What is Azure Sphere?

Azure Sphere is a high-end application platform, equipped with integrated security and communications features, for Internet-connected devices, including an MCU, custom Linux-based operating system, and security services. Cloud-based security.

Azure Sphere MCU integrates real-time processing capabilities with the ability to run advanced operating systems. An Azure Sphere MCU, along with its operating system and application platform, allows creation of security devices, Internet connections that can be updated, controlled, monitored and maintained remotely.

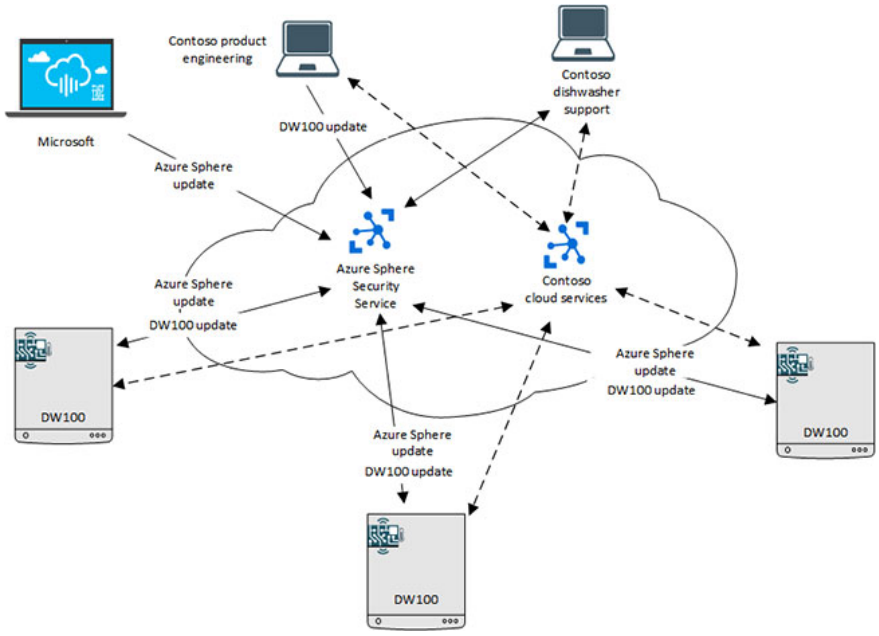
Learn about Azure Sphere

What is Azure Sphere?

Azure Sphere is a high-end application platform, equipped with integrated communications and security features, for Internet-connected devices. It includes a microcontroller (MCU), custom high-level Linux-based operating system, and cloud-based security services.

How Azure Sphere works

To understand how Azure Sphere works in a real world environment, consider this scenario:



Dishwasher network connection

Contoso, Ltd., a manufacturer of electrical appliances, has embedded MCU Azure Sphere into its dishwasher products. The DW100 dishwasher combines the MCU with a number of high-end sensors and applications running on the MCU Azure Sphere. The application communicates with Azure Sphere Security Service and Contoso cloud services.

Dishwasher network connection

Start from the top left and move clockwise:

1. Microsoft releases updates for the Azure Sphere operating system through the Azure Sphere Security Service.
2. Contoso's product technical department releases updates for the DW100 application through the Azure Sphere Security Service.
3. Azure Sphere Security Service deploys updated operating systems and Contoso DW100 application software for dishwashers at end user locations.
4. The Contoso dishwasher support center communicates with Azure Sphere Security Service to determine which version of the Azure Sphere software and DW100 application software will run on each end user's device, collecting any reporting data. Which bug has been reported, then contact the Contoso cloud service for more information.
5. Contoso cloud services support application troubleshooting, data analysis, and customer interaction. Contoso cloud services can be hosted by Microsoft Azure, another vendor's cloud service, or Contoso's own cloud.
6. Contoso DW100 models at end-user locations download application software and the operating system is updated via connection to Azure Sphere Security Service. They can also contact the Contoso cloud service application to report additional data.

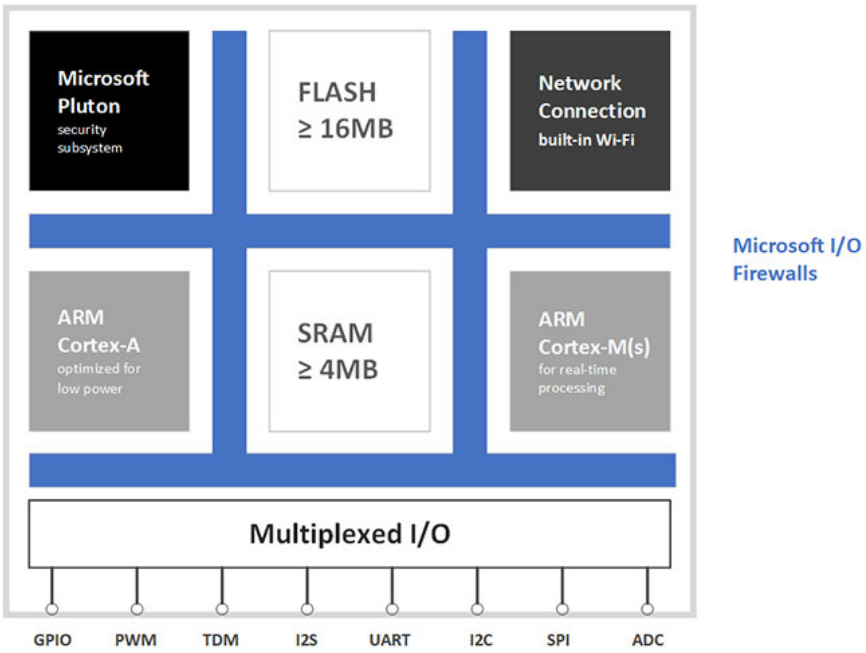
7 security features of Azure Sphere

The Azure Sphere platform is designed around these 7 properties:

1. **Use the Hardware Root of Trust process** : The Hardware Root of Trust ensures that the device and its identity cannot be separated, thus preventing device tampering. Each Azure Sphere MCU is identified by a cryptographic key, created and protected by the Pluton security subsystem hardware designed by Microsoft. This ensures hardware security, anti-tampering from the factory to the end user.
2. **Trusted Computing Base (TCB)** : Most of the device's software is still outside the Trusted Computing Base (TCB - a collection of all hardware, firmware and / or software components that are important for security). Only the Security Monitor, the Pluton runtime, and the Pluton subsystem, all provided by Microsoft, run on the TCB.
3. **Defense in depth** : Defense in depth is a concept used in information security, where many layers of security control are placed in IT systems, providing a variety of mitigation measures against each threat. Each software layer in the Azure Sphere platform verifies that the layer above it is also secure.
4. **Roadblock** : The roadblock to limit the scope of any problems. Azure Sphere MCU provides countermeasures, including firewalls to prevent security breaches in one component affecting other components. A limited sandbox runtime environment prevents applications from damaging code or security data.
5. **Certificate-based authentication** : The use of signed certificates, authenticated by a cryptographic key, provides a level of authentication much stronger than a password. The Azure Sphere platform requires all software elements to be validated. Communicate between device and cloud to the device that requires certificate-based authentication.
6. **Renewable security** (a concept developed after the continuous hacking of analog TV encryption systems in the late 1980s. Simply put, instead of completely replacing a hacked encryption system, only a small part needs to be replaced to make it secure again): Device software is automatically updated to fix known security vulnerabilities or breaches, without requiring intervention from the product manufacturer or end user. Azure Sphere Security Service automatically updates the Azure Sphere operating system and applications.
7. **Crash reports** : Errors in software or device hardware are typical examples of emerging security attacks. Communication from device to cloud provides early warning of potential errors. Azure Sphere devices can automatically report operational and failure data to a cloud-based analysis system, and updates and services can be performed remotely.

Technical parameters

Hardware architecture



Hardware architecture

1. Azure Sphere MCU hardware architecture

Each core and its associated subsystem are in a different trusted domain. In each class, resource segregation and zoning provide additional security measures.

1. Microsoft Pluton security subsystem

The Pluton security subsystem includes a security processor core, encryption tool, hardware random number generator, public and private key generation, asymmetric and symmetric encryption, and support for ECDSA verification.

1. High-end application core

The high-end application core has the ARM Cortex-A subsystem with full MMU. It allows localization of hardware-based processes and is responsible for executing the operating system, high-end applications, and services.

1. Real-time core

Real-time core (s) with I / O ARM Cortex-M subsystem can run applications in real time as bare-metal code or RTOS (Real-Time Operating System). Such applications can map peripherals and communicate with advanced applications, but do not have direct access to the internet.

1. Connect and get in touch

The first Azure Sphere MCU provides WiFi 802.11 b / g / n operating at both 2.4GHz and 5GHz. Advanced applications can configure, use, and query wireless communication subsystems, but they cannot be directly programmed. Instead of using WiFi, properly equipped Azure Sphere devices can communicate over Ethernet networks.

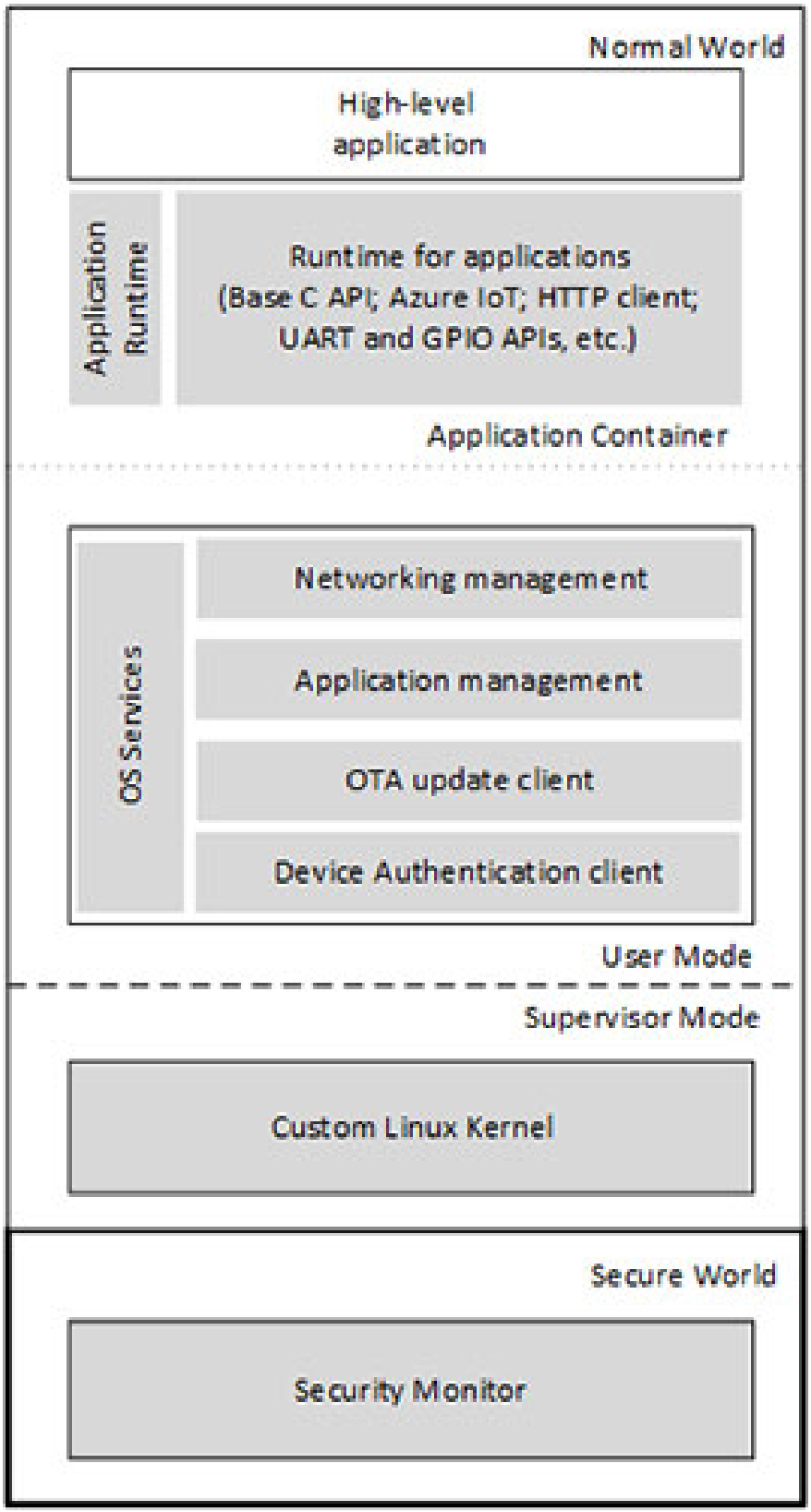
1. Most likely I / O

The Azure Sphere platform supports multiple I / O capabilities, so you can configure embedded devices to suit market and product requirements. I / O peripherals can be mapped to high-end application cores or real-time cores.

1. Microsoft firewall
2. Flash and RAM integrated

Azure Sphere MCUs include a minimum of 4MB of RAM and 16MB of integrated flash memory.

Software architecture and operating system



Software architecture and operating system

1. High-end application platform

Microsoft provides and maintains all software other than device-specific applications. All software running on the device, including high-end applications, is signed by a Microsoft certification authority (CA). Application updates are distributed via the reliable Microsoft pipeline and the compatibility of each update with the Azure Sphere device hardware is verified prior to installation.

1. Runtime

The Microsoft provided runtime is based on a subset of the POSIX standard. It includes libraries and runtime services in NW user mode. This environment supports the high-level applications you create.

1. Service operating system

The operating system services store the high-level application containers and is responsible for communicating with the Azure Sphere Security Service.

1. Linux custom kernel

A custom Linux-based kernel runs in Supervisor mode, along with a boot loader. Security supervision

1. Security supervision

Security monitoring provided by Microsoft runs in SW. It is responsible for protecting sensitive hardware, such as memory, flash, and other shared MCU resources, only for limited access to these resources.