Università degli Studi di Padova

Master's degree ICT Internet Multimedia Engineering

Department of Information Engineering (DEI)
Master degree on ICT for Internet and Multimedia Engineering (MIME)

Internet of Things and Smart Cities
14 – IoT platforms

Marco Giordani (marco.giordani@unipd.it)
Department of Information Engineering (DEI) – SIGNET Research Group
University of Padova – Via Gradenigo 6/B, 35131, Padova (Italy)

Special thanks to: Dr. Sara Baldoni

Overview

Introduction

- An **IoT platform** is a collection of components providing some functionalities which are common to different IoT systems.
- An IoT system designer can focus on their specific product features and rely on the platform for the common functionalities.
- This allows to reduce complexity, cost, and the time needed for development.

Overview

Requirements

Producer side	Platform side
Miniaturized sensor	Data processing
Component integration	User data aggregation (cross-population trends)
Battery design	Mobile app
Wireless connectivity	Security features
Firmware	Database management
Data fusion	

IoT platforms

Introduction

- An IoT platform needs to be reliable, customizable, scalable and resilient.
- An IoT platform can include the following **functionalities**:
  - Data acquisition from the edge.
  - Data routing.
  - Integration with cloud services (processing, storage, analytics, visualization).
  - Security management.
  - Device management.
  - Development tools and kits (SDKs).

IoT platforms

Introduction

- Usually, there is a **cloud based IoT core** (or **hub**) which establishes connectivity and security between edge devices and cloud services.
  - It is a gateway implementing bi-directional messaging, which filters/routes the messages.
  - The core is accessed through standard protocols such as TCP, HTTP and MQTT.
- IoT core and cloud services are offered as "managed services": the user pays for it, on a usage basis.
- Due to the variety of IoT objects, no support for raw sensor connectivity.
- Users are responsible for creating a software that that interfaces to their specific sensors and makes them compatible with the IoT platforms.

IoT platforms

Introduction

- There are many variants of IoT platforms that are available from commercial vendors and the open-source community.
  - Commercial cloud providers tend to provide rather comprehensive and robust IoT platforms that build upon their existing infrastructure and technology.
- The two most popular IoT platforms, in terms of breadth of coverage, relevance and market presence, are:

  - **Amazon AWS IoT.**
  - **Microsoft Azure IoT.**

Amazon Web Services (AWS)

https://aws.amazon.com

Platform

- The Amazon IoT platform is known as **AWS IoT**.
- It is an example of **Infrastructure as a Service (IaaS)**.
- It is composed of:
  - An **IoT core** which offers cloud-hosted functionalities;
  - An **edge gateway** for external execution (**Greengrass**).
    - Greengrass provides a subset of IoT core functionalities, and resides in the user premises, outside the AWS cloud perimeter.
  - A real-time **operating system** for microcontroller-based things (**FreeRTOS**).
    - FreeRTOS allows the construction of IoT things and constrained devices that can be connected to the AWS IoT cloud.

Amazon Web Services (AWS)

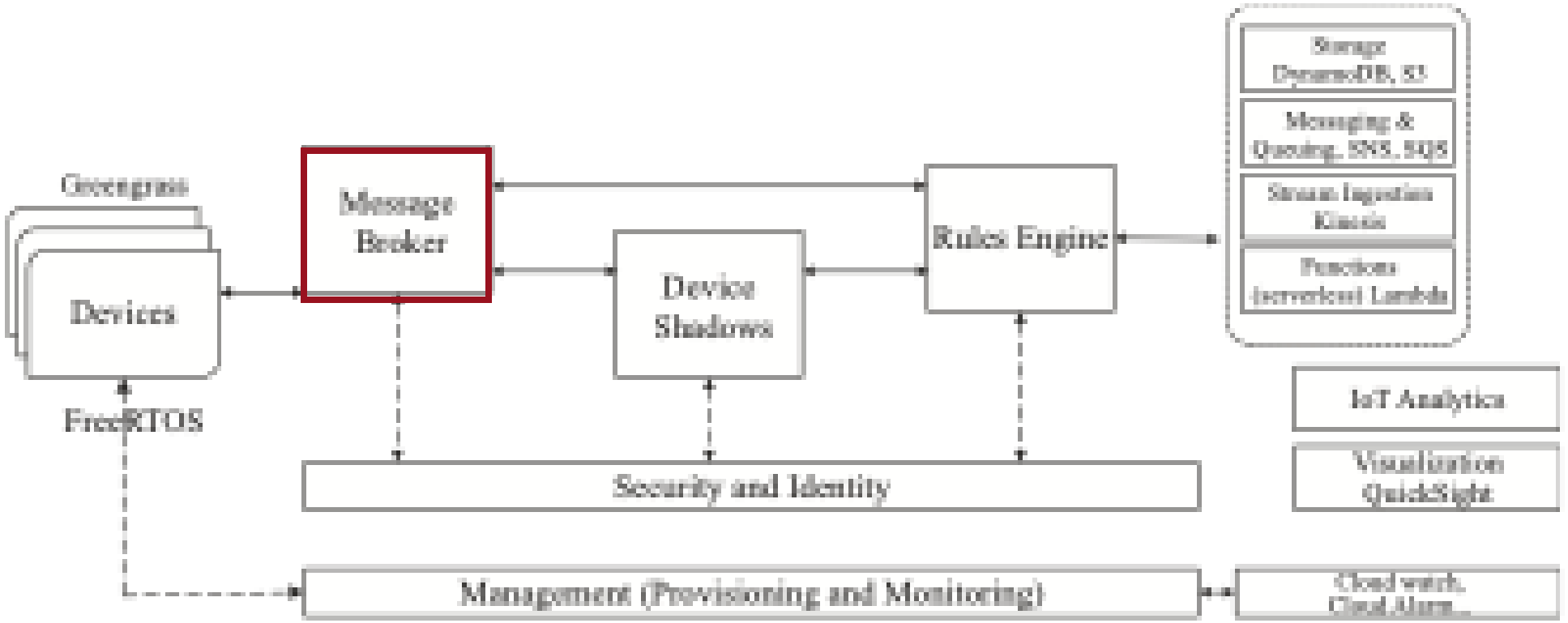
AWS IoT core

- The **IoT core** is composed of:
  - **Data plane**: Drives sensor data into the cloud for processing and storage
    - Message broker.
    - Rules engine.
    - Device shadows (Digital twins).
  - **Control plane**: security and management components.

Amazon Web Services (AWS)

AWS IoT core: Data plane

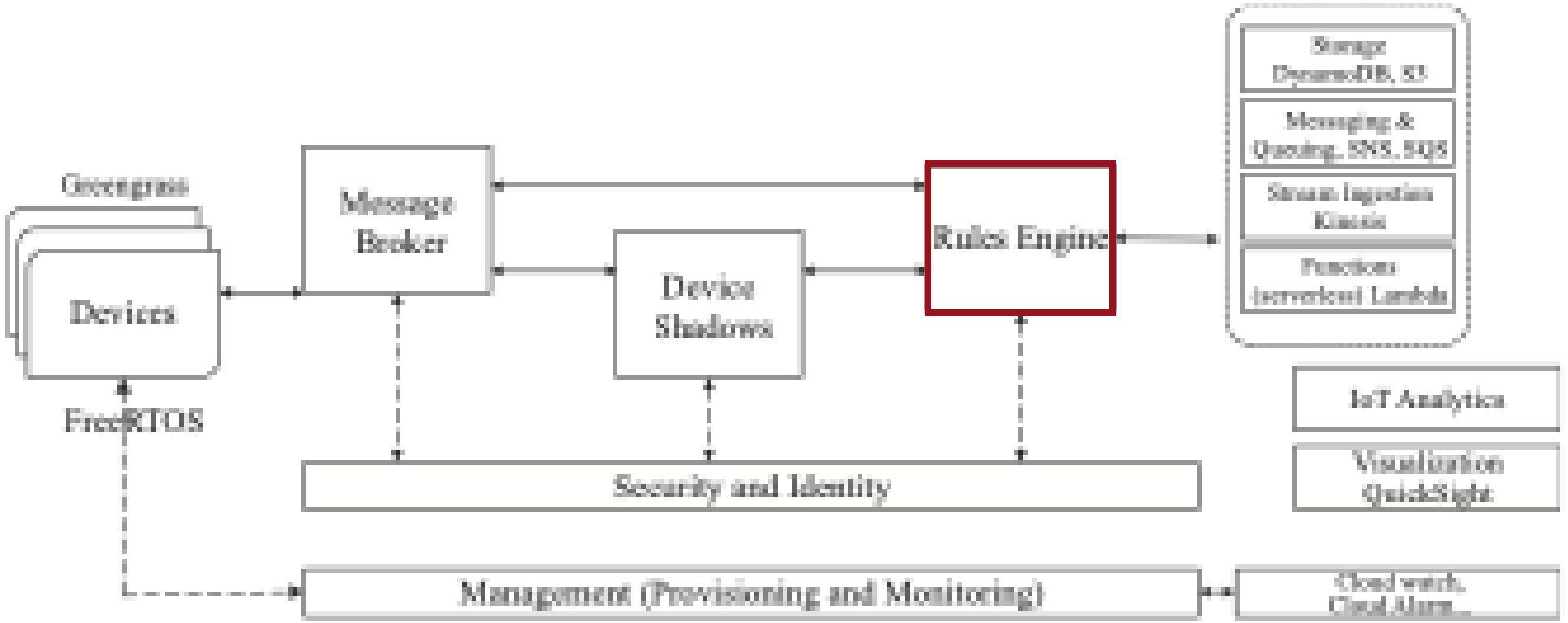
- Supports publish/subscribe via **MQTT**.



Amazon Web Services (AWS)

AWS IoT core: Data plane

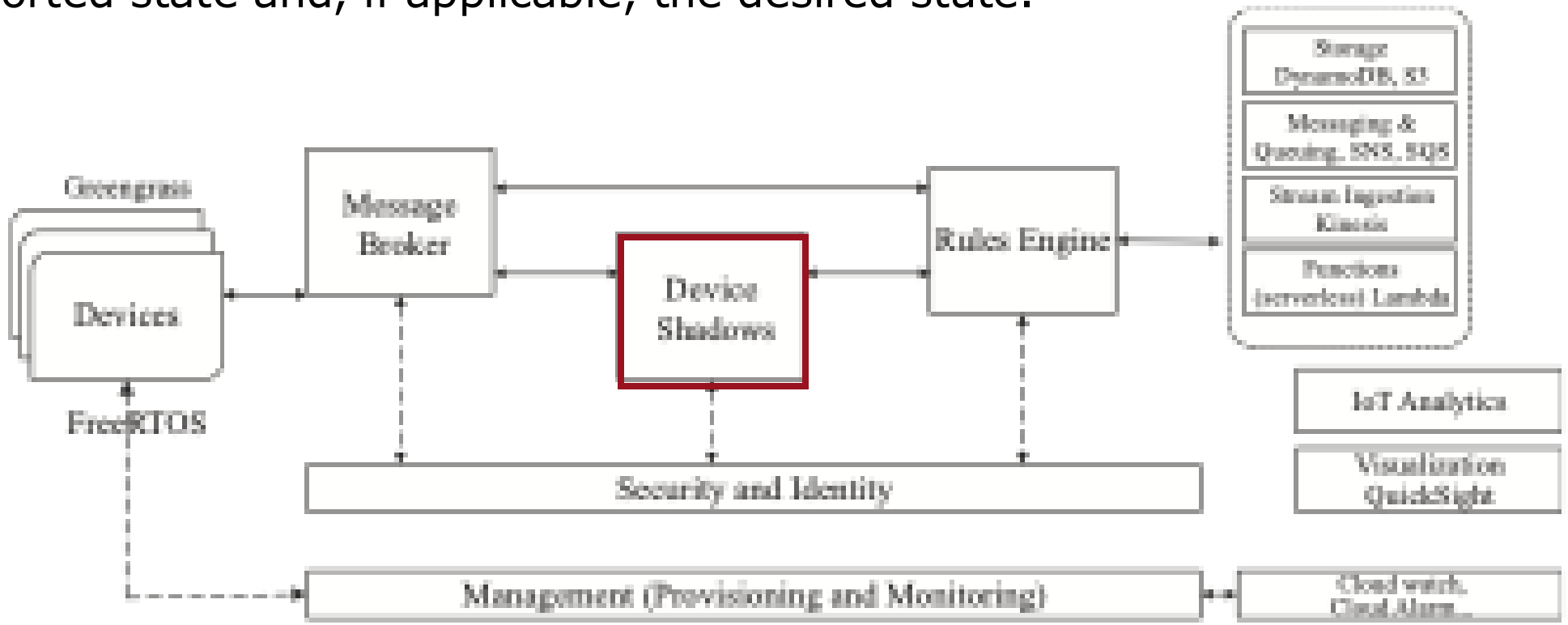
- Processes the payloads to route them to other services.



Amazon Web Services (AWS)

AWS IoT core: Data plane

- **Shadows** are persistent digital representations of the devices containing the last reported state and, if applicable, the desired state.



Amazon Web Services (AWS)

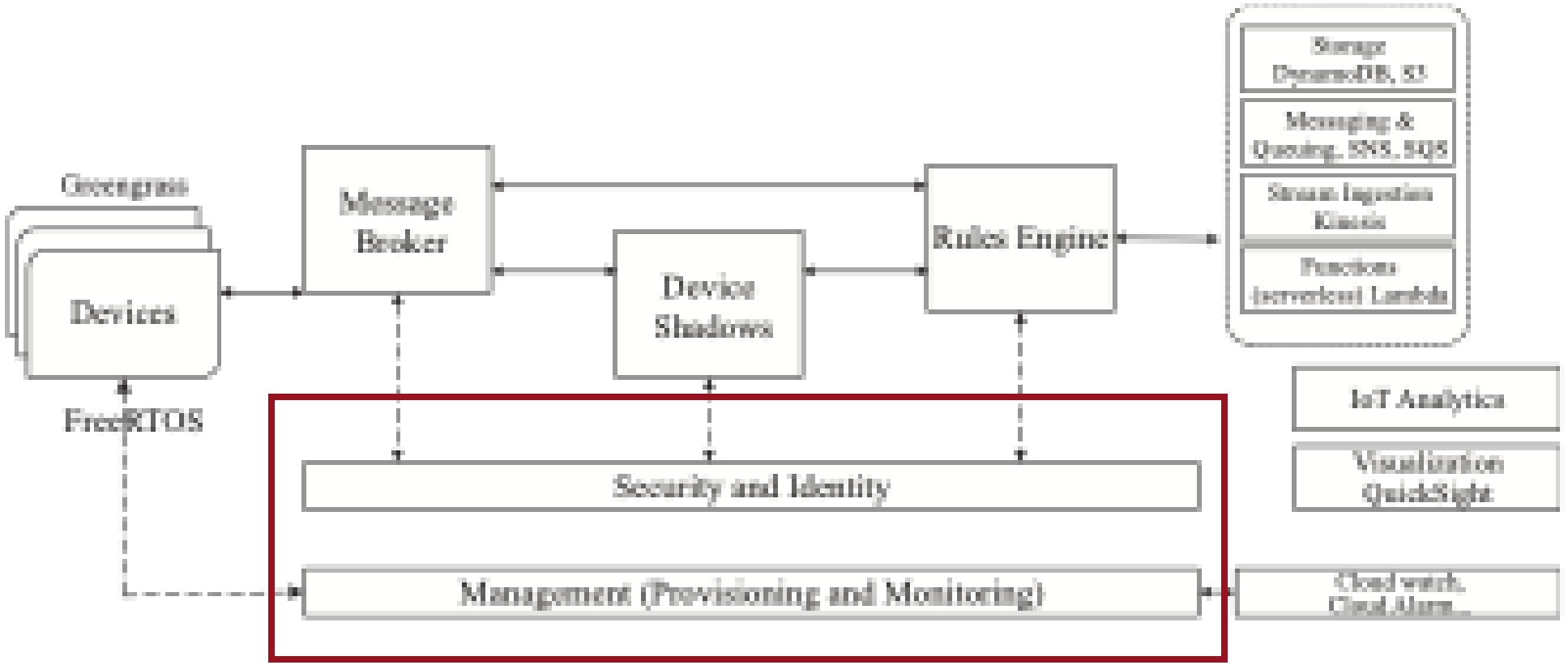
AWS IoT core: Data plane

- The use of shadows allows for the following functionalities:
  - Cloud services access **shadows** to obtain the last known reading and to initiate actions by modifying the desired state to what an output should be.
  - If there is a discrepancy between a reported and a desired state, the shadow instructs the endpoint to initiate the necessary action.
  - Completion of the action is confirmed when the endpoint reports a new state that matches the desired one.
  - Shadows allows applications and services to operate on the last known data even when devices are **disconnected**, thus minimizing disruptions caused by the temporary outages.
  - Cloud services can operate with a simple output abstraction of the desired state, with the edge software handling device-specific steps and protocols.

Amazon Web Services (AWS)

AWS IoT core: Control plane

- Control plane: security and management components.



Amazon Web Services (AWS)

AWS IoT core: Control plane

- The **security** component allows to:
  - Secure the connection and the payload exchange.
  - Handle authentication of devices.
  - Manage authorization. Authorization is expressed as a policy attached to each entity before it accesses the system.
- The **management** component allows to:
  - Register devices (through an ID, custom attributes and security certificates).
  - Perform remote management (software update, security patches, reboot, …).

Amazon Web Services (AWS)

AWS supporting services

- AWS additionally provide supporting services such as:
  - Database (e.g., Amazon Simple Storage (S3) and DynamoDB).
  - Messaging: the **Simple Notification Service (SNS)** sends and receives notifications through SMS, email and social media.
  - Queuing: the **Simple Queue Service (SQS)** stores data in queues retrieved by apps.
  - IoT analytics: interoperates with Amazon general analytics providing tools for data cleansing, forecasting, image, video, and text analysis. It can be integrated with user-supplied functions (data filtering, interpolation, outlier elimination...).
  - General visualization service (**QuickSight**).

Amazon Web Services (AWS)

AWS IoT Edge: FreeRTOS

- Real-time OS (**RTOS**) designed for microcontrollers and small microprocessors.
- Can support the deterministic execution of real-time tasks, memory allocation, static and intertask coordination primitives (e.g., notifications, message queues, multiple types of semaphores, and stream and message buffers).
- Extensions for AWS IoT connectivity, security, and over-the-air updates.
- Primarily intended to enable IoT things and constrained devices to be connected to AWS IoT cloud directly or via a supporting gateway (e.g., Greengrass).

Amazon Web Services (AWS)

AWS IoT Edge: Greengrass

- Software acting as an **edge gateway** to provide secure connection and exchange of data and commands even when disconnected from the cloud.
- It operates at the edge (e.g., on premises and outside of AWS trusted perimeter).
- It easily connects to larger AWS IoT installations through the cloud and provides a local execution environment for cloud-developed services.
- **Data plane** functions:
  - Local message broker, device shadows, Lambda runtime, and support for local execution of ML inference engines.
- **Control plane** functions:
  - Security and authentication management, support for local secrets manager, and hardware security modules including trusted platform module (TPM).

Microsoft Azure IoT

https://azure.microsoft.com/

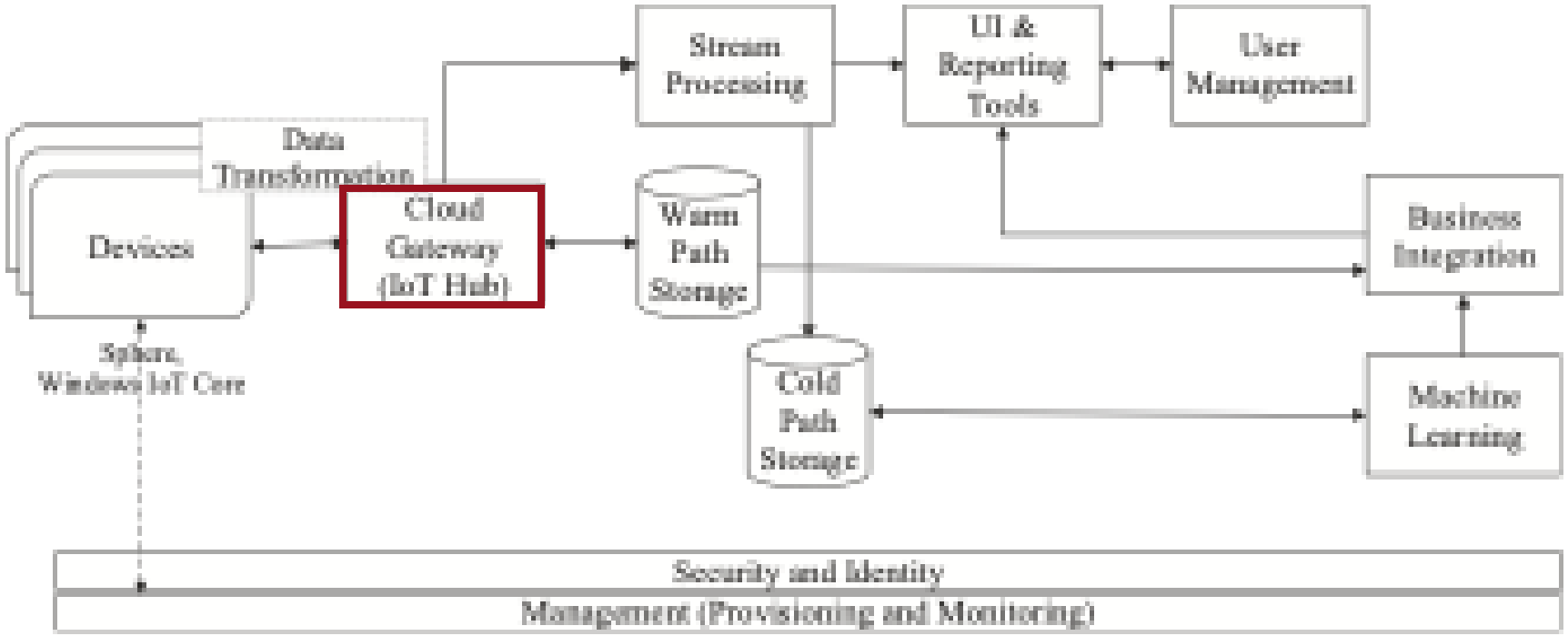
Platform

- It is another example of **Infrastructure as a Service (IaaS)**.
- The main component is the **IoT Hub**: It is the linchpin between the data sources and the cloud back-end processing services is a cloud hosted IoT gateway.
  - It provides the first-point interface for data ingestion and ensures authenticated and secure communication between endpoints and cloud services.
  - It supports brokered-based bidirectional communication and routing of messages based on their type and processing rules.
  - Data routing.
  - Device twins (digital twins).
  - Control plane: security and management.

Microsoft Azure IoT

Azure IoT Hub: Data plane

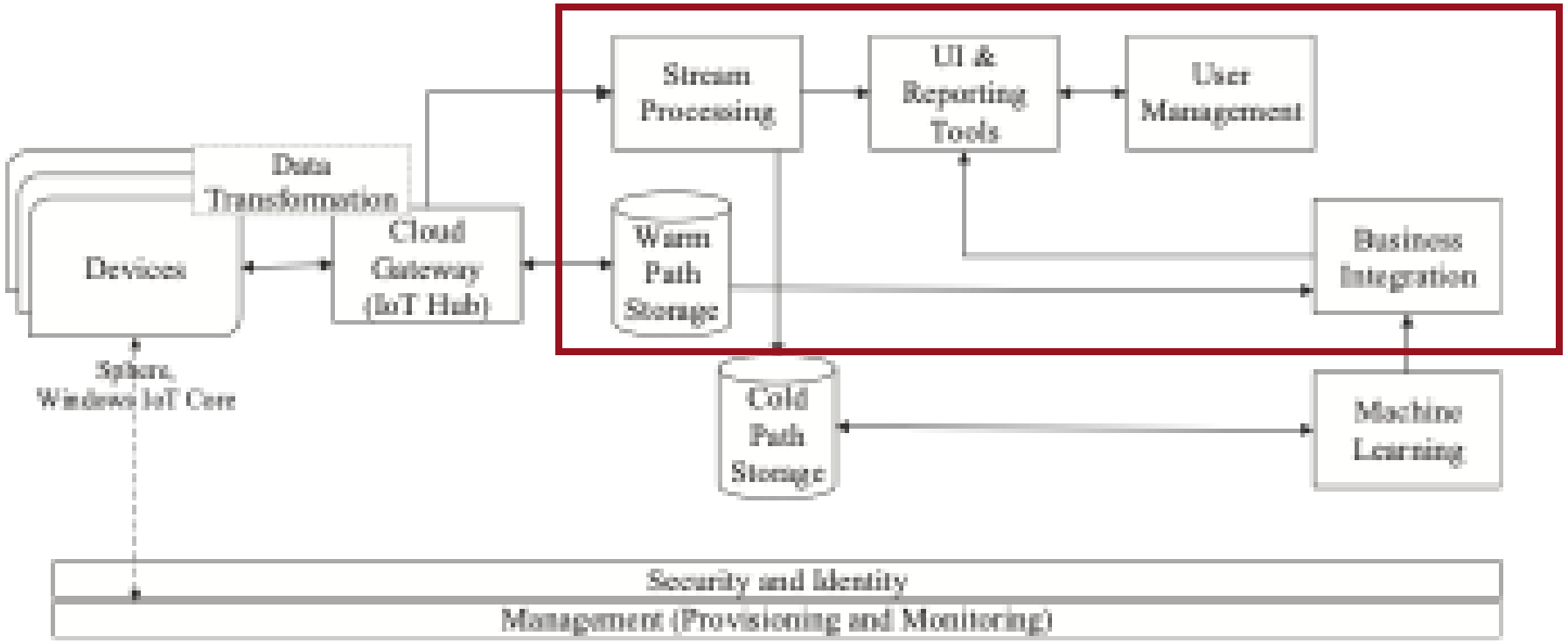
- Device connectivity modes include posting via HTTP and brokered messaging via AMQPP and MQTT in both native and web-socket variants.



Microsoft Azure IoT

Azure IoT Hub: Data plane

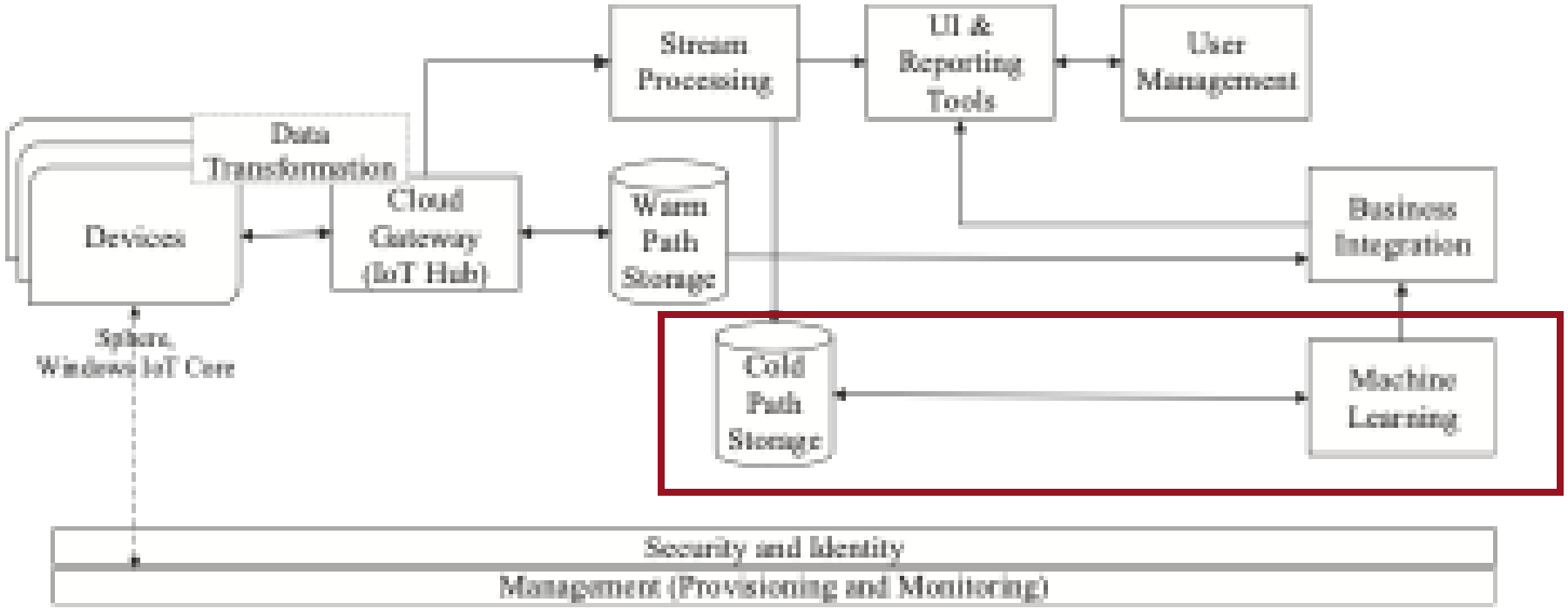
- **Warm path** (towards the stream processing for low-latency processing).



Microsoft Azure IoT

Azure IoT Hub: Data plane

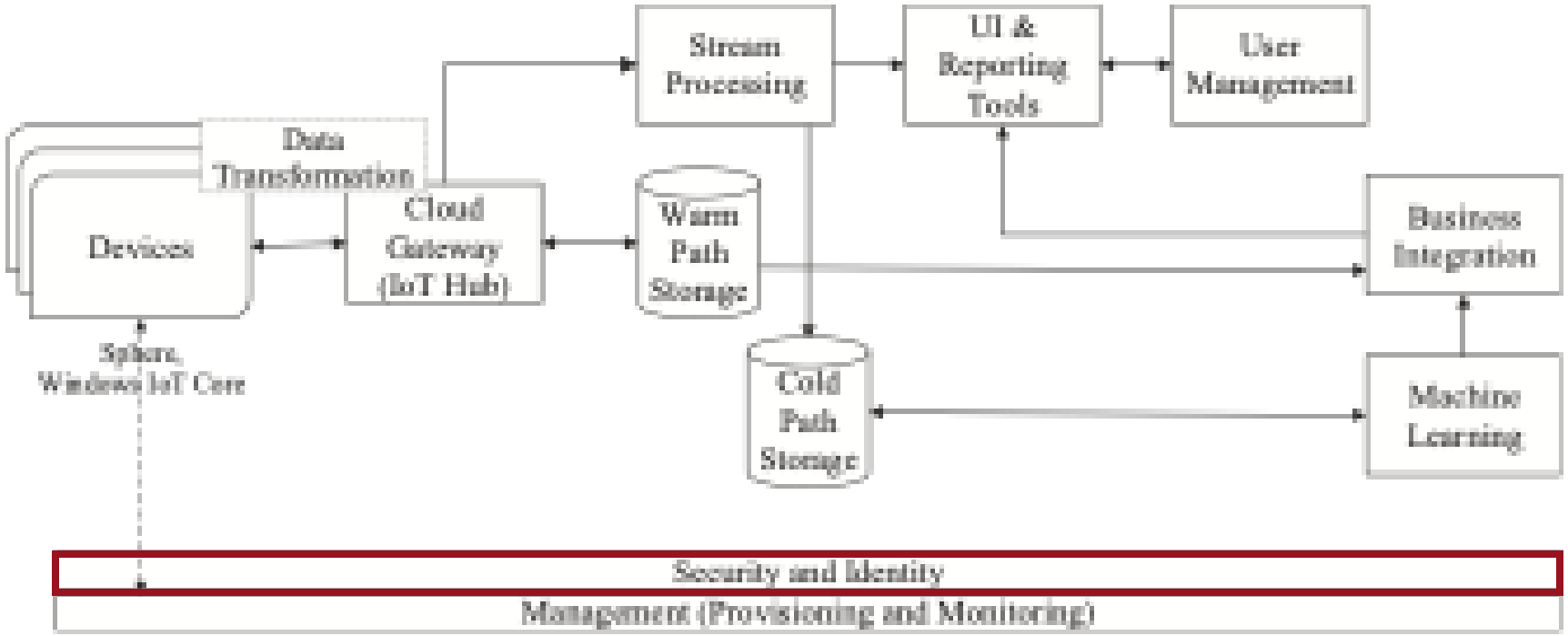
- **Cold path** (towards the storage): supports more complex queries on larger aggregate data sets that may be required by analytics and ML that take longer time.



Microsoft Azure IoT

Azure IoT Hub: Control plane

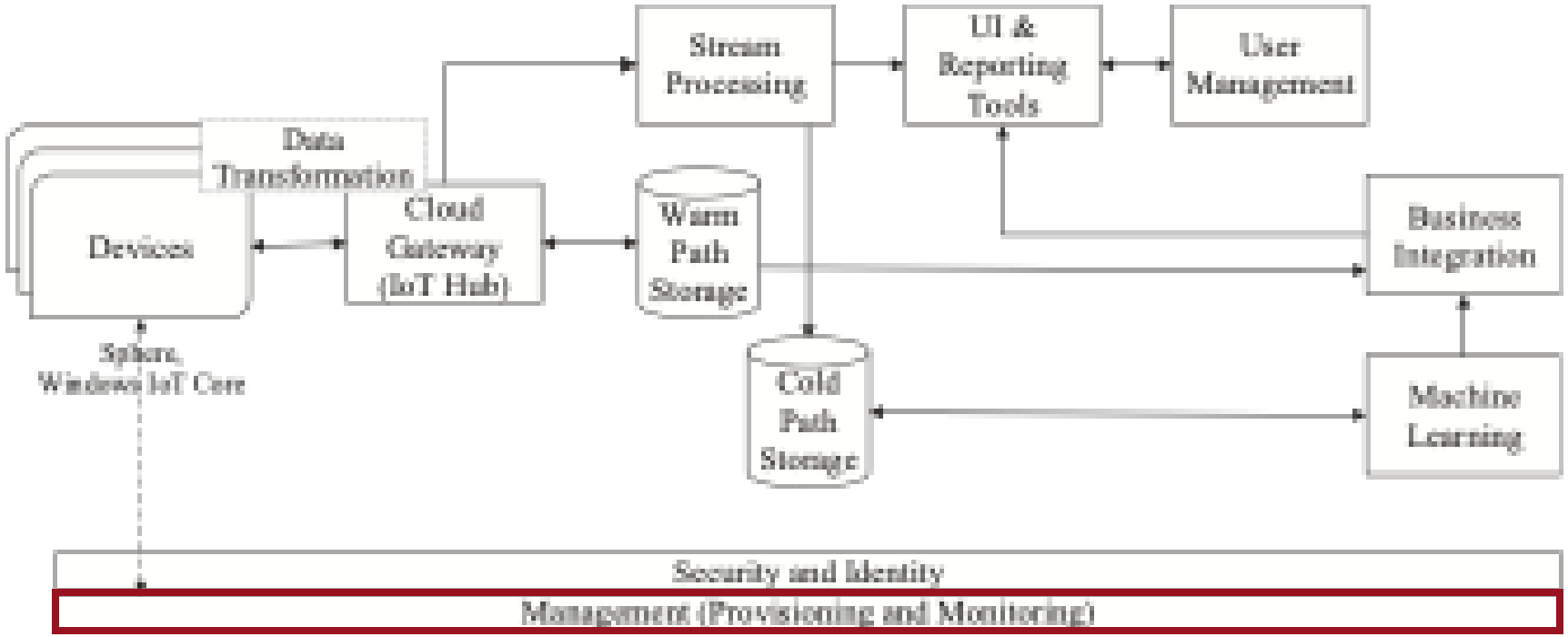
- **Security**: authentication, rule-based authorization and encryption (at the transport layer using TLS or DTLS for TCP and UDP connections, respectively).



Microsoft Azure IoT

Azure IoT Hub: Control plane

- **Management**: Device planning, provisioning (identity and security credentials), and retirement of individual devices and in bulk for groups.



Microsoft Azure IoT

Azure IoT supporting services

- Azure IoT provides additional supporting services such as:
  - **Time Series Insights (TSI)**: an analytics storage and visualization service.
  - **CosmosDB**: a NoSQL database.
  - **Azure monitor**: a tool which allows the connection to a device for extracting its logs and obtain insights about the operation of the system (+ visualization functionality).
  - **Azure IoT Edge**: it provides the following functionalities:
    - It runs on customer premises outside the cloud.
    - It provides a subset of IoT functions, support for local execution of applications.
    - It allows cloud connectivity.
    - When connectivity to the cloud is lost, the IoT Edge hub goes into the offline mode and buffers messages destined to go to the cloud.

Microsoft Azure IoT

Azure IoT Edge

- Edge devices can connect to the cloud via an IoT hub assuming they meet security requirements and can handle the required protocols and procedures.
- For less capable and legacy devices, Microsoft provides the **Azure IoT Edge** that runs on customer premises and outside of the cloud. It provides:
  - Device upward cloud connectivity and performs communications gateway functions and protocol and format conversions if necessary.
  - Connection multiplexing for underlying devices over a common single connection to the cloud (congestion control and isolatation to support security).
  - Data format and protocol translations, if needed.
  - Support for local execution of applications, and limited operation when offline.
  - Hardware security features, such as trusted platform module (TPM) and hardware security module (HSM), if available.

Microsoft Azure IoT

Azure IoT Edge

- Azure IoT Edge includes two operating systems that may be used at the edge to streamline development and cloud connectivity:
  - **Windows IoT Core**: a scaled down version of Windows OS targeted for embedded devices that uses tools and interfaces familiar to Windows developers.
  - **Azure sphere**: an OS designed for constrained edge devices. It is a secure operating system for real- time processing that supports cloud connectivity and over-the-air software and security updates.

Microsoft Azure IoT

Azure IoT Saas and PaaS

- Azure IoT offerings also include SaaS and PaaS variants:
  - **Azure IoT Central** (SaaS): intended to simplify the development of IoT solutions that do not require much service customization.
    - It makes use of Azure IoT architecture and services (such as the IoT hub and the basic analytics), without exposing their intricacies directly to the users.
    - Dashboard and functions can be accessed from browsers on PCs and tablet.
    - It can be used to define and manage connected devices.
  - **Azure IoT solutions accelerators** (PaaS): complete IoT reference solutions for common IoT scenarios with open-source code that users can customize and deploy.
    - Focus primarily on the application part and connection with Azure IoT services.
    - Main scenarios: remote monitoring, connected factory, predictive maintenance, device simulation.

Other IoT cloud platforms

Examples

- Google IoT: https://cloud.google.com/architecture/connected-devices/iot-platform-product-architecture
- IBM Watson: https://www.ibm.com/it-it/watson
- Oracle IoT Cloud: https://docs.oracle.com/en/cloud/paas/iot-cloud/index.html
- Cisco IoT Cloud Connect: https://www.cisco.com/c/en/us/solutions/internet-of-things/iot-control-center.html
- ThingWorx IIoT Platform: https://www.ptc.com/en/products/thingworx
- Altair SmartWorks: https://altair.com/altair-iot-studio
- …