IoT Edge within the IoT Framework

Axel Dittmann
Diplom-Betriebswirt (FH)
Diplom-Wirtschaftsinformatiker (FH)
Global Technical Solution Specialist IOT
CISSP, MCP
Twitter: @DittmannAxel
Waves of Innovation

Cloud
Globally available, unlimited compute resources

IoT
Harnessing signals from sensors and devices, managed centrally by the cloud

Edge
Intelligence offloaded from the cloud to IoT devices

AI
Breakthrough intelligence capabilities, in the cloud and on the edge
When to use edge?
Challenges today create high barriers to entry

**Cloud barriers**
- High volume of data collection sources
- High cost of transporting data to the cloud
- Limits to real-time insights

**Edge barriers**
- High developer skillset for hardware, cloud, edge
- Custom code for everything = No standardization
- Manual set up and integration = Does not scale
Introducing Azure IoT Edge

A service spanning cloud and edge to run cloud intelligence directly on your IoT devices

- Use existing AI, cloud analytics or create your own code
- Deploy workloads as containers via IoT Edge runtime
- Manage devices and containers centrally in the cloud
- Secure solution from chipset to cloud
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**
- Low latency tight control loops require near real-time response
- Protocol translation & data normalization
- Privacy of data and protection of IP

Symmetry
Operational patterns for Azure IoT Edge

- **Protocol translation** – Collect data using any protocol and translate to IoT friendly protocols (e.g. Modbus -> MQTT)

- **On-prem data aggregation and analysis** – Aggregate and save on bandwidth, cost, privacy, IP

- **Offline** – Short or long term

- **Deploy intelligence at the edge** – Azure Machine Learning and AI, Azure Stream Analytics, Functions, your own code
IoT Pattern + Edge

Azure IoT Edge

Aztec IoT Hub

Cloud Gateway

Insights

Actions

Things

Actions
Azure IoT Edge V2 (preview)

- Container based workloads
- Azure Functions
- Azure Stream Analytics
- Azure Machine Learning
- Cognitive Services
- Offline / Synchronized Device Twins
- Local Storage
- Container Management
- Local “IoT Hub”
- HA/DR, Cloud Dev/Test Support

Azure IoT Edge

- Azure Machine Learning (Container)
- Azure Stream Analytics (Container)
- Azure Functions (Container)
- Cognitive Services (Container)
- Custom Code (Container)

Devices

IoT Hub

Edge Hub

Container Management

Local Storage

Device Twin

Module Twin

Device Twin

Module Twin

Device Twin

Module Twin

Device Twin

Module Twin

Device Twin

Module Twin

Device Twin

Module Twin

Device Twin
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 provide 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
Example – Machine Learning on the Edge

Replaying pump readings

Well site

Azure IoT Edge
Next steps

1. Learn more
   aka.ms/azure-iot-edge

2. Get started
   docs.microsoft.com/azure/iot-edge
Thank You
**IoT device lifecycle**

- **PLAN**: Group devices and control access according to your organization's needs.
- **PROVISION**: Securely authenticate devices, on-board for management, and provision for service.
- **CONFIGURE**: Provide updates, configuration, and applications to assign the purpose of each device.
- **MONITOR**: Monitor device inventory, health and security while providing proactive remediation of issues.
- **RETIRED**: Replace or decommission devices after failure, upgrade cycle or service lifetime.
Comprehensive Set of Capabilities for IoT Solutions

- **SaaS**
  - Microsoft IoT Central IoT SaaS
  - Azure IoT Suite
    - Remote Monitoring
    - Predictive Maintenance
    - Connected factory

- **PaaS**
  - Azure Stream Analytics
  - Azure HD Insight
  - Azure Time Series Insights
  - Azure Event Hubs
  - Azure Machine Learning
  - Azure Data Lake Analytics
  - Cosmos DB
  - Azure Data Lake

- **PaaS Services & Device Support**
  - Azure IoT Device SDK
  - Certified Devices Azure Certified for IoT
  - Security Program for Azure IoT
  - Windows 10 IoT Core
  - Azure IoT Hub
    - Azure IoT Hub Device Provisioning Service
  - Azure IoT Edge
  - Microsoft Flow
    - Microsoft Power BI
  - Azure Logic Apps
    - Azure Active Directory
  - Notification Hubs
  - Azure Monitor
  - Azure Websites
  - Azure Websites

- **Device Support**
  - Edge Support
  - IoT Services
  - Data & Analytics Services
  - Visualization & Integration Services
Azure IoT Reference Architecture

**Device Connectivity and Management**
- IP capable devices
- Existing IoT devices
- Low power devices

**Data Processing, Analytics and Management**
- Stream Processors
- Storage
- Device Metadata
- Analytics & Machine Learning
- App Backend

**Business Connectivity**
- Solution UX
- Business Integration

**Optional solution component**
- Custom Protocol Gateway (Cloud Service, VM)

**Azure IoT solution component**
- Gateway
- Cloud Gateway
- Existing Flow JVM/ Azure Container Service

**Intelligence and Interaction** (HoloLens, Cortana, etc)

**Device provisioning**
## The Seven Properties of Highly Secure Devices:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware-based Root of Trust</td>
<td>Unforgeable cryptographic key generated and protected by hardware.</td>
<td>Does the device have an unforgeable identity, inseparable from the hardware?</td>
</tr>
<tr>
<td>Small Trusted Computing Base</td>
<td>Security enforcement features protected from other hardware and software.</td>
<td>Is most of the device’s software outside the device’s trusted computing base?</td>
</tr>
<tr>
<td>Defense in Depth</td>
<td>Multiple countermeasures mitigate the consequences of any one successful attack.</td>
<td>Is the device still protected if the security of one layer of device software is breached?</td>
</tr>
<tr>
<td>Compartamentalization</td>
<td>Internal barriers limit the reach of any single failure.</td>
<td>Can a compromised software sub-component be reset &amp; restarted independently?</td>
</tr>
<tr>
<td>Certificate-based Authentication</td>
<td>Trust brokered using signed certificates, proven by unforgeable cryptographic keys.</td>
<td>Does the device use certificates instead of passwords for authentication?</td>
</tr>
<tr>
<td>Renewable Security</td>
<td>Device security renewed to overcome evolving threats and security breaches.</td>
<td>Is the device’s software updated automatically?</td>
</tr>
<tr>
<td>Failure Reporting</td>
<td>Device failures automatically reported to cloud-based failure analysis system.</td>
<td>Does the device report failures to its creator?</td>
</tr>
</tbody>
</table>

= Silicon support required. = OS support required. = Cloud Service support required.