Traditional Embedded Development Is Dead. Long Live The Cloud Revolution

Traditional embedded development is dead. Today, advances in software and tools enable organizations to easily integrate their devices en-masse onto the cloud without the conventional onboarding challenges of unknown devices for customers and cloud services. Ideally, all applications should be considered “edge processing” with a tether, thick or thin, back to a centralised processing resource for analysis, making the concept of isolated compute islands passé.

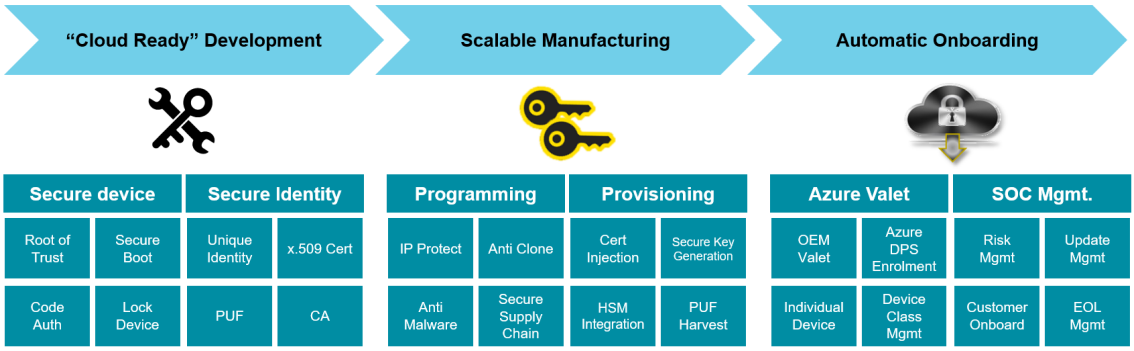
This perspective is highly simplified. The embedded industry typically takes years to embrace new concepts and technologies, having learned through experience to avoid proverbial “silver bullet” solutions. Even so, many embedded systems are transitioning from disconnected islands through to edge computing. This move is driving significant changes in performance requirements, communication stack integration, AI/ML, and many other features on next-generation applications. This transition is impelling security requirements and the mandatory compliance frameworks for consumer, industrial and critical national infrastructure marketplaces, as every connection is a potential attack vector into the system.

The Embedded Cloud Revolution

In partnership with Microsoft Azure, Secure Thingz, an IAR Systems company, has developed new cloud provisioning and onboarding techniques. This approach enables rapid development, volume manufacturing, and integrated update management. This valuable extension to secure provisioning technology is revolutionizing embedded development for the cloud by eliminating traditional late-onboarding barriers.

There is no lack of opinion and discussion around edge-orientated compute's pros and cons, benefits, and challenges. Topics like the location of resources and data pre-processing, and to what extent, and the balance between determinacy and lag, system availability, and robustness to outages, are all vital decisions that deserve careful consideration. The impacts of the significant October 2021 social media outages, which disrupted numerous connected devices, failed to operate successfully due to DNS flaws. However, many of these issues boil

down to design decisions driven by application, cost, time to market, and complexity. Cloud connectivity is a significant challenge because security and connectivity integrate many different concepts, and customer requirements continually evolve.



Key Advantages

The top three advantages of cloud-centric embedded development are:

- Faster and easier connection: Designing for connectivity and updates is fundamental.
- Resolving the onboarding issue at source: Connecting billions of devices from thousands of vendors is a challenge of industry proportions.
- Production management for unique devices: enabling targeting updates, feature enhancements, and lifecycle management.

Perceived Barriers

- Many cloud vendors see onboarding as the single most significant pain point in their flow, both to them and for customers, and the biggest challenge to Chief Information & Secur Officer integrating IoT devices into internal networks.
- Provisioning to ensure a sufficient identity, ownership, and defined cybersecurity risk, is the biggest single inhibitor to the rise of IoT in industrial, transportation, and infrastructure applications.

For developers, the simple challenge of "cloud connectivity" breaks down into the need for a secure communications stack, root of trust and identity challenges, certificate injection, secure boot, update mechanisms, and many other demands. Additionally, daunting challenges exist for Production, Device Services, and the Enterprise. For the Enterprise, the new legislation changes the business model and puts the burden of lifecycle support, vulnerability disclosure, and update management on the organization, eliminating the traditional "ship and forget" mindset. For Device Services, the need to ultimately integrate into a customers' Security Operation Centres (SOC), with the requirement to deliver formal authentication and measurable security across confidentiality, integrity, and availability, is critical.

Production is a particularly challenging aspect of cloud and security integration. It impacts systems geared to homogeneous and repeatable manufacture, with the need for genuinely

unique cryptographic identities ensuring each is universally unique whilst still having standard certificate structures based on x.509 certificates. Ensuring that these identities are cloud-ready and onboarded into whichever cloud compute network the user desires heightens the challenge.

Moving to the Cloud

Two effective alternatives exist to address the production challenges of homogeneous manufacturing with differentiated identity and root of trust. First, developers may integrate a separate Subscriber Identity Module (SIM), like in mobile phones. This method requires integrating a SIM card and presents size and logistical issues. An alternative is an iSIM (integrated SIM), however this approach requires an additional processor built into the silicon, with specific cost and availability implications. The second strategy is to lock down the device with a robust Secure Boot Manager (SBM). This approach ensures that all code operating on the device is produced and injected securely, with robust code authentication, little added cost, and a small amount of memory to extend the boot process. It also ensures rapid engineering adoption and a simple release cycle for a wider availability of devices, including many popular devices used today. The solution's flexibility supports self-signing certificate structures for organizations that wish to own the device identity or third-party certificate frameworks for those looking to outsource.

Using the SBM approach, developers can engineer a vast array of devices for security and inject a standard certificate for Azure cloud connectivity. This certificate framework enables developers to rapidly design for millions of devices to be produced with unique identities. It valets these credentials into the Azure cloud service. With SBM, all produced devices are identified into the cloud so that the Azure service knows the OEM vendor and device capabilities. The end users are confident that the device integrates easily, has been produced correctly, and released as part of a secure supply chain, reducing purchasing risk and integration costs.

Today, this new cloud-orientated flow builds on existing development processes operating with significant partners and customers and leverages standard industry production mechanisms. It has nearly zero impact on modern production flows, is available via major electronic component distributors, and is accessible across numerous devices. There is no upper or lower limit on device numbers, ensuring a simple pathway to market for simple prototypes and early market adoption through high-volume applications.

Summary

Connecting and onboarding devices to the cloud is probably the single biggest challenge to the industry right now, primarily due to the number of partners and device types. Leveraging the extended flow from Secure Thingz allows embedded developers to design and provision "cloud-ready" for Microsoft Azure, reducing development costs and customer integration challenges while removing cybersecurity risks associated with adding devices to networks.