomous control design. For example, the IoT device on a connected ice cream vending machine might autonomously control the proper internal temperature of the machine to preserve the quality of the ice cream. If the internal temperature of the machine exceeded its threshold, then the IoT device would send a message to a back-end system notifying the machine owner.

Semi-autonomous control means that authority is granted to the IoT device for most circumstances, but for some actions machine control will come from other sources. For example, while a water pump is operating within reasonable parameters, the IoT device can manage the pump's performance autonomously. However, to switch on or off the water pump, a rule is created that authorization needs to come from another source like an operations control center system or another application.

Non-autonomous control means that machine control comes from another source, not from the IoT device. Non-autonomous control of an IoT device is fairly common when a device has very low processing power. It is also common to use non-autonomous control when the set of assets being controlled function as a system. For example, a smart traffic management system requires rapid analysis of data from thousands or tens of thousands of assets. Data from the entire system — not just 1 or 2 assets — are required to make real-time decisions about traffic flow, parking, bus systems and rail transport. In this case, non-autonomous control of IoT devices is most suitable.

Multi-layer control means that machine control occurs at the global layer and optionally at the regional or localized layer. In addition, the platform might control multiple IoT solutions each with its own platform architecture and design parameters. For example, an enterprise might have 15 globally distributed facilities manufacturing specialty plastics. This enterprise might choose to implement IoT solutions for factory floor automation, smart logistics tracking and personnel surveillance. It would be logical to have multi-layer control of IoT devices knowing that operations staff at each of the 15 facilities would need control of some connected assets for their facility while operations staff at the enterprise's global operations monitoring center would need control of other types of assets across the 15 facilities.

DATA PROCESSING DEPTH

Data processing depth is the hierarchical layer where machine-related data is analyzed and acted upon.

Data processing depth — one of the most common aspects of an IoT solution — is the second IoT platform design parameter. This design parameter helps enterprises stipulate the level at which IoT data is processed. For some IoT solutions, data are processed locally on a device. This is particularly true when IoT devices have fairly high processing power as in the case of edge-based solutions. In other solutions, data processing is highly distributed with data being shared with multiple platforms and applications for processing. Data processing can be completed by one or many isolated machines or a cluster of interconnected machines. The depth of data processing is related to the performance on each machine individually and on the cluster of machines. There are 3 options for the level of data processing.

Localized processing means that data are processed on-device. There are numerous reasons why data are processed on-device including mobile network bandwidth or coverage constraints; latency concerns; intensive data processing requirements; and data security concerns. For example, autonomous driving vehicles use localized, on-device data processing to handle driver and vehicle safety functions where communications latency could be an issue.

Data processing depth is the hierarchical layer where machine-related data is analyzed and acted upon

Centralized processing means that data are processed at a single location. In the case of centralized processing, an IoT platform processes data from one or more connected assets at a centralized location. Sometimes enterprises choose centralized data processing when there are security or privacy concerns associated with the collected IoT data or when the platform must support very high volumes of data generated by very low cost, low performance IoT endpoints. For example, a medium-sized enterprise might be running a fleet management solution to track its high value assets during transportation. This enterprise might choose to do all of its IoT data processing at a centralized location to keep the location of fleet cargo secure. Some enterprises have technology, business or regulatory requirements to keep data centralized, in-country or compliant. A well architected platform provides security across connectivity domains, hierarchical layers and northbound and southbound integrations.

Distributed processing means that data are processed on multiple devices and in multiple locations. This type of processing affords the most flexibility for an enterprise that wants to process and analyze IoT data. These data processing locations could be arranged in a geographic or logical hierarchy, allowing an enterprise like a water utility to process some data at a local pump room where a series of pumps are operating in tandem, other data at remote water system valves and water towers and aggregated data at a state or national level in its headquarter offices. In addition, distributed processing allows an enterprise to manage multiple IoT solutions with different architectures at multiple locations.

INTEGRATION TOPOLOGY

Integration topology is the relative closeness of the IoT platform to a customer's northbound business systems and peer platforms.

Integration topology is the third IoT platform design parameter. Enterprises can decide the relative closeness of the IoT platform to its northbound business systems (e.g., ERP, inventory management, trouble ticketing, CRM/SFA and others) and peer platforms (e.g., MES and SCADA platforms). An enterprise's decision on integration topology is based on various technology and business requirements. Sometimes an enterprise's decision is most strongly based on data privacy and security issues, while other times it is based on the current location of legacy industrial management systems. There are 2 options for the integration topology.

Adjacent location means that the IoT platform is located in the same geo-location or logical hierarchy as an enterprise's most relevant northbound business system or peer platform. Enterprises that choose an adjacent location for these systems often have data privacy or security issues associated with their solutions. It is also possible that enterprises wish to minimize the risks associated with latency or communications failures across the systems. For example, an electric utility might choose to keep its IoT platform adjacent to its ERP and trouble ticketing systems. This would minimize any risks associated with latency and communications failures. In addition, it would ensure that all machine data would be confined within the same facility to meet data privacy concerns.

Non-adjacent location means that the IoT platform is located in a different geo-location or logical hierarchy as an enterprise's most relevant northbound business system or peer platform. There are many reasons why an enterprise would choose non-adjacency of its platforms and systems. The most obvious reason would be to gain the cost benefits of having distributed data systems. Leading IoT platform vendors provide their solutions as multi-tenant cloud offerings, thereby passing on the savings they incur by having large relationships with cloud hosting companies. In cases where IoT machine data are not particularly sensitive and the risks of communications latency are small, enterprises are often comfortable with non-adjacency of their IoT and northbound systems. For example, a municipality with a connected street light solution might use a non-adjacent IoT platform. The risks of data privacy and security are minimal for the sensor data on connected street lights, while the cost savings of having a platform hosted in a multi-tenant vendor environment fits within a municipality's budget.

> Integration topology is the closeness of the IoT platform to northbound business systems and peer platforms

IOT USE CASE EXAMPLES

Throughout this research report MachNation has presented various IoT use-case examples and their IoT platform design parameters. An enterprise's unique business needs and limitations will dictate the enterprise's choice of IoT platform design parameters. That said, there are some general guidelines that MachNation can offer in the selection of an IoT platform architecture.

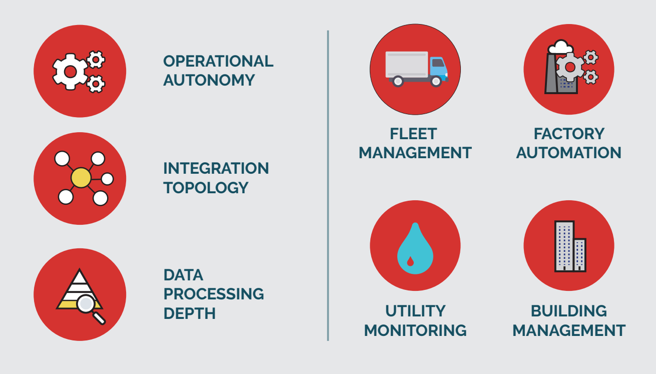
Mission critical systems. Some IoT solutions are linked to mission critical processes. Examples of these types of solutions include municipal water distribution monitoring, electricity management, first responder management, toxic chemicals manufacturing control and others. In these cases if systems fail, then vital human services can be interrupted having serious consequences.

For these types of mission critical solutions, MachNation would anticipate:

- multi-layer operational autonomy to allow IoT devices to control themselves while also allowing operational systems to control IoT devices
- distributed data processing to allow processing of device data on-device to minimize the intensive flow of data and at various hierarchical layers
- adjacent integration topology putting the IoT platform adjacent to northbound systems and peer platforms.

Consumable goods. Some IoT solutions are linked to consumer or business consumables. Examples would be products purchased through vending machines, single-use coffee refills (Nespresso) and customized soda flavor dispensers (Coca-Cola Freestyle). These IoT solutions often conduct once a day sensing/monitoring, send fairly low quantities of IoT data and are generally considered non-mission critical solutions. The IoT device collects data daily and consumables are reordered based on trending data. Oftentimes, an understanding of the trends in data are more important than the data at a single point in time.

FIGURE 4 IoT: Platform Design Parameters and Use Cases



For these types of mission critical solutions, MachNation would anticipate:

- non-autonomous or semi-autonomous control so the IoT device can alter the environment (e.g., temperature, humidity, etc.) in which the consumables are kept
- centralized data processing to allow processing of device data at one centralized facility to conduct trend analyses
- non-adjacent integration topology as putting the IoT platform adjacent to northbound systems and peer platforms is less important than in mission critical processes.

Low-power monitoring service. Some IoT solutions are linked to services using IoT devices powered by NB-IoT, LTE Cat M, LoRaWAN or Sigfox networks. A typical example would be a municipal street parking space detector. Each IoT device would have low power consumption, a long battery life, very little data transfer and fairly high reliability requirements. These IoT solutions would communicate sporadically throughout the day based on consumer usage. Communications would be almost exclusively upstream, although the device would need to be capable of receiving information occasionally for systems updates.

For these types of low-power monitoring services, MachNation would anticipate:

- non-autonomous control as low-power IoT devices have minimal processing power
- centralized data processing so all analyses are efficiently completed
- adjacent integration topology as providing relatively high up-time would be important for the functioning of the monitoring service.

IOT PLATFORM MANAGEMENT

Leading IoT platform vendors have the necessary capabilities to manage a distributed IoT platform architecture. These platform vendors have a set of technology tools, partners and services to manage the full lifecycle of each of the platform software components in the architecture including the scheduled distribution of continuously evolving analytics models. In particular, these vendors are able to advise in the upfront architectural design; provide the developer tools to manage device and platform deployment in proof-of-concept and full production modes; and offer tools to handle provisioning, de-provisioning, updates/upgrades of IoT devices on the platform at scale. In addition, the architectural requirements of an IoT platform can change over time: a leading IoT platform should be able to handle these changes with minimal to no interruptions to an enterprise. For example, a typical fleet management solution might start with a fairly simple architecture with centralized processing and non-autonomous control, but as the enterprise adds additional use cases like in-vehicle refrigeration control with on-board user interfaces, the IoT platform will have to seamlessly support localized processing and fully autonomous control. A leading IoT platform can manage all these distributed architectural requirements for an enterprise customer.

CONCLUSION

There is much literature on choosing high quality IoT platform vendors for an IoT deployment, but practical guidance on deploying IoT platforms is lacking in the market. This analyst insight article presents a structure that enterprises can use when specifying the design parameters for an IoT platform architecture. There are myriad considerations and limitations that impact IoT platform architecture. Enterprises need to find quality IoT platform vendors that deeply understand the ways to support an IoT platform efficiently and provide for future growth potential.

Enterprises should choose IoT platform vendors that can supplying the broad range of design parameters described in this analyst insight article. Specifically, leading IoT platform vendors should be able to help enterprises specifying their level of operational autonomy, depth of data processing and integration topology required in their IoT solution deployments. In addition, IoT platform vendors should be able to provide multiple examples of current customers that have already deployed these architectures. By providing this practical advice, IoT platform vendors can ensure success for their enterprise customers, minimize deployment risks and smooth the way for addition of new applications to an IoT solution.

For more information about IoT platform architecture, please contact MachNation at info@machnation.com.

BROUGHT TO YOU BY SOFTWARE AG

With over 10,000 customers in over 70 countries, Software AG is an enterprise software company headquartered in Darmstadt, Germany. Software AG, with 2016 revenue of EUR 872 million, offers its solutions and services to enterprises, service providers and the public sector. The Software AG IoT solution is based on the 2017 acquisition of Cumulocity, a Düsseldorf-headquartered Nokia Siemens Networks spin-off. Software AG focuses its growth of Cumulocity IoT on direct and indirect sales by providing its distributed IoT platform across cloud, on-premises and edge deployments. Cumulocity IoT is frequently white labeled or embedded into broader services from companies such as Deutsche Telekom, Siemens and Gardner Denver.

For more information please see www.softwareag.com/iot.

MachNation is the only insight services firm exclusively dedicated to covering the future of Internet of Things (IoT) middleware, platforms, applications and services. MachNation specializes in understanding and predicting these technology sectors including their impact on digitization, hardware, communication services and support tools. MachNation specialists have provided guidance to the majority of the world's leading IT and communications firms.

www.machnation.com