Hype Cycle for Embedded Software and Systems, 2020

Published: 14 July 2020 **ID:** G00441495

Analyst(s): Alan Priestley

This Hype Cycle charts the progress and potential of embedded software and system technologies. The information here should be used to select the best tools, software, hardware, messaging, security and communications systems as they become the core building blocks for the Internet of Things.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

Embedded software and systems are the foundational blocks that enable the digitization of the physical world, the Internet of Things (IoT) and play a role that cannot be overemphasized.

Software for embedded systems has transitioned from executing a simple set of tasks running on low performance microcontrollers (MCUs) to requiring complex multitasking operations running on high performance multicore MCUs and microprocessors (MPUs), often demanding low latency, with deterministic and real-time operation. Increasingly advanced analytics techniques, leveraging deep neural networks (DNNs) must be integrated. Consequently, developing embedded applications can still be an expensive and complex task. Addressing this challenge, we have scripting languages to accelerate development, standardized network protocols and a diverse range of competitive hardware platforms. Delivering solutions that are both secure and capable of being remotely updated, while supporting multiple operating systems and processor types, presents an increasingly complex challenge, but one that the industry is working hard to mitigate.

The Hype Cycle

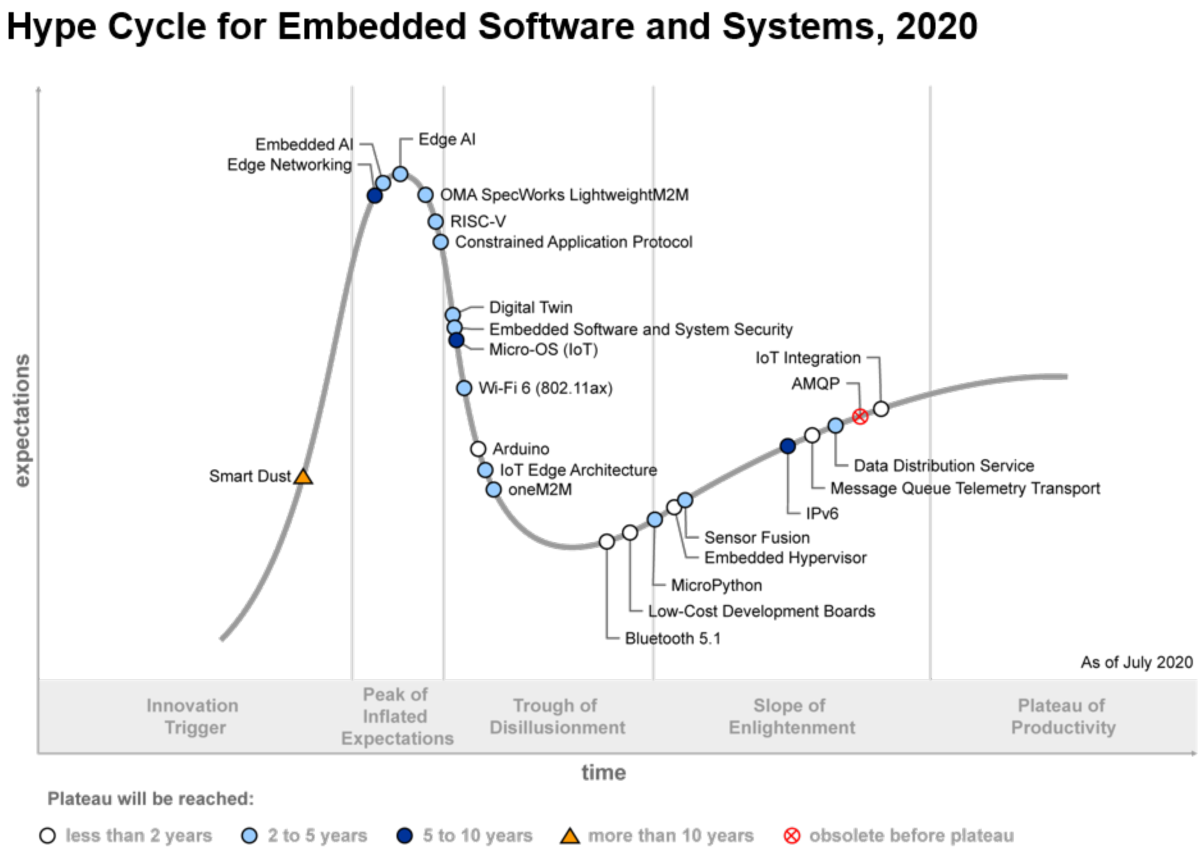
The IoT creates a demand for sophisticated embedded software and system technologies to deliver enhanced automation and intelligence in consumer, enterprise and operational technology endpoints, as well as edge computer systems.

Traditionally, chip vendors have provided board support packages and firmware, while software vendors focused on delivering operating systems, hypervisors, middleware and abstraction layers. However, the complexity of modern software requires that the chip vendors add features into their chips to simplify software implementations. These include encryption accelerators and logic blocks to accelerate DNN-based artificial intelligence (AI) workloads. Software vendors are also extending their toolsets, adding libraries and predeveloped code modules to ease the addition of complex AI-based functionality to embedded software applications. At the same time, the use of embedded hypervisors and high-performance MCU and MPUs are enabling embedded systems to run multiple complex software applications. This requires product managers at original design manufacturers (ODMs) and OEMs leverage a wide range of tools and techniques to ensure all software elements interoperate smoothly.

This Hype Cycle provides an overview of current and evolving tools, techniques and standards, delivering insights on their evolution, adoption, business benefit and impact. This enables OEMs, ODMs and interested enterprises to develop an overall perspective, examine how tools, techniques and approaches can be adopted, as well as determine how their maturity compares alongside each other. In addition, it aids decision making when developing or choosing embedded products and solutions that best fit business objectives.

Twenty-four innovations are highlighted in this Hype Cycle, covering AI, processing, communications and security technologies, along with key developments in embedded software. There is a notable cluster of technologies at the Peak of Inflated Expectations; this is a reflection of the IoT, which has seen a great deal of hype in recent years. Many of these technologies will take a number of years before reaching the Plateau of Productivity.

Figure 1. Hype Cycle for Embedded Software and Systems, 2020



Source: Gartner
ID: 441495

The Priority Matrix

The Priority Matrix maps the time to mainstream adoption of a technology against its benefit rating. Relatively few technologies are designated as having transformational benefit; this intuitively fits with the reality of technology development. **Embedded AI, Smart Dust** and **Digital Twin** are examples of technologies that have the potential to cause significant disruption to the embedded software and systems industry, due to their radical new approaches and promise of high utility. Figure 2 indicates that most of the technologies on the Hype Cycle occupy the middle ground of high benefit and are two-to-five years away from mainstream adoption, with seven high-impact technologies expected to reach the mainstream over the next five years.

Figure 2. Priority Matrix for Embedded Software and Systems, 2020

Priority Matrix for Embedded Software and Systems, 2020

benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational	Embedded Hypervisor	Digital Twin Edge AI		Smart Dust
high	Arduino Bluetooth 5.1 IoT Integration	Embedded AI Embedded Software and System Security IoT Edge Architecture Sensor Fusion Wi-Fi 6 (802.11ax)		
moderate	Low-Cost Development Boards Message Queue Telemetry Transport	Constrained Application Protocol Data Distribution Service MicroPython OMA SpecWorks LightweightM2M oneM2M RISC-V	Edge Networking Micro-OS (IoT)	
low			IPv6	

As of July 2020

Source: Gartner
ID: 441495

Off the Hype Cycle

A number of technologies are approaching the Plateau of Productivity, but no new technologies have moved beyond the plateau in this iteration.

On the Rise

Smart Dust

Analysis By: George Brocklehurst

Definition: Smart dust is a type of distributed sense and control network, consisting of self-contained “motes,” targeting a volume of less than 1 cubic millimeter. These motes have the capability to sense, compute, communicate and power their own activities. They support a distributed sensing network, such as temperature, pressure, movement and humidity sensing, using mesh networking to achieve communication coverage.

Position and Adoption Speed Justification: The aspired size of these motes presents two key challenges, in power and communication. Self-powering motes using energy harvesting will be key in reaching the full potential of smart dust, but their small size limits the energy that can be recovered and stored. Similarly, RF communications face power as well as transmission range challenges due to the tiny antennae. Smart dust proponents have embraced these limitations by finding high value use cases that value size over connectivity range.

We witnessed an activity peak when IBM (in March 2018) announced a 1m3 x86 equivalent mote with applications in supply chain tracking supported through block chain. Two months later, University of Michigan announced a 0.03m3 precision temperature monitoring mote with medical applications including tumor monitoring. One month later MIT announced a graphene-enabled 0.01m3 mote grafted onto a colloid particle for diagnostic journeys through anything from human digestive systems to oil and gas pipelines.

In terms of commercialization, CubeWorks, a University of Michigan spin out has established three products ranging in size and capability. They have focused on high value use cases addressing environmental and security monitoring as well as applications in pharmaceutical and biomedical science. While these solutions are larger than 1 mm3, ranging from 14 mm3 up to 1.6 cm3, they are a significant step forward in understanding the challenges of productizing smart dust.

While most of the announcements still come from lab-based research we are seeing signs of early commercialization and Gartner expects this to grow over the next one to two years. Initial routes to market are fairly modest but they pave the way for the more transformational applications of the technology to come. Consequently, this innovation profile takes another step up the Peak of Inflated Expectations.

User Advice: Research into smart dust should be viewed as a vehicle for innovations that will also benefit other operational and market activities. Most near-term return on investments will come from commercialization of these innovations, including transfer to the somewhat larger IoT endpoint technologies.

- Smart dust is embryonic and should be tracked within innovation teams. Tracking should examine both smart dust research activity and trajectories of the associated technologies within industry.
- Lead adopters should consider taking equity stakes in university commercialization efforts. Early successes and adjacent commercialization opportunities will be enabled by hardware innovations where IP protection will create barriers.
- Consideration must be given to the complexity of mass data communication and processing. The density of wirelessly communicating things will present new challenges in cross-channel interference and coordinated transmissions that will require new protocols and techniques to address possibly the use of biologically inspired algorithms (like swarm research).

- Motes have limited communication range and processing so gateway architecture — how to collect and aggregate data — is critical to scale.

IoT use-case characteristics that benefit from emerging products are applications that need:

- Very high sensor density over a small area.
- Very tiny sensors that are either covert or don't disrupt a sensitive process
- Migratory sensors, for example, in liquid flows.

Which can also accept:

- Very short range communications.
- Fairly simple processing and somewhat limited data storage in each node.

Business Impact: The potential benefits of smart dust are wide-ranging, compelling and transformational extending IoT's "situational awareness." The concept of this technology transitions the Internet of Things into the Internet of Everything, which carries profound implications for the architecture of collecting, processing and interpreting data. A world with widespread adoption of smart dust will require radical innovations in all the systems that would convert captured data into some useful action. A further generational step, with innovations such as neural dust, will transform the way humans interact with their surroundings, emerging initially through medical advancements, such as prosthetic control, and then into broader possibilities.

In the medium term, the breakthroughs from pursuing this research will also have high impact and will help the IoT to meet its potential for lowering cost and power while increasing local processing and endpoint intelligence.

Equal to smart dust's transformational potential are its legal, ethical, security and privacy ramifications.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Cornell University; CubeWorks; EPIC Semiconductor; HP Inc.; IBM; MonoLets; University of California; University of Michigan

At the Peak

Edge Networking

Analysis By: Tim Zimmerman; Joe Skorupa

Definition: Edge networking is a diverse set of communication technologies and architectures that connect end-user devices and sensors to the edge of the communication infrastructure. For WAN connected devices, this includes cellular, private cellular, LPWAN and satellite. For on-premises, connectivity includes traditional Ethernet and Wi-Fi, but also over 40 industrial automation protocols and building automation protocols.

Position and Adoption Speed Justification: Edge networking has been traditionally siloed. Cellular, private cellular and LPWAN connectivity are addressed by different vendors as compared to on-premises solutions, which, for many industrial automation protocols, were vendor-specific. The visibility of IoT for security risk and discovery as well as for network convergence and business benefits has also shone a light on the IoT solution architectures.

The focus on end-to-end IoT architecture as part of the overall network strategy, the advances in edge computing and communication technology, and the convergence of networking require integration of edge networking decisions into the overall architecture. Hence, this technology is moving slowly through the Hype Cycle. The flexibility of private cellular (such as CBRS), higher speeds of cellular 5G as well as the device integration of NB-IoT are indicating the convergence of solutions that require WAN coverage. The ability to use private cellular (CBRS or 5G) for on-premises applications, such as large manufacturing facility applications, shows the overlap of WAN with on-premises communication technologies. In the same vein of convergence, the more widely used industrial protocols are moving to an IP-based definition, which allows for coexistence with traditional enterprise communication infrastructures. Additionally, the availability of 802.11ax for local-area networking and the announcement of 802.11be (6 GHz) provide additional control of device connectivity options and higher performance. High-performance on-premises connectivity will allow device communications to flow upstream to edge computing platforms or core networking resources while addressing congestion and higher density. Implementation of the standards associated with Time-Sensitive Networking (TSN) for wired Ethernet connectivity will allow best-effort enterprise infrastructure to provide services that address latency-sensitive applications and promote additional convergence.

User Advice: End users should:

- Be aware that WAN and WLAN/LAN solutions today require different and separate communication infrastructures.
- Invest in shared spectrum communications (such as CBRS, 5G, NB-IoT) for large, open environments that could be indoors (utilities or manufacturing plants) or outdoors. 5G infrastructure is currently being rolled out across different geographies but private LTE (CBRS) can address location-specific requirements. It is imperative to understand whether 5G-specific attributes for throughput, latency and device density are required by your applications, and if so, whether 5G service is available. Also identify whether NB-IoT or CBRS is available, and whether new devices (which will be required) support the required functionality.
- Invest in WLAN for indoor enterprise applications or defined outdoor environments such as stadiums or parks. Monitor the technology (both 802.11ax and 802.11be); do not pay any premiums for the new functionality and ensure that any short-term purchase is upgradable to the final standard.

- Mandate support for 802.11u to allow migration of applications connectivity from WAN to WLAN infrastructures.

Business Impact: The short-term value proposition will be the consolidation of many different, siloed communication types into one or two with the ability to move between two technologies. This will simplify procurement, deployment and operations. The longer-term value will be commoditization of the hardware and lower prices across all vertical markets globally to achieve the desired business outcome.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Belden (Hirschmann); Cambium Networks; Cisco; Federated Wireless; Hewlett Packard Enterprise; Hewlett Packard Enterprise (Aruba); Orange Business Services; Siemens; Verizon; Vodafone Group

Recommended Reading: "Exploring the Edge: 12 Frontiers of Edge Computing"

Embedded AI

Analysis By: Amy Teng; Alan Priestley

Definition: Embedded AI refers to the use of AI/ML techniques within embedded systems to enable analysis of locally captured data. This requirement is particularly critical for electronic equipment where decision latency must be minimized for operational efficiency and safety. It can also enable always-on use cases targeting battery-operated devices requiring low-power operation.

Position and Adoption Speed Justification: There is an increasing demand for embedded systems to analyze and interpret the data they capture by leveraging AI/ML locally.

Virtually all major MCU vendors have expanded their toolchain to include compilers, model conversion tools, libraries and application samples (such as object and gesture recognition) to enable embedded AI. Additionally, the emergence of Tiny machine learning (tinyML) has encouraged many new lightweight ML algorithms. In February 2020, Apple acquired an AI star-up, Xnor.ai, focusing on BNN (Binarized Neural Network), which is a type of tinyML.

Vendors are also enhancing the AI capabilities of their embedded processors by integrating hardware logic blocks into chips to optimize and advance inference performance. Renesas Electronics has introduced a MPU with an embedded Dynamically Reconfigurable Processor (DRP), a programmable on-chip logic block that can be reconfigured via firmware updates. This enables the processor to be easily updated with the latest AI algorithms. NXP has a general-purpose MCU with heterogeneous cores (ARM Cortex M33 and Cadence Tensilica HiFi 4 DSP) targeting audio/video analytics applications.

ARM's Cortex-M55 is the first Armv8.1-M based MCU core with Helium vector extensions focusing at DSP/ML compute capabilities, and Ethos-U55 — the first micro-NPU that will co-work with Cortex-M by providing configurable MCAs and weight compressions. These two technologies together with ARM's software development frameworks enable partners and developers to quickly expand to embedded AI/ML applications by reusing current assets and experiences. Semiconductor vendors are integrating these hardware IP block into their product lineups, and more products are expected to be available for market adoption from 2021.

In addition to the forth mentioned vendor activities, we expect the market continue to vibrant throughout the year, as a result we updated its position toward to the peak of HC.

User Advice: Adoption of embedded AI requires a clear workflow and vendor support on tools, especially where the embedded system is used for real-time response and control. As the market is at an early stage of adoption, IT leaders must:

- Determine where (endpoint, edge or cloud) is best to execute AI based data analytics.
- Identify the subset of applications in your OT system or product portfolios that can be meaningfully impacted using embedded AI.
- Evaluate the availability of reference designs that are close to your target application, chip vendors, their solutions and design partners. Focus on their ability of translating and optimizing your trained model into local systems.
- Evaluate the process of updating algorithms — ensure no security vulnerability is created due to changing designs.

Business Impact: Embedded AI enables devices to analyze captured data using AI/ML techniques locally, reducing the need to transfer data to a remote data center for analysis. This can reduce latency and enhance operational efficiency. Companies who own, sell or serve IoT and industrial electronics, ranging from OT machines, factory equipment, IoT sensors to consumer electronics, will be positively impacted depending on inclusion of and the value created by AI.

Initial justification will come from business cases focusing on first-order operational savings, for example, predictive maintenance — these are the easiest and clearest to define. As adoption picks up, Gartner expects to see additional value created through dynamic and real-time optimization of manufacturing lines to incoming orders and workloads, intelligent buildings that optimize employee productivity.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Arm; Cartesiam; NXP Semiconductors; One Tech; Renesas Electronics; STMicroelectronics

Recommended Reading: "Market Share Analysis: Microcontrollers, Worldwide, 2019"

Edge AI

Analysis By: Alan Priestley; Erick Brethenoux; Eric Goodness

Definition: Edge AI refers to the use of AI techniques embedded in IoT endpoints, gateways and edge servers, in applications ranging from autonomous vehicles to streaming analytics. While predominantly focused on AI Inference, more sophisticated system may include a local training capability to provide in-situ optimization of the AI models.

Position and Adoption Speed Justification: Edge AI will be implemented in a range of different ways, depending on the application and design constraints of the equipment being deployed — form factor, power budget (specifically, battery powered versus mains powered), data volume, decision latency, location, security requirements etc.:

- Data captured at an IoT endpoint and transferred to an AI system hosted within an edge computer, gateway or aggregation point: In this architecture, the IoT endpoint is a peripheral to the AI system. The endpoint acts as a data gatherer that feeds this data to the AI system. An example of this is environmental sensors deployed for a smart agriculture application.
- AI embedded in the IoT endpoint: In this architecture, the IoT endpoint is capable of running AI models to interpret data captured by the endpoint and drives some of the endpoints' functions. In this case, the AI model (such as a machine learning model) is trained (and updated) on a central system and deployed to the IoT endpoint. An example is a medical wearable that leverages sensor data and AI to help visually impaired people navigate the world in their daily lives.

The applications that are starting to see increasing adoption of edge AI include those that are latency sensitive (such as autonomous navigation), data intensive (like video analytics), and require an increasing amount of autonomy for local decision making. While many of these applications are still in R&D or trial phases, and widespread adoption is at least a few years away, other such as video analytics (leveraging deep learning methods and deployed as deep learning models at the endpoints or in edge servers) are starting to see adoption — driven by the rapid growth in deployment of surveillance cameras and the need for real-time interpretation of captured video streams.

User Advice: Enterprise architecture and technology innovation leaders should:

- Determine whether the new AI developments in machine learning (ML) are applicable to their IoT deployments, or whether traditional centralized data analytics and AI methodologies are adequate.
- Evaluate when to consider AI at the edge versus a centralized solution. Applications that have high-communications costs are sensitive to latency, or ingest high volumes of data at the edge are good candidates for AI.
- Assess the different technologies available to support edge AI and the viability of the vendors offering them — many potential vendors are startups, which may have interesting products but limited support capabilities.

- Estimate carefully and pragmatically the appropriate level of autonomy and trustworthiness for AI systems deployed on edge systems.
- Assess the risk associated with the nondeterministic nature of many AI techniques where it may not be possible to control or replicate the analysis results.
- Use edge gateways and servers as the aggregation and filtering point to perform most of the edge analytics functions. Make an exception for compute-intensive endpoints, where AI-based analytics can be performed on the devices themselves.

Business Impact: By incorporating AI techniques at the edge, enterprises may be positively impacted as follows:

- Improved operational efficiency, such as enhanced visual inspection systems in a manufacturing setting.
- Enhanced customer experience, with faster execution time, performed at the edge.
- Reduced latency in decision-making, with the use of streaming analytics and migration to an event-based architecture.,
- Communication cost reduction, with less data traffic between the edge and the cloud.
- Increased availability even when the edge is disconnected from the network.

Enhanced local decision autonomy for edge systems.

Reduced storage demand through a more reactive exploitation of the data and a better estimate of its potential obsolescence.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Amazon; Baidu; Google; Huawei; Intel; Matroid; Microsoft; Neurala; NVIDIA; Qualcomm

Recommended Reading: “Exploring the Edge: 12 Frontiers of Edge Computing”

“5 Questions a Product Manager Must Ask When Creating an AI-Enabled Edge Product Strategy”

“Use Edge AI to Drive Revenue Growth, Forecasting, Customer Engagement and Workforce Planning”

“Cool Vendors in AI Semiconductors”

OMA SpecWorks LightweightM2M

Analysis By: Bill Ray

Definition: LightweightM2M (LwM2M) is a common, global specification developed by the OMA SpecWorks for managing "lightweight" IoT devices across multiple networks. Using a REST-based architecture, LwM2M manages communication's use between client software on a device and server software. LwM2M was designed to provide device and policy management while supporting efficient and secure data transfer among diverse IoT endpoints.

Position and Adoption Speed Justification: With the focus on developing a device management protocol for sensor networks and low-power, low-data IoT devices, the Open Mobile Alliance (OMA) released the LightweightM2M specification in February 2017. In March 2018, the OMA partnered with the IPSO Alliance to form OMA SpecWorks, a standards development organization focused on enabling smart object interoperability. In February 2019, version 1.1 of the standard was published which facilitates the inclusion of non-IP networks.

Gartner is forecasting increased investment in low-power networks (such as NB-IoT) which offer very limited bandwidth to specific endpoints. This provides an ideal use case for LightweightM2M, so the adoption of the standard will increase as those networks grow. The launch of AT&T's LwM2M interoperability program, in 2020, is indicative of progress. However, adoption is happening quite slowly with the result that the profile has only moved slightly along the Hype Cycle this year, though we remain optimistic about its potential.

User Advice: Application developers and device OEMs should consider LwM2M, among other standards, to simplify and unify their application and product development, particularly in the cellular landscape. OMA SpecWorks also established a comprehensive set of resources dedicated to the developer community to facilitate adoption of the protocol and speed development cycles. Full advantage of these resources should be made.

Make use of the open standard, the available development kits, and the expansion of LwM2M developer resources, for fast and easy implementation.

Business Impact: The IoT market is awash in standards and protocols, creating a highly fragmented marketplace that can slow product design and innovation. With OMA SpecWorks supporting companies and focus on device management, LwM2M is one of the better-positioned standards to achieve widespread adoption. If the standard gains prominence among OEMs and developers, it could play an important role in consolidating design choices for IoT product developers, gain substantial economies of scale and help enterprises achieve lower-integration costs and faster time to market products/services. The OMA has a strong list of companies supporting LwM2M, including the top cellular chipset architects, chipset manufacturers, infrastructure providers and module manufacturers. With suitable investment these companies could help the standard gain broader momentum in the coming years as MNOs continue to expand their IoT initiatives and solutions.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: AT&T; China Mobile; Ericsson; Microsoft Azure; Nokia; Qualcomm; Sierra Wireless

Recommended Reading: "Use the IoT Platform Solution Reference Model to Help Design Your End-to-End IoT Business Solutions"

"Innovation Opportunities Will Be Enabled as 5G Evolves Through 2025"

RISC-V

Analysis By: Bill Ray; Martin Reynolds

Definition: RISC-V is an open, free, instruction-set architecture for embedded-chip designs which may be used by vendors in their chip designs without patent or licensing fees. The architecture has consistent 32- and 64-bit instruction sets. Developers may extend the functionality, while retaining a common core architecture to ensure compatibility across implementations.

Position and Adoption Speed Justification: The advantage of using RISC-V over competitors, such as Arm, is not only the reduction in license fees but also the flexibility that permits designers to extend the chip architecture (something which generally requires a rare and technically challenging architectural license). The core RISC-V IP is freely available but use of the RISC-V logo on commercial products requires membership of the RISC-V International.

RISC-V is the first major new processor core architecture in decades. From the same genealogy as the MIPS architecture, its design reflects modern practices in computer architecture. More important, however, is the relatively complete ecosystem of IP, toolchains and software. Moving applications to RISC-V is a relatively straightforward process and brings significant savings to volume users.

Several major semiconductor companies have invested in products based on RISC-V, including Microchip Technology, which uses a RISC-V-based microprocessor soft core in its PolarFire FPGA SoC, and Samsung Electronics, which has incorporated RISC-V into its Exynos system. Membership of the RISC-V International includes Espressif Systems, Google, Huawei, Marvell, NVIDIA, NXP Semiconductors, Qualcomm, Samsung Electronics and Western Digital. RISC-V is displacing embedded controllers at Western Digital and NVIDIA. SiFive offers RISC-V cores instantiated with low-cost custom logic, reducing barriers to entry for custom chips.

Concerns over restrictions on trade have created a lot of interest in RISC-V from China, where open platforms are seen as an important tool in avoiding reliance on foreign suppliers. With such interest, and millions of RISC-V incarnations shipping, the profile has been nudged over the peak.

User Advice: Arm and competing cores are inexpensive and capable, as long as there is sufficient volume to cover the license fees. As the RISC-V license makes no restriction on commercialization of the core, nor imposes any open-source requirements on the added enhancements (in contrast to projects using the GPL, such as the Linux OS), RISC-V is an attractive alternative to license-bearing cores such as Arm or MIPS, and offers more capability than low-cost cores available as design libraries.

Therefore, RISC-V opens opportunities where either low-volume customization, or high-volume cost reduction, represent a product or business opportunity. For example. NVIDIA and Western Digital are switching their product lines to use RISC-V cores in place of licensed cores from other vendors. SiFive offers RISC-V cores in conjunction with a low-cost, small-volume custom silicon product that can bring a custom chip to lower price points than otherwise possible.

Companies in the MCU or SoC business should evaluate how RISC-V could be integrated into their product offerings, potentially reducing license fees and increasing flexibility in embedded environments currently dominated by Arm cores. Software companies should be ready to offer RISC-V-compatible versions of their embedded offerings.

Business Impact: RISC-V is unlikely to compete with flagship A-series designs from Arm, at least in the medium term. However, in embedded applications aligned with Arm R or M cores, RISC-V can usefully be combined with custom architectural features that can enable new feature price points in a final product. This capability maps well to IoT endpoints where existing solutions are not feature-competitive when built with competing solutions.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Andes Technology; Bluespec; Codasip; SiFive

Recommended Reading: "Emerging Technology Analysis: Opportunities of Open Instruction Set Architecture RISC-V"

"How Your Business Should Realize the Benefits of the OEM-Foundry-Direct Revolution"

"OEM-Foundry Direct: Evaluate Your ASIC Business Case"

Constrained Application Protocol

Analysis By: Saniye Alaybeyi

Definition: The Constrained Application Protocol (CoAP) is "a specialized web transfer protocol for use with constrained networks and nodes" for machine-to-machine (M2M) applications.

Position and Adoption Speed Justification: CoAP uses an interaction model similar to the client/server model of HTTP, but M2M implementations are typically implemented using CoAP acting in both server and client roles (referred to as "endpoints"). The current specification for CoAP faces some obstacles in the form of semantics, security limitations and test cases. A few companies have released some CoAP-based products, indicating that the RESTful trend for low-power embedded networks will continue generating interest. The open-source community has been providing momentum for CoAP, with implementations in C, C# (ported to TinyOS), Java and Python, for example.

With the amount of resource-constrained IoT devices on the rise and the promise of CoAP for IoT device authentication via delegated CoAP authentication and authorization framework, CoAP hype could accelerate and it could become mainstream in two to five years. In March 2019, Internet Engineering Task Force (IETF) introduced a new, optional CoAP protocol extension for extended token lengths. In 2020, the need to architect for change is increasing. IT leaders are using CoAP and APIs where possible to modularize systems, reducing complexity and making it easier to switch hardware or software components in the future. We continue to remain optimistic about the future adoption of CoAP and advancing this technology forward in our Hype Cycle.

User Advice: Developers should address security limitations — for example, achieving datagram transport layer security/transport layer security (DTLS/TLS) translation when CoAP/HTTP mapping is used as a proxy. Standard programming language implementations will lower development cost and effort. If developers are using CoAP at the endpoints, they must make sure CoAP is supported by the IoT platform they are using.

Business Impact: CoAP helps reduce application development for low-power networks due to its ability to maintain reliability while allowing easy integration with existing internet technologies.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Arm; Hitachi; Nke Watteco; NXP Semiconductors; QuEST Global (EXILANT Technologies)

Recommended Reading: "Top 10 Strategic Technology Trends for 2020: Empowered Edge"

"How to Deliver a Truly Hybrid Integration Platform in Steps"

"Magic Quadrant for Application Security Testing"

Sliding Into the Trough

Digital Twin

Analysis By: Alfonso Velosa; Benoit Lheureux; Marc Halpern

Definition: A digital twin is a virtual representation of an entity such as an asset, person or process and is developed to support business objectives. The three types of digital twins are discrete, composite and organizational. Digital twin class elements include the model, rules, relations and data properties. Digital twin instance elements include the model, data, unique one-to-one association, and monitorability.

Position and Adoption Speed Justification: The idea of modelling people, physical assets, and processes continues to gain traction, especially as the architecture for the future of applications includes digital twins as features of an application, and as stand-alone supplements to portfolios of applications that address an entity.

- People: Digital twins are the evolution of trends including customer 360-degrees, patient electronic health records, and fitness monitors. Their near-term uses include health monitoring and employee safety, particularly in response to the pandemic.
- Physical assets: Digital twins adoption aligns to Internet of Things (IoT) trends. For owner/operators, near-term use includes lowering maintenance costs and increasing asset uptime for equipment users in factories, hospitals, utilities, among others. For product original equipment manufacturers (OEMs), near-term uses include product differentiation, business model differentiation through new product service models, and obtaining customer data.
- Processes: Digital twins are being developed to model IT organizations, financial exchanges, and processes such as purchase orders.

The digital twin profile has moved past the Peak of Inflated Expectations, based on enterprise confusion driven by conflicting vendor marketing and on challenges implementing digital twins. Gartner's CIO Survey 2020 shows that 6% of enterprises have implemented digital twins, although less than 1% of assets have digital twins. Another 41% of enterprises expect to deploy digital twins within three years. These trends lead us to shorten the time to plateau down to two to five years. In the next decade, digital twins will become the dominant design pattern for digital solutions.

User Advice: CIOs should work to guide and protect business adoption of digital twins:

- **Business outcomes:** Work with business leaders to establish clear business objectives for digital twins. In parallel, establish an IT vision for digital twins, to establish a coherent approach to support the business units.
- **Technology:** Start with models that are as simple as possible of the entities that are of interest for your business process, whether basic, such as the location of vehicles or a very high fidelity models of a human heart. Determine what data is necessary to "feed" the models and the types of analytics needed; a corollary here is the need to verify and drive data quality. Don't let the dearth of standards limit innovation. Assess how composite and organizational digital twins will require integration and custom development.
- **Governance and accountability:** Engage the business unit to identify champions, budget support, and to co-build the digital twin strategy and roadmap. Establish a joint business and IT governance process for digital twins, covering their alignment to business KPIs, short- and long-term value, and their updates and life cycle management.
- **Digital ownership and ethics:** Work with business and legal teams to establish a policy on ownership of the digital twin models and data, as well as who may participate. In parallel, establish a digital ethics policy to guide the organization to develop twins that positively support the enterprise while serving employees, customers or citizens. This policy will set guidelines to engage ecosystem stakeholders about what data may be shared and what monetization experiments to conduct.

- **Vendors selection:** Understand most technology providers are still developing their strategy and mostly offer enabling technology. A small number of technology providers have digital twin portfolios which align with specific vertical markets.

Business Impact: Digital twins are transformational as they enable business to drive new digital business models as well as update existing models. For example, they enable superior asset utilization, service optimization and improved customer experience. They create new ways to operate, such as consumption of physical outcomes instead of the capital expenditure acquisition of industrial assets, or new ways to drive an ecosystem or supply chains. And they will open new ways to monetize data.

Digital twins will challenge most enterprises to change their thinking of master data from an IT practice to one that engages the business units and IT to get a more comprehensive situational awareness of assets, people, or processes. In addition, a digital twin can be expensive to maintain, and its value centers on remaining a live model, synchronized with the entity.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: AVEVA; Bentley Systems; C3.ai; Cognite; GE Digital; Mavim; Microsoft; QPR Software; Schneider Electric; ThoughtWire

Recommended Reading: “Market Guide for Digital Twin Portfolios and Enabling Technologies”

“Survey Analysis: IoT Digital Twin Adoption Proliferates Across Many Sourcing Options”

“Toolkit: Enterprise Readiness for Digital Twin Deployment”

“Market Trends: Software Providers Ramp Up to Serve the Emerging Digital Twin Market”

“Software Product Managers Should Exploit the Full Revenue Potential of Digital Twins”

Embedded Software and System Security

Analysis By: Ruggero Contu; Barika Pace

Definition: Embedded software and system (ESS) security is a technology and practice designed by engineers and developers to protect hardware and firmware from cyberattacks and assist in delivering integrity and confidentiality of the data that those systems process. ESS may have varying life cycles, including ones measured in decades and may be subject to both physical and digital attacks of varied forms and strengths.

Position and Adoption Speed Justification: ESS security is evolving to address growth in the industrial, commercial and consumer markets. This is happening also through support of secure microcontroller units (MCUs) that act as the basic hardware to protect the embedded software, data storage, processing power and communications between devices. The historic ESS design lacked security, focused on reliable and maintainable code, with little emphasis on protection. OT and IoT introduce new application and platform security requirements for ESS. ESS hardware and firmware standards aren't universally adopted, although international standards for handling data security, authentication and encryption do exist. However, these techniques have not yet been tested in hostile environments where IoT devices may operate. Device hardware may have to last decades. Device discovery, provisioning, upgrading and remediation must be protected. Expect new regulatory initiatives, such as the one announced by the U.K. government in May 2019, aimed to driving a better security by design approach ("Plans Announced to Introduce New Laws for Internet Connected Devices"), the approved California Security of Connected Devices Law and also the in-force European GDPR privacy requirements. These are likely to accelerate adoption of more stringent ESS security practices. The increasing compliance requirements as well as increased security awareness within enterprise and consumer sector are the main factors behind the progress in the positioning and adoption. As a result of these facts, some Hype Cycle progress has been made since 2017 in standard system-on-chip designs, more flexible configurations to meet industry-specific requirements, and integration with existing key management and secure data read/write mechanisms. As such, it has passed the Peak of Inflated Expectations and marked progress will begin to accelerate in these areas.

User Advice: ESS security is critical for organizations deploying endpoints and edge computing for IoT and OT systems. ESS requirements are complex: Devices can have long field lives, are physically accessible to attackers and require long-term management. Security and risk management leaders must:

- Establish governance and planning practices that incorporate embedded security functionality into design and management.
- Expand security architecture and planning to address decentralization of processing architecture into the network and to edge computing.
- Allocate organizational responsibilities to coordinate counterparts and business managers using ESS in business scenarios.
- Drive service-level agreements and audits of ESS-affected systems to ensure high-risk systems are designed properly.
- Address supply chain and partner ecosystem security via skill set and process changes to address their critical role in ESS.

Business Impact: Increasing ESS usage is a symptom of the changes reshaping current information and IT security technologies, processes and organizations. This will impact the enterprise in:

- Secure fit-for-purpose and less expensive technologies in business scenarios: ESS use in devices affects how chip vendors, service providers, manufacturers, developers and others plan. ESS use reshapes semiconductors, electronics industries, business scenarios and pricing. As environments grow more complex, business scenarios must expand to include ESS considerations.

- ESS allows for more monitoring and data collection of digital business performance, enabling big data initiatives to be augmented with information from OT security, IoT security and physical security data, and providing data context for business intelligence. ESS also contributes to advanced machine learning and broader artificial intelligence initiatives in security by contributing hardware-based and firmware-based performance and behavior.
- The scale of deployments using ESS requires changes in how organizations employ enterprise security intelligence. New tools to reduce data complexity for security are becoming available. ESS security is evolving, but is ultimately determined by ESS development, deployment and use in digital business initiatives and the risks they incur.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Arm; CENTRI; Green Hills Software; Infineon Technologies; Intel; Microsoft Azure; Mocana; Qualcomm; Symantec; Thales

Recommended Reading: "Market Trends: IoT Edge Device Security, 2020"

"Forecast: Enterprise and Automotive IoT Edge Device Security, Worldwide, 2018-2024"

"Emerging Technology Analysis: Cyber-Physical Systems Security Is an Opportunity for Security Product Managers"

"How to Develop a Security Vision and Strategy for Cyber-Physical Systems"

"Market Insight: Tech CEOs Must Act Before Convergence Kills Your Stand-Alone OT/IoT Product Solution"

Micro-OS (IoT)

Analysis By: Martin Reynolds

Definition: A micro-OS (IoT) is an embedded real-time operating system (RTOS) that provides the minimum resources needed to support a computing device. The footprint may be as small as 256 bytes. Using a micro-OS in a product improves software security and reliability over monolithic code, and makes modifications and enhancements easier.

Position and Adoption Speed Justification: Micro-OSs have existed for many years, but increasingly sophisticated microcontrollers have rendered them somewhat obsolete. A few dollars of extra cost could support a stripped-down Linux. However, the proliferation of IoT devices and the need to drive costs down and reliability up create new opportunities for these small operating systems.

The technology is well-developed, with multiple vendors, open-sourced or available code, and sizes range from a few hundred bytes to a few megabytes. Amazon has integrated FreeRTOS into its IoT portfolio to promote its IoT initiatives.

Compared to, say Arduino, a micro-OS brings full multithreading capability; this feature makes it possible to run multiple functions independently of each other. The micro-OS, therefore, increases code reliability by creating some separation between functions. The more structured code also makes it easier to port the code to a new architecture.

Compared to Linux, even the smallest Linux systems require hundreds of megabytes of storage and a 32-bit processor. However, micro-OSs represent a significant step up in capability and complexity, while decreasing cost and risk relative to a monolithic system design.

Of particular note are the controllers manufactured by Espressif Systems, which integrate a 32-bit microcontroller core and a Wi-Fi interface into a single chip. This device is available in tiny single board computers for less than $6 in single unit quantities, supported by a richly customized FreeRTOS toolset. As a micro-OS platform, it brings advanced wireless connectivity without the burden of a full operating system.

User Advice: For small IoT devices where cost and power consumption are critical, use a low-power microcontroller supported by a micro-OS. A micro-OS is also useful for core security functions, where the microcontroller provides access and control for security features of a larger system, in a manner similar to that of a Trusted Platform Module (TPM).

In many cases, a micro-OS will fit inside the memory on the chip. This capability can significantly increase product security, as it is difficult to track code execution or download the binary code.

Although monolithic code can do the job, a micro-OS adds flexibility and reliability. A micro-OS is particularly important where the device must run several functions in parallel.

If you are developing an IoT product, look to systems that run a micro-OS to give you a semiconductor system cost well under $10, even with a wireless interface. The development tools are inexpensive, and enable your teams to prototype IoT devices with both lower risk and cost than associated with more sophisticated Linux systems.

If you are using a cloud-based system, trial the inexpensive microcontrollers offered by Amazon and Microsoft. These microcontrollers are well secured and managed at the hardware level.

Business Impact: Low-cost, low-power microcontrollers, in conjunction with a micro-OS, can reduce power consumption and increase software reliability of edge devices. These are critical attributes for a profitable IoT project and can significantly reduce operating costs. For example, an 8-bit system with a micro-OS might deliver several years of battery life, compared with months for a similar function implemented with an advanced OS. Software update costs and battery replacement costs are important factors in the cost of an IoT project, as they scale with the number of endpoints.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Amazon Web Services; Espressif Systems; Micrium; Microchip Technology; MicroPython; TinyOS

Wi-Fi 6 (802.11ax)

Analysis By: Tim Zimmerman

Definition: Wi-Fi 6 (802.11ax) is the latest iteration of the IEEE 802.11 WLAN family. Its main enhancements are allowing the network to control device connectivity for the first time and to improve the efficiency of existing 2.4GHz and 5GHz spectrum, thereby increasing throughput in densely populated areas. As such, its goal is to support a larger number of devices including IoT that are properly connected to the network.

Position and Adoption Speed Justification: IEEE, the standards body of 802.11-based technologies, started the High Efficiency WLAN (HEW) Study Group in May 2013 to examine the most pressing needs for the next-generation Wi-Fi technology. Ratification of the new Wi-Fi 6 (802.11ax) standard was expected in late 2019 but was delayed until 2020 and perhaps longer due to COVID-19. Prestandards-based networking equipment has already been released by a majority of the key/leading vendors. Successive Wi-Fi technologies have increased per-device throughput at an impressive rate through the years (from 802.11b 11 Mbps to 10 Gbps expected from the new standard).

The number of IoT devices and the convergence of building automation and line of business devices onto the enterprise communication infrastructure continues to contribute to congestion. 802.11ax will be able to more intelligently use network resources instead of letting the device make connectivity decision as previous versions of the standard allowed. Advancements allow differing streams to communicate to multiple devices simultaneously as well as cutting latency by as much as 75%.

User Advice:

- We advise clients not to pay a premium for any adoption of Wi-Fi 6 (802.11ax) unless existing wireless solution do not provide the performance and functionality needed to meet defined end-user requirements.
- For IT leaders, Wi-Fi 6 (802.11ax) represents an opportunity to significantly improve performance for special use cases such as dense device deployments, they are advised to monitor the standardization timeline and product availability to find the right entry point for future infrastructure upgrades as well as availability of client devices that will support the new standard.
- We advise clients that “Wi-Fi 6 certification” currently does not mean 802.11ax compliant since the standard is not ratified. Any organization that purchases prestandard products should have the ability to upgrade or update their product at no cost to be standards compliant.

Business Impact: Wi-Fi 6 (802.11ax) is the first Wi-Fi technology that will be able to support large-scale IoT usage scenarios and other high density environments using existing 2.4GHz and 5GHz spectrum via its use of OFDMA.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Broadcom; Cisco; Extreme Networks; Hewlett Packard Enterprise (Aruba); Huawei; Intel; Juniper Networks (Mist Systems); Qualcomm

Recommended Reading: "Magic Quadrant for Wired and Wireless LAN Access Infrastructure"

"Critical Capabilities for Wired and Wireless LAN Access Infrastructure"

Arduino

Analysis By: Bill Ray

Definition: Arduino is an open-source platform and integrated development environment that facilitates the rapid creation of script-based applications to be run on low-power (open source) hardware. Arduino is focused on gathering data from sensors and triggering actuators, making it ideal for IoT development and proof of concept.

Position and Adoption Speed Justification: Arduino comprises both a hardware platform and an integrated development environment. Applications can be developed in C++, but most Arduino development is done with the Arduino scripting language. However they are developed, applications execute directly on the hardware (without an intermediating operating system). Sketches can do local processing, but the focus is on interacting with physical objects through analog and digital inputs and outputs. Although Arduino was created for educational use, its open-source nature has spawned an industry supplying development boards, connected sensors, actuators and documentation, and it often finds a home in product prototypes. Arduino is a natural choice for companies looking to create proof of concept or prototypes for the IoT market, but it is also seeping into commercial products, thanks to the low cost and high reliability of the Arduino hardware.

Early in 2020, Arduino launched a new hardware platform, branded Portenta, aimed at industrial applications. Portenta is modular, with support for popular cloud services and an additional fast interface which allows easier integration with existing hardware. The launch of Portenta pushed Arduino further toward the Trough of Disillusionment, as it moves beyond education into the more-competitive single-board computing market.

User Advice: The focus of Arduino is on interfacing with the physical world, and it should not be confused with edge processing solutions. However, the speed of development is unmatched, and the simplicity of the sketch syntax is such that any competent software developer can start developing in a matter of hours. Combination solutions, which use a second processor (running an OS such as Linux) to analyze the collected data, can address the limitations of Arduino.

Therefore, there is little reason to build Arduino experience within a company, as it can be developed when needed. Arduino should be the first option when considering how to create proof-of-concept or prototype hardware for the IoT, and the idea of using the same platform for production systems should be fully evaluated alongside available alternatives. Arduino can be integrated into production systems at board level, effectively extending the prototyping environment into production.

Business Impact: Arduino is aimed very specifically at the IoT, including industrial applications. Therefore, it will be of interest only to companies creating, or looking to create, products within that area. It does offer extremely fast development, which can enable ROI evaluation for IoT projects, but must be connected to local aggregation points if significant edge processing is needed.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Arduino; Microchip Technology

Recommended Reading: "Emerging Technology Analysis: Opportunities of Open Instruction Set Architecture RISC-V"

"Solution Criteria for Unified Endpoint Management Systems"

IoT Edge Architecture

Analysis By: Aapo Markkanen

Definition: IoT edge architecture represents hardware, software and communications elements that optimize capabilities such as compute, storage, networking and analytics to be deployed closer to where IoT data is produced or consumed. Edge architecture defines how information generated by sensors and endpoints is aggregated and handled at the edge of a network or a data center. Under an IoT edge architecture, intelligence within a connected system is distributed according to where the use case requires it the most.

Position and Adoption Speed Justification: IoT edge architecture is further approaching the Trough of Disillusionment, reflecting a growing awareness of the involved technical challenges among both end users and vendors. The fact that edge processing and storage will be necessary solution elements in many IoT deployments has by now become clear to both sides of the market. End users are increasingly often including edge capabilities in their product and technology evaluation, while practically all major vendors targeting IoT enablement are trying to address the edge in one form or another. The implementations can be, however, hindered by issues such as limited device interoperability and difficult developer environments, as well as integration with legacy edge systems. Furthermore, the cost of implementing and operating edge computing products remains often prohibitively high, especially when deploying such products at scale. Consequently, the business case for deploying an advanced IoT edge architecture is not always there, even if the use cases for doing so are. The dynamic varies notably by industry vertical. For example, investing in an edge architecture in consumer IoT is not nearly as feasible as it is in industrial IoT, where applications typically require robust edge capabilities by necessity.

User Advice: There are many ways to implement an IoT edge architecture. Enterprises deploying IoT must align their overall technical architecture to the targeted business outcomes associated with the use case, determining where in the system the data should be handled in order to maximize its business value. Importantly, upgrading storage and processing capabilities at the edge is often also a good opportunity to adopt a wider event-based architecture. The established alignment must then be maintained throughout deployment and implementation. Further key recommendations include:

- Establish a formal IoT architecture that addresses device management, embedded software, security, local analytics, data filtering and normalization, protocol translation, data storage, as well as connectivity.
- Plan the edge deployment in the context of a wider edge-to-cloud strategy — and not in isolation, separate from cloud investments.
- Utilize vertical-specific, prevalidated edge solutions, where possible, as these can be readily deployed with the help of system integrators that can also contribute some degree of solution customization as needed.
- Expect longer development cycles, as well as recurring maintenance commitments, if building edge solutions predominantly in-house.
- Carry out a thorough proof of concept before broad deployment — for example, studying how the selected solution elements behave in the deployment environment, and assessing the implementation and integration requirements.
- Future-proof the edge deployment by using a modular design under which different technology elements can be later upgraded or replaced without undermining the system's other elements. In deployments with enough processing power and network bandwidth, containerized microservices should be considered.

Business Impact: A well-defined and carefully designed IoT edge architecture is a critical building block for the majority of IoT initiatives, particularly in industrial verticals. Optimal IoT edge architectures balance technical elements, such as data analytics, security and scalability, against the overall business requirements and integration complexity. The choices related to the edge architecture will have a direct impact on the IoT project's upfront costs (especially integration), as well as operational costs (especially communications). Such choices will also largely determine what level of flexibility the enterprise will have in terms of making changes to its IoT-enabled assets and, thus, the business operations that they contribute to.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Advantech; Atos; Cisco; Dell; FogHorn; Lenovo; Microsoft; Rigado; Wind River; ZEDEDA

Recommended Reading: "Market Trends: Early Edge Computing Adopters Prefer Existing System Vendors; Cloud Providers Are Well-Placed"

"Market Guide for Edge Computing Solutions for Industrial IoT"

"How to Overcome Four Major Challenges in Edge Computing"

"Top 10 Strategic Technology Trends for 2020: Empowered Edge"

oneM2M

Analysis By: Chris Meering

Definition: oneM2M is a standards initiative aimed at developing a common, global machine-to-machine (M2M) specification initially focusing on the service layer. The goal of the initiative is to identify a common service layer architecture by identifying the gaps in existing standards and creating specifications to fill these gaps. oneM2M was formed in 2012 and is supported by eight of the world's preeminent ICT standards development organizations.

Position and Adoption Speed Justification: Release 4 (planned 4Q20) further addresses interworking with 3GPP network services together with edge computing, vehicular applications and semantic interoperability capabilities.

While a number of companies have adopted oneM2M as part of their platform stacks, there were few market announcements in 2019 to indicate an increase in the modest adoption levels. For a technology whose value proposition is based on interoperability, this is clearly a concern.

Despite increasing involvement with other industry verticals, we maintain our concern of oneM2M being too focused on the communications service provider (CSP) industry to become relevant to the majority of IoT developers and increase the benefit rating above moderate. As a result, the profile continues to move toward the Trough of Disillusionment, but with a time to plateau at two to five years.

Reaction to Release 4 is key: If well-received, the new capabilities may increase relevance to the technology, whereas if not, we may have to draw a conclusion that oneM2M simply doesn't have much of a further upside.

User Advice: New agreements such as the collaboration with the IoT Connectivity Alliance (ICA), an open standards alliance initialized by Alibaba Group, is likely to grow awareness in China and beyond. Similarly government support via the Indian standards body, TSDSI, for the use of oneM2M across smart city deployments will increase the attractiveness to developers and OEMs.

The provision of essential services often required industrial IoT deployments, together with the ongoing activities with the Industrial Internet Consortium (IIC) increases the attractiveness to additional markets. Similarly, oneM2M continues to evolve the Smart Device Template (SDT), to provide a simple, modular and agnostic framework to enable seamless management of smart home devices in the consumer market.

Such developments, together with the plans for Release 4, continue to address to some extent Gartner's earlier criticism that oneM2M is overly focused on the needs of the CSP ecosystem.

oneM2M's attempts to broaden the market for developer and OEM applications by increasingly positioning its role in IoT solutions as an interoperability hub that works across different industry verticals and industry-specific protocols.

Application developers and OEMs should look at oneM2M, in areas that are intrinsically complex multiparticipant ecosystems such as smart cities, to simplify their application development — enabling utilization of applications across different service platforms and intraindustry and interindustry service integration.

However they should also be mindful of the disadvantages — limited vendor support, CSP dominance and technical complexity — when making their decisions on investing in this technology. Many IoT solutions do not require the multivendor interoperability, or support on many different transport layers offered.

Business Impact: oneM2M can help vendors active in the CSP domain achieve mass-market economies of scale through faster time to market for their products/services at lower capital and operating costs. For service providers, it lowers both capital expenditure (capex) and operating expenditure (opex) through enabling the use of a single IoT platform from all products and services or to manage cloud APIs. In principle, the standard can reduce complexity for developers and help future-proof their applications by making migration onto another vendor's platform more feasible. However, in practice, backing a largely unproven and developing standard always involves substantial business risks.

oneM2M warrants attention in geographies and industry verticals where platforms supporting the standard stand a good chance of being widely adopted, such as smart cities in countries such as India, South Korea and China. Additionally, developers should look to opportunities where network operators have deployed oneM2M compliant platforms.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Chordant; Deutsche Telekom; Huawei; KEPCO; LG CNS; Litmus; Orange; Samsung SDS; SK Telecom; ZTE

Recommended Reading: "Market Trends: A Comprehensive Approach to CSP IoT Platform Selection Will Enhance Market Positioning"

"Designing an IoT Reference Architecture"

"A Guidance Framework for Architecting the Internet of Things Edge"

Bluetooth 5.1

Analysis By: Tim Zimmerman; Annette Zimmermann

Definition: Bluetooth 5.1 is the latest-generation Bluetooth technology approved by the Bluetooth Special Interest Group (SIG) in January 2019, and is now shipping. The biggest benefit of version 5.1 is the addition of angle of arrival (AoA) and angle of departure (AoD), which are used for locating and tracking devices.

Position and Adoption Speed Justification: Bluetooth has been one of the most popular wireless technologies with billions of Bluetooth devices shipped each year. With its latest enhancements, Bluetooth 5.1 is expected to be widely adopted, which is why it is moving through the Hype Cycle so quickly. Mainstream adoption use cases for Bluetooth 5.1 in upcoming devices include not only location and proximity sensing, but also improvements in broadcast advertising, performance, connection stability and battery life.

Implementation of AoA functionality will require additional external infrastructure measurements as well as beacons with new directional antennas to provide AoD information; both will increase the overall cost of the solution. This will slow the adoption momentum as the market moves to newer beacon technology, but we expect faster adoption as the market expands with the new capabilities. We agree with the Bluetooth SIG that the market will begin to see AoD for applications such as warehouse pallet tracking, where a mobile beacon can be deployed and provide valuable location information by using the existing infrastructure.

User Advice: When considering BLE use cases, use BLE 5.1. However, advancements in the technology should not garner additional expense for the beacons. According to the Bluetooth SIG, location service is one of the fastest-growing solution areas for Bluetooth technology, and will be used for both the consumer market and enterprise solutions. Users need to use version 5.1 beacons not only for broadcast solutions in wayfinding applications or for supplemental beaconing, but also for the integration of advertising, location information, directionality and performance enhancement, which can be achieved with the updated technology. Users need to be aware that AoA and AoD are important advancements in Bluetooth solutions, are best for fixed beacon solutions, and will be more challenging for mobile devices such as smartphones or asset tags that may rotate in a lot of different orientations in their deployed use case.

Business Impact: Bluetooth 5.1 maintains backward compatibility, but new functionality such as AoA and AoD will require beacons with directional antenna support, which will increase the cost. The location services functionality as well as the ability to create advertising or information beacons will accelerate the adoption. However, there may be implementation differences associated with AoA and AoD that will require testing to ensure compatibility.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Apple; Broadcom; MediaTek; Nordic Semiconductor; Qualcomm; Samsung Electronics

Recommended Reading: "Magic Quadrant for Indoor Location Services, Global"

"Critical Capabilities for Indoor Location Services, Global"

"Market Guide for Indoor Location Application Platforms"

Low-Cost Development Boards

Analysis By: Bill Ray

Definition: Low-cost development boards (LCDBs) are a type of embedded computer with an easy-to-use development environment and a price point below $50. Most are entry-level electronic platforms that allow developers to configure the design easily to fit their requirements. Boards are created by chip vendors (including Analog Devices and Texas Instruments) or specialist third parties, such as Adafruit and the Raspberry Pi Foundation.

Position and Adoption Speed Justification: LCDBs are designed for prototyping applications, but they are increasingly finding their way into production systems. Hardware cost can be as low as $7 (for an Adafruit Trinket) to $55 for a Raspberry Pi 4, or higher, but common to all such boards is a supported development environment allowing fast software development. This creates a rapid return on minimal investment. Many LCDBs are based on open-source hardware and software, enabling an active ecosystem of companies and hobbyists creating hardware extensions and software libraries.

Hybrid companies, such as Pycom, supply LCDBs that are also available in SoC form (for PCB surface mounting). This enables development to quickly move from prototyping to production without changes to the hardware design or the software. Many LCDBs are never integrated into larger products — having been used for unique projects or just for experimentation — but the vendors are increasingly aware that supporting customers in bridging the gap between the LCDB and production hardware is a worthwhile investment.

Low-power networks, including LoRa, Bluetooth and NB-IoT, are increasingly being integrated into LCDBs by manufacturers keen to promote specific networking technologies. The addition of connectivity opens a host of new applications, all of which need exploring and prototyping, creating new markets for LCDBs.

Despite this activity enterprise adoption is still sporadic. Internal prototypes are often neglected before return on investment (ROI) can be established, or projects pushed by individual staff fail for lack of management backing. For these reasons, the LCDB has moved along the Hype Cycle but only to the first steps beyond the Trough of Disillusionment.

User Advice: With greater processing and communications, more boards with greater functionality will enter the market. Some are targeting specific IoT applications, while others highlight specific technologies, such as AI or novel sensors. Internet of Things (IoT) application vendors must collaborate with development board vendors to understand the capabilities of these emerging boards. This can help to provide fast prototypes and shorten time to market. Also, sensors and wireless connectivity are the key for IoT applications. IoT application vendors will have to collaborate with wireless connectivity and sensor vendors to develop suitable LCDBs to fit the emerging demand in IoT endpoints.

Security remains a big issue for IoT endpoints. Some platforms, such as the popular Arduino, do not have comprehensive security solutions, and this must be considered when considering the use of such boards in commercial products.

Business Impact: LCDBs accelerate IoT-enabled device development from idea to prototype and even to mass production. This is critical to new product development, since it can shorten the time to market. LCDBs enable more small-scale startups and individual developers to innovate in the fragmented IoT market. In order to enjoy the benefit of increasing sales after materializing prototypes to real products, major semiconductor vendors use their existing chips to create/support corresponding boards.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Adafruit; MediaTek; Qualcomm; Samsung; STMicroelectronics; Texas Instruments

Recommended Reading: "Drive Smarter Savings With Foundational Cost Definitions"

"The Technical Professional's Guide to Edge Infrastructure"

MicroPython

Analysis By: Bill Ray

Definition: MicroPython is an implementation of the Python 3 programming language created to run on microcontrollers; it is now available on a wide range of embedded platforms. MicroPython offers fast development, simple code maintenance, and access to a wide range of existing software and source code modules.

Position and Adoption Speed Justification: Python is a high-level programming language, suited to fast development and easy maintenance. MicroPython brought these advantages to an embedded environment and led to the creation of CircuitPython (which extends support to Adafruit's popular range of embedded platforms) and Zerynth (which adds real-time processing).

Python was originally heralded as an ideal language for educational applications, being selected as the default development environment for the Raspberry Pi Foundation. MicroPython provides a subset of the Python language but replicates the structure and syntax so that developers can take their skills and their applications into low-end hardware. Support for MicroPython has been steadily increasing with the processing power available in embedded systems. We also see more API libraries and peripheral support being added.

Despite this success, MicroPython is still mostly the preserve of educational users and the maker (hobbyist) community. Professional developers, and enterprises, have been slow to realize the opportunity of MicroPython, so it has only progressed slightly toward the Plateau of Productivity.

User Advice: Adopt MicroPython to accelerate development and reduce development costs if time to market is critical. As an interpreted language, Python requires more processing power than low-level languages, so it requires boards with 32-bit microcontrollers. This limitation has become less important as IoT increasingly adopts 32-bit microcontrollers for most applications.

MicroPython is a robust platform for commercial development of products for IoT, particularly small endpoints with limited functionality — including networked sensors or actuators with limited local functionality (such as temperature control or automated ventilation). Anyone developing IoT applications should ensure they are employing developers capable of creating and maintaining applications written in MicroPython.

Business Impact: MicroPython enables rapid development of embedded applications which previously required knowledge of C. Widespread adoption will increase the utility and penetration of network edge intelligence.

As an interpreted language, Python (including MicroPython) does not make use of a compiler (or linker) during development. This adds resilience to application development, while reducing the developer toolchain. It also frees developers to use their preferred environment and (potentially) reduces the cost of developer seats. However, it also creates a risk of fragmentation of the development process, including version control, backup systems and documentation, all of which must be carefully managed.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Adafruit; MicroPython; Pycom

Recommended Reading: “Top 10 Strategic Technology Trends for 2020: Democratization”

“How to Automate Your Network Using DevOps Practices and Infrastructure as Code”

Climbing the Slope

Embedded Hypervisor

Analysis By: Alan Priestley

Definition: An embedded hypervisor provides a software virtualization layer that allows multiple OSs or execution environments to run simultaneously on an embedded processor. Unlike hypervisors used on desktop and general-purpose servers, an embedded hypervisor will typically support the real-time operation and security requirements of many embedded systems.

Position and Adoption Speed Justification: High-performance-embedded processors have instruction sets and hardware features to enable software virtualization. This has enabled embedded hypervisors to become an integral part of embedded software development and a wide range of embedded projects are now integrating virtualization through embedded hypervisors. Complex embedded systems and IoT endpoints utilize sophisticated OSs and applications. An embedded hypervisor enables isolation between various software functional blocks, simplifying system design and minimizing the impact of updating or replacing a given functional block. Security in IoT endpoint devices is also a major focus area for device manufacturers and embedded hypervisors are increasingly becoming the de facto approach to secure an embedded OS. By leveraging embedded hypervisors, system designers are able to isolate safety functions from nonsafety functions, saving on hardware costs and streamlining the certification process. With the growth in deployment of IoT endpoints with high-performance processors employing embedded virtualization, enabling greater functional integration and security in devices, we are advancing this technology forward toward the plateau in this year's Hype Cycle.

User Advice: Embedded hypervisors enable technology product managers to develop systems that support multiple OS environments, allowing greater integration of system functions and product features, enhancing user experience. This makes possible the addition or porting of new embedded software and running it alongside the existing legacy software (and vice versa) when using existing or a new hardware platform. When evaluating embedded processors from new designs product managers should ensure that the selected device includes virtualization extensions to its instruction set to minimize the performance impact of implementing an embedded hypervisor and to enforce isolation between virtualized environments.

Embedded hypervisors play an important role in designs with multicore processors, as they enable the distribution of tasks and applications from different operating systems, including RTOS, across the cores. This will be crucial in managing the power efficiency in multicore systems by dynamically switching off cores.

The use of an embedded hypervisor provides product managers with independent and isolated development environments for OS, middleware and device driver components. An embedded hypervisor also provides a mechanism to deploy legacy/mature applications on to new device hardware, isolating new applications from stable and prevalidated functionality. The flexibility it offers to all the players in the value chain, including semiconductor chip vendors, is immense.

Business Impact: Technology product managers at IoT endpoint vendors can utilize embedded hypervisors to reduce time to market, by leveraging the ability to integrate a wide range of available applications in separated isolated environments.

The ability to create isolated execution environments on the main system processor for real-time, security and mission-critical functions reduces the need for separate dedicated processors for every functional block and isolates non-mission-critical applications, such as user interfaces, from the rest of the software applications.

Embedded hypervisors enable the easy portability of existing software applications from legacy systems to new equipment types. The ability to isolate different software functions can simplify complex designs enabling a single processor to support multiple different type of functionality. An embedded hypervisor can also be used to enhance security, enable key software functions to execute in their own isolated environment.

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: BlackBerry QNX; Green Hills Software; IBM; Mentor a Siemens Business; Microsoft; SYSGO; Trustonic; VMware; Wind River; XtratuM

Recommended Reading: “Addressing the Hardware Design Challenges Created by Edge Computing”

“Market Trends: Edge Computing Creates New Equipment Design Challenges”

“Forecast: IoT Semiconductors, Worldwide, 1Q20 Update”

Sensor Fusion

Analysis By: Amy Teng

Definition: Sensor fusion is a process that aggregates and “fuses” many disparate sensor inputs to increase sensor data accuracy and/or sensing coverage for the system to develop insights and decisions. A sensor fusion solution usually includes a set of sensors, a hardware sensor hub, a fusion engine and a software sensor fusion stack.

Position and Adoption Speed Justification: Sensor fusion for automotive and industrial systems has been prevalent for decades. Sensor fusion also exists in smartphones and tablets where the sensor data has been interpreted by OS allowing app developers access through APIs.

During the past few years, sensor fusion has evolved to include lidar, radar and visual sensing for autonomous cars, SLAM (simultaneous localization and mapping) for drones and robots, and six degrees of freedom (6DoF) visual and 3D audio immersion for (head mounted displays) HMDs.

Technology evolution of autonomous things and Internet of Things (IoT) will keep on pushing the number and the diversity of sensor and sensing technology to a higher level, driving continuous enhancement of sensor fusion technology. Sensor fusion algorithms' development has been benefited by the growing leverages of artificial intelligence/machine learning (AI/ML) technology. When this combined with improved sensor accuracy and advanced computational power of sensor engine, sensor fusion can analyze faster and better than before. Therefore, we moved its position a bit forward

User Advice: Sensor fusion software stacks can be derived from three resources: open source, sensor companies and software companies who focus on serving customers who have sensor fusion requirement. Sensor fusion software can be ported to a variety of different hardware platforms, ranging from application processors, general purpose microprocessors and microcontrollers, programmable logic, integrated combo sensors, and purpose-built devices like Microsoft's customized holographic processing unit (HPU) for HoloLens. Consider discrete, low-power sensor hub solution to offload the process of main processor when designing for power constraint and long battery life applications.

Build a central platform to manage sensor fusion algorithms across different products and applications to gain reuse efficiency. For example, a smartwatch and wristband can share same algorithm for detecting a wearer's gesture and posture, the two devices can also share the same voice actuated algorithm with smart speakers.

Leverage AI/ML to accelerate the pattern recognition of sensor signals and shorten sensor fusion development time.

Sensor fusion can also offer reduced size and weight, which is particularly important in drone applications.

Business Impact: Sensor fusion technology is a key element of enabling real-time contextual analysis because it comprehends the status of a system. Additionally, leverages AI/ML and clever manipulation of different types of input sensors to train model will explore new algorithms, resulting in new insights or new applications unseen before. For example, fusion of sound waves and surface vibration of sound source can create a new type of noise-cancellation device.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: CEVA (Hillcrest Labs); CyweeMotion; Kionix; Knowles; NXP; Qualcomm; QuickLogic; Renesas; STMicroelectronics; TDK (InvenSense)

Recommended Reading: "Cool Vendors in Novel Sensors"

"Cool Vendors in Novel Sensors"

“Market Trends: Supplying Intelligent Sensors for the IoT Takes Cooperation, Integration and Software”

IPv6

Analysis By: Neil Rickard

Definition: Internet Protocol version 6 (IPv6) is the next version of Internet Protocol (IP). It’s designed to overcome several key limitations of Internet Protocol version 4 (IPv4) — in particular, the exhaustion of public IPv4 addresses.

Position and Adoption Speed Justification: Public IPv4 address exhaustion means new public IP addresses will be IPv6 only. The continued growth of the internet, including consumer internet access in emerging markets, mobile devices and the Internet of Things (IoT), will increasingly be accommodated using IPv6. Google IPv6 Statistics show nearly 30% of users accessing Google do so using IPv6. However, the installed base of IPv4 infrastructure is huge and it will not migrate soon as migration costs are high. Also, there is an active market for IPv4 address transfers between organizations. Hence through at least 2025, the public internet will carry both IPv4 and IPv6 traffic.

Many network operators have been early adopters of IPv6 to facilitate continued growth. However, for enterprises, the actual depletion date for public addresses isn’t critical because most enterprises use private IP addressing inside their organizations. Additionally, they typically already have the few public IP addresses they need for external services. Although most enterprises have little need to transition their internal systems to IPv6, they do need to enable IPv6 support on their public internet presence to ensure successful communication with IPv6-based consumers. Many organizations have already done this.

Enterprises are increasingly discovering pockets of IPv6 appearing within their network environments, especially in IoT use cases. These include sensor networks, process automation systems and building environmental control networks, because many of these systems will only support IPv6.

User Advice: Selective deployment of IPv6 is now advisable, especially for public-facing services, but a large-scale replacement of existing IPv4 services is still not recommended as migration costs and risks are substantial. Network planners should separate their IPv6 strategies into public internet presence, user LANs, data center LANs, and specialty networks such as IoT.

Enabling IPv6 on the enterprise public internet presence is now becoming critical. Because an expanding part of the internet’s population will be natively IPv6 — especially in Asia, the developing world and 3G/4G/5G mobile networks — public-facing services (such as websites) should be migrated to IPv6 as soon as possible. Nearly 30% of all websites (by traffic volumes) have already enabled IPv6. Supporting external IPv6 connectivity will improve performance and visibility for enterprises’ IPv6-only customers, partners and remote employees connecting via an IPv6-only internet provider or IPv6-only mobile devices. Organizations that do not enable IPv6 for these services will be forced to connect to such users via operators’ network address translation gateways, which could easily become overwhelmed and may be unable to cope with complex translations.

There are far fewer benefits to deploying IPv6 internally to the enterprise. The migration costs are high for established IP networks, and attempts to transition even midsize networks have revealed many unexpected problems and hidden costs. As IPv6 is a new protocol and tends to be deployed with public addressing, rather than network address translation (NAT), network security must be completely rethought. It is generally easier to continue with private IPv4 addressing internally to the enterprise; if additional IPv4 addresses are required for external connections, these can be obtained through address trading. Gartner estimates that fewer than 5% of all intranets are IPv6-enabled.

Although we do not currently recommend migrating to IPv6 for all internal systems, enterprises should proceed with their IPv6 planning, including determining which systems and equipment are IPv6-ready and which are not, as well as establishing a transition roadmap. Larger network service companies, such as NTT Communications, offer professional services to assist in this activity. As businesses replace network and IT infrastructure, every new item of hardware or software with network capability should have IPv6 support so that the eventual transition will be easier and less expensive. Leading network services and cloud services support both IPv4 and IPv6 but it is important for enterprises to determine the options, limitations and cost of such support.

New greenfield networks should be built to support both protocols from the outset. In addition, organizations that undertake a large-scale IPv6 deployment are likely to need DDI platforms: a DNS, a Dynamic Host Configuration Protocol (DHCP) and an IP address management platform.

Expect to support both IPv4 and IPv6 through at least 2025. In some specialty networks, IPv6 provides a specific advantage when, for example, scale is critical, intercompany/interagency addressing is required, or networks are frequently set up and torn down.

Business Impact: The key for most businesses is to avoid connectivity disruptions that new users running the IPv6 protocol could create. The adoption of IPv6 beyond this requirement will typically be time-consuming and costly with few, if any, benefits.

Benefit Rating: Low

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: BlueCat; Cisco Systems; Citrix; Infoblox; NTT Communications; Tata Communications; Verizon

Message Queue Telemetry Transport

Analysis By: Anushree Verma

Definition: Message Queue Telemetry Transport (MQTT) is an open message protocol originally designed for machine-to-machine (M2M) communications for use with constrained networks. It enables the transfer of messages between a server and several devices, such as sensors, phones or computers, based on a publish-and-subscribe messaging paradigm. MQTT provides three qualities of service: “at most once,” “at least once” and “exactly once.”

Position and Adoption Speed Justification: Open, royalty-free and lightweight, MQTT primarily targets M2M and Internet of Things (IoT) integration over low-bandwidth, high-latency and unreliable TCP/IP networks. There is a further specification called MQTT for Sensor Networks (MQTT-SN) for embedded devices on non-TCP/IP networks.

MQTT v.3.1.1 was approved by the Organization for the Advancement of Structured Information Standards (OASIS) for standardization in November 2014, and as an ISO standard (ISO/IEC 20922) in June 2016. MQTT v.5 has also been approved on 3 April 2019 by OASIS.

MQTT has matured to now be considered one of the major standards in IoT. Most IoT vendors and many message-oriented middleware vendors have some type of MQTT capability as part of their multiprotocol approach. This accounts for its advancement in its position and time to plateau to be in less than two years.

User Advice: Developers wanting to minimize IT costs for their mobile and embedded systems and IoT initiatives and leverage a connectivity protocol in constrained environments should evaluate MQTT.

The open-standard nature of MQTT, availability of open-source implementations and cloud-service-based MQTT offerings provide developers with a range of deployment options. Organizations wishing to implement multivendor M2M scenarios while minimizing vendor lock-in risk should consider MQTT as the underlying connectivity layer.

MQTT use is not constrained to M2M use cases. Users looking for a “universal” messaging layer to integrate M2M, mobile applications and enterprise applications should evaluate the suitability of MQTT against other protocols.

Developers should be aware that MQTT transmits data in clear text. Consequently for this, for secure or mission-critical applications, security add-ons will be required potentially impacting memory-constrained IoT hardware designs.

Business Impact: MQTT is a connectivity protocol for constrained environments. This standard for messaging helps businesses achieve faster time to market for their products and services by combining M2M, mobile and enterprise applications, and cloud based services providing a reasonable degree of vendor independence and flexibility.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: arm; Apache Software Foundation; Eurotech Group; IBM; Microsoft (Azure); PubNub; Red Hat; Software AG; Solace; TIBCO Software

Recommended Reading: "Market Guide for Industrial IoT Gateways"

"A Guidance Framework for Architecting the Internet of Things Edge"

"Designing an IoT Reference Architecture"

Data Distribution Service

Analysis By: Saniye Alaybeyi

Definition: Data distribution service (DDS) is a brokerless middleware messaging protocol designed to enable network interoperability for connected machines, enterprise systems and mobile devices. It provides scalability, performance and quality of service required to support data centric applications, besides a global data space for analytics, enabling flexible real-time system integration.

Position and Adoption Speed Justification: DDS has been around since the release of its first version in 2003. It evolved specifically to enable real-time, nonstop systems. DDS supports efficient bandwidth usage and low latency. There are about ten implementations of DDS, propagating the standard into system designs in healthcare, transportation, communications, energy, industrial, defense and other industries. In industrial IoT and autonomous cars, DDS and its data-centric nature make it possible to connect applications with a shared data model and open data bus, regardless of proximity, platform, language, physical network, transport protocol and network topology.

DDS continues to face indirect challenges, facing a loss of mind share to other protocols, such as Message Queuing Telemetry Transport (MQTT) and Advanced Message Queuing Protocol (AMQP), which are being promoted by big vendors such as IBM, Cisco and Microsoft. DDS also faces competition from other brokerless messaging frameworks like ZeroMQ and NNG — nanomsg-NG. However, use of DDS in autonomous vehicle and robotic use cases is promising. Autonomous vehicles are highly complex systems. Manufacturers need to ensure their systems can operate in diverse real-time environments, meet safety and security requirements, scale and interoperate within all autonomous vehicle systems that DDS can satisfy. On the other hand, DDS is not lightweight, and it is yet to be deployed on low-footprint devices. Therefore, it faces stiff competition from other messaging protocols, such as CoAP. DDS is designed for closed environments/networks of devices (for example, in a vehicle or building). Vendors like Real-Time Innovations (RTI) have workarounds for this (RTI Routing Service).

User Advice: Designers of resourceful devices for industrial, automotive (including autonomous vehicles), healthcare and other industries — where the requirements for reliability, security and longevity are high — should consider the use of DDS for network interoperability to achieve the desired quality of service. DDS skills are rarely available in the market. DDS will require a long learning curve.

Business Impact: DDS can help businesses with true "real-time," mission-critical and data-centric use cases with high reliability and low latency requirements.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: ADLINK; IBM; Milsoft; OCI; Real-Time Innovations (RTI); SourceForge; Twin Oaks Computing

Recommended Reading: "Market Guide for Industrial IoT Gateways"

"Choose the Best Integration Tool for Your Needs Based on the Three Basic Patterns of Integration"

"Designing an IoT Reference Architecture"

AMQP

Analysis By: Saniye Alaybeyi

Definition: The advanced message queuing protocol (AMQP) is a formal standard for implementing message-oriented middleware (MOM) that supports message queuing and publish-and-subscribe messaging paradigms. MOM provides asynchronous program-to-program communication between two or more components of an application or between two or more applications. AMQP specifies the wire protocol so messages can be exchanged among software components and MOM can be supplied by various vendors that implement the same version of AMQP without gateways or adapters.

Position and Adoption Speed Justification: The current version of the AMQP standard was published in 2011. There have not been significant changes to AMQP protocol in recent years and this topic does not come up during Gartner client conversations. Therefore, Gartner decided to make AMQP obsolete before plateau.

User Advice: Architects, middleware experts and development managers should select MOM primarily on the quality of the product and the vendor, with support for AMQP as a secondary consideration. The desirability of using an AMQP-based MOM product, and the weight that should be assigned to AMQP, depends on the nature of the application:

- Cost-conscious, leading-edge project teams that are confident in the abilities of their middleware staff should give AMQP-based products positive consideration, especially if they have already adopted an open-source strategy or are buying multiple products from an AMQP vendor.
- Mainstream project teams should view AMQP support as a relatively minor feature for MOM products.
- Interoperability is not guaranteed between AMQP versions, and even among the same AMQP version. There can be interoperability issues between an AMQP broker or MOM service and AMQP clients (between message producers and consumers). Users should be aware of the distinction between AMQP 0.9.1 and 1.0 and should pick one and stick with that version and the vendors that support it.

- Most project teams concerned with near- or medium-term benefits, and with no foreseeable need to integrate messaging with business partners, should not give any special consideration to AMQP. They should select their MOM product on other criteria, regardless of whether it supports AMQP.

Business Impact: The implications of AMQP are theoretically far-reaching, although major benefits depend on wide adoption that might not occur. So far, adoption of AMQP has been as either the core runtime of a messaging provider or an additional wire protocol to existing messaging products, with most users still choosing single-vendor solutions. Interest from vendors is moving toward more modern messaging engines, such as Apache Kafka, with few new AMQP implementations coming to market in recent times.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Amazon Web Services (AWS); Apache Software Foundation; IBM; INETCO Systems; Kaazing; Microsoft; Red Hat; Solace; SwiftMQ; VMware (Pivotal)

Recommended Reading: “Streaming Architectures With Kafka”

“Market Guide for Industrial IoT Gateways”

“Choose the Best Integration Tool for Your Needs Based on the Three Basic Patterns of Integration”

“How to Choose Your Best-Fit Decision Management Suite Vendor”

IoT Integration

Analysis By: Benoit Lheureux

Definition: IoT integration refers to integration requirements and technologies needed to assemble end-to-end IoT-enabled business solutions that include IoT-specific integration challenges, such as integrating IoT devices, IoT data, digital twins and multiple IoT platforms. Other more traditional integration challenges include enterprise application and data integration, business process integration, SaaS integration, and B2B/ecosystem integration, as well as mobile app and legacy system integration.

Position and Adoption Speed Justification: IoT projects involve the integration of business application data and processes — competencies that are widely available. But such projects also introduced new integration requirements, such for as IoT devices, mobile apps, digital twins, hybrid edge-to-cloud infrastructure, large data volumes, and IoT time series event streaming and analysis. Most mid-to-large-sized companies can address some but not all these needs, so they are expanding their integration skills to compensate. Most IoT platforms offer some basic integration capabilities, including device communications (for example, MQTT) and API gateways management (for example, to govern API access), and a limited number of adapters to facilitate integration with a few applications. While many IoT platforms still do not support all IoT device protocols (such as OPC-UA), strong translation, complex application workflow, and a complete portfolio of adapters for business applications and SaaS to be integrated, we have moved this Hype Cycle entry further toward the Plateau of Productivity because iPaaS (needed to address these needs) is widely available from third-party TSPs, and many of the larger TSPs that offer IoT platforms (like GE Digital, Hitachi, IBM, Microsoft, SAP) do offer an iPaaS in addition to their IoT platform (see “Technology Insight for Enterprise Integration PaaS”).

User Advice: Comprehensive integration skills and technologies will help IT leaders more successfully implement IoT projects. Nearly every IoT implementer has adopted an “API-first” approach for integration, using APIs provided by IoT platforms for IoT device connectivity, data synchronization and process integration. Typically, features include event-stream processing, RESTful APIs and, sometimes, message-oriented middleware (MOM), such as MQTT. However, these approaches, alone, do not address crucial integration needs such as semantic integration (to translate data from one format to another) or workflow (to orchestrate the linking of data, events and processes across many systems). IoT implementers must also at times integrate multiple IoT platforms, for example, to get data from IoT-connected products from an OEM’s IoT platform. Thus, IoT implementers often discover that they must also leverage stand-alone integration technology, such as iPaaS, API management, ESB suites and ETL tools in order to fully meet their IoT project integration requirements. Sometimes IoT implementers will also benefit from data exchanges, to help propagate IoT data to external business partners (see “Use APIs to Modernize EDI for B2B Ecosystem Integration”). For IoT project implementers, the goal is to more broadly adopt a pervasive integration approach using a holistic set of integration skills and technologies to address all forms of integration required in their projects. For example, IoT integration needs should be addressed in your hybrid integration platform (see “How to Deliver a Truly Hybrid Integration Platform in Steps”).

Business Impact: All end-to-end IoT business solutions require device, application, data and process integration (see “Use the IoT Platform Solution Reference Model to Help Design Your End-to-End IoT Business Solutions”). The challenges are nontrivial, often involving extraordinary:

- Heterogeneity (that is, multiple types of IoT devices, products and equipment, data, vendors, and systems to integrate)
- Distribution (that is, IoT devices, products and equipment are often remotely located across long distances and multiple geographies)
- Performance and scalability (that is, large numbers of IoT devices, products and equipment with high API throughputs and large volumes of time series data)

The cost of such integration includes:

- Integration skills development and integration development time
- Integration middleware or services (ESB software, iPaaS, data integration tools and API management, data exchanges or brokers)

- Integration products focused on operational technology (OT) integration (such as from OSIsoft and Skkynet) may be needed and must be licensed separately
- IT services fees when outsourcing integration to a system integrator

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Alleantia; Dell Boomi; Informatica; Microsoft; Reekoh; Salesforce (MuleSoft); Skkynet; Sky Republic; SnapLogic; Software AG

Recommended Reading: “Market Guide for Digital Twin Portfolios and Enabling Technologies”

“Choose the Best Integration Tool for Your Needs Based on the Three Basic Patterns of Integration”

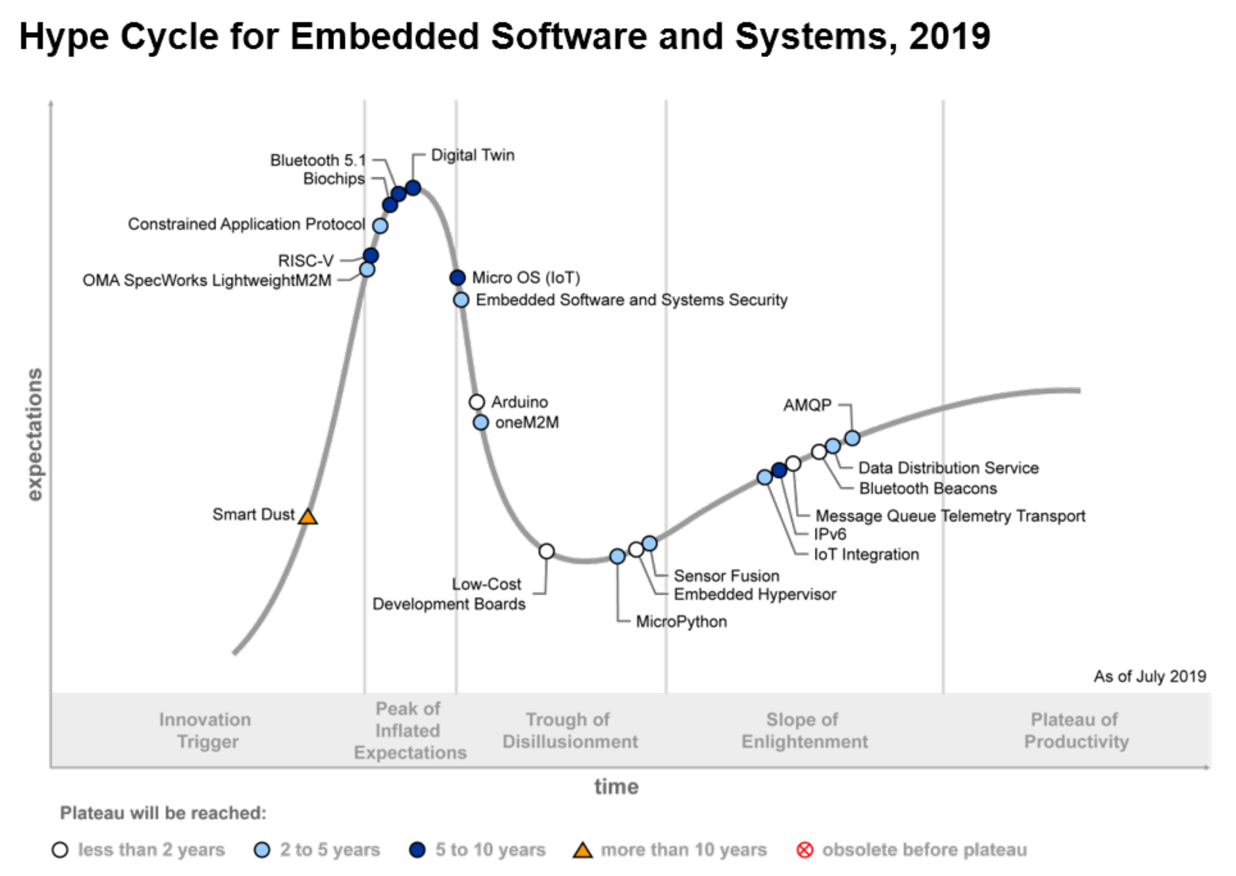
“What to Expect When You’re Expecting Digital Twins”

“Survey Analysis: Digital Twins Are Poised for Proliferation”

“Use the IoT Platform Solution Reference Model to Help Design Your End-to-End IoT Business Solutions”

Appendixes

Figure 3. Hype Cycle for Embedded Software and Systems, 2019



Source: Gartner
ID: 370060

Gartner

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant press and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the technology's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the technology are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the technology to reach the Plateau of Productivity.

Source: Gartner (July 2020)

Table 2. Benefit Ratings

Benefit Rating	Definition
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2020)

Table 3. Maturity Levels

Maturity Level	Status	Products/Vendors
Embryonic	▪ In labs	▪ None
Emerging	▪ Commercialization by vendors ▪ Pilots and deployments by industry leaders	▪ First generation ▪ High price ▪ Much customization
Adolescent	▪ Maturing technology capabilities and process understanding ▪ Uptake beyond early adopters	▪ Second generation ▪ Less customization
Early mainstream	▪ Proven technology ▪ Vendors, technology and adoption rapidly evolving	▪ Third generation ▪ More out of box methodologies
Mature mainstream	▪ Robust technology ▪ Not much evolution in vendors or technology	▪ Several dominant vendors
Legacy	▪ Not appropriate for new developments ▪ Cost of migration constrains replacement	▪ Maintenance revenue focus
Obsolete	▪ Rarely used	▪ Used/resale market only

Source: Gartner (July 2020)

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Hiring Guide: Embedded Software Engineer

Increase Your Competitive Advantage With the Right Embedded Analytics Platform Provider

Hype Cycle for IoT Standards and Protocols, 2020

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp