VMWare Launch – Edge & IoT

WELCOME!

Develop Intelligence

Allen R. Sanders
Senior Technology Instructor

Join Us in Making Learning Technology Easier

Our mission…

Over 16 years ago, we embarked on a journey to improve the world by making learning technology easy and accessible to everyone.

…impacts everyone daily.

And it's working. Today, we're known for delivering customized tech learning programs that drive innovation and transform organizations.

In fact, when you talk on the phone, watch a movie, connect with friends on social media, drive a car, fly on a plane, shop online, and order a latte with your mobile app, you are experiencing the impact of our solutions.

Over The Past Few Decades, We've Provided

Over **62,300,000** expert-led learning hours

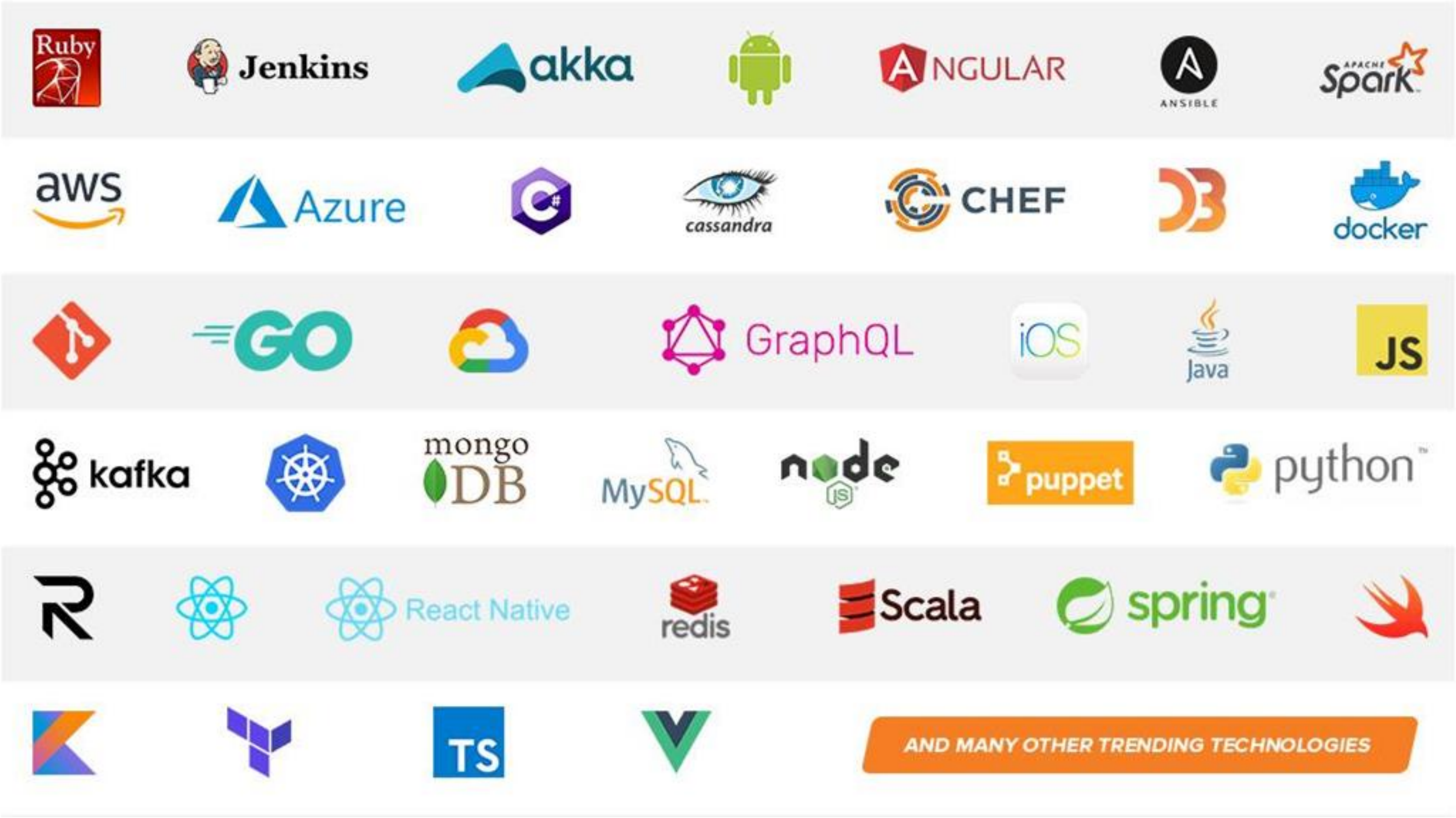
In 2019 Alone, We Provided

Training to over **13,500** engineers

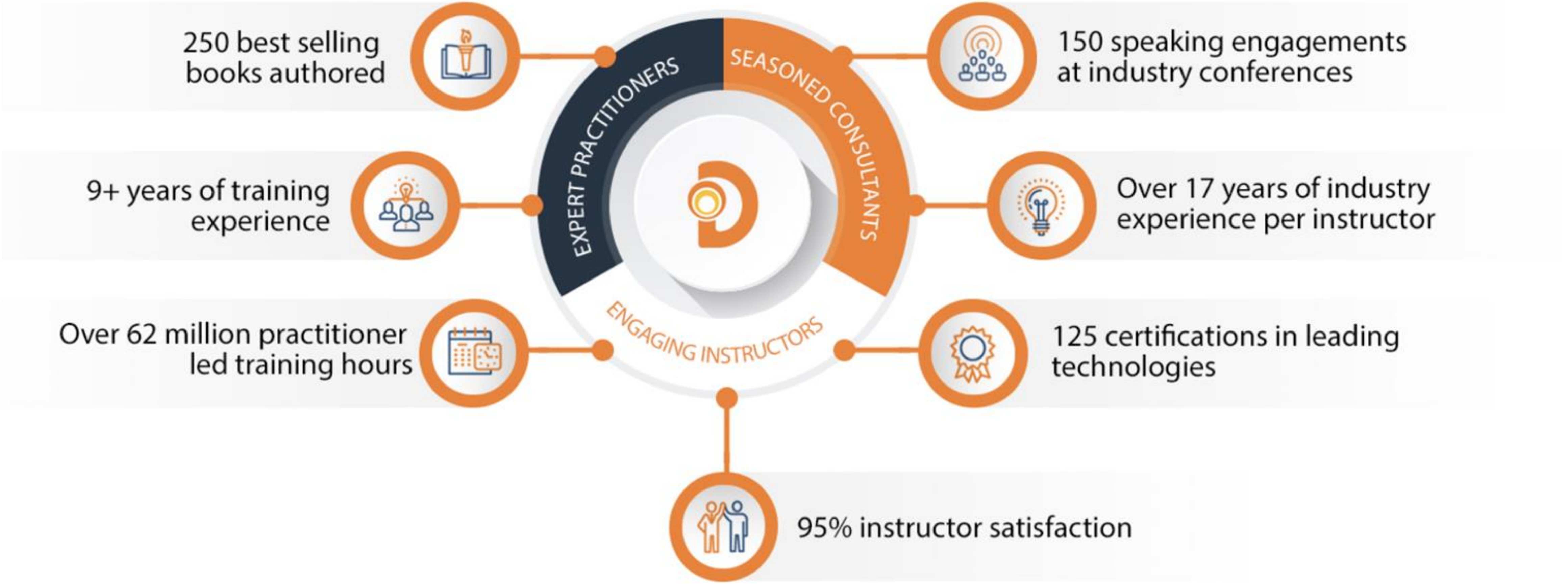
Over **120** active trainers, with an average of over two decades of experience each.

Programs in **30** countries

Technologies we cover



World Class Practitioners



250 best selling books authored

9+ years of training experience

Over 62 million practitioner led training hours

150 speaking engagements at industry conferences

Over 17 years of industry experience per instructor

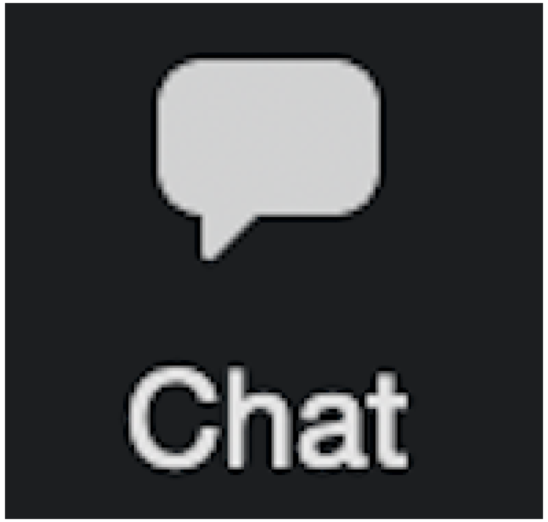
125 certifications in leading technologies

95% instructor satisfaction

Virtual Training Expectations for You

Arrive on time / return on time

Mute unless speaking



Use chat or ask questions verbally

Virtual Training Expectations for Me

I pledge to:

- Make this as interesting and interactive as possible
- Ask questions in order to stimulate discussion
- Use whatever resources I have at hand to explain the material
- Try my best to manage verbal responses so that everyone who wants to speak can do so

Quick review of key Zoom features that may be helpful for our course

Purpose

- ➢ Exposure to key Edge & IoT concepts including:
  - Edge & Fog computing
  - Device management
  - Data management
  - Security & compliance
  - Gaining intelligence from data
  - Operational support considerations

Objectives

Upon completion of this course, you should be able to:

- Describe foundational Edge & IoT concepts
- Understand how Edge & IoT strategies enable delivery of critical business systems
- Identify potential technical challenges encountered when building out an Edge / IoT solution and explore options for remediating

Let’s Get to Know One Another

Tell me about you:

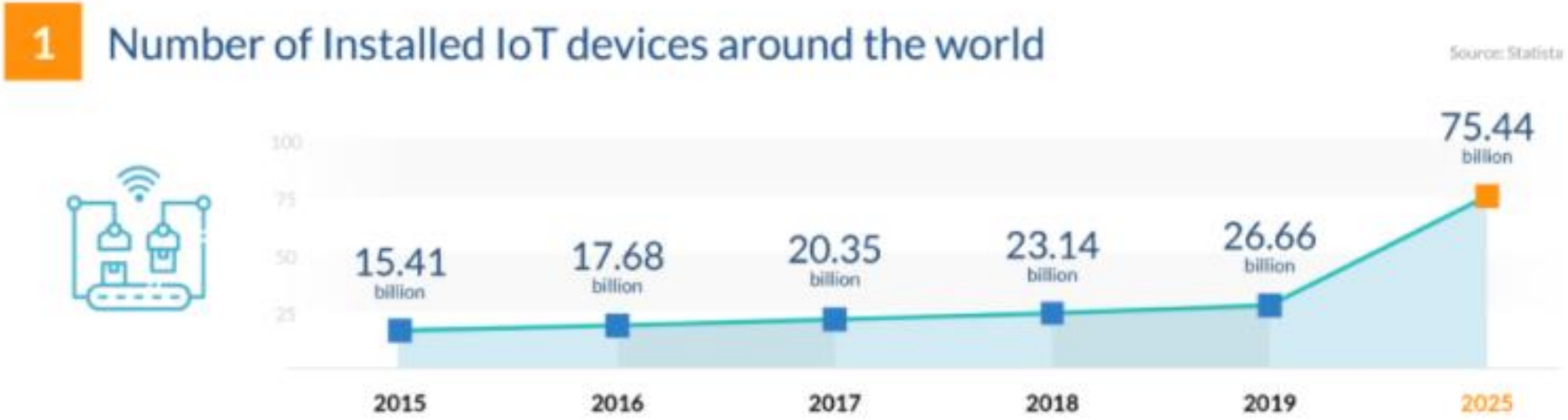
- Name
- Current role
- How long you’ve been at the company
- What’s one thing you’re hoping to get out of this course?

I’ll tell you a little about me…

Introduction

Industry Trends

From https://financesonline.com/iot-trends



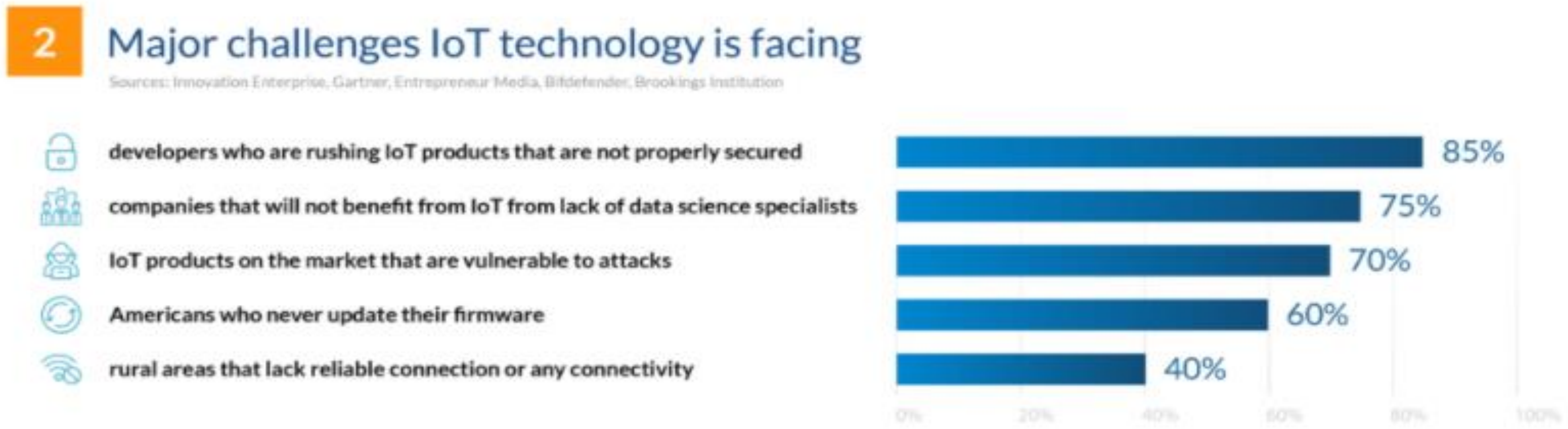
1 Number of Installed IoT devices around the world

Source: Statista

Challenges potentially encountered with that amount of projected growth?

Industry Trends

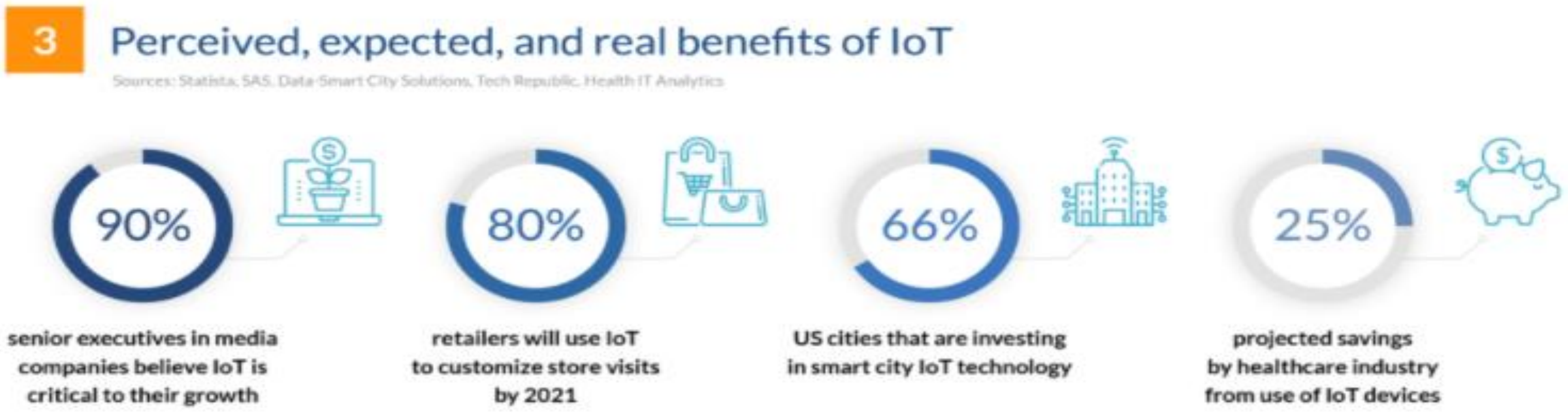
From https://financesonline.com/iot-trends



Options for mitigating those challenges?

Industry Trends

From https://financesonline.com/iot-trends



3 Perceived, expected, and real benefits of IoT

Sources: Statista, SAS, Data-Smart City Solutions, Tech Republic, Health IT Analytics

90%

senior executives in media companies believe IoT is critical to their growth

80%

retailers will use IoT to customize store visits by 2021

66%

US cities that are investing in smart city IoT technology

25%

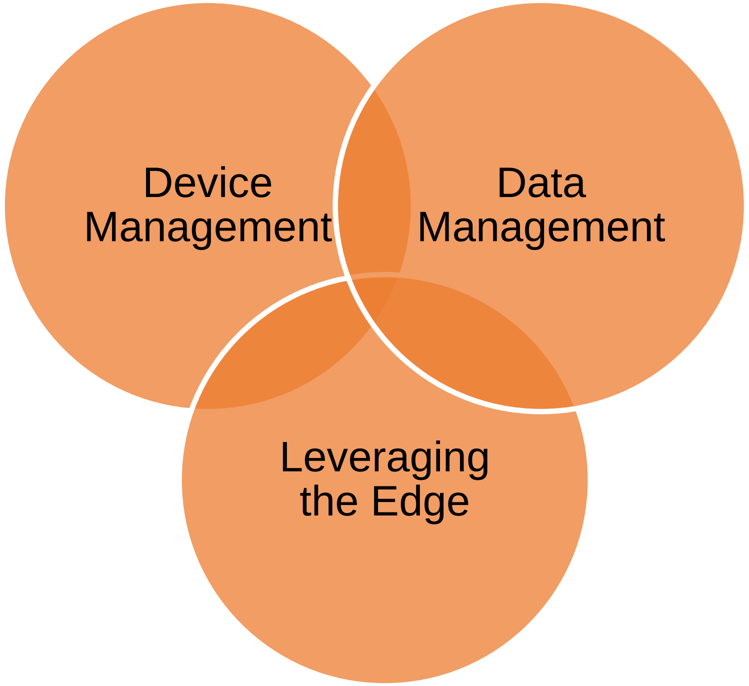
projected savings by healthcare industry from use of IoT devices

How do we help customers realize those benefits?

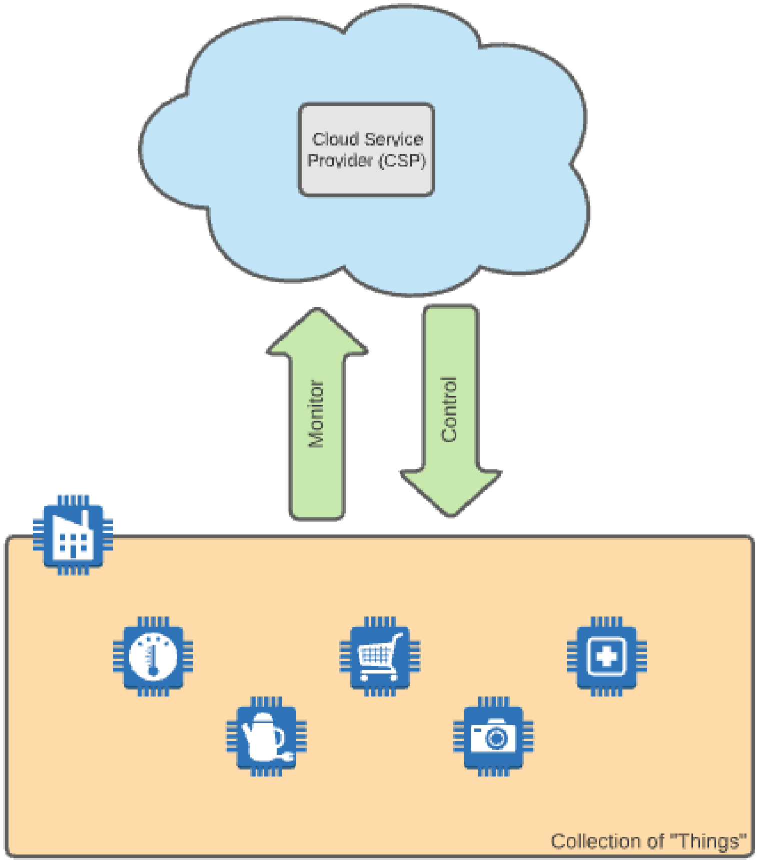
Industry Trends

Areas of focus:

- Accommodating orders of magnitude of growth
- Preventing known (or unknown) challenges from impeding success
- As a business, effectively leveraging opportunities to meet customer needs



Cloud-Centric IoT (CIoT)



Potential issues with this type of architecture?

Cloud-Centric IoT (CIoT) – Potential Issues

Bandwidth

- Data size
- Data frequency

Latency

- Impact of processing delays
- Inability to react in “real-time”

Need for “Always On”

- Long transmission distances
- Intermittent network connectivity

Resource Constraints

- Not enough on-device power for processing complexity
- End-to-end transmission consumes precious energy

Security

- Sometimes remote and outside
- Insufficient on-device capability to prevent service interruption or data “spoofing”

Fog & Edge Computing

At its simplest, involves the injection of intermediate components:

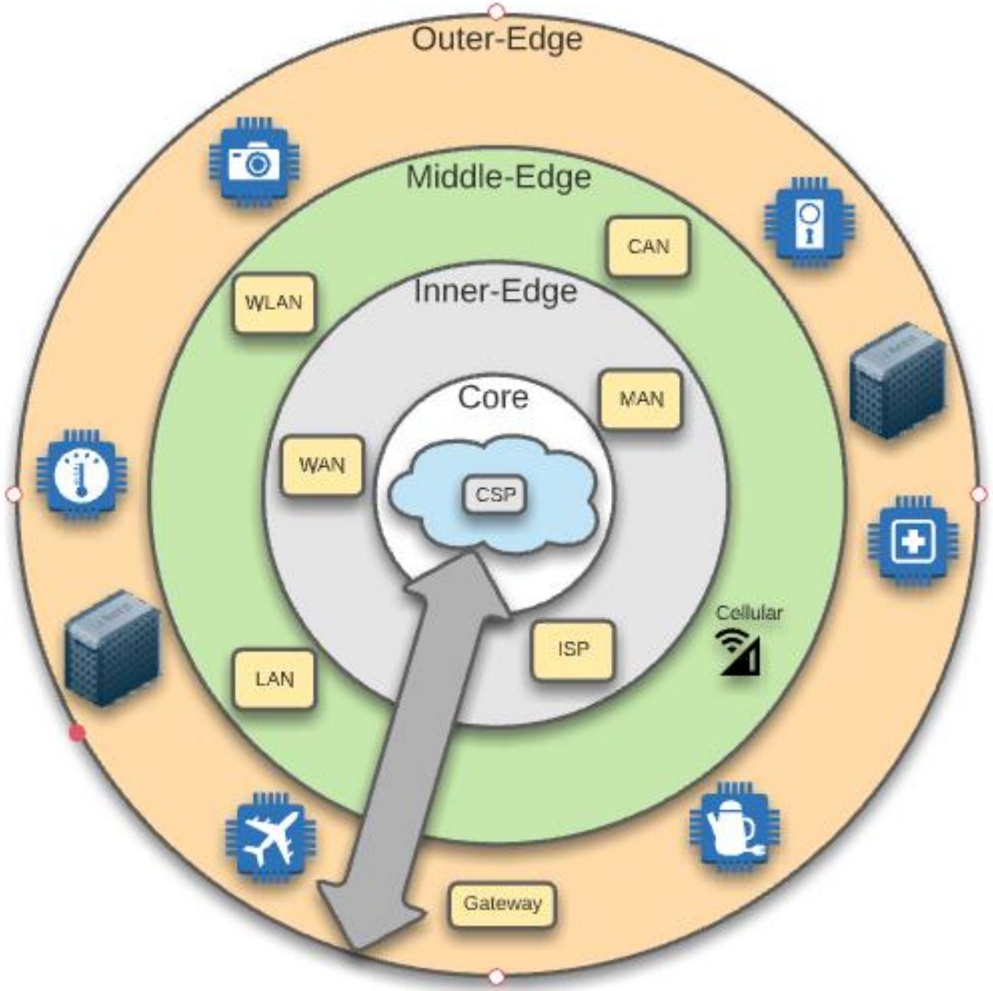
- Bring more power closer to the “things”
- Offload processing
- Optimize what gets transmitted
- Caching to remediate intermittent connectivity issues
- Supplement with additional layers of security

Fog & Edge Computing

Can include three distinct layers:

- Inner or near edge
- Middle edge
- Outer or far edge

Fog & Edge Computing – Layers



CSP – Cloud Service Provider
WAN – Wide Area Network
ISP – Internet Service Provider
MAN – Metropolitan Area Network
LAN – Local Area Network
WLAN – Wireless Local Area Network
CAN – Campus Area Network

Fog & Edge Computing – Advantages

Security

Cognition

Agility

Latency

Efficiency

Fog & Edge Computing – S.C.A.L.E.

Security:

- Additional layers of protection
- Can support security patches to devices in remote areas
- Improves speed with which patches can be applied

Fog & Edge Computing – S.C.A.L.E.

Cognition:

- More processing power closer to the device
- Means more sophisticated decision-making (“smart devices”)
- Can include components that enable self-healing
- Provides options for even simplest of “things”

Fog & Edge Computing – S.C.A.L.E.

Agility:

- Provides additional “levers” for configuration and operation
- Enables commoditization of intermediate layer capabilities
- Supports reuse of open software interfaces and SDK’s

Fog & Edge Computing – S.C.A.L.E.

Latency:

- Improves speed of response to and from the “things”
- Optimizes communications by localizing aggregation and processing
- Data travels faster over shorter routes

Fog & Edge Computing – S.C.A.L.E.

Efficiency:

- Caching and batching can improve overall performance
- Data analysis can be completed closer to the device
- Can generate results faster by execution closer to the data source
- Cloud communication still available but data transmitted can be filtered

How Are Advantages Realized?

Storage

- Data caching & temporary storage
- Data stability & consistency even with network “blips”

Compute

- Hardware & software for localized execution of logic
- Multiple hosting options (including containerization)

Acceleration

- Networking acceleration – network virtualization and software-defined network (SDN)
- Computing acceleration – vertical and horizontal scaling

Networking

- Vertical networking – efficient communication across the edge layers
- Horizontal networking – efficient communication within the edge layers

Control

- Control over deployment
- Control over device behavior & configuration
- Control over management of disparate protocols
- Control of security

Case Study

Case Study is focused on modernization and digitization of an in-home nursing assistance service. Current state:

- Service maintains in-home care with in-person, routine visits every 4 days
- ~400 patients within a 125-mile radius of a major metropolitan area
- Routine visits include checking vitals, delivery of medication, and, in some cases, special care
- Average age of patients is 71+ years old
- Patients will not be able to administer any IT infrastructure installed in the home
- Network connectivity can be inconsistent at times with intermittent, temporary drops
- Historical data tracking is important to assess quality of patient care and identify potential improvements
- HIPAA regulations (health privacy) dictate a need for responsible stewardship of the data

✓ What questions would you ask to gain additional requirements information?

✓ If you were going to implement an Edge/IoT solution for this case study, what major software/hardware components might you include?

✓ What kind of challenges do you anticipate encountering with implementation? What are some key things to “keep in mind”?

Device Management

Device Management

Device Management

- To be secure, IoT systems must manage all points of data ingress and egress
- Unknown devices should remain restricted
- Need a repeatable process for onboarding/offboarding devices

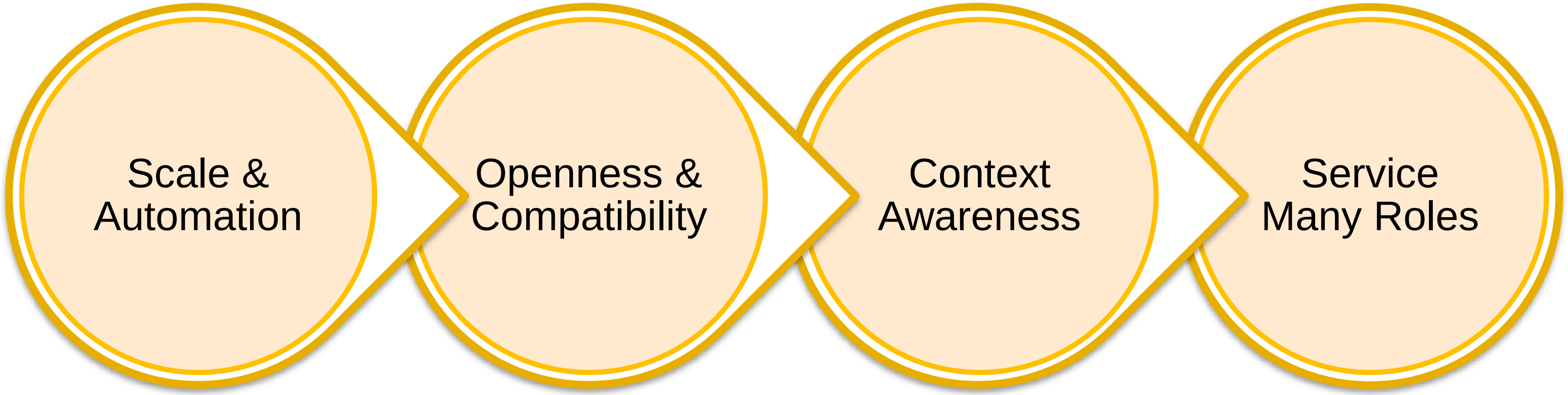
Device Management

- In addition to onboarding, mechanisms for device maintenance required
- Firmware updates, security patches, reboots/resets
- Supported by a structured lifecycle

Device Management

- In many cases, must accommodate hundreds or thousands of devices
- May include devices located miles away or in remote areas
- Means manual configuration not always feasible

Principles



Scale & Automation

Openness & Compatibility

Context Awareness

Service Many Roles

Scale & Automation

- Keep human-to-device ratio cost effective (bulk processing)
- Automate as much as possible
- Enable secure remote management techniques over distance

Openness & Compatibility

- Device ecosystem includes multiple variants
- Can include different profiles, platforms, and protocols
- Requires strategies that:
  - ➢ Can accommodate the variants
  - ➢ Unify where possible from reporting and support perspectives

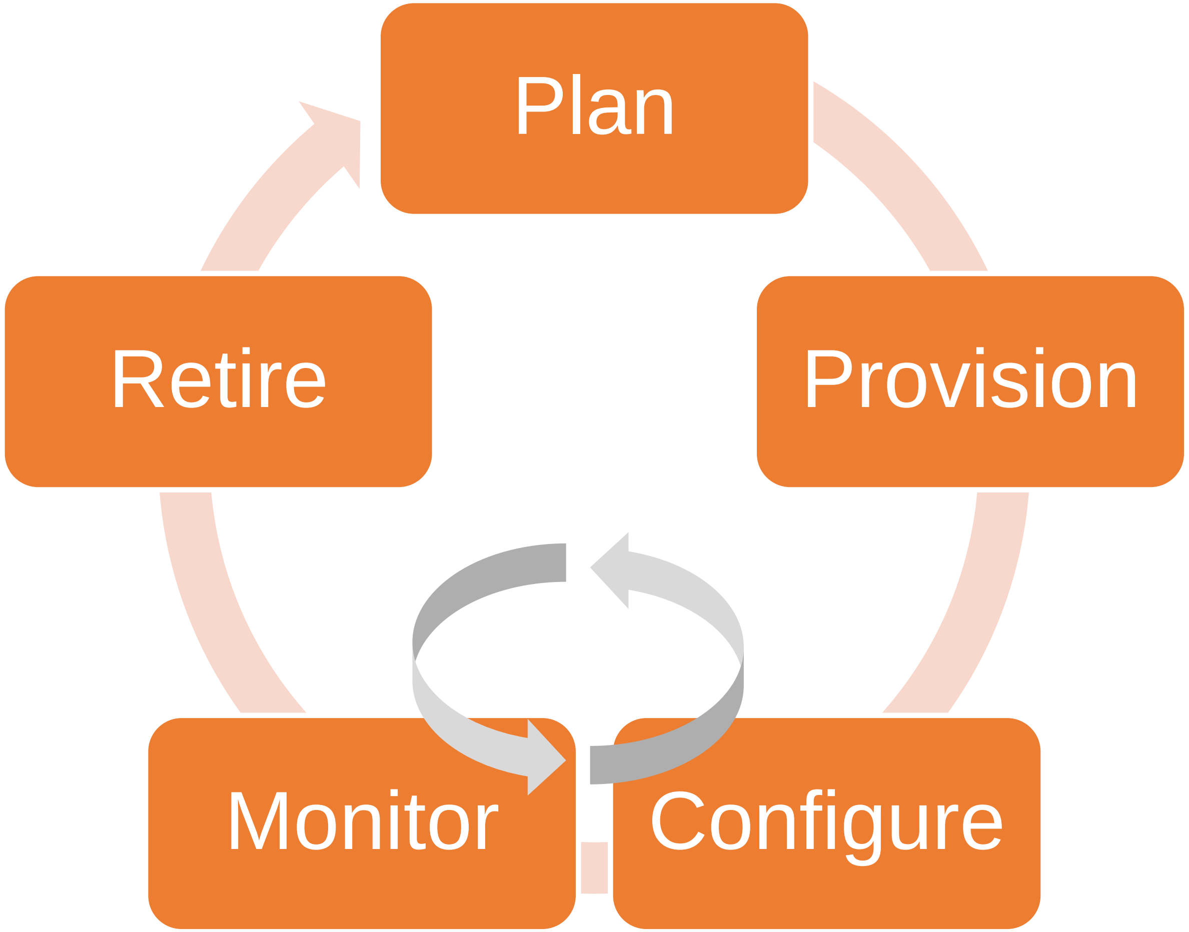
Context Awareness

- IoT environments need to maintain awareness of critical factors like:
  - SLAs for maintenance windows
  - Network and power states
  - Geo-location information (in some applications)
- In some systems, lack of awareness can be damaging or dangerous

Service Many Roles

- Operational support requirements must be understood
- Reporting & dashboarding are key
- Need ways to tailor detail to different types of stakeholders

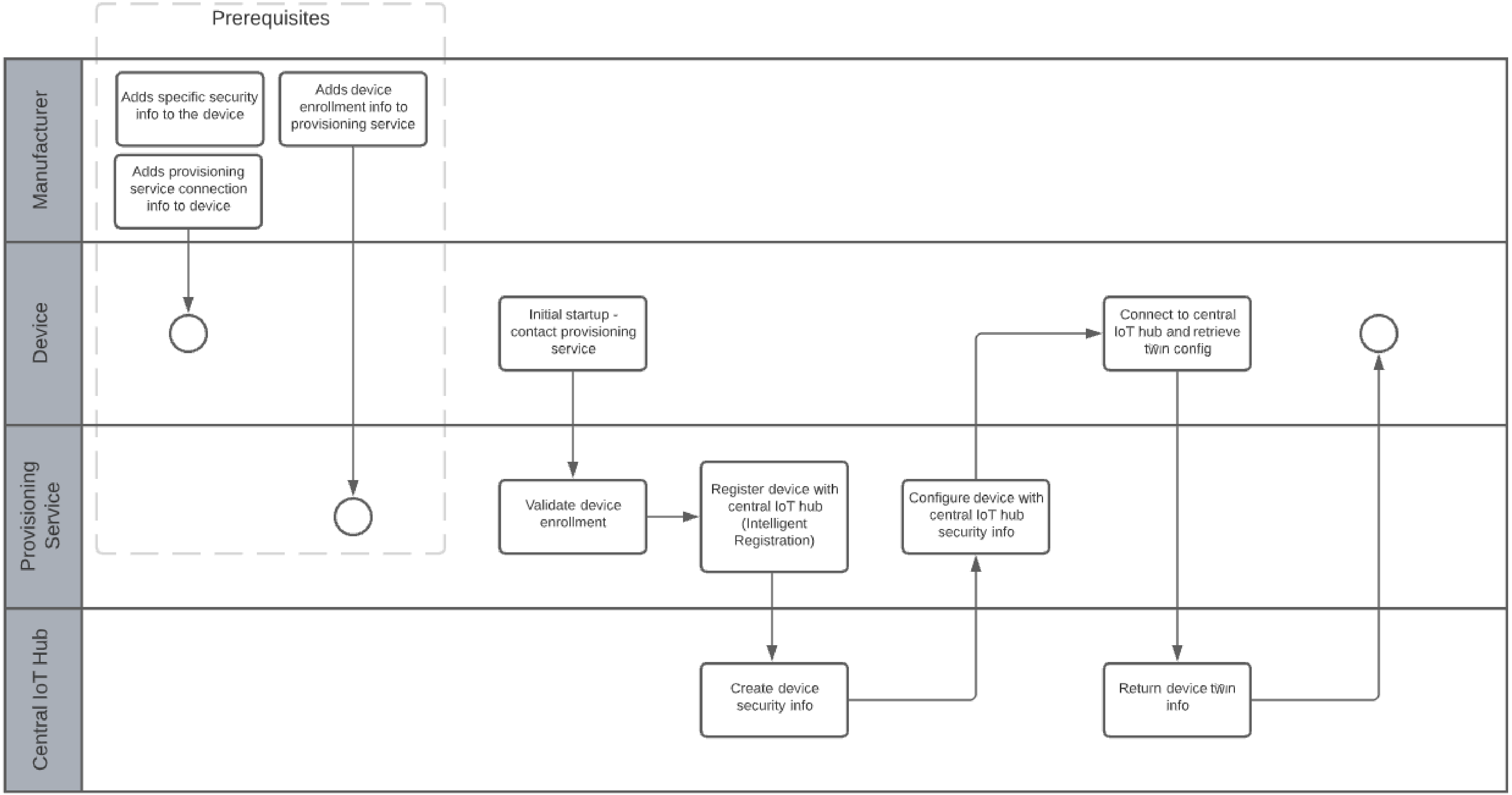
Device Lifecycle



Device Planning

- Develop strategies for grouping of devices for bulk operations
- Understand how device will be utilized
- Understand context awareness requirements

Device Provisioning


Prerequisites
Manufacturer
Device
Provisioning Service
Central IoT Hub
Adds specific security info to the device
Adds device enrollment info to provisioning service
Adds provisioning service connection info to device
Initial startup - contact provisioning service
Connect to central IoT hub and retrieve twin config
Validate device enrollment
Register device with central IoT hub (Intelligent Registration)
Configure device with central IoT hub security info
Create device security info
Return device twin info

Central IoT Hub – Device Registration

- Various strategies can be used to assign a device to a hub:
  - Lowest latency (geographically closest)
  - Evenly weighted distribution
  - Static configuration (e.g., assignment based on device grouping)
  - Custom logic

Device Twins

- Provides digital representation of a physical device
- Synchronized to the central IoT hub
- Enables awareness of device in Cloud without constant interaction

Device Twins

- Utilizes “desired” properties to push configuration from Cloud to device
- Utilizes “reported” properties to communicate info from device to Cloud
- Enables config sync between back-end and device

Device Twins

- Examples include:
  - ➢ Use of twin by Cloud to communicate frequency updates to device
  - ➢ Use of twin by device to report on status of requested updates
  - ➢ Use of twin by Cloud to query device state
  - ➢ Use of twin by device to report status of long-running ops (e.g., firmware updates)

Device Configuration

- Enable bulk configuration updates, including firmware upgrades
- Maintain health of device and data
- Execute securely – configuration validation

Device Monitoring

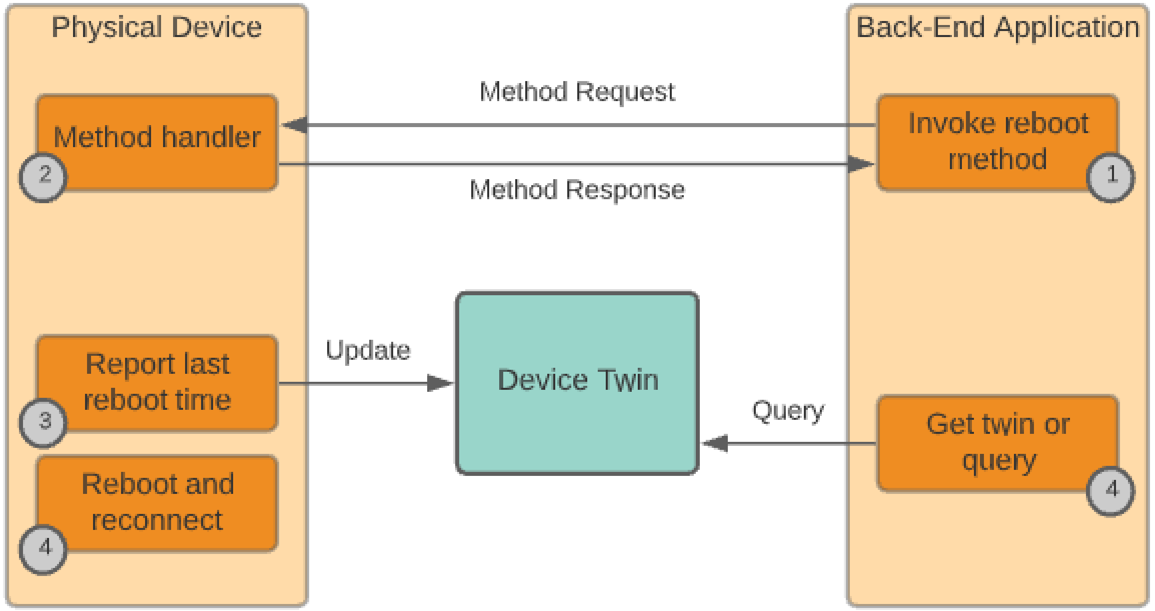
- Monitor:
  - Device health
  - Status of in-process operations (e.g., firmware upgrades)
  - Alerts for issues to be reported and remediated
- Reporting/dashboarding

Device Retirement

- Replacement for failed devices
- Device upgrades at end of service lifetime
- Can leverage device twin for transferring config to replacement
- Alternatively, can archive twin if not being replaced

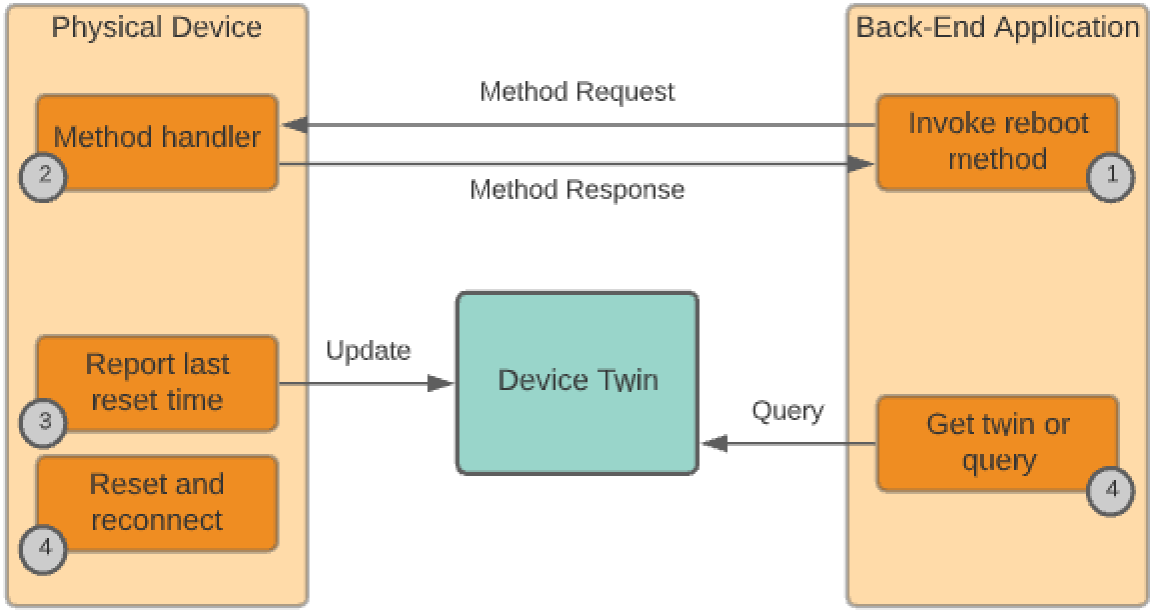
Device Management Patterns

Reboot



Device Management Patterns

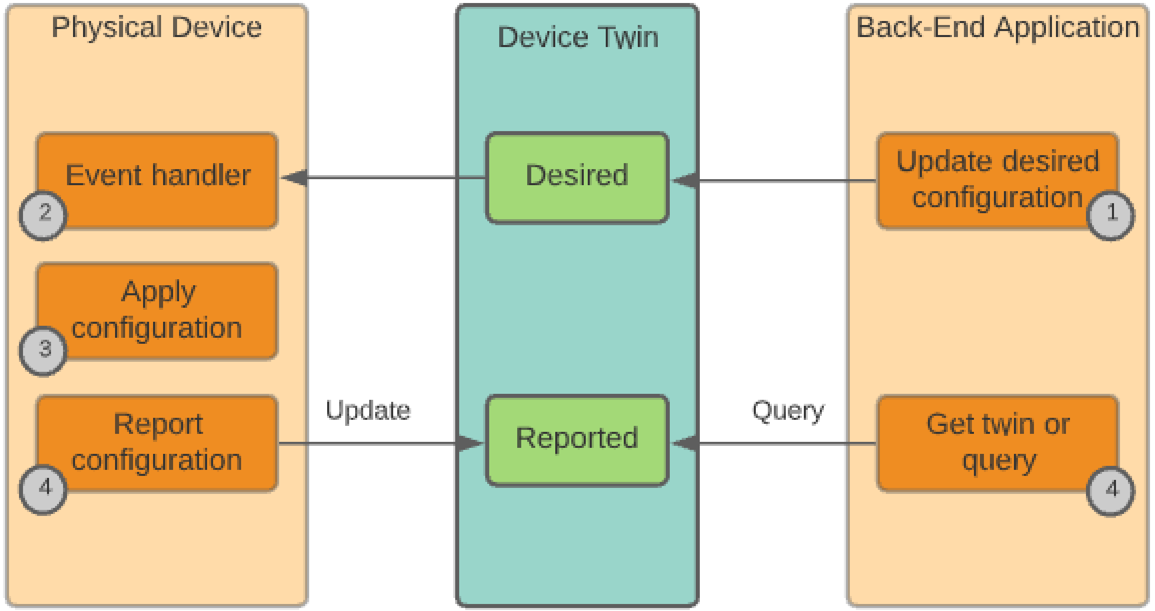
Factory Reset



Device Management Patterns

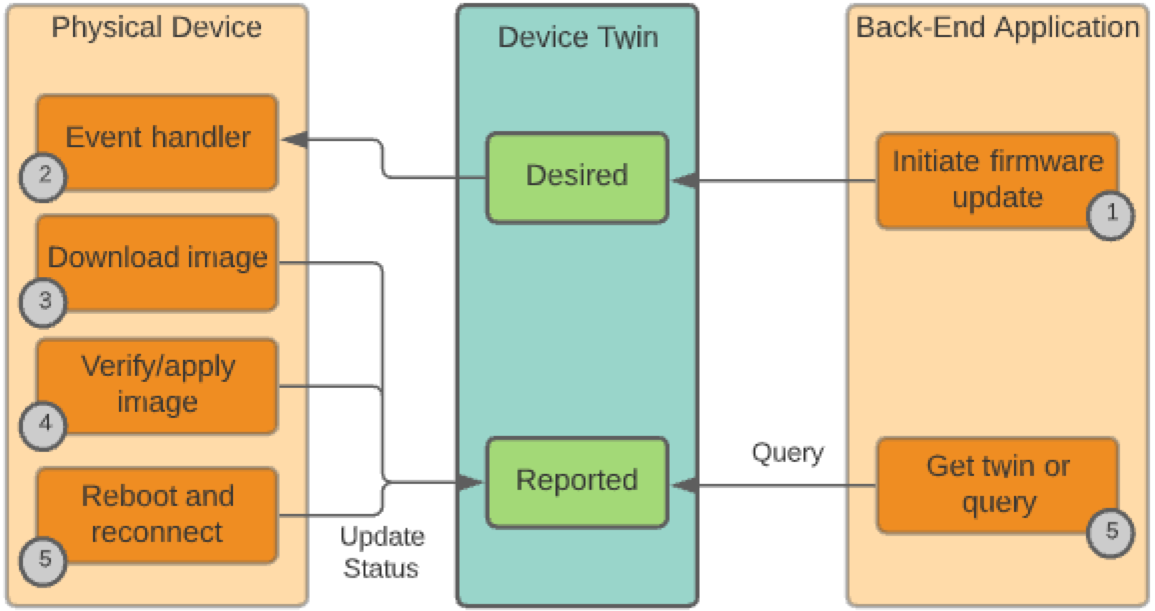
Develop Intelligence

Configuration



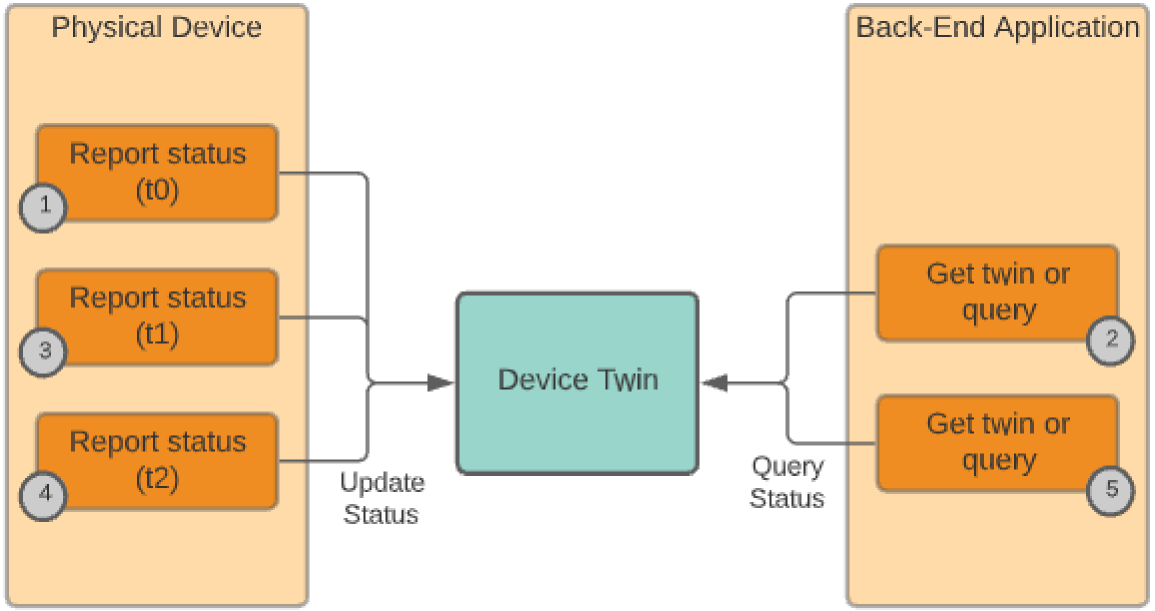
Device Management Patterns

Firmware Update



Device Management Patterns

Progress & Status



Case Study

Your team has been hired to design and implement an autonomous vehicle powered by Edge & IoT. High-level requirements are as follows:

- Standard routes must be supported – point A to point B
- Turns, lane changes, regular traffic stops must occur safely
- If weather forecast for an area the vehicle is about to enter indicates treacherous driving conditions, the vehicle should automatically adjust in speed, stopping distance, etc.
- If the vehicle is approaching an area where there is significant construction, the vehicle should find an alternate, more efficient route but must confirm with the user before switching to it
- The user should be allowed to take control of the vehicle at any time
- Information about miles, speeds, maneuvers, weather conditions, and road conditions should be aggregated to a central location for analysis and Machine Learning to foster continuous improvement in safety and utility

✓ What major software/hardware components would you consider including?
✓ What would be the "devices" in this scenario?
✓ What would device registration, configuration, monitoring, and retirement look like in this scenario from an Edge/IoT perspective?

Demo

Device Telemetry

- Represents the device payload (e.g., temperature/humidity readings)
- Usually time series-based or event driven
- Can also include streaming data (e.g., video feeds over time)
- Based on number of devices and/or rate, can result in massive amounts of data

Device Telemetry

- Transmission may utilize one of multiple protocols (depending on platform):
  - HTTP
  - MQTT (Message Queuing Telemetry Transport)
  - AMQP (Advanced Message Queuing Protocol)
- Depending on application, payload may require translation
- For example, binary format to JSON or proprietary to common standard

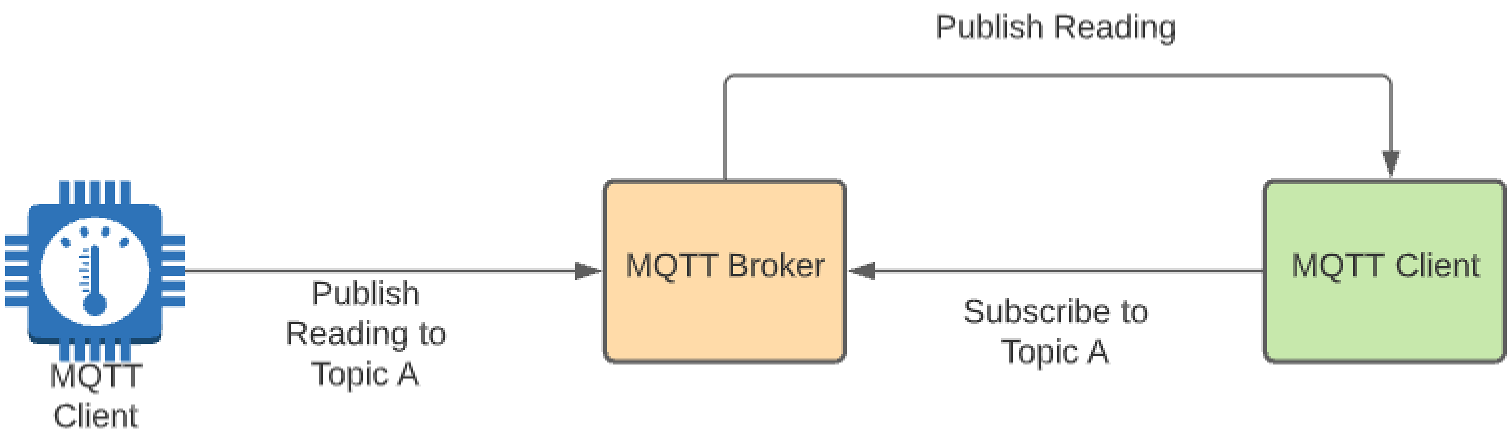
MQTT Protocol

- Lightweight publish/subscribe transport protocol
- Requires small code footprint
- Message size optimized to preserve network bandwidth

MQTT Protocol

- Supports bidirectional communication (D2C & C2D)
- Mechanisms for reliable message delivery built in
- Can accommodate unreliable networks through persistent sessions

MQTT Protocol



AMQP

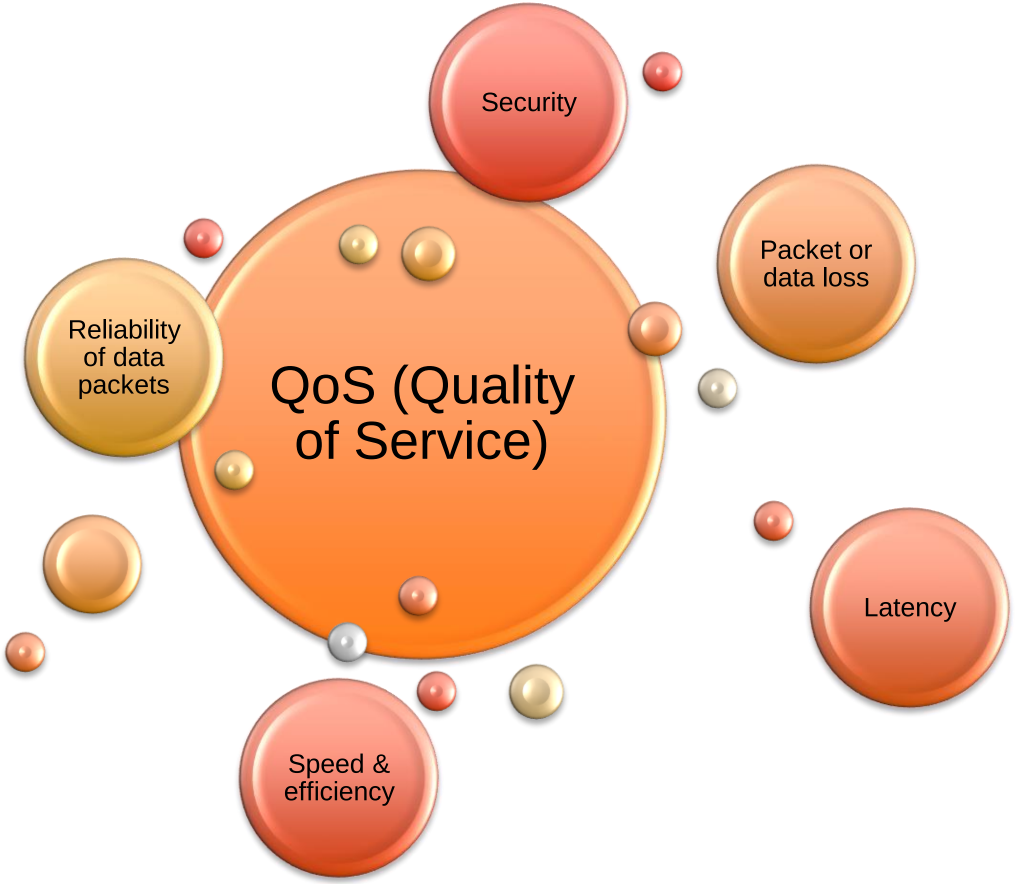
- Peer-to-peer protocol for message exchange
- Does not require broker in middle
- Open source vs. vendor driven
- More powerful (but also “heavier”) than MQTT

MQTT vs. AMQP

MQTT	AMQP
Simpler	More sophisticated
Mostly vendor-driven	Open source and customer-driven
Simple publish-subscribe	Multiple message exchange options
Non-transactional	Transactional
Exclusively broker-based	Peer-to-peer
Smaller footprint	Larger footprint
Better fit for resource-constrained integrations	Better-fit for more complex integrations

MQTT Protocol – Drilldown

With IP based protocols (TCP or UDP), generally concerned with:

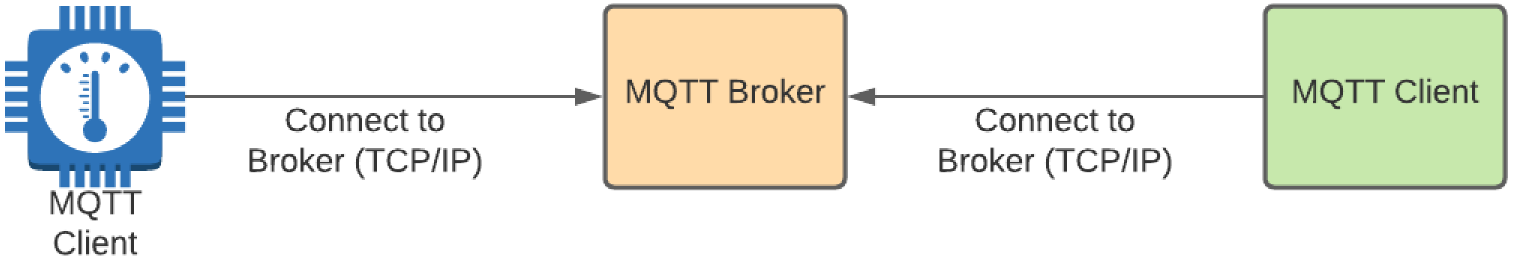


MQTT Protocol – Drilldown

- Publish/subscribe (aka pub/sub) helps promote reliability in message exchange
- Intermediate broker helps manage the exchange
- Keeps sender/receiver loosely coupled to one another
- MQTT includes support for QoS configuration as well

MQTT Protocol – Broker Connection

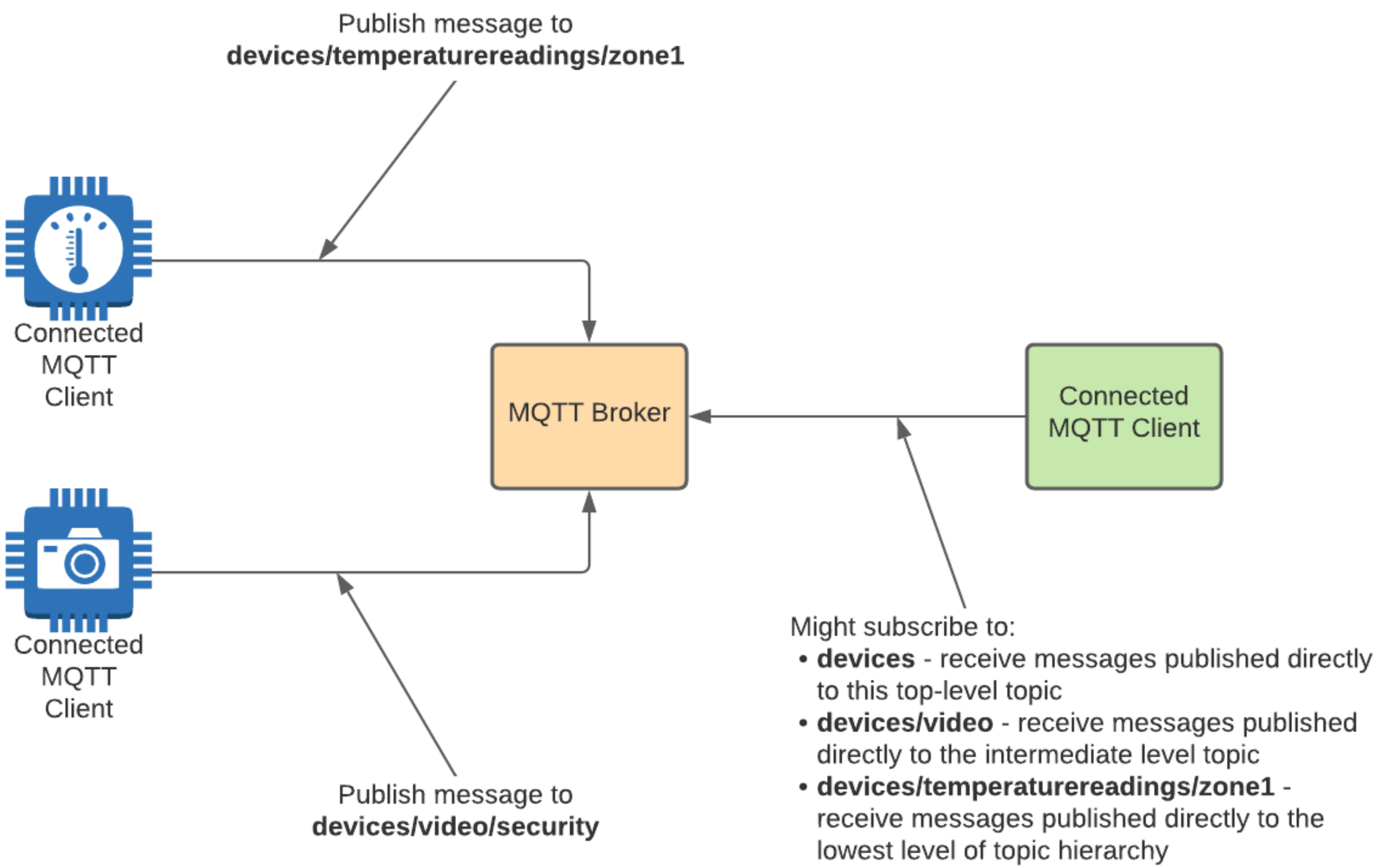
First step to enabling pub/sub integration:



MQTT Protocol – Topics

- Messages are transmitted with MQTT using topics
- Topic is a case-sensitive name that defines a “bucket” for message data
- Supports hierarchical organization of “bucket” names
- Can publish or subscribe to specific “bucket” along the hierarchy
- Also supports wildcards for subscribers

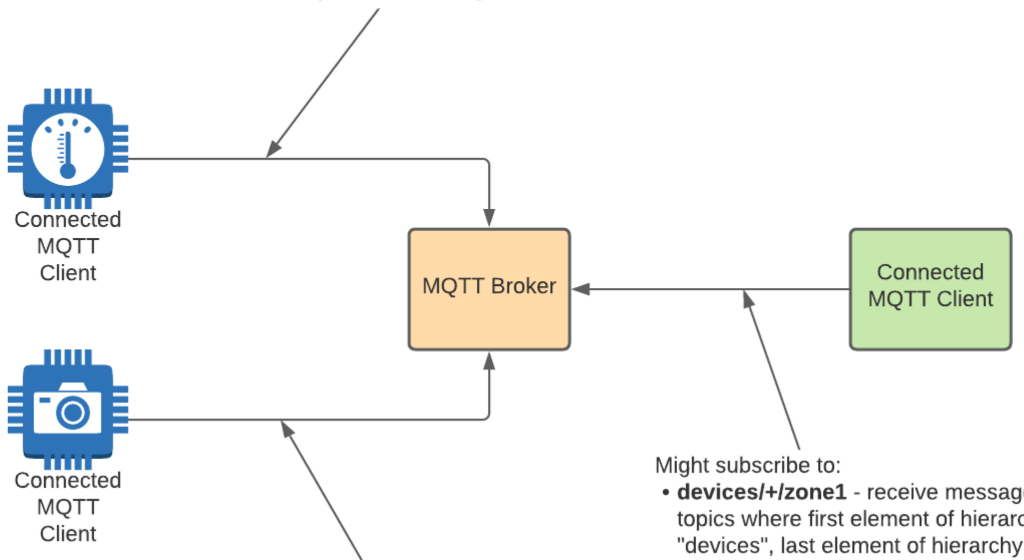
MQTT Protocol – Topics



Might subscribe to:

- **devices** - receive messages published directly to this top-level topic
- **devices/video** - receive messages published directly to the intermediate level topic
- **devices/temperaturereadings/zone1** - receive messages published directly to the lowest level of topic hierarchy

MQTT Protocol – Wildcard Topics



Publish message to **devices/temperaturereadings/zone1**

Publish message to **devices/video/security**

Might subscribe to:

- **devices/+/zone1** - receive messages from topics where first element of hierarchy is "devices", last element of hierarchy is "zone1", and matching to any intermediate named topic (e.g., would match messages published to both **devices/temperaturereadings/zone1** and **devices/video/zone1**)
- **devices/temperaturereadings/#** - receive messages published to that level of subtopic and any additional subtopics (e.g., would match messages published to **devices/temperaturereadings/zone1**, **devices/temperaturereadings/zone2**, and **devices/temperaturereadings/zone1/aisle1**)

MQTT Protocol – Wildcard Topics

- Be wise about the use of wildcard topics
- Otherwise, potentially run the risk of large volumes of message “noise”
- Subscriber may be required to filter out several unnecessary messages

MQTT Protocol – Wildcard Topics

- Also puts additional strain on broker
- Be as specific and as targeted as possible with messaging
- Balance against convenience of wildcards for relevant use cases

MQTT Protocol – Message Structure

- Every MQTT message packaged within a “control packet”
- Like an envelope that contains context and data for a message
- Focus is on keeping message compact – max 260 MB (but most are smaller)

MQTT Protocol – Message Structure

- Control packet includes:
  - Fixed header – required; includes packet type and size info
  - Variable header – optional; includes protocol info and may include auth credentials
  - Payload – optional; may contain message data

MQTT Protocol – Control Packet Types

- Control packet types include:

Type	Transmission Direction	Purpose
CONNECT	Client to Server	First packet sent from client after establishing connection
CONNACK	Server to Client	Acknowledgment of CONNECT
PUBLISH	Client to Server, Server to Client	Transmit new message
SUBSCRIBE	Client to Server	Requesting subscription to one or more topics
UNSUBSCRIBE	Client to Server	Unsubscribe from one or more topics
DISCONNECT	Client to Server	Indicates clean disconnect from server

- There are others primarily utilized with QoS levels

MQTT Protocol – QoS Levels

- Available Quality of Service levels in the protocol:
  - QoS 0 – Fire and forget; no attempt made by sender to retry
  - QoS 1 – At least once; sender retries until receiver sends PUBACK control packet
  - QoS 2 – At most once; at protocol level, series of control packets exchanged to ensure delivery without duplication
- Be aware – not all target platforms will support

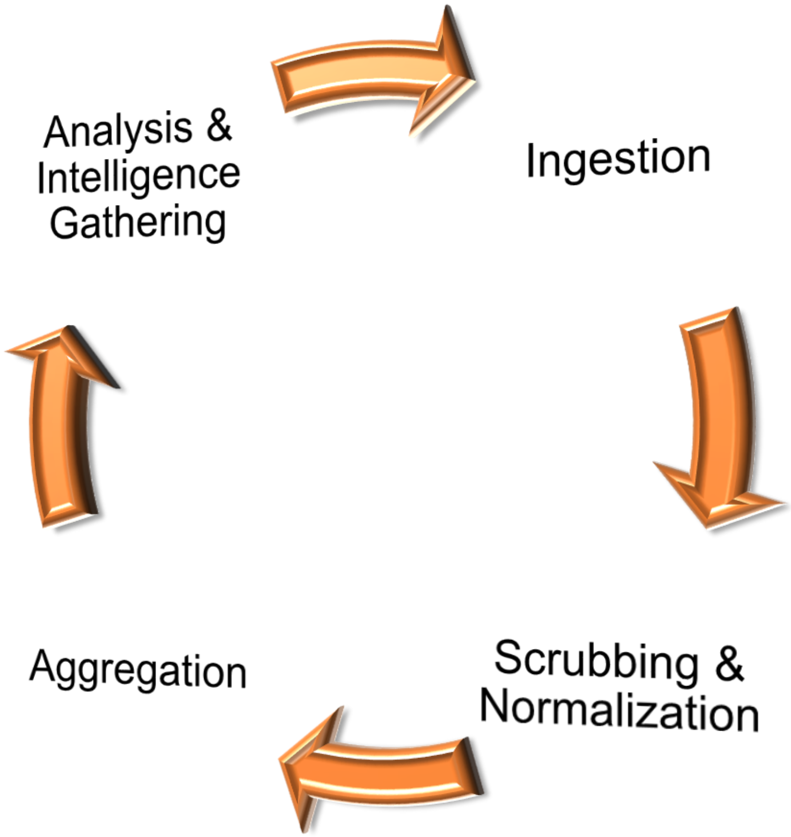
MQTT Protocol – Libraries

- Multiple utility libraries available to facilitate MQTT connectivity
- Supports multiple platforms and languages
- Insulates from many of the low-level details of MQTT

Demo

Data Management

Data Management – Stages



Ingestion

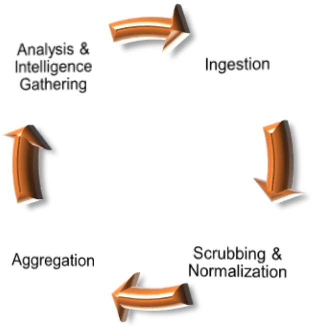
Scrubbing & Normalization

Aggregation

Analysis & Intelligence Gathering

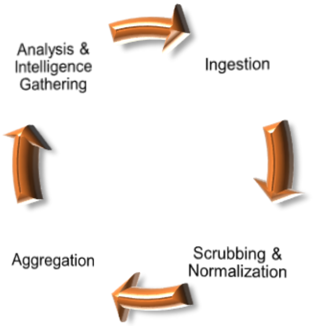
Data Ingestion

- Includes telemetry information previously discussed
- Could be via message exchange or streaming
- Depending on size/scope, may translate to LARGE amounts of incoming data



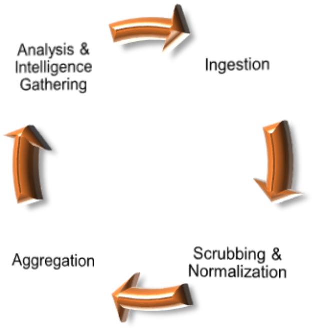
Data Ingestion

- Because of potential scale, bandwidth may be a concern
- Depending on application, latency may also be a concern
- Data may require translation (e.g., from low-level bytes to object or JSON)



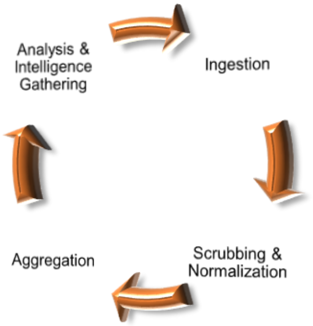
Data Ingestion

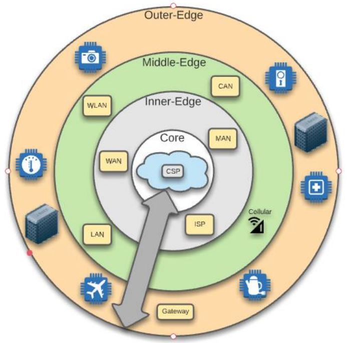
- Event hubs or streaming analytics platforms support ingestion at scale
- Provide time and context-aware processing for correct sequencing
- Data may flow through intermediate storage on way to final processing
- Depending on sensitivity of data, could require robust security at each stop



Data Ingestion – What About the Edge?

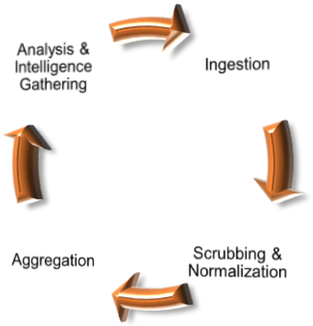
- Edge components (e.g., gateways) can help optimize
- Preliminary processing at the edge can be used to filter what really matters
- Potential for bundling or compressing data for transmit to cloud
- Can help with bandwidth or latency issues





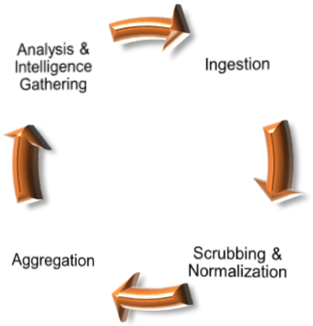
Data Scrubbing & Normalization

- Depending on payload, some portions of the data may not be needed
- Or some portions might contain sensitive detail
- Those parts not needed or sensitive can be “scrubbed” to exclude



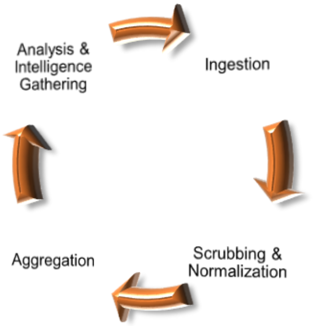
Data Scrubbing & Normalization

- Represents another potential optimization that can preserve storage
- In other cases, similar data may be coming in multiple, disparate formats
- For example, 2 different temperature sensors both providing temp/humidity detail



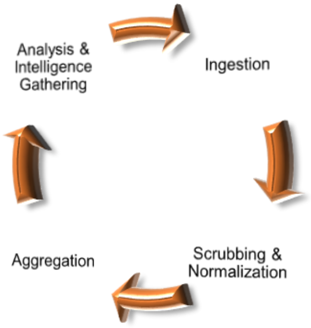
Data Scrubbing & Normalization

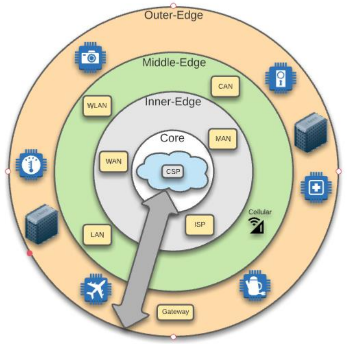
- Normalization can bring consistency to the disparate content
- By normalizing, becomes a single dataset for comprehensive analysis
- Normalization may happen as part of ingestion or as part of a separate step



Data Scrubbing & Normalization – What About the Edge?

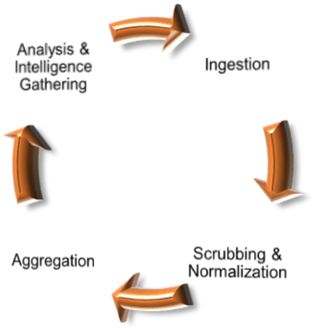
- Depending on complexity, may execute faster closer to the data
- Might involve proprietary algorithms best kept within full control
- Allows addressing of sensitive data before routed to Cloud
- Can also provide additional optimization (relative to bandwidth)





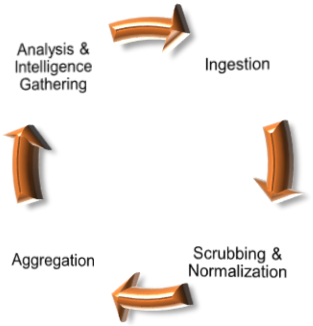
Data Aggregation

- Helps provide full picture of data from multiple streams
- May also be used to enrich with info from other data sources
- Data will be stored in persistent storage for downstream analysis & reporting



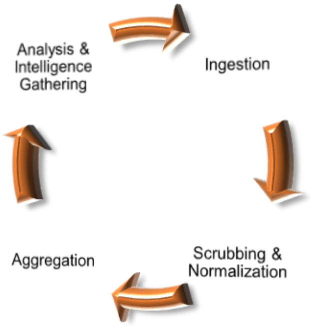
Data Aggregation

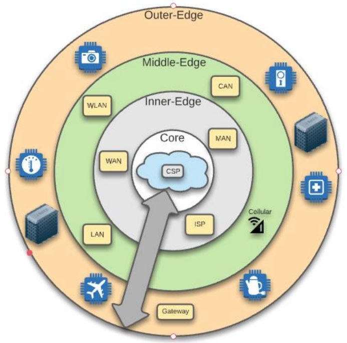
- In statistical analysis, the larger the sample size, the more accurate the inference
- To manage costs, large sets of data may leverage different types of storage:
  - Hot storage – most recent data and most relevant for current analysis
  - Cool storage – data not actively used but potentially relevant (short-term trends)
  - Cold or archive storage – data kept for historical purposes and long-term trending
- Security of the stored data and encryption at rest become critical



Data Aggregation – What About the Edge?

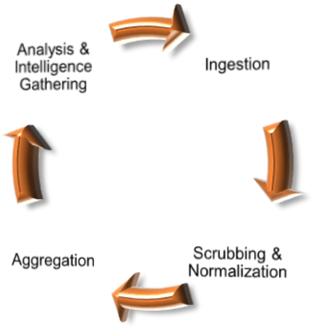
- Provides an additional layer of storage
- Data not transmitted to Cloud (due to optimizations) may still be valuable to keep
- Enables storage of sensitive data in “raw” format in controlled environment
- Can help balance costs against short to mid-term retention requirements





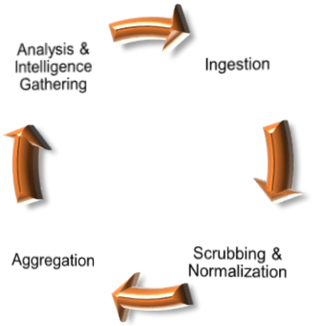
Data Analysis & Intelligence Gathering

- In the digital age, data is the competitive edge
- Companies that manage their data as a critical asset succeed
- Keys:
  - ➢ Aggregating efficiently
  - ➢ Analyzing effectively



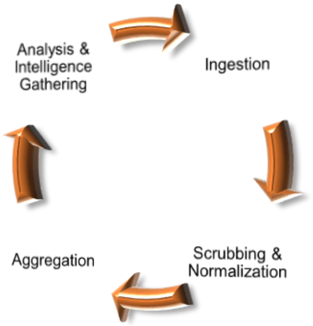
Data Analysis & Intelligence Gathering

- Goal is to identify and leverage the most important data points
- Importance is measured by business value-driven decision-making
- What can I learn about today’s customers, scenarios, or business cases?
- What can I effectively predict about tomorrows?



Data Analysis & Intelligence Gathering

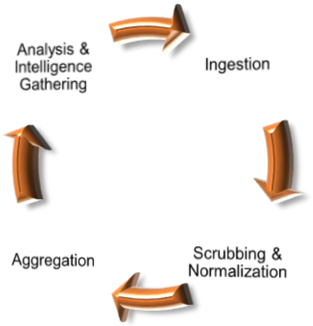
Scenario: Temperature sensors have been steadily recording and aggregating readings from a high-profile data center for a major bank. Initially, the intent was to support being reactive – enabling staff to adjust when an alert was received about an excessively high or low reading (since it can lead to equipment damage or malfunction). Going forward, leadership would like to investigate coupling historical data with current data to understand what kind of proactive intelligence can be gained.



- ✓ What kinds of intelligence do think could be gleaned from this data?
- ✓ How might the company leverage the information in a more proactive manner?
- ✓ What other kinds of information could the data be enriched with to provide more comprehensive value and decisioning?

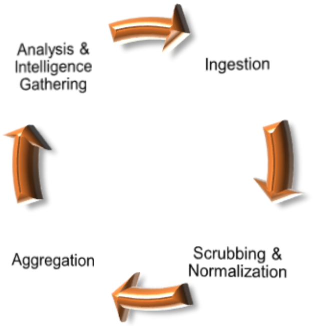
Data Analysis & Intelligence Gathering

- Requires balancing of competing concerns:
  - ➢ To increase quality of intelligence, more data is required (sometimes MUCH more)
  - ➢ But massive datasets can be complex to manage and process

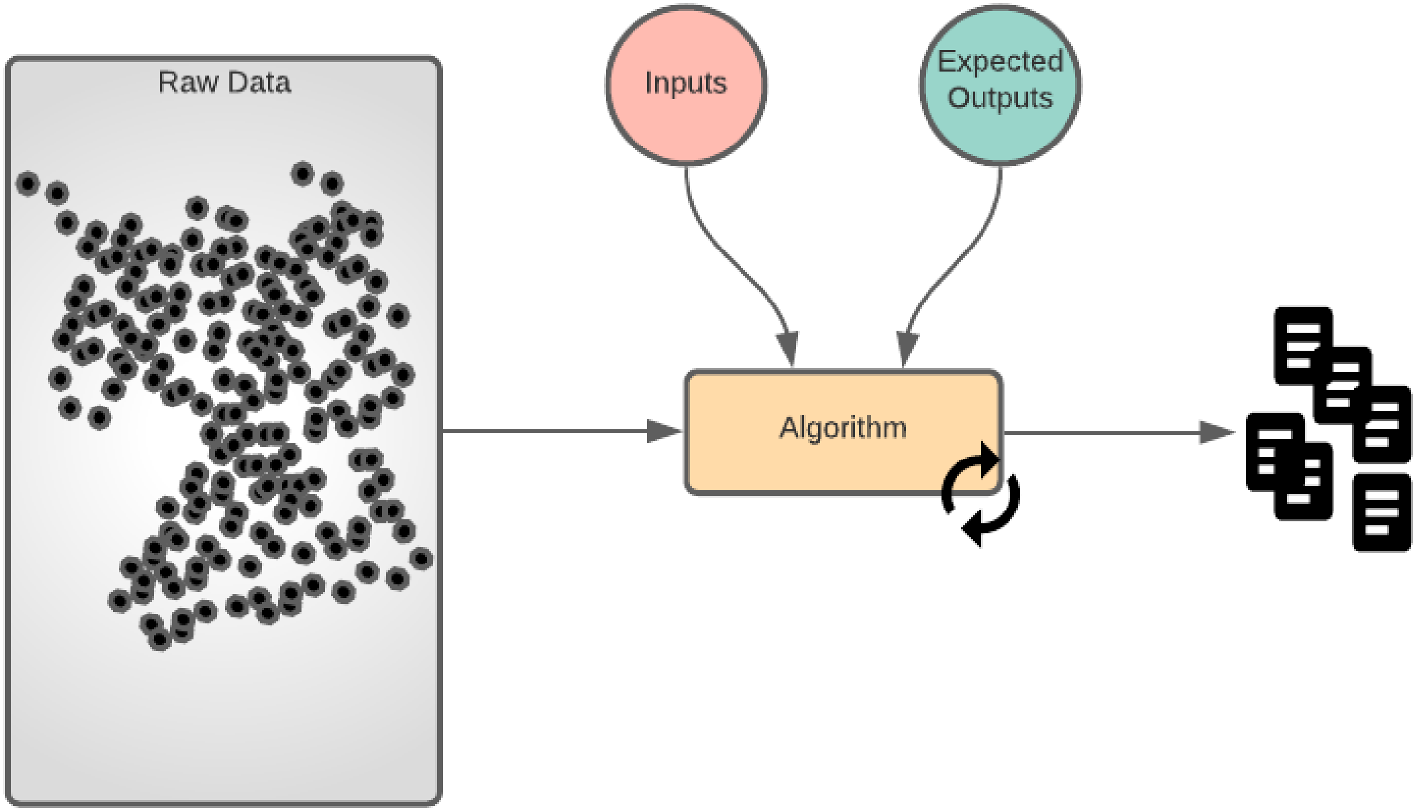


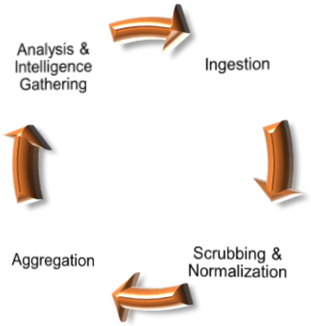
Data Analysis & Intelligence Gathering

- Enter ML / AI:
  - ➢ Algorithms are used to build mathematical models from existing data
  - ➢ Results in a mathematical “trajectory” (and confidence level)
  - ➢ Algorithms can be configured to learn and improve over time
- Hyperscale available in the Cloud brings near-limitless power to bear

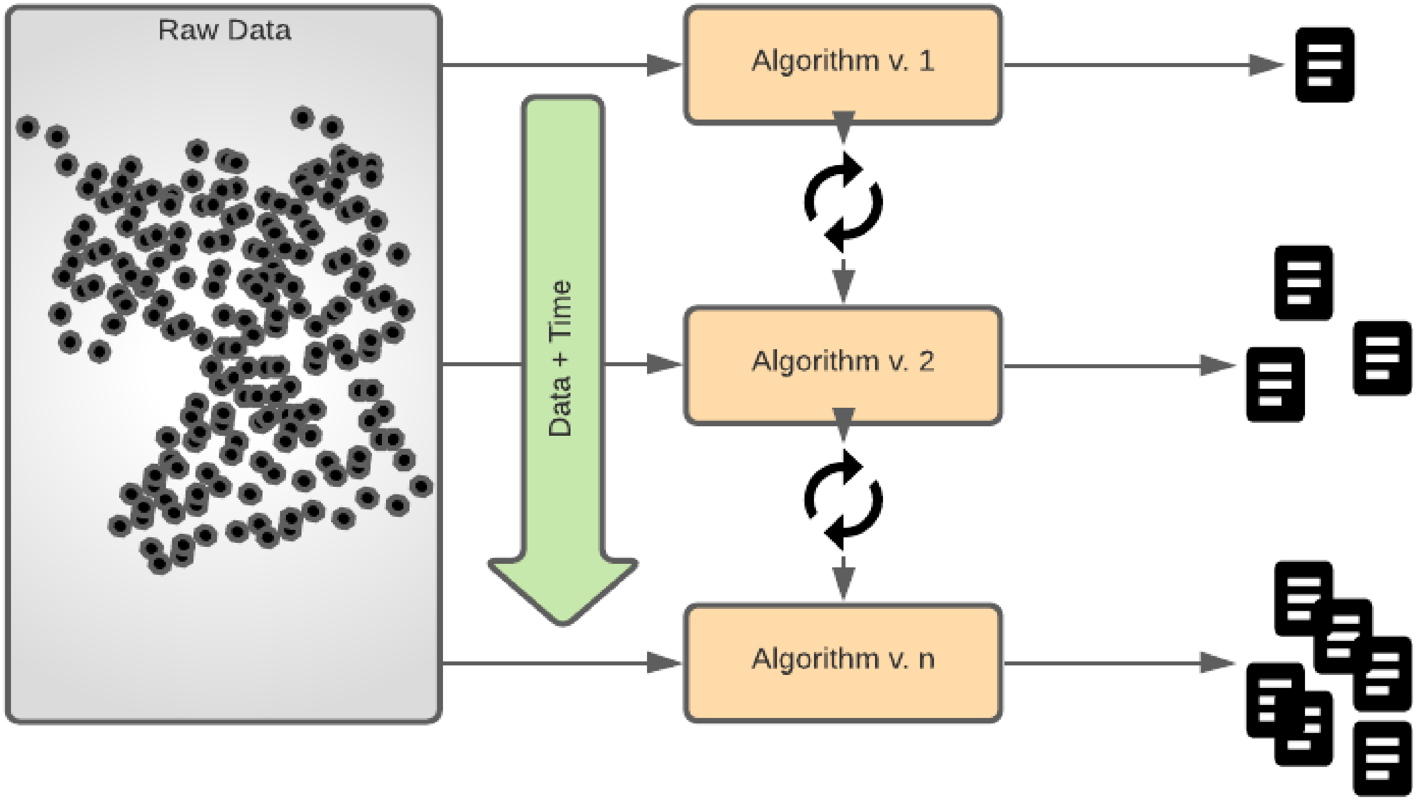


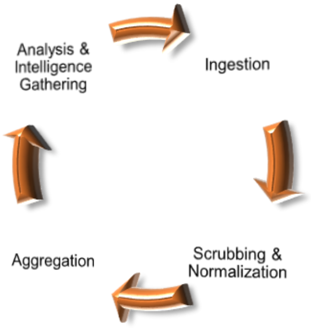
Supervised Learning



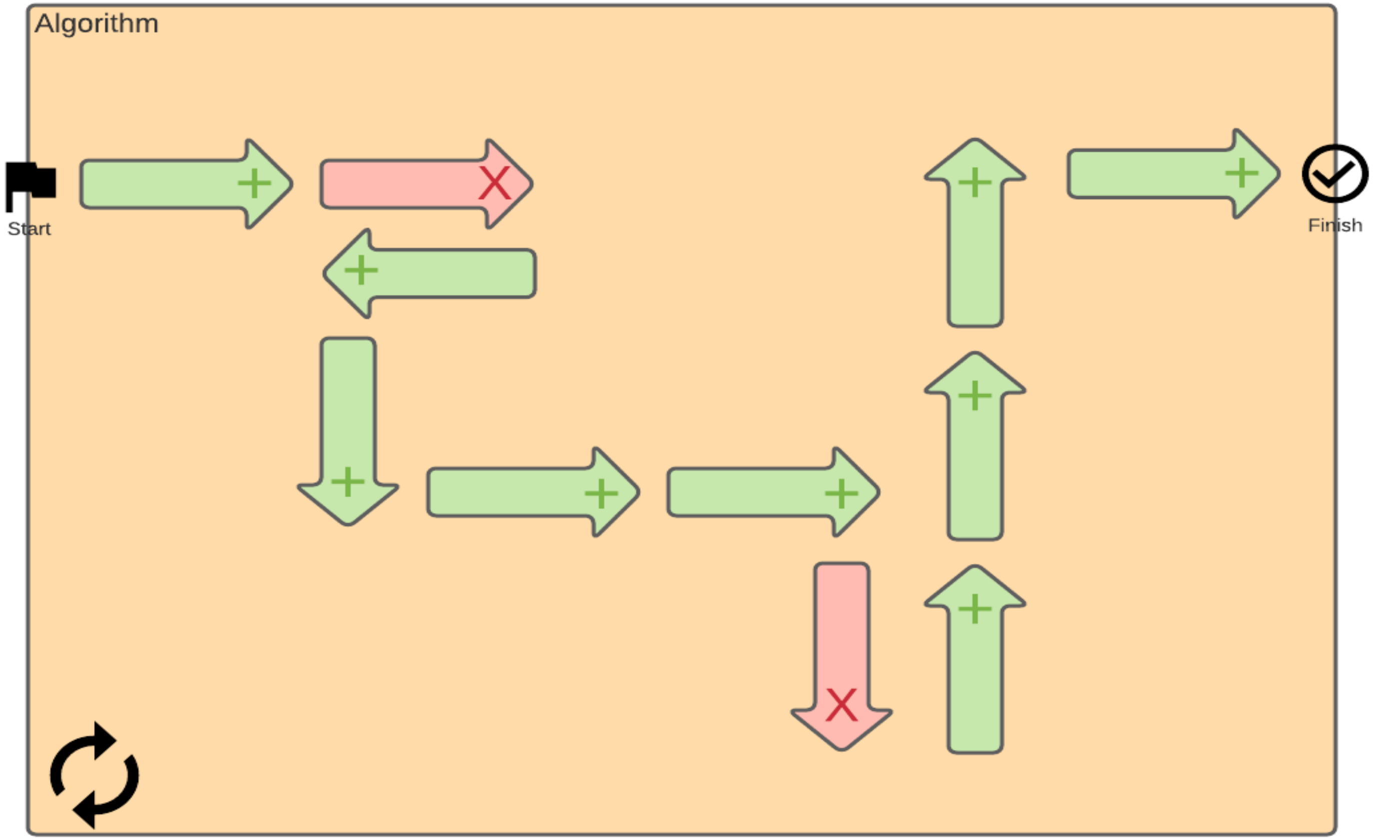


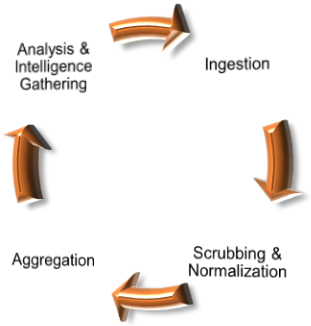
Unsupervised Learning





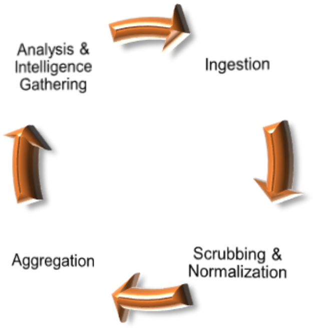
Reinforcement Learning





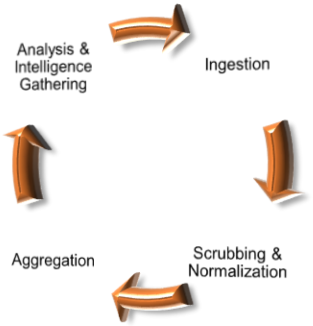
Data Analysis & Intelligence Gathering – What About the Edge?

- With powerful systems at the Edge, sophisticated analysis can be localized
- Can also provide controlled environment for validating algorithms
- Potential options for additional layers of optimization prior to Cloud transmission
- With K8S and containerization at Edge, supports “smart workflow”



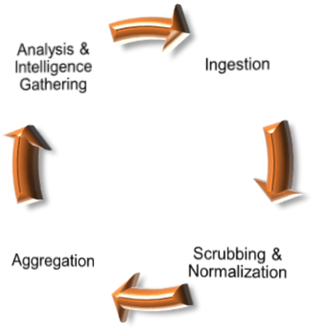
Monitoring vs. Control

- Monitoring tracks key information over time
- Ingestion + Intelligent Analysis → Proactive Response Opportunities
- Leveraged on dashboards for snapshot views
- Leveraged in alerts to notify of negative conditions or negative trending



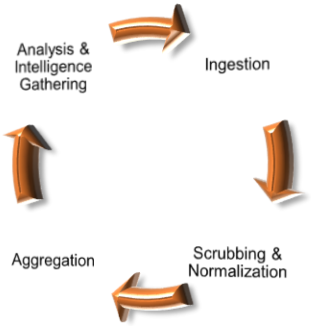
Monitoring vs. Control

- Control includes C2D (Cloud-to-Device) instruction or configuration
- In response to intelligence gathered, can automatically adjust operations
- Can also include updates to operating configuration
- Security requirements may be stricter for control



Monitoring vs. Control

Scenario: Temperature sensors have been steadily recording and aggregating readings from a high-profile data center for a major bank. Initially, the intent was to support being reactive – enabling staff to adjust when an alert was received about an excessively high or low reading (since it can lead to equipment damage or malfunction). Going forward, leadership would like to investigate coupling historical data with current data to understand what kind of proactive intelligence can be gained.



- ✓ In this scenario, what are some potential candidates for configuration control?
- ✓ What are some potential candidates for automatic adjustment to operating environment based on information gathered from the monitoring detail?

Demo

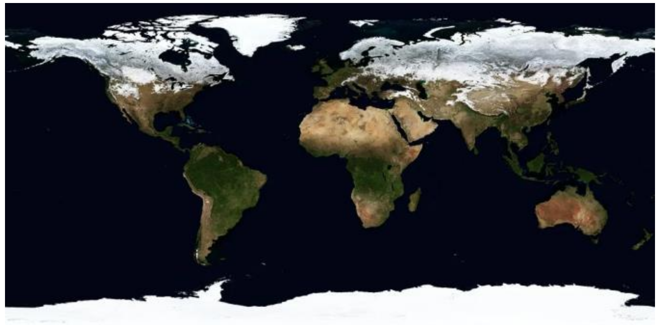
Security & Compliance

Standards & Compliance Categories

- Can include:
  - By geographical region
  - By industry
  - By technology

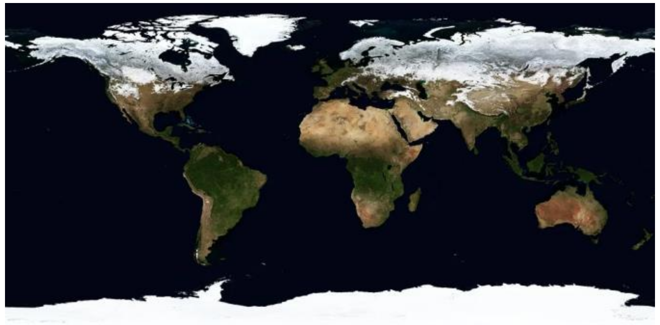
Standards & Compliance by Region

- Standards and compliance enforcement can vary by area of the world
- For example, the EU likely has different requirements than the US:
  - ➢ Federal Communications Commission (FCC) certification in the US
  - ➢ General Data Protection Regulation (GDPR) in the EU



Standards & Compliance by Region

- Can include considerations for:
  - How data is transmitted
  - How data is secured, managed, and used
  - Physical or systems security of the device or Edge component itself



Standards & Compliance by Region

- Failure to adhere can limit ability to do business in the region
- Or can result in significant penalties and/or reputational damage
- Can add permutations to approach to build out of the tech

Standards & Compliance by Industry

- Different industries may have different regulations
- There can also be a difference in physical requirements
- Think remote oil field vs. data center vs. nuclear power plant

Standards & Compliance by Industry

- Regulations often driven by types of data being gathered
- Medical devices likely subject to HIPAA regulations
- Point-of-Sale (POS) devices may require PCI compliance

Standards & Compliance by Industry

- Depending on the industry, failure to comply may have devastating impact
- Think potential exposure for autonomous vehicles, for example

Standards & Compliance by Technology

- Today's devices offer multiple technology options
- Some options better accommodate specific operating requirements
- For example, low power/long range or more robust remote connectivity
- Let's look at a few

Standards & Compliance by Technology

- Bluetooth Smart (aka Bluetooth Low Energy or BLE):
  - ➢ Wireless PAN (Personal Area Network) technology
  - ➢ Targets considerably reduced power consumption with comparable comm range
  - ➢ Goal is smaller size (and, by extension, lower cost)
  - ➢ Compatible with large install base of existing mobile and computers

Standards & Compliance by Technology

- DECT Ultra Low Energy (ULE):
  - ➢ Wireless technology targeting smart home applications
  - ➢ Includes home automation, home security, and climate control
  - ➢ Basic implementation uses a “star network topology” – base + nodes
  - ➢ Ample range coupled for lower power consumption

Standards & Compliance by Technology

- ZigBee:
  - Designed for small scale projects requiring wireless connectivity
  - Used in home automation, medical device data collection, etc.
  - Low power consumption
  - Also, low bandwidth, low data rate, and requires closer proximity
  - Intended to be simpler and less expensive
  - Can integrate with a mesh network to extend reach

Standards & Compliance by Technology

- 6LoWPAN:
  - Acronym for IPv6 over Low-power Wireless PAN
  - Uses encapsulation and header compression
  - Enables send of IPv6 packets over LR-WPANs (low-rate wireless PAN)
  - Targets devices with very limited form factor

Standards & Compliance by Technology

- LoRaWAN:
  - Proprietary long-range/low power technology for wide area networks
  - LoRa defines physical layer
  - LoRaWAN defines upper networking layers
  - Cloud-based protocol
  - Acts as network layer protocol for managing comm between devices and gateways

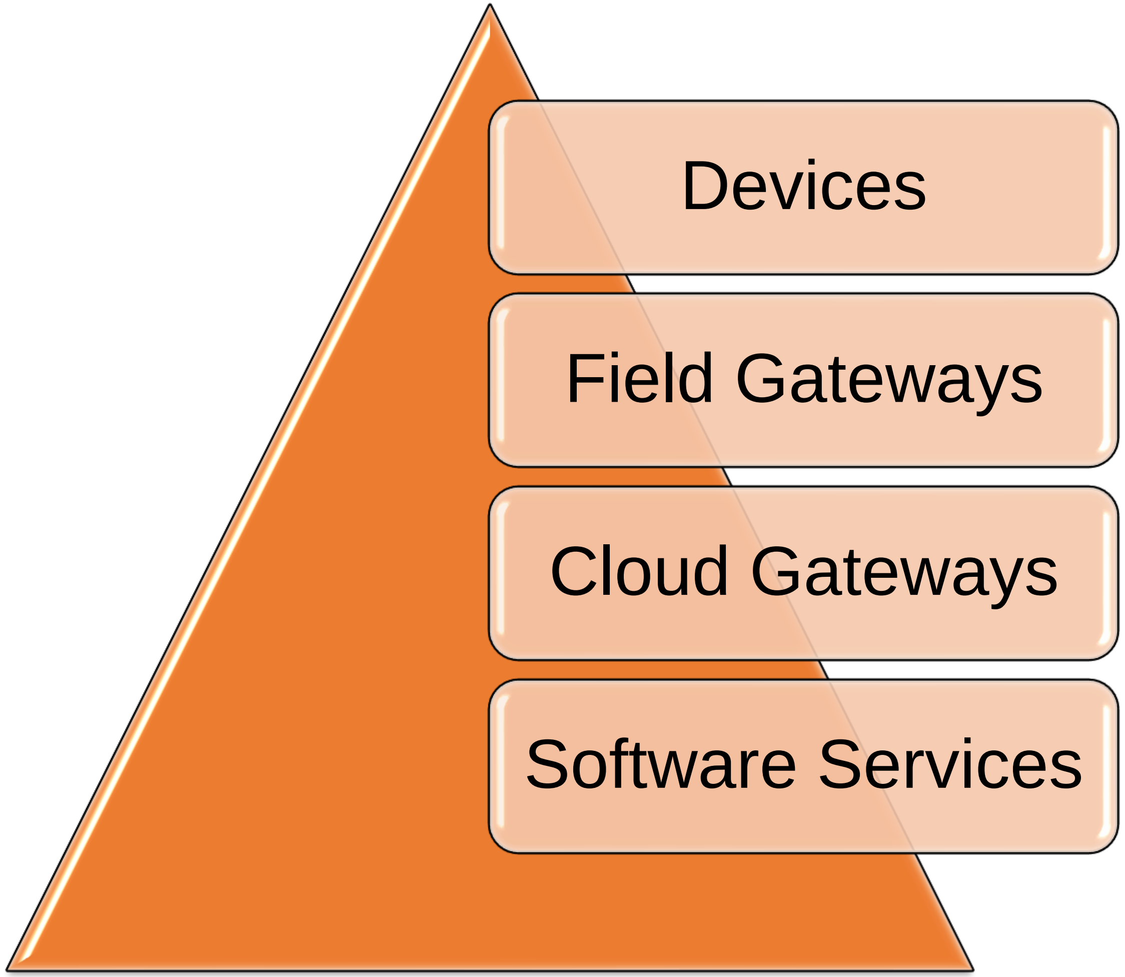
Assessing Security Risks

- To secure a solution, attack surfaces and potential threats must be identified
- Common practice utilizes something called threat modeling
- Includes modeling and analyzing possible attack vectors based on application

Assessing Security Risks

- Risk assessment should account for different “zones” of execution
- Security requirements for device in remote oil field different from secure data center
- And, ideally, threat modeling would be executed during design & dev phases

Typical Threat Zones



Devices

Field Gateways

Cloud Gateways

Software Services

Security Considerations

- Effective Edge/IoT systems depend on a trustworthy network of:
  - Data producers
  - Data consumers
- Potential exposure could include physical tampering with a device in that network
- But tampering might also include considerations as well

Security Considerations

- Need to be able to trust and secure:
  - ➢ The identity of a device
  - ➢ The integrity of the software running on it
  - ➢ The integrity of its hardware
  - ➢ The data sent or stored
- Applies to both a sensor and Edge device (gateway, etc.)

Securing Device Identity

- As discussed in section on device provisioning, devices are registered securely
- Often utilizes one of the following to secure identity:
  - ➢ An X.509 certificate securely stored on the device
  - ➢ Trusted Platform Module (TPM) providing chip-based security configuration
- Identifies and provides ongoing verification of device with data target

Securing Device Identity

- Only registered devices should be able to connect and send data
- Secure identity can periodically (or continually) be verified
- Keys used to affirm identity must be protected
- Secure identity is about establishing a trust relationship

IoT Device Certificates

- According to studies, IoT devices are under attack within 5 mins of coming online
- Complex attacks on networks increase every year (2,851% growth since 2017)
- Device certificates can support secure identity and encryption

IoT Device Certificates

- May leverage Public Key Infrastructure (PKI)
  - Digital certificate – AKA public key cert; cryptographically links public key with owner
  - Certificate authority (CA) – trusted party/entity that issues digital security cert
  - Registration authority (RA) – AKA subordinate CA; authenticates requests for a cert and then forwards to CA
  - Certificate store – storage system (e.g., database) containing info about issued keys and certs

IoT Device Certificates

- Combined with device registration
- Cert is associated with registered device and used like a network “passport”
- Ensures added layer of security which is revokable (even for registered devices)

Provisioning IoT Device Certificates

- Third-party certificate vendors and scalable, managed digital cert services
- High-volume private cert management, especially for behind the firewall
- High-volume private cert uses MDM (mobile device management) systems to generate and distribute certs
- Low-volume manual cert management – simpler but can be less secure/scalable

IoT Device Certificates – Benefits

- Additional layer of security and data encryption
- Maintains immutable record of activity with dates, time, and key detail
- Enable tamper-resistant features – in software and/or data

IoT Device Certificates – Challenges

- Managing certs can be time consuming and difficult, especially for large fleets
- Need to proactively manage expiration dates which can vary greatly
- The wrong provisioning strategy can make it difficult to succeed

Securing Device Software

- Edge/IoT devices are often common, commodity implementations
- Streamlined commonality helps to keep down costs
- However, can also lead to exposure

Securing Device Software

- When implementation is common, attack vectors may be well-known
- For a given device type, attackers may already have tried & true strategies
- Enforced standards can lead to advanced understanding of vulnerabilities

Securing Device Software

- Attackers do not necessarily need to assume device identity
- Can inject malicious code into existing software flow where identity appears valid
- Software integrity is usually verified using code signing mechanisms

Securing Device Hardware

- Secure software running on insecure hardware is still exposed
- Devices (especially Edge devices) need hardware root of trust
- There are a couple of options:
  - Trusted Platform Modules (TPMs)
  - Hardware Security Modules (HSMs)

Securing Device Hardware – TPM

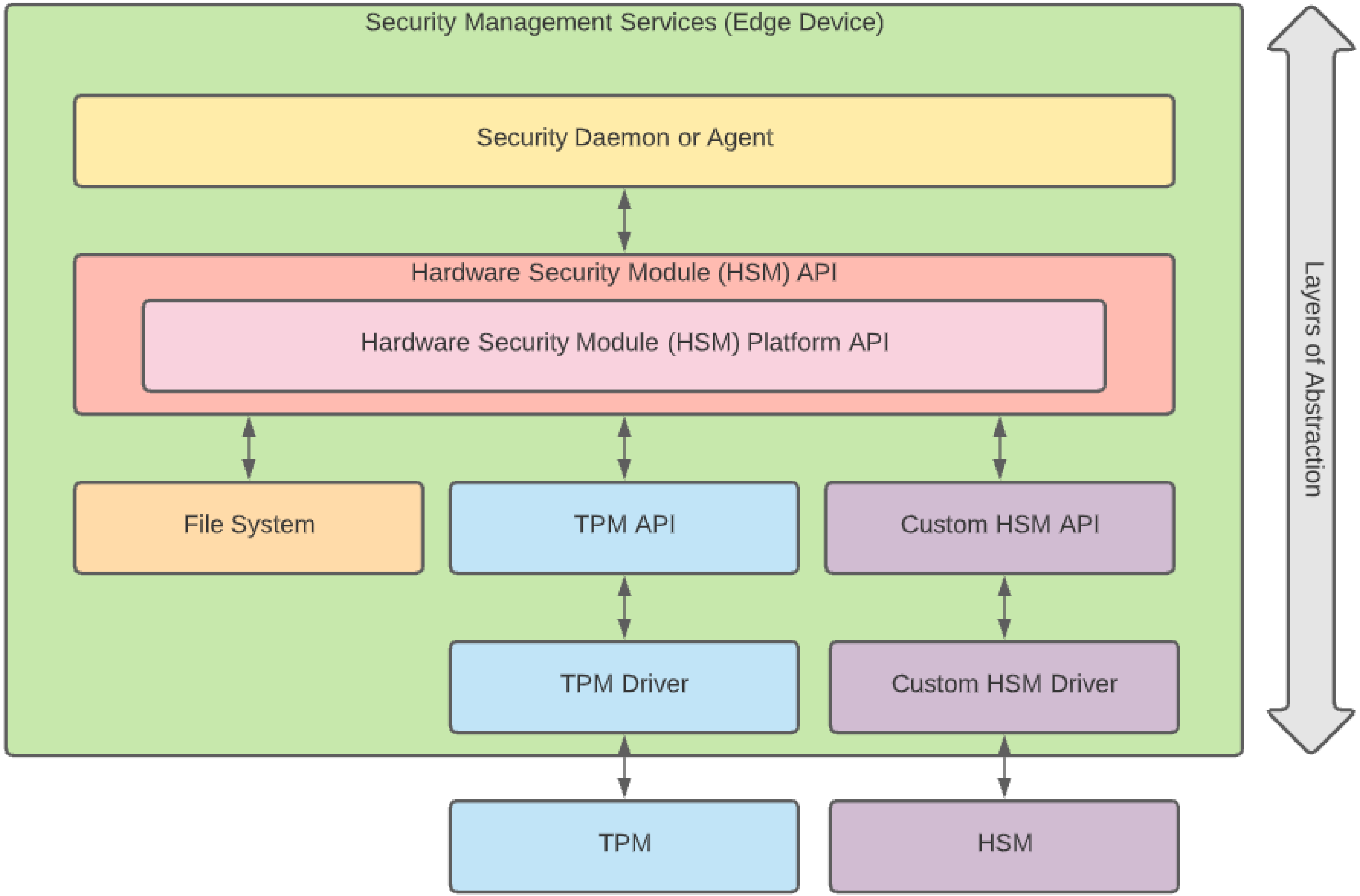
- Set of protocols that can be implemented in hardware, firmware, or software
- Firmware or software options represent "virtual" TPMs
- Not as secure as the hardware implementation
- Storing keys in TPM prevent malicious attempts to retrieve

Securing Device Hardware – HSM

- Custom, vendor-provided modules for securing hardware
- Need to confirm integrity and security of module for target application
- Will likely also need a “wrapper” that enables API-based integration with the HSM

Securing Device Hardware

Uses end-to-end secure certificate generation and transmittal functions for establishing trust relationships across the components


Security Management Services (Edge Device)
Security Daemon or Agent
Hardware Security Module (HSM) API
Hardware Security Module (HSM) Platform API
File System
TPM API
Custom HSM API
TPM Driver
Custom HSM Driver
TPM
HSM
Layers of Abstraction

Security Promises

- Represent capabilities or guarantees for security of keys
- Three common types:
  - Standard promise
  - Secure element
  - Secure enclave

Standard Promise

- Supports previously described security workflow
- Guarantees persistence of secrets on Edge device’s file system
- Usually utilized to facilitate startup tasks for initial build out of Edge/IoT network
- Not viable for production usage – should be seen as dev or test-only option

Secure Element

- Supports all capabilities available with standard promise
- Adds secure storage of secrets in TPM or HSM
- Baseline recommended approach for production

Secure Enclave

- Supports all capabilities available with secure element
- Also allows definition of something called Trusted Applications (TA)
- Enables security of runtime environment in addition to secrets

Secure Enclave

- TA runs within Trusted Execution Environment (TEE)
- Provides a protected execution workspace (or enclave)
- Prevents any outside access to code running in the TEE

Secure Enclave

- Part of an emerging trend called Trusted Edge Computing
- Helps protect against new attack vectors arising from modern Edge integration
- More secure but provides code built for TEE

Securing Data in Motion

- Security required as data flows through the ether between producer and consumer
- If attacker able to intercept information flowing between the two:
  - Potentially exposes sensitive information contained within header or payload
  - Could allow insertion of alternate, damaging control instruction for C2D

Securing Data in Motion

- Certificate/secrets-based Transport Layer Security (TLS) can be used to protect
- Highlights the previously discussed need to protect security keys
- Impact can range from trivial to devastating (depending on application)

Securing Data at Rest

- Aggregated data stored on a device in plain text can create a vulnerability
- In previous topic on data management, goal is gained intelligence from the data
- If the data at rest has been compromised:
  - May lead to inaccurate conclusions from analysis
  - Could provide competitor or bad actor access to a company’s competitive advantage
- As with “in motion”, certificate-based encryption in storage is key

Threat Modeling

Scenario #1: Mesh-enabled network of security cameras aggregating video from a college campus to help monitor and ensure safety of students & faculty

Scenario #2: System of devices and Edge technology used to track train cars entering and leaving loading & dispatch stations and their cargo

Scenario #3: System of devices and Edge technology used to monitor multiple drills in large oil fields for malfunction or required maintenance

- ✓ What are the potential attack vectors in the scenario?
- ✓ What are the potential consequences if a vulnerability were exploited?
- ✓ What are some high-level approaches that could be taken to secure?

Operations

Metrics, Measurement & Assessment

“Every line is the perfect length if you don’t measure it.”

- Marty Rubin

“What gets measured gets managed.”

- Pearl Zhu

“If you don’t collect any metrics, you’re flying blind. If you collect and focus on too many, they may be obstructing your field of view.”

- Scott M. Graffius

“What science has failed to notice is that the measurement has become more real than the thing being measured.”

- R.A. Delmonico

Metrics, Measurement & Assessment

“That which cannot be measured cannot be proven.”

- Anthony W. Richardson

“All conflict in the world is essentially about our differences in measurement.”

- Joseph Rain

“It is impossible to escape the impression that people commonly use false standards of measurement – that they seek power, success and wealth for themselves and admire them in others, and that they underestimate what is of true value in life.”

- Sigmund Freud

Metrics, Measurement & Assessment

"Too many organizations treat [IoT] as a technology project, as opposed to what it really is, which is a business transformation project using technology. First rule of IoT club: Don't talk about IoT. Talk about business using IoT."

-Alfonso Velosa, research vice president and analyst for IoT at Gartner

Scale

Scenario: A manufacturing company has been piloting a small set of sensors (50) in one of their US locations for monitoring status and any operational anomalies for manufacturing equipment. The pilot effort has proven to be very successful and senior leadership would now like to extend the use of the IoT solution to all US locations (27 locations and 17K pieces of manufacturing equipment) over the course of the next year. The following year, leadership would like to extend the technology to global reach which would include an additional 52 international factories and 46K pieces of manufacturing equipment.

- ✓ If your team was charged with implementing the goals outlined in the scenario, what kinds of questions might you ask to gain important requirements detail?
- ✓ What kinds of challenges might you face in attempting to implement (People, Process, and Technology)?
- ✓ What kinds of challenges might you face in attempting to support?

Performance at Scale

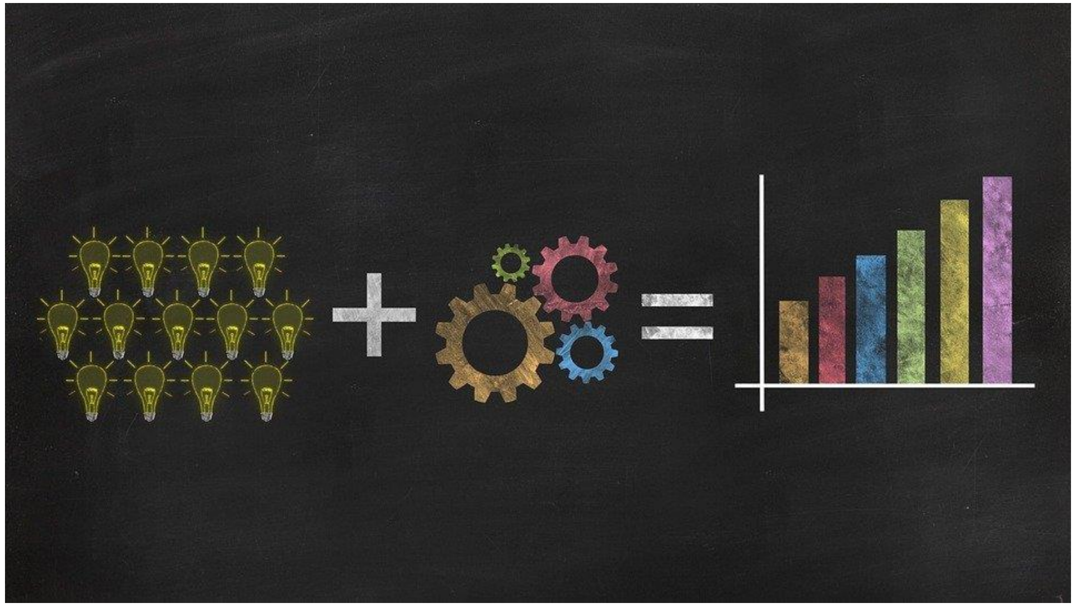
- Depending on application, volume of devices & data could be significant
- As discussed, requires management at scale on multiple levels:
  - ➢ Device management
  - ➢ Software management
  - ➢ Data management

Performance at Scale

- Execution for a small number of devices is more straightforward
- Execution for thousands or tens of thousands of devices is a different story
- With that volume, requires a much different approach

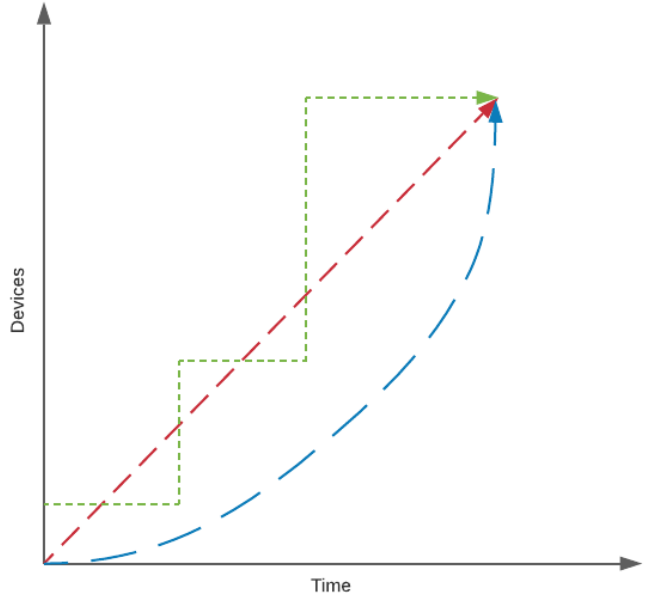
Strategies for Scaling IoT

- Set a clear business objective
  - Business goals should drive technology for IoT
  - Evaluate whether (or not) adding/enhancing IoT can make the company more successful
  - Enables the correlation of scaling tasks (and any “bumps”) to value



Strategies for Scaling IoT

- Start small and build up
  - ➢ Trial run with smaller sets of devices can help confirm configuration
  - ➢ Each new set of “onboarded” devices should have metrics for success and ROI
  - ➢ Allows for correction (if needed) as you go (Agile)



Strategies for Scaling IoT

- Create a specialized team or CoE (Center of Excellence)
  - Organize a group to manage IoT priorities and curate best practices
  - Needs to include senior management buy-in and participation
  - Build continuous improvement into the DNA

Strategies for Scaling IoT

- Understand and assess maturity
  - Honestly and objectively assess progress of status against targets
  - Identify next level(s) of maturity and steps required to achieve
  - There is no standing still – technology efforts progress or regress

DevOps & Automation

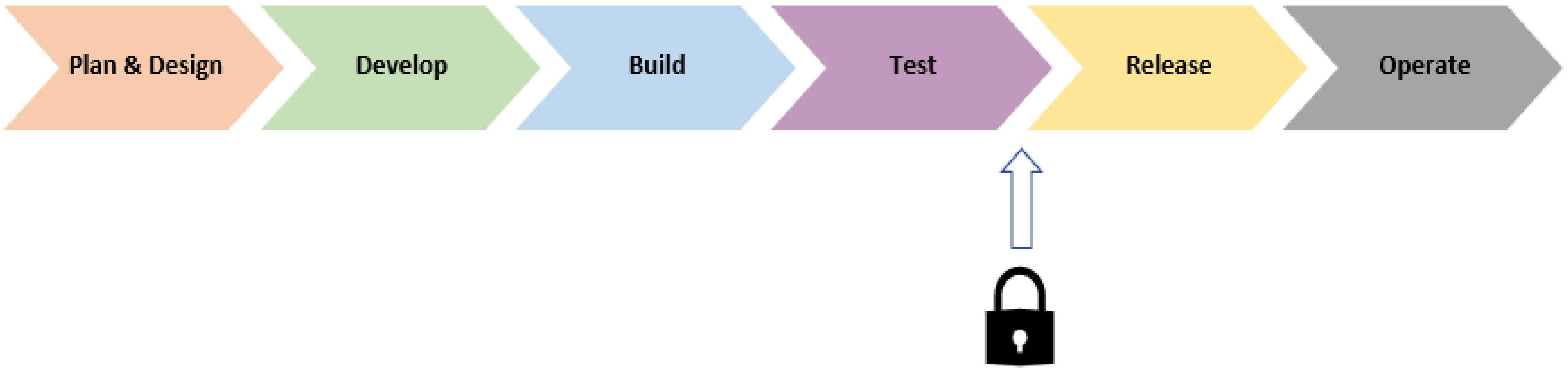
- As with other software applications, DevOps can provide lift
- Key principle of DevOps is automation
- Continuous Integration & Continuous Delivery can be applied to Edge/IoT as well

DevOps & Automation

- Presents opportunities to apply scripting to:
  - Automate onboarding, offboarding, and configuration of devices
  - Deployment & configuration of Edge components
  - Deployment & configuration of Cloud services used to aggregate & analyze data
- Practicing principles of DevSecOps helps ensure security is “shifted left”

DevOps & Automation

- What is often done:



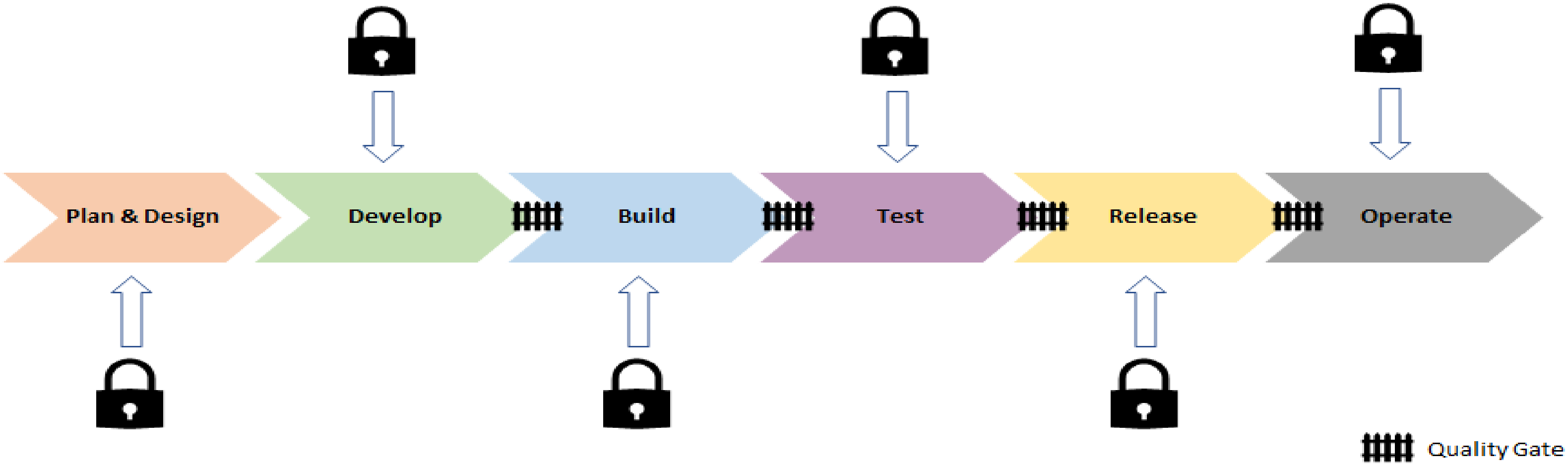
What are the potential challenges with taking this approach?

DevOps & Automation

- Potential challenges:
  - At this point, there may not be enough time in schedule to absorb change
  - Activities required to remediate may be complex
  - May require revisit of one or more previous phases to properly address

DevOps & Automation

- Better approach:



DevOps & Automation

- Plan & Design – Threat modeling, data protection, and risk assessment
- Develop – SAST (Static Application Security Testing) tools
- Build – SAST and SCA (Software Composition Analysis) tooling
- Test – DAST (Dynamic Application Security Testing) tools, passive/active scans and "fuzzing"
- Release – Additional security-specific scanning, port scans, and log validation
- Operate – Monitoring & alerting, RCA (Root Cause Analysis)

DevOps & Automation

- Quality gates guard against moving security defects forward
- In true DevOps fashion:
  - Information gathered from early phases feeds into later phases
  - Lessons learned feed continuous improvement of overall process

Data Visualization & Dashboarding

- Computers are great at “crunching” large amounts of raw data
- For humans, sometimes a “picture is worth a million bytes”
- With dashboarding & graphical visualization, it can be much easier to see trends
- Data science and forecasting can help with extrapolating for the future

Data Visualization & Dashboarding

- Tools like Power BI or Tableau (among others) provide powerful options
- Able to integrate through connectors with multiple data sources
- Visualizations & charts can be layered onto large datasets to provide insight

Data Visualization & Dashboarding

- Often the tools support regular data refresh for fuller picture over time
- Tools leverage defined authentication/authorization against data sources
- Helps ensure ongoing, end-to-end security of key data

IT & OT Convergence

- IT/OT is the convergence of:
  - ➢ Information Technology (IT)
  - ➢ Operational Technology (OT)
- Important to understand distinction (and overlap) from an operational perspective

IT & OT Convergence

- Broadly speaking:
  - IT – use of technology/process to create, store, secure, and exchange electronic data
  - OT – traditionally associated with monitoring events, processes, and devices as part of enterprise and industrial operations management

IT & OT Convergence

- OT considerations:
  - Includes ICS (Industrial Control Systems) and SCADA (Supervisory Control and Data Acquisition)
  - Not traditionally networked technology (i.e., WAN or Internet)
  - Often use closed, proprietary protocols and lower-level embedded tech
  - Security requirements traditionally different due to how connected

Types of Convergence

- Process convergence
- Software and data convergence
- Physical convergence

Process Convergence

- Convergence of IT & OT workflows
- Process reform so each can benefit from the other
- Can require organizational change (sometimes significant) to achieve

Software and Data Convergence

- Technical convergence at the software and data layers
- Can include unification of disparate IT or OT protocols toward standardization
- Separate, siloed data stores need to converge to provide comprehensive visibility

Physical Convergence

- Includes hardware convergence (or retrofit) to unify
- Depending on size of gap, may mean replacement rather than upgrade
- Often required to fully enable software and data convergence

IT/OT Convergence at the Edge

- The Edge can assist with convergence:
  - Bridging the gaps during transition (e.g., at the network layer)
  - What lacks in unified software or hardware may be mitigated (at least temporarily) with the intelligent Edge
  - Any changes that cannot be implemented (due to cost constraints) can be abstracted at the Edge

IT/OT Convergence – Benefits

- Less siloed IT and OT departments
- Reduced development and support costs (e.g., predictive maintenance)
- Faster time to market for converged tech
- More efficient energy/resource usage

IT/OT Convergence – Benefits

- Improved compliance with regulatory standards (via modernization)
- Improved automation for older, proprietary OT devices
- Improved visibility through expanded real-time data reporting
- More efficient asset management (1 stream instead of 2)

IT/OT Convergence – Challenges

- Requires organizational change which can be significant and difficult
- Modernizing and improving security might be impeded by existing tech or lack of knowledge
- Reskilling through training can be a challenge to coordinate and execute
- Integration of siloed areas can have multiple, hidden issues

Absorbing Enhancements

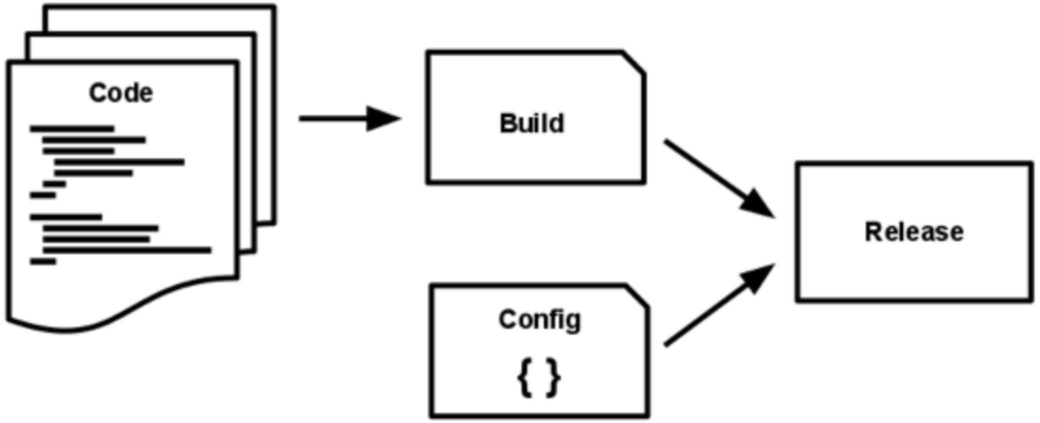
- As with all other technology types, Edge/IoT is ever-evolving
- Enhancements are likely to occur in multiple areas:
  - Communication protocols
  - Device hardware and software
  - Edge hardware and software
  - Cloud services

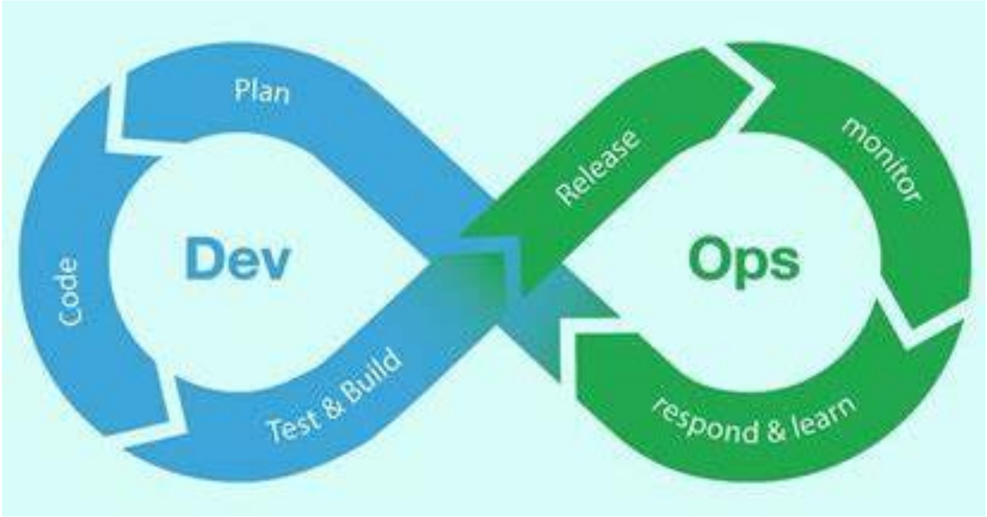
Absorbing Enhancements

- A company’s Edge/IoT strategy must be able to embrace the change
- Otherwise, run the risk of missing out on advancements & new capabilities
- Must be able to balance orderly absorption of change against volume

Absorbing Enhancements

- Requires intermediate environments within DevOps pipeline
- Need a way to test the enhancements to verify and help avoid regression
- Additionally, provides mechanism for validating deployment of change at scale





Absorbing Enhancements

- In some cases, update may not suffice
- Some enhancements will require replacement to realize benefits
- DevOps & asset management strategy must be able to support structured approach to upgrades (both hardware & software)

Demo

VMWare Product/Technology Alignment

VMware Product/Technology Alignment

Case Study: VMware Edge (https://www.vmware.com/hk/solutions/edge-internet-of-things.html)

Case Study: Workspace IoT Endpoint Management (https://www.vmware.com/products/workspace-one/workspace-iot.html)

THANK YOU

Develop Intelligence