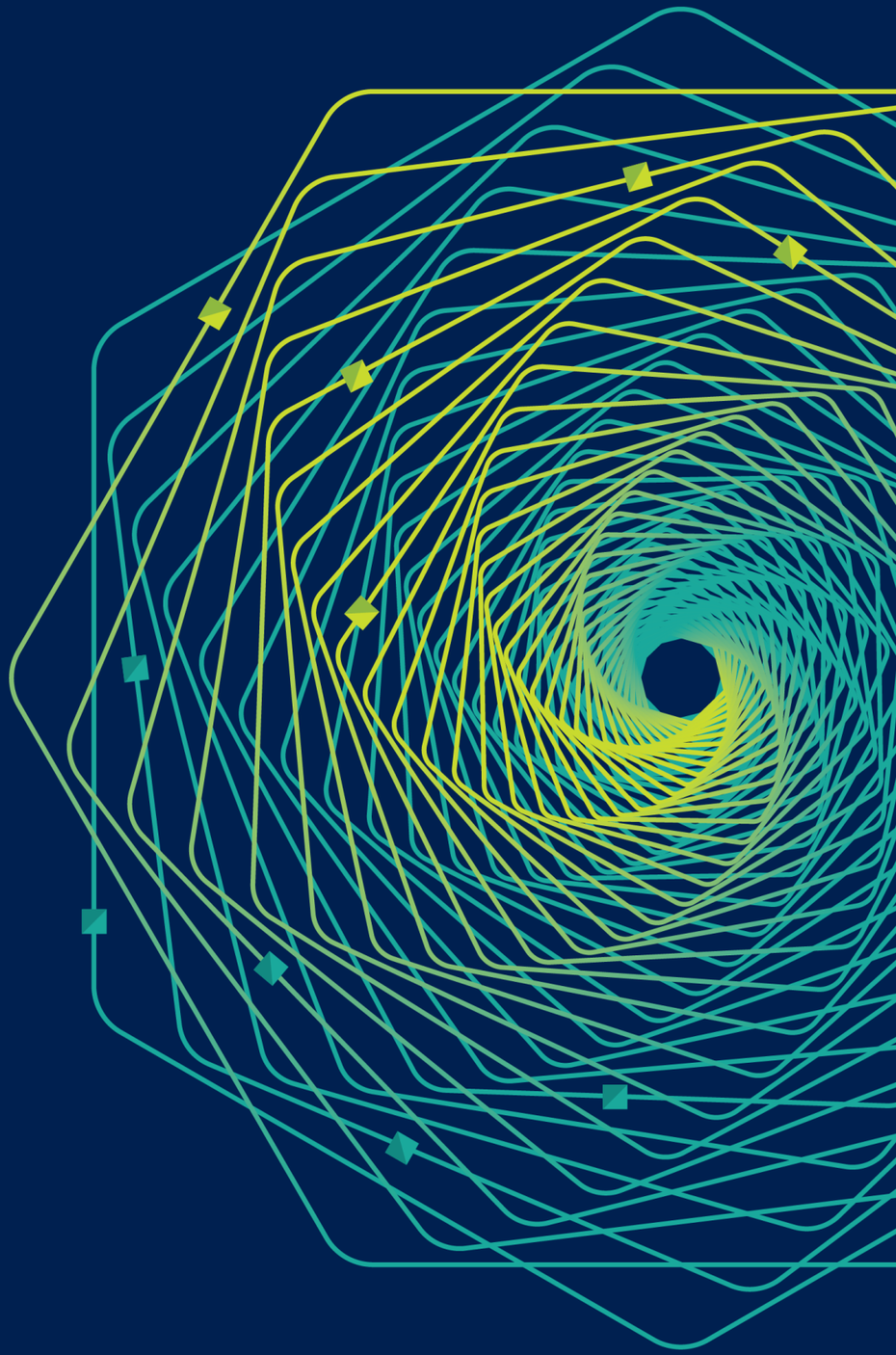
Microsoft

Bringing the cloud closer to the edge

Arjmand Samuel

Edge Engineering lead

Microsoft Azure IoT



Customers and Partners are already transforming their industries

Steelcase

"43 percent of workers do not think their office is a great place to do creative work." **With IoT in the work environment, people can tell organizations what spaces are successful and why**.

RAC

Reduced its accident rate by 25% and fuel usage by 20%, reporting annual savings of **$1.8 million**.

CBRE

CBRE 360 mobile apps allows users to locate colleagues, navigate the workplace and reserve workspaces, and access food and beverage as well as basic building and concierge services.

thyssenkrupp

Data from sensors and systems to **create valuable business intelligence and reduce downtime by 50%**

Tetra Pak

Cut down-time cut for each packaging line by up to 48 hours, **saving €30,000 for customers.**

HERSHEY'S

Licorice extruders on Twizzler's production line are performing at peak optimization, **saving over $500K/year on materials alone.**

Rolls-Royce

Rolls Royce "power by the hour" model provides maximize availability by **cutting fuel consumption by 1% and up to $250,000 per plane, per year**.

KOHLER

KOHLER Konnect allows consumers to personalize their bath and kitchen experiences and automate everyday tasks.

FINNING CAT

Enabled customers to transport more than 1M additional tons of cargo, and **reduce fuel consumption by 17%**

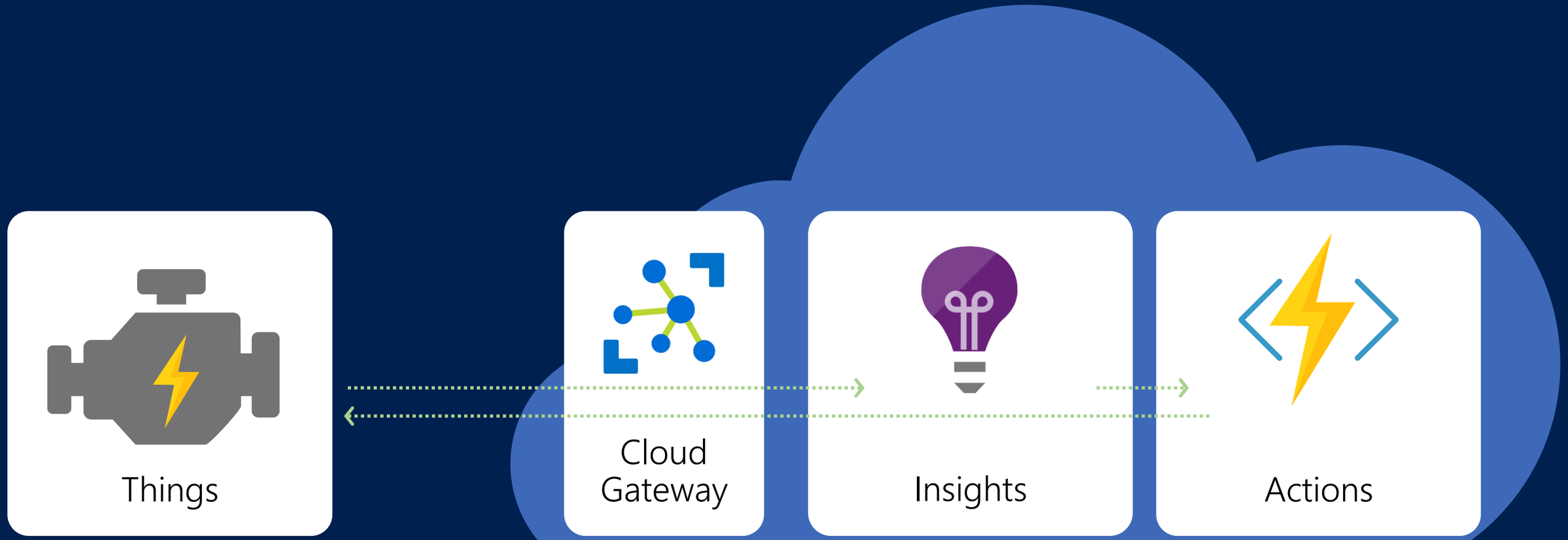
Johnson Controls

Connected chillers are back online 9x faster than unconnected equipment, **avoiding more than $300,000 in hourly downtime costs.**

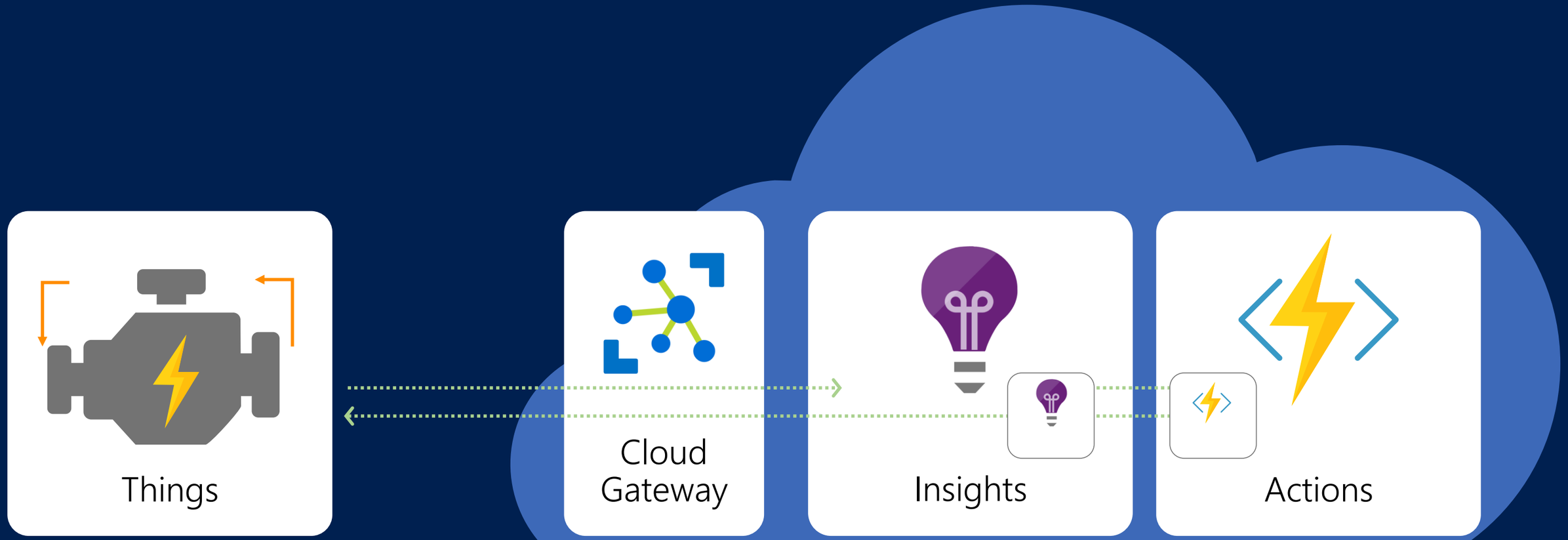
BMW · FUJITSU · KUKA · Rockwell Automation · Schneider Electric · DUNAV NET · Mercedes-Benz · LIEBHERR · JABIL · ABB


ZEROTECH
CAN TELEMATICS
LIEBHERR
BMW
Steelcase
GRUNDFOS
fathym
Schneider Electric
NAV CANADA
MATTEL
WEKA
RENAULT NISSAN
GOJO
Ford
innovate
ABB
ABT RAAMS
ABUS
aegex
ATF SERVICES
avatarion
CITIZENSERVICES
AvePoint
AXELERATE
BAX ENERGY
Beijer automotive
Transport for London
BLUE DYNAMICS
BLUE FROG
btt
Buenos Aires Ciudad
BUNN
CAN TELEMATICS
CardioDiagnostics
care innovations
CARNEGIE MELLON UNIVERSITY
CHIPING
IMTAS
COATS
COMON
coop LA COOP SEI TU.
Power Generation
CYBERCOM GROUP
DAIMLER
DRONEGRID
DRONEWORKS
DUNAV NET
D·C DRENTHECOLLEGE
TECHNOLOGIES
ECOLAB
edp
EMAAR
EnBW
ENGIE Cofely
evoqua
FINNING
FUSE THRU
GAA
Geratriz
GTI
甘来 | Born for Smart Vending
HERSHEY
Homebase
Honeywell
INDENTIVE
INGENU
JABIL
Jcible
Johnson Controls
KING WAY
KONGSBERG
KUKA
LG CNS
LG Electronics
IOMOTE
Ville d'Ottignies-Louvain-la-Neuve
MARS drinks
Mondelēz International
MoveInSync
NAV CANADA
新希望六和 NEW HOPE LIUHE
NEXCOM The Intelligent Systems
origis
OSIsoft.
P97 networks
Plas.md
POLITECNICO MILANO 1863
powel
PRODATA mobility Brasil
Proxfinity.
quorum
RAC
realbox
Roche
RockStep
Rockwell Automation
Rolls-Royce
SAMSUNG
SANDVIK Coromant
saxa
Scomi Scomi Engineering
sensoria
SERAKU
SFE
SkyAlert
SLAC NATIONAL ACCELERATOR LABORATORY
SOLOINSIGHT
Soup Stock Tokyo
STOCKROSE
takasolutions
targetbase
TechnoKom
TEXA
THE YIELD
thermoplan
things expert
thyssenkrupp
TRANSNET
ZPMC
tofugear
weka health solutions
Tetra Pak
www.ZIONCHINA.com

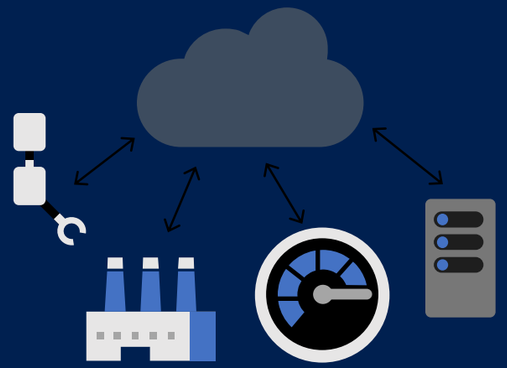
IoT Application pattern



IoT Application pattern + Edge



IoT in the Cloud and on the Edge

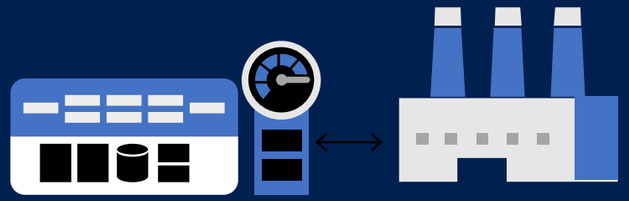


IoT in the Cloud

Remote monitoring and management

Merging remote data from multiple IoT devices

Infinite compute and storage to train machine learning and other advanced AI tools



IoT on the Edge

Offline operations

Privacy of data and protection of IP

Pre-process data On-Prem, e.g., video streams

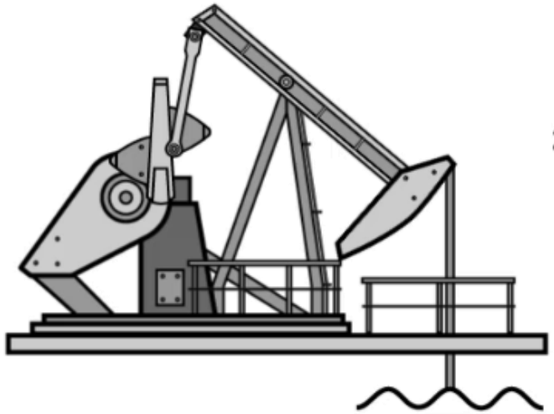
Near real-time response, e.g. low latency control loops

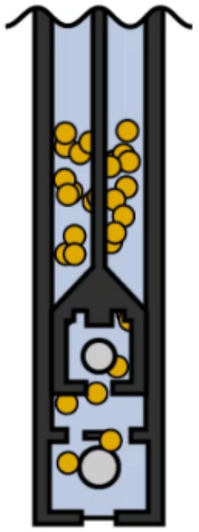
Protocol translation & data normalization

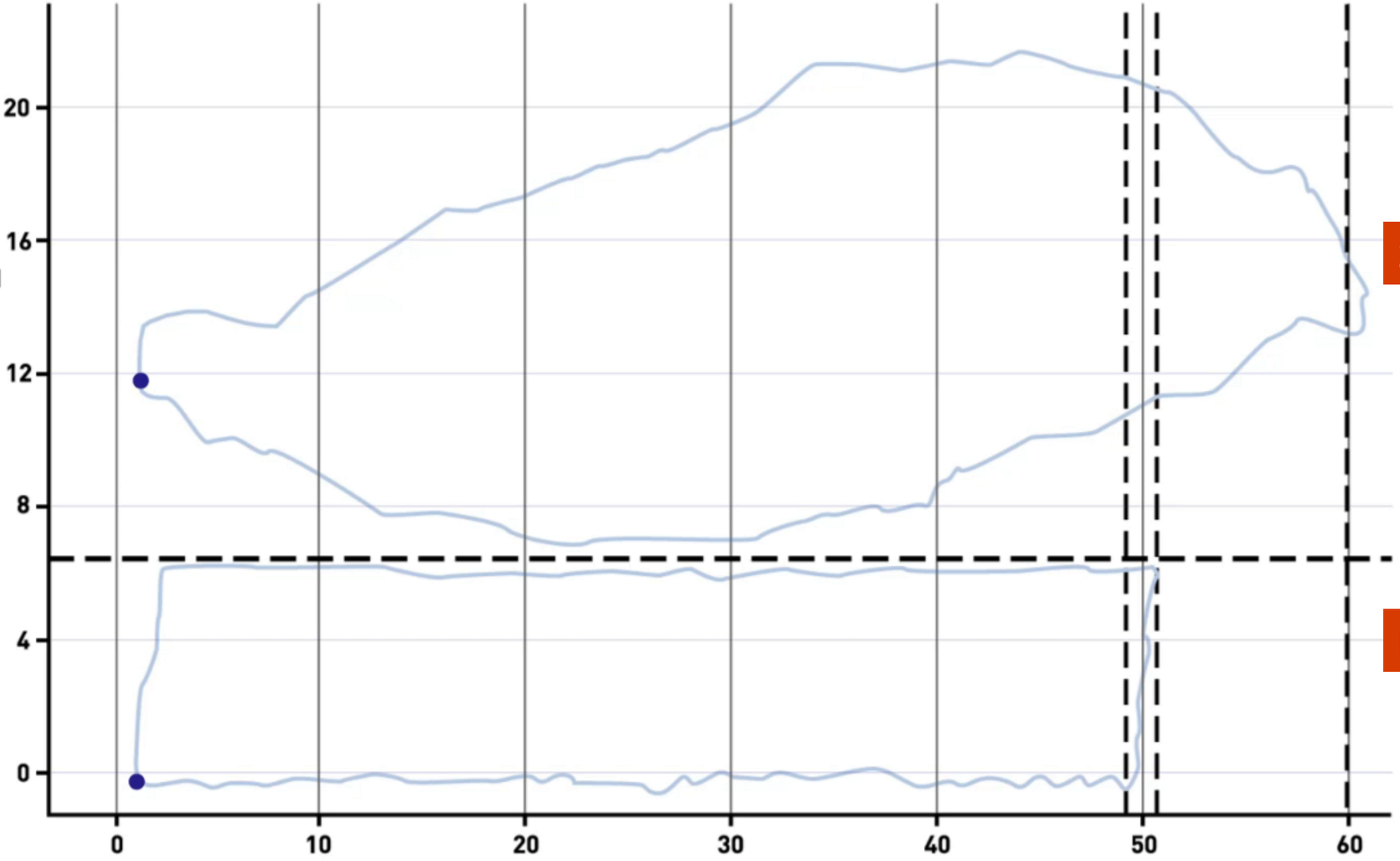
Consistency

Edge in action – Low latency control loops based on machine intelligence

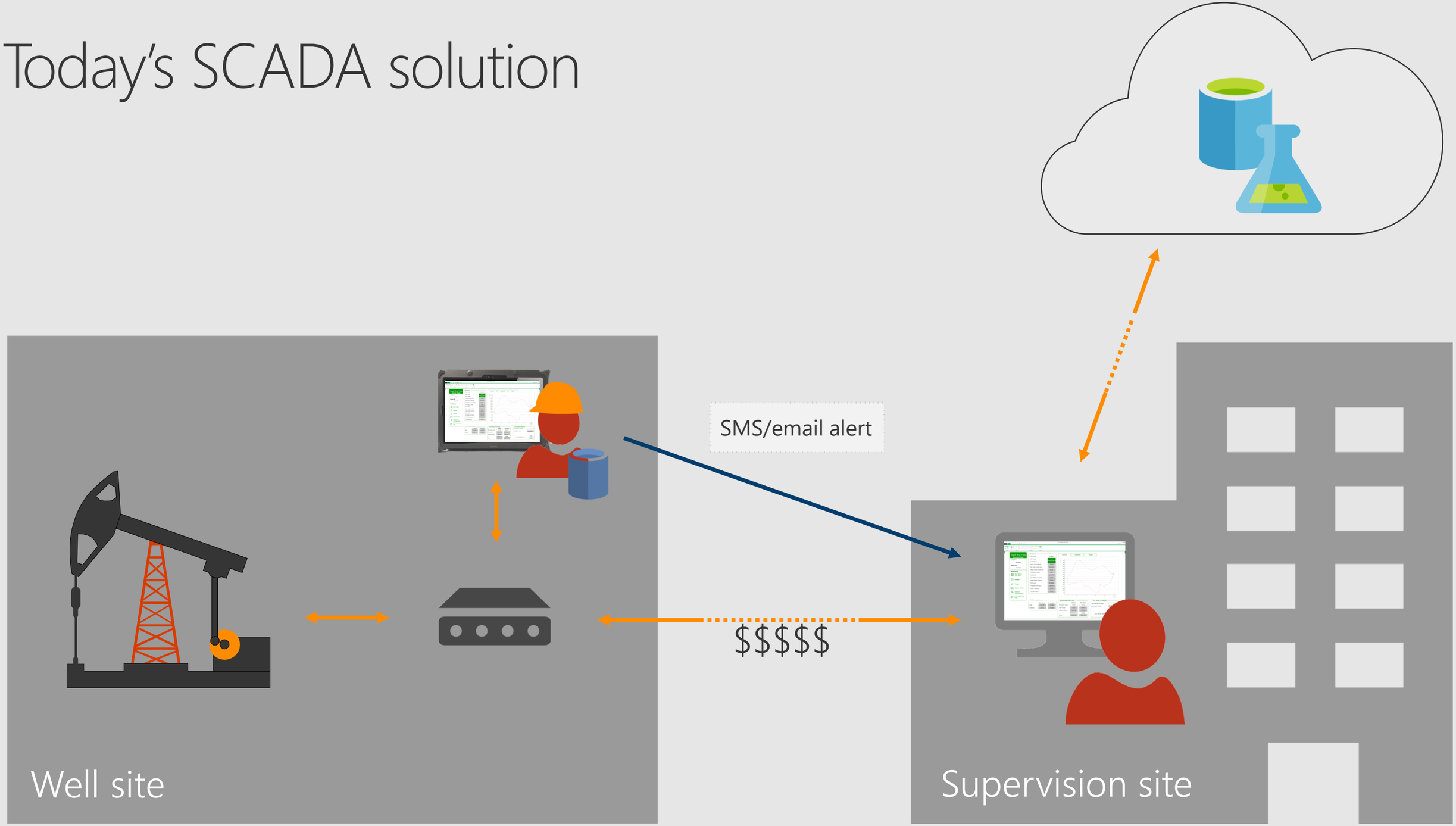
Fluid load



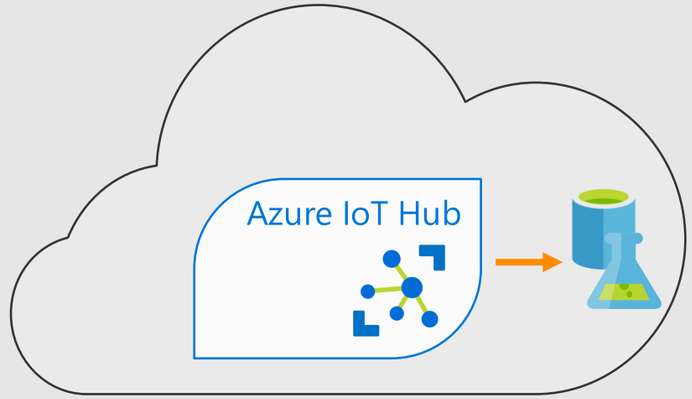


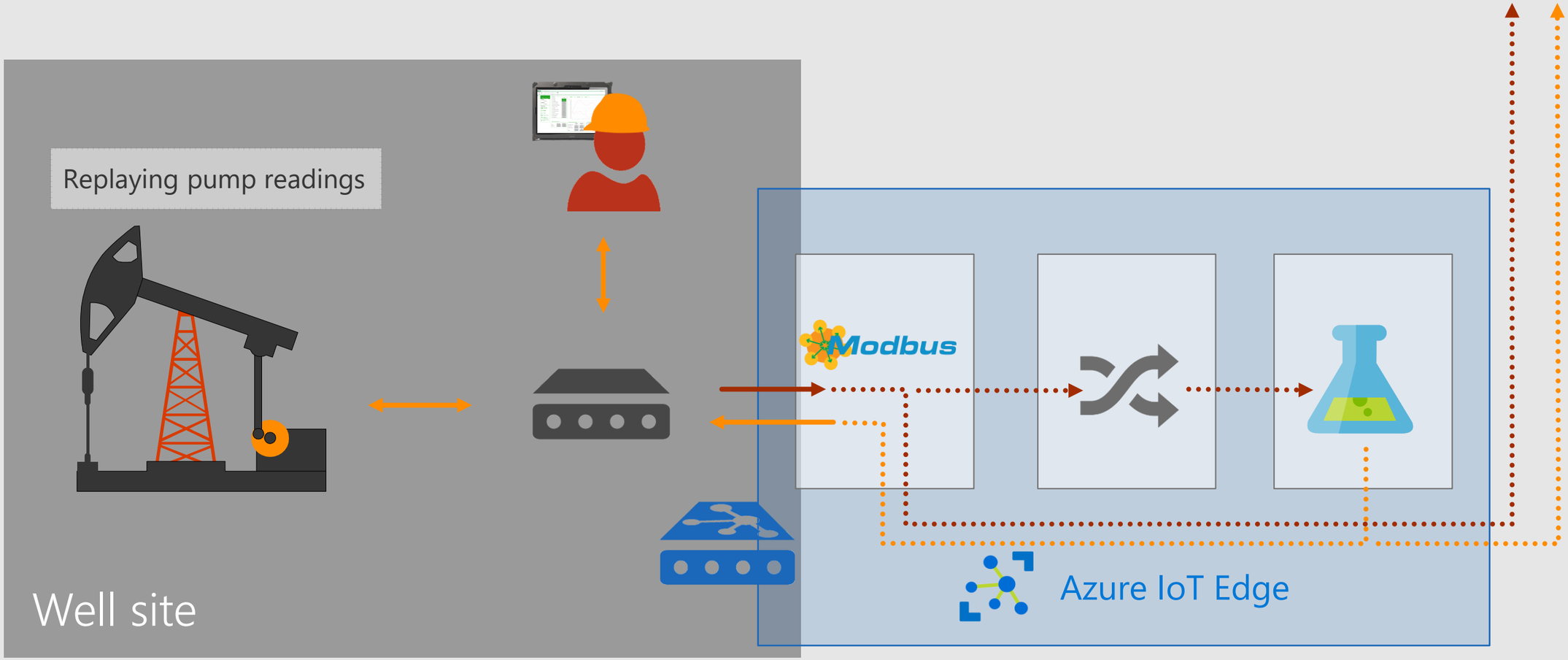


Today's SCADA solution



IoT Edge and ML in action

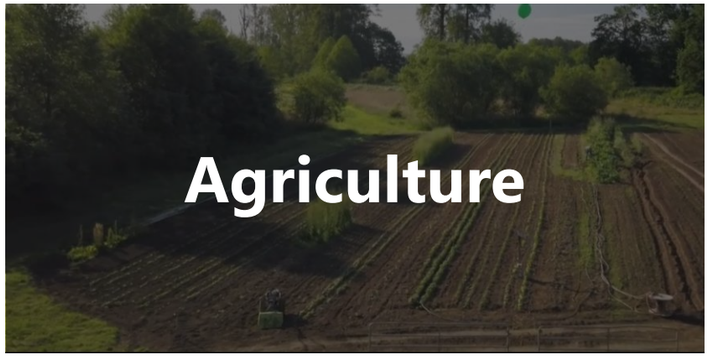




Edge in action - Real-time artificial intelligence on the Edge

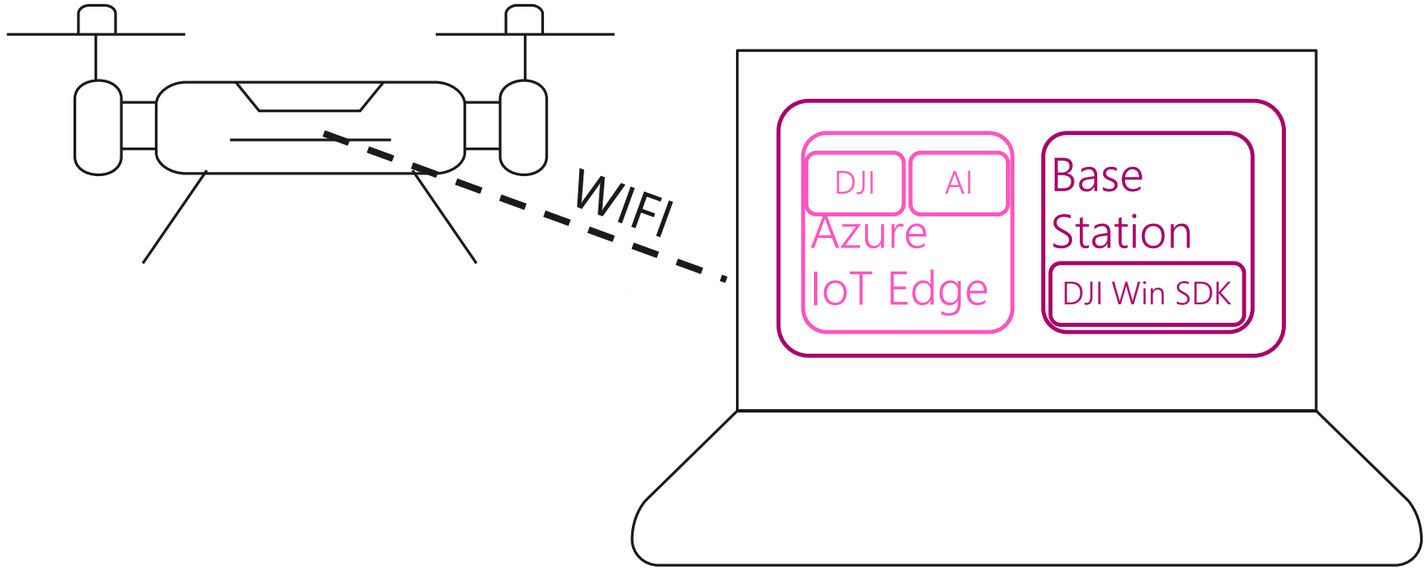
DJI M210 with **payload** running Azure IoT Edge

Many use cases for drones with local Computer Vision capabilities

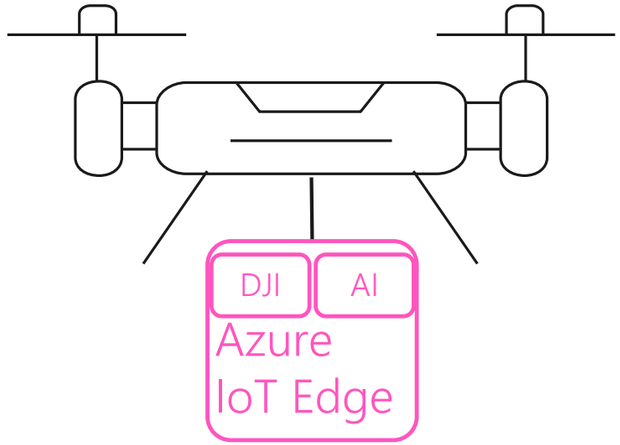


Push AI workloads to any DJI drones with IoT Edge

From base station



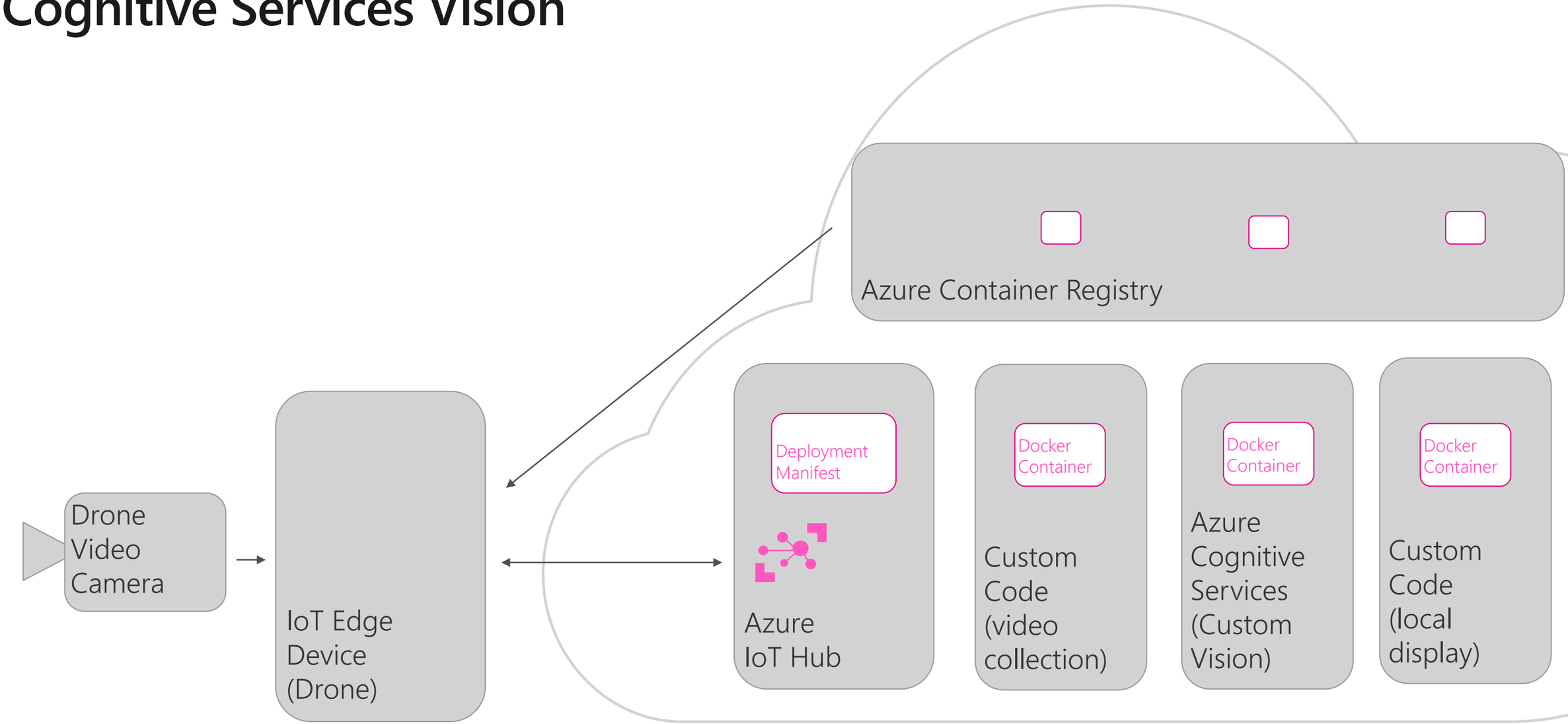
Onflight



DJI Mavic Air

DJI Matrice M210

Azure IoT Edge Deployment
Cognitive Services Vision



AZURE IOT EDGE

ready for the enterprise

Azure IoT Edge

Key Features

OPEN

- Open source Azure IoT Edge
- Moby-based container runtime, compatible with Docker containers
- Cross platform on Linux and Windows
- Azure Edge Marketplace for Edge modules

SECURE

- Zero-touch provisioning of Edge devices at scale with Device Provisioning Service
- Security Manager for end to end security and support for variety of hardware-based root of trust
- Ability to be completely offline for long periods of time

INTELLIGENT

- Services onboarded
  - Custom Vision
  - Azure Functions
  - Azure Stream Analytics
  - SQL Server of Edge
  - Azure Machine Learning

ENTERPRISE READY

- Scaled deployments with Automatic Device Management Service
- Module SDKs in multiple languages (C, C#, Node, Python, Java)
- Development tooling in VSCode
- Multi-person development tools for CI/CD using VSTS

Design principles

Secure

Provides a secure connection to the Azure IoT Edge, update software/firmware/configuration remotely, collect state and telemetry and monitor security of the device

Cloud managed

Enables rich management of Azure IoT Edge from Azure, provides a complete solution instead of just an SDK

Cross-platform

Enables Azure IoT Edge to target the most popular edge operating systems, such as Windows and Linux

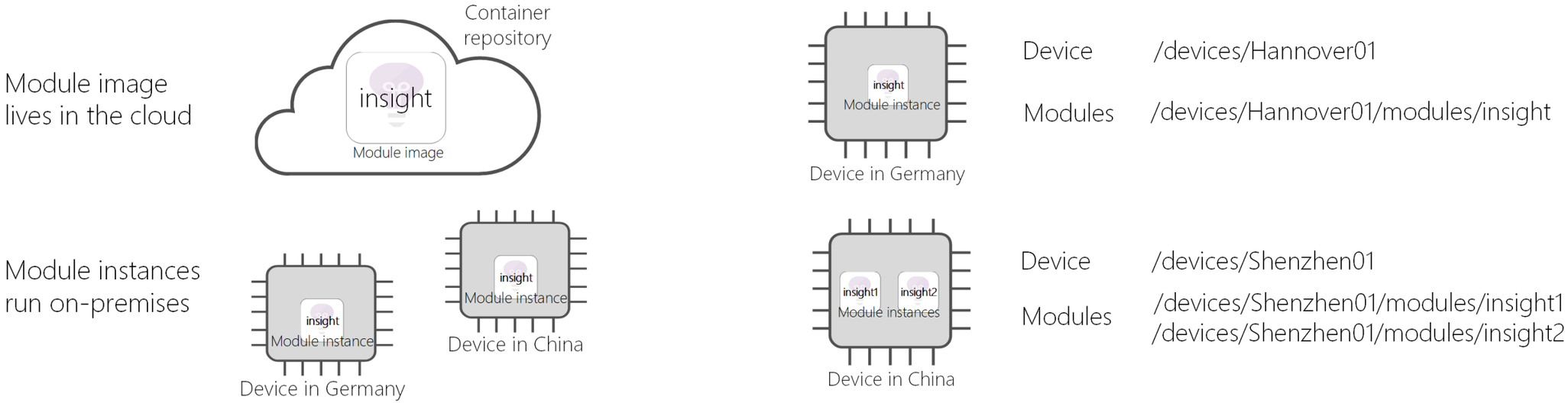
Portable

Enables Dev/Test of edge workloads in the cloud with later deployment to the edge as part of a continuous integration / continuous deployment pipeline

Extensible

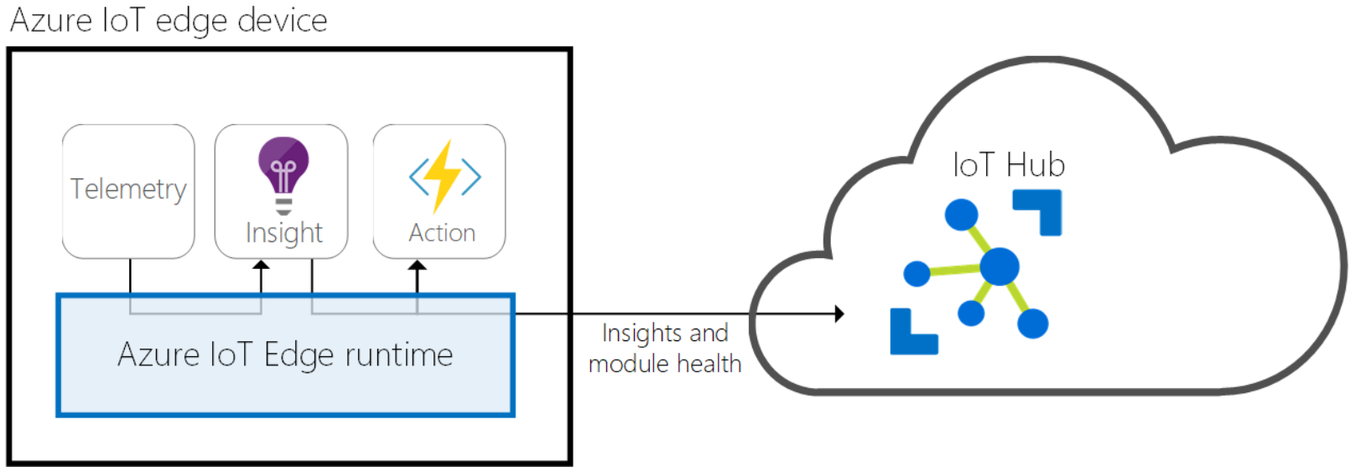
Enables seamless deployment of advanced capabilities such as AI from Microsoft, and any third party, today and tomorrow

Concept – Module



- A **module image** is a package containing the software that defines a module.
- A **module instance** is the specific unit of computation running the module image on an IoT Edge device. The module instance is started by the IoT Edge runtime.
- A **module identity** is a piece of information (including security credentials) stored in IoT Hub, that is associated to each module instance.
- A **module twin** is a JSON document stored in IoT Hub, that contains state information for a module instance, including metadata, configurations, and conditions.
- SDKs to develop custom modules in multiple languages (C#, C, Python, Java, Node.JS)

Concept – Azure IoT Edge Runtime



- Installs and updates workloads on the device.
- Maintains Azure IoT Edge security standards on the device.
- Ensures that IoT Edge modules are always running.
- Reports module health to the cloud for remote monitoring.
- Facilitates communication between downstream leaf devices and the IoT Edge device.
- Facilitates communication between modules on the IoT Edge device.
- Facilitates communication between the IoT Edge device and the cloud

Concept - Routing

```
FROM <source> WHERE <condition> INTO <sink>
```

Sources – source of messages

```
/messages/modules/{mid}/outputs/{out1}
```

Condition – expression on messages properties/body

```
sensorType = “temp” and alert = true
```

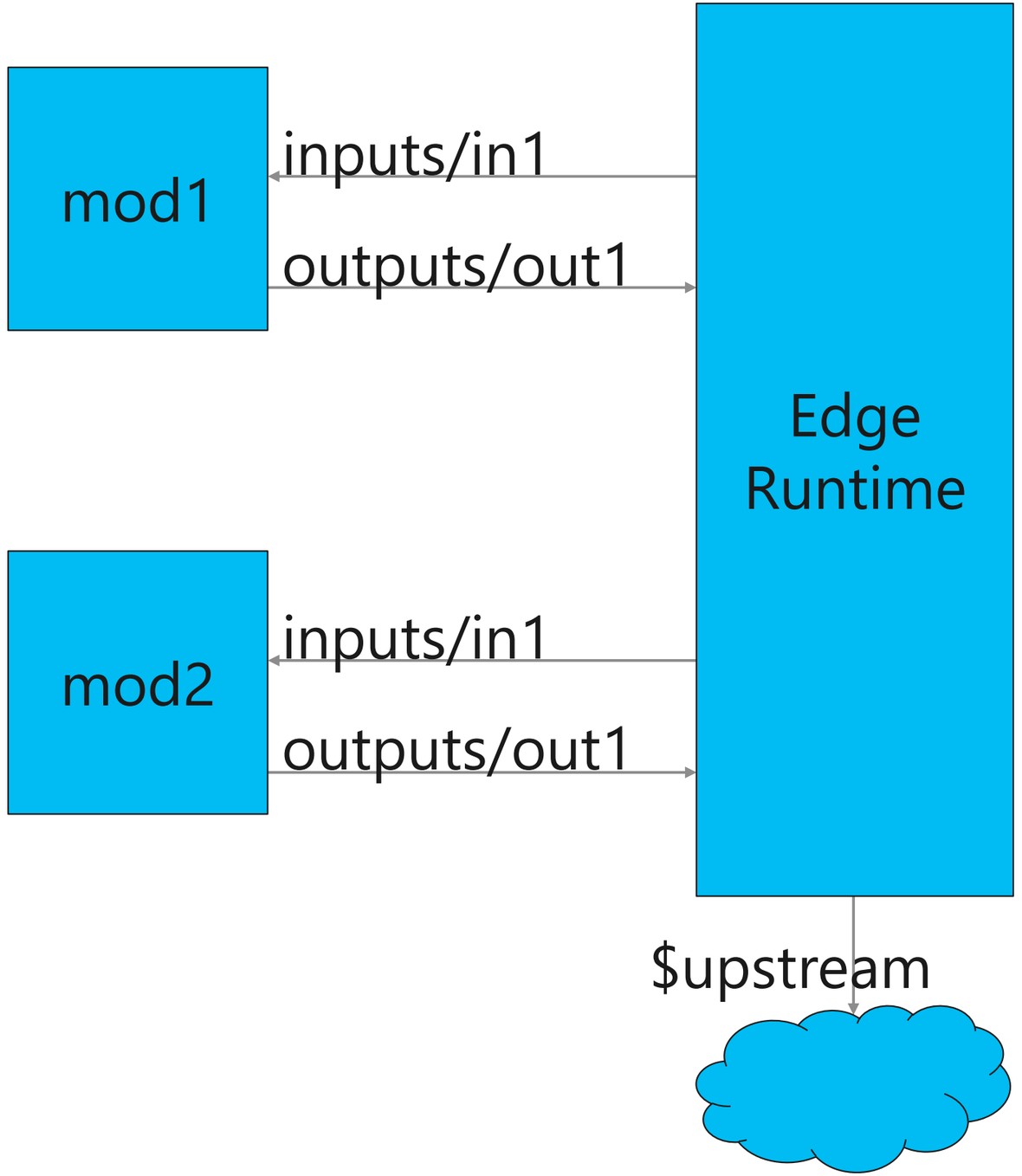
Sinks – destination for messages (endpoints)

```
$upstream
brokeredEndpoint(“/modules/{mid}/inputs/{in1}”)
```

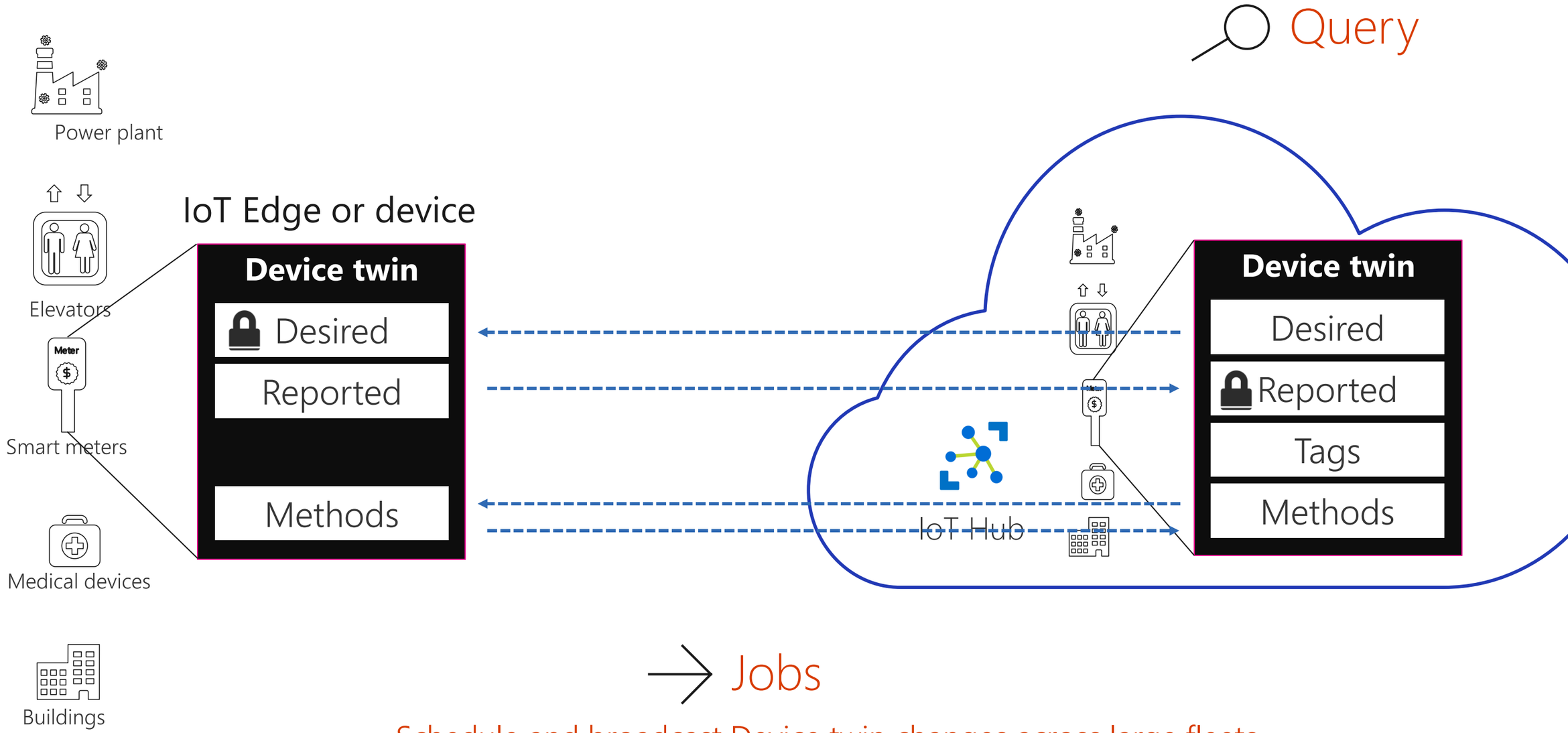
For example:

```
FROM /messages/modules/mod1/outputs/*
WHERE sensorType = “temp”
INTO brokeredEndpoint(“/modules/mod2/inputs/in1”)
```

[Query Language]



Concept – Device Management



Jobs

Schedule and broadcast Device twin changes across large fleets

IoT Edge in action

- Container based workloads
- AI Services
- Azure Functions
- Azure Stream Analytics
- Azure Machine Learning
- Your own code using module SDK

IoT Edge operator

Automatic Device Management Service

1 – Edge device provisioned with right agents for scenario

2 – Select Edge node to deploy to

3 – Define modules on Edge node via device twin

4 – Define message routes for modules on edge node via device twin

5 – Define Module twins for module configurations (parameters)

IoT Hub

Module Twin

Device Twin

Container Modules

IoT Edge

Container Module

Container Module

Container Module

Container Module

Module Twin

Device Twin
- Module
- Routes

Edge runtime

Device Provisioning

Security Manager
- Secure Boot
- Secure Storage

Hardware based root of trust

Local storage

IoT Device with IoT Device SDK

Connects to Edge Hub (Owns a device twin)

IoT Device (e.g. BLE)

Connects to BLE Module for protocol translation (configured via BLE Module twin)

- Edge device with security requirements
- Rich OS – Linux or Windows
- Docker-compatible container management system

Additional Security Threats at the Edge

Readily available tools and experience

The same tools and experience from other disciplines like failure analysis and patent research are easily repurposed for attacks.

Physical accessibility

Subject to physical analysis like on power and timing, and attacks based on micro-probing, fault injections, and environmental tampering.

Requires assertive defense

Non-standard security protocols

Proprietary hardware procedures for common security needs like secure hardware enforcements for secure boot and firmware updates precludes public scrutiny.

Heterogeneous hardware

Expands threat surface across architecture, vendor, and capabilities unlike a relatively more uniform datacenter hardware.

Rich development environment

The necessary mixture of scripted and compiled software using many technologies to enrich user experience also increases the probability for vulnerabilities.

Requires uniformity

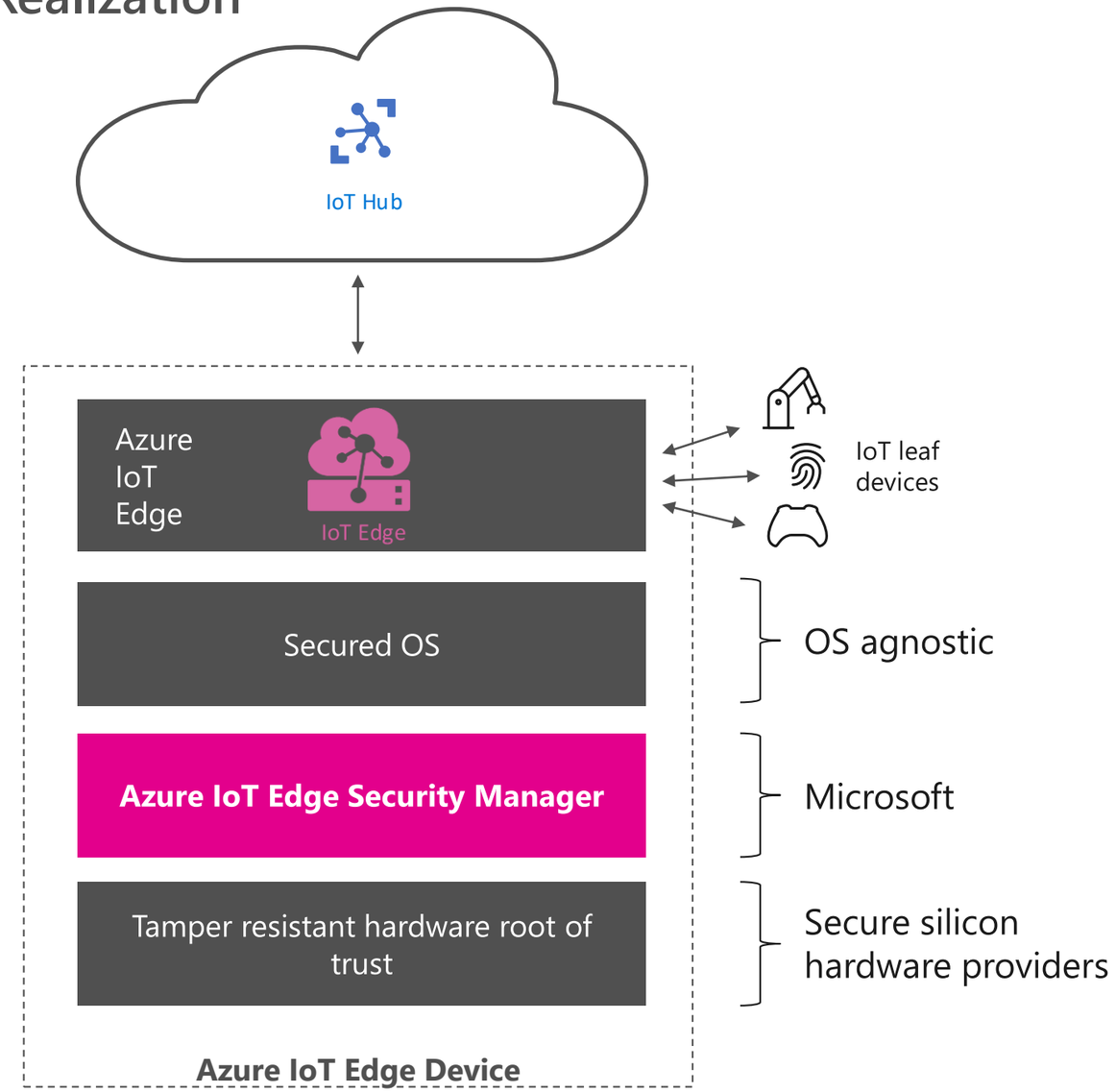
https://azure.microsoft.com/en-us/blog/securing-the-intelligent-edge/

A Framework for Ecosystem Managed Security

Principles

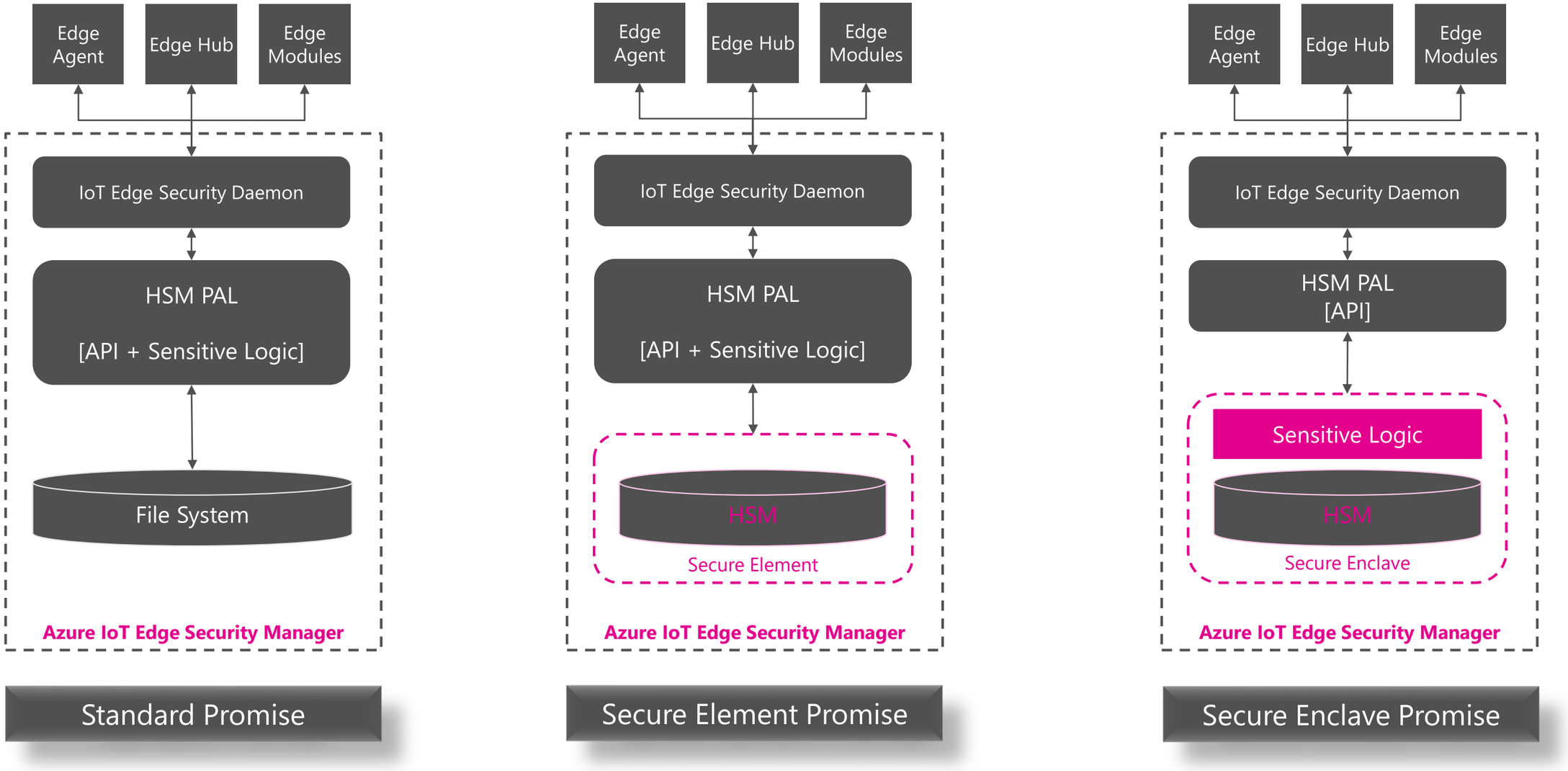
Protected General Computing	Application execution with runtime integrity checking
Secure Execution Environment	Privileged executions and systems resource access control
Secure Boot/Updates	Bootstrapping and recovery
Hardware Root of Trust	Trust anchor and tamper resistance

Realization



Azure IoT Edge *Device* Security Promises

What is the maximum protection you can expect if the device fell into wrong custody?



HSM PAL = Hardware Secure Module Platform Abstraction Layer

Enabling the intelligent edge spectrum

GPU/DSP

FPGA

Sensor Tier | Constrained Tier | Interactive Tier | Industrial Tier | Gateway Tier | Accelerated Tier

LOW POWER CAPABILITIES

HIGH POWER CAPABILITIES

Azure IoT Edge hardware requirements

Rich OS – Windows or Linux

Flexible HW – ARM or x64

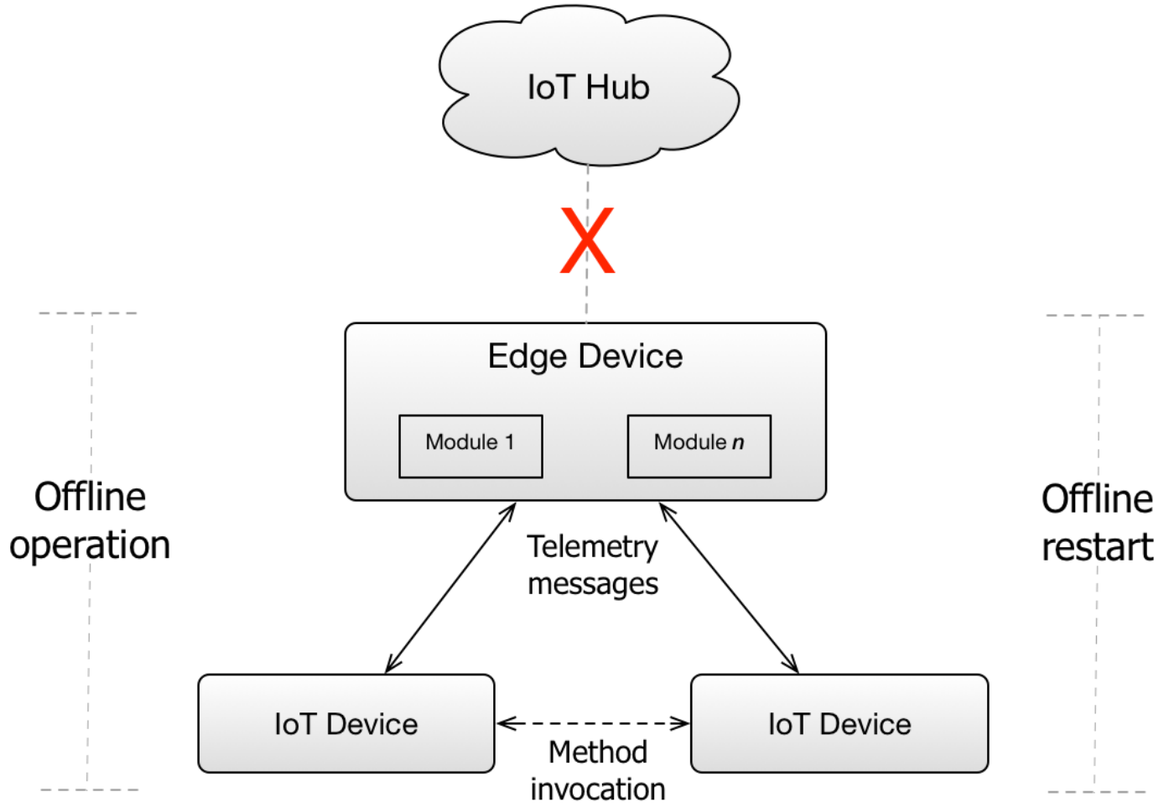
Moby-compatible container runtime

Hardware based security – HSM or Enclave

Hardware sizing depends on workload

Extended Offline

- Indefinite offline operation after one-time sync with IoT Hub!
- Downstream IoT devices can connect to offline Edge device and queue messages for deferred cloud delivery - no code changes, just works!
- Edge + downstream devices can restart and reauthenticate when offline.
- Local Inter-device communication facilitated by Edge Runtime.



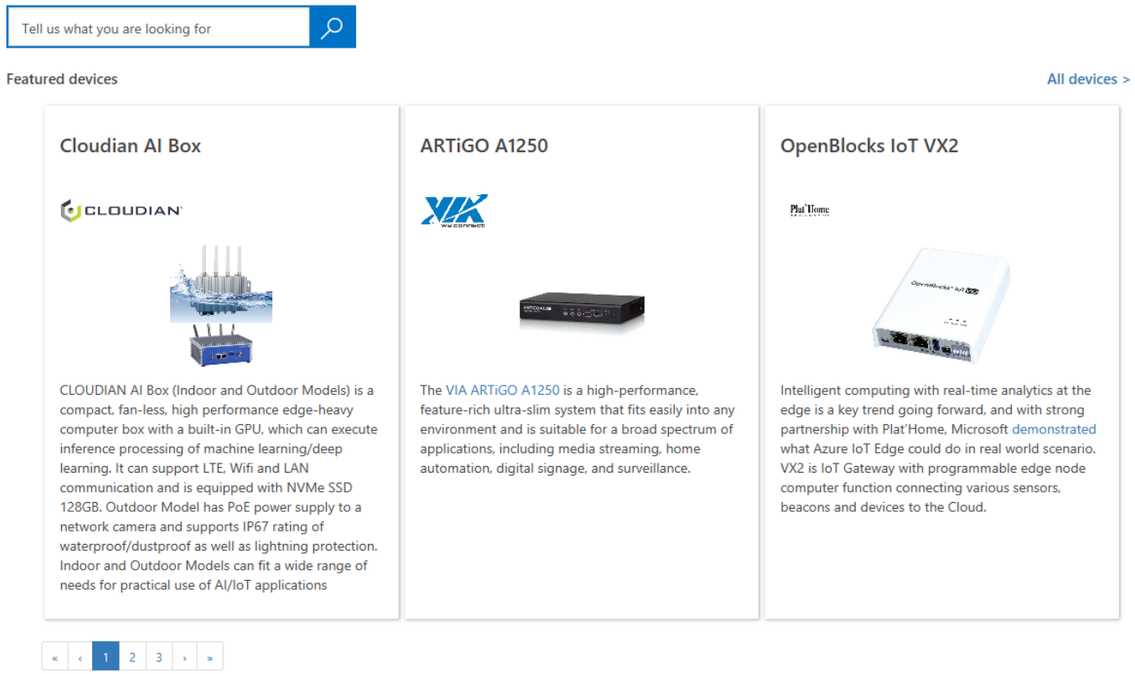
3rd parties can now publish IoT Edge modules into the marketplace!

aka.ms/iot-edge-marketplace

- **Solution developers can save development effort**
  - Discover and integrate certified modules with peace of mind
- **Publishers can showcase their solutions with wide reach**
  - Extend your reach by going to market with Microsoft, a leader in IoT
  - Sign-up: aka.ms/iot-edge-marketplace-signup
- **Coming soon: monetization beyond BYOL**
  - Partners wont need to create an expensive billing system
  - Customers will get one consolidated Azure bill

Azure IoT Edge certified devices

- **Simplifying IoT solution development**
  - All Azure IoT Edge certified devices comes with Azure IoT Edge ***pre-installed***
  - Basic device management functionalities (reboot, FW updates) are validated
- **All certified IoT Edge devices are featured**
  - New landing page in device catalog features all certified IoT Edge devices
- **Increasing momentum**
  - There are 9 certified IoT Edge devices and more to come
  - To learn more about the program requirements, please visit http://aka.ms/certfaq



Edge computing research challenges

- Scale
  - Deploying a fleet of Edge devices with zero touch
  - Managing a fleet of Edge devices centrally
  - Adapting Edge workloads based on constraints (HW, cost, network, etc.)

- Security
  - Moving cloud workloads to on-prem Edge devices requires new security models
  - Securing not just the device, but also data, with provenance
  - Security models for a highly distributed occasionally connected devices

- Operations
  - High availability with low cost devices
  - Multi-vendor, multi-purpose devices – how to control and manage
  - Diverse hardware architectures, OSes, operating conditions

Finally…

- Deploy Azure services to Azure IoT Edge devices
- Deploy your own code in language of your choice
- Manage Azure IoT Edge and downstream devices
- Do all of this securely, in a scalable fashion from the Azure IoT Hub

Azure IoT Edge is free and open source
github.com/azure/iotedge

Research
Faculty Summit 2018

Thank you!