Hype Cycle for IoT Standards and Protocols, 2020

Published: 30 June 2020 **ID:** G00448213

Analyst(s): Bill Ray

This Hype Cycle charts standards around connectivity, security and messaging systems for the Internet of Things. This year sees several new additions that can be used, alongside existing technologies, to ensure project interoperability and longevity.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

The Internet of Things (IoT) continues to deliver real benefits to those prepared to invest in it, but standards still aren't keeping up with deployments, forcing companies to look at proprietary solutions. It remains easy to develop (and sell) nonstandard systems, but those companies that adopt such proprietary solutions will have to bear the cost of supporting that infrastructure in a decade's time. Early adopters that eschew evolving standards risk long-term problems with interoperability.

Adopting or endorsing standards is an effective way of signaling commitment, as well as promoting an open approach. Where standards are still evolving, there are opportunities for early adopters to shape the standard, creating additional revenue by promoting patented intellectual property or preferred technical approaches.

Deciding to support or endorse a standard is not just a matter of technical compatibility. Issues such as technology obsolescence, ROI and vendor availability should be considered alongside interoperability.

The Hype Cycle

This Hype Cycle provides a view into tomorrow's technology standards and shows how Gartner sees some of the most interesting and significant standards and protocols relating to the IoT. Most of the technologies in this Hype Cycle should be viewed as underlying and enabling technologies that facilitate and support a wide range of IoT products and solutions. Their adoption rates will vary across different industries, with some being more industry-specific than others.

Since the IoT is a combination of multiple technologies, a plethora of standards are available — and a considerable amount of consolidation and attrition is to be expected (and, indeed, welcomed). In the last year, we've seen some of the most important standards cluster around the Trough of Disillusionment. In some cases, such as LoRA, this location reflects a completed standard that lacks deployment. In other cases, such as hardware-based security, it shows a standard at the last stages of development. Early adopters may take the opportunity to shape evolving standards, promoting their own (perhaps patented) intellectual property or pushing a preferred technical approach.

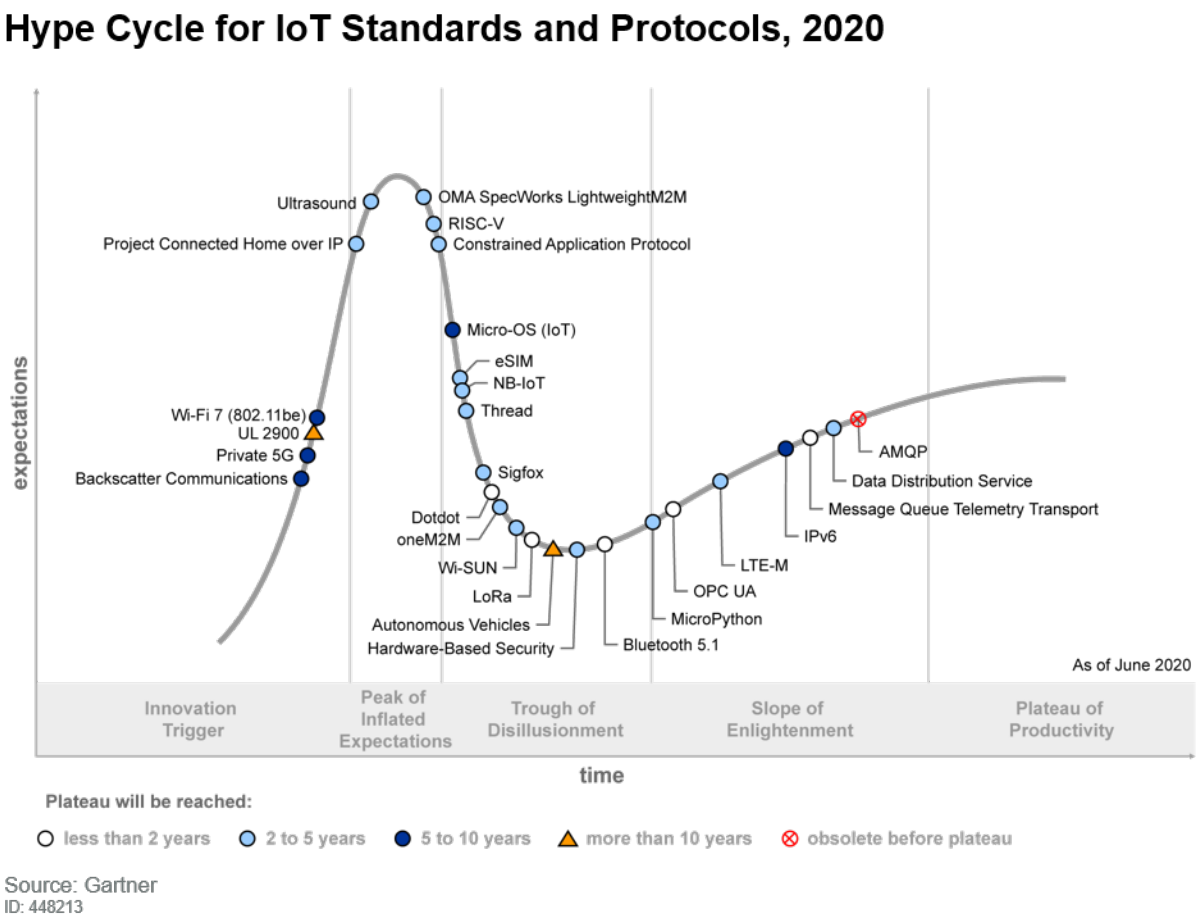
Several critical standards have summitted the Peak of Inflated Expectations this year, including OMA SpecWorks LightwieghtM2M, the Constrained Application Protocol and RISC-V. Overall, the Hype Cycle is becoming more weighted toward the Plateau of Productivity — reflecting the maturity of IoT itself.

However, that's not to say that innovation has stopped: New standards and protocols are still being added. Private 5G, for example, has been enabled with the release of additional radio spectrum and offers ultrareliable connections suited to safety-of-life applications. Wi-Fi 6 has been removed this year, having made its way to the Plateau of Productivity and making way for Wi-Fi 7 (802.11be). Perhaps most important, in the consumer IoT, is the addition of Project Connected Home over IP.

This new standard hopes to unify home automation products, and it has some significant industry backing.

We still see many standards overlapping, or competing directly, especially in areas with large commercial potential. There are also areas of the IoT in which standards are incomplete or lack full-stack support. Consequently, new standards will continue to emerge in the coming years.

Figure 1. Hype Cycle for IoT Standards and Protocols, 2020



Source: Gartner
ID: 448213

The Priority Matrix

The Priority Matrix maps the time to mainstream adoption of a technology against its benefit rating. Five technology standards have been designated with a low benefit rating in this Hype Cycle. In some cases, this reflects uncertain market demand (like Ultrasound and Dotdot), while others are minor updates that smooth the experience — rather than shift the paradigm (like IPv6).

Again, eSIM is the only technology that has been designated as encouraging transformational benefit within a decade, because it can fundamentally change the user-operator relationship.

Figure 2 shows that the IoT continues to innovate rapidly. In five years, another 15 standards should be well on their way to the Plateau of Productivity, making the whole IoT more scalable and productive. Technical innovation hasn't stopped, but the preponderance of technologies past the Peak of Inflated Expectations shows how the IoT is maturing.

Figure 2. Priority Matrix for IoT Standards and Protocols, 2020

Priority Matrix for IoT Standards and Protocols, 2020

benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational		eSIM		Autonomous Vehicles
high	**Bluetooth 5.1** **LoRa** **OPC UA**	**NB-IoT**	Private 5G	
moderate	**Message Queue Telemetry Transport**	Constrained Application Protocol Data Distribution Service Hardware-Based Security LTE-M MicroPython OMA SpecWorks LightweightM2M oneM2M Project Connected Home over IP RISC-V Wi-SUN	Backscatter Communications Micro-OS (IoT) Wi-Fi 7 (802.11be)	UL 2900
low	Dotdot	Sigfox Thread Ultrasound	IPv6	

As of June 2020

Source: Gartner
ID: 448213

Off the Hype Cycle

The speed of IoT development continues to impact the Hype Cycle, as technologies fall out of favor (and off the Hype Cycle) with surprising celerity. 802.11ai has been removed this year, having failed to make an impact, despite being heavily promoted by the Wi-Fi Alliance. Wi-Fi 6 (802.11ax) has become fully productive, as have Bluetooth Beacons. Trusted Environments has been replaced with

Hardware-Based Security, which more accurately represents the way trusted environments are implemented in IoT deployments.

On the Rise

Backscatter Communications

Analysis By: Nick Jones

Definition: Backscatter communications, sometimes known as ambient backscatter communications (AmBC) modulates information onto ambient wireless signals by intermittently reflecting or absorbing them. This allows communication with very low power consumption — orders of magnitude less than conventional radios. AmBC has been demonstrated using ambient signals, such as Wi-Fi, FM radio and TV, and typically has limited range — a few tens of meters.

Position and Adoption Speed Justification: In many Internet of Things (IoT) devices, the dominant consumer of battery power is wireless transmission. Thus, AmBC has considerable potential for low-power equipment, such as sensors in areas where there is sufficient background wireless to be exploited (e.g., in smart homes or offices). AmBC could be used to substantially extend IoT device battery life or, in conjunction with technologies such as power harvesting and supercapacitors, could enable battery-free devices. Researchers have demonstrated AmBC systems compatible with existing standards, such as Bluetooth or LoRa.

Backscatter principles are already used by some radio frequency identification (RFID) systems; however, in 2020, the use of AmBC for general-purpose networking is mostly an academic research topic with no broadly available standards or hardware. The limited range of AmBC systems restricts the scope of appropriate devices and applications. However, researchers are likely to improve performance and features through 2025. The high level of immaturity means AmBC has only advanced slightly on the Hype Cycle during the past year.

User Advice: It's likely that the earliest AmBC applications will emerge in areas such as sensors in the smart home or office, where there is significant ambient RF to be exploited. We expect first-generation standards to emerge from organizations such as IEEE in the three- to five-year time frame. Implementations intended for specific single-vendor applications, where standards and interoperability aren't required, may emerge more rapidly.

Innovation groups and technology monitoring teams should track the evolution of AmBC technologies, vendors and standards to determine when the technology is sufficiently mature to create prototypes and integrate into products. In particular, look for innovation opportunities where ultra-low-power consumption can enable new applications and devices. Consider opportunities enabled by AmBC combined with thermal, vibration, RF or solar power harvesting to enable battery-free devices. Also explore the opportunities of hybrid systems, which combine AmBC with more conventional wireless protocols when no ambient wireless is available to remodulate. Look for early opportunities in cases where AmBC systems generate signals compatible with an existing wireless standard, such as Bluetooth.

When AmBC becomes more mainstream, the quality of in-building wireless coverage (e.g., from Wi-Fi or cellular systems) will become even more important. This is because the signal will be used to power backscatter systems, as well as support its primary communications function.

Business Impact: It will take several years before AmBC becomes sufficiently mature and standardized for large-scale deployment. When it does, it will enable innovative IoT devices with exceptionally long battery life — effectively infinite life in cases where sufficient power can be harvested from the environment. The elimination of a battery will also enable devices to be smaller, lighter and significantly less expensive. The most promising applications will involve those "things" for which power consumption is dominated by wireless transmission. They require little power for other purposes, such as computation and providing a user experience. Therefore, simple devices, such as sensors or beacons, that require only short-range communications are likely to provide the best opportunities. Backscatter networks may eventually enable small, low-cost, disposable IoT devices.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Jeeva Wireless

Recommended Reading: "The Top 10 Wireless Technologies and Trends That Will Drive Innovation"

"Market Trends: IoT Endpoints Will Need New Technologies to Achieve Scale"

Private 5G

Analysis By: Sylvain Fabre; Joe Skorupa

Definition: Private 5G is defined as a private mobile network (PMN) based on 3GPP 5G to interconnect people/things in an enterprise. CSPs and TSPs have the potential to offer 5G PMN to various verticals, such as Industry 4.0, mining, oil, utility and railroad companies; IoT service providers, university campuses, stadiums/arenas etc. Private 5G offerings provide a separate network from the public network. It can include voice, video, messaging, and broadband data and IoT/M2M use cases with higher performance requirements.

Position and Adoption Speed Justification: Most enterprises use cases that justify a need to deploy a Private Mobile Network (PMN) that requires cellular connectivity for mobility, will be adequately served with a 4G network. Where 5G is justified, a PMN can provide the required functionality earlier than what the local CSPs may have deployed on their public infrastructure. There is another class of use cases however, not focused on mobility but requiring a high performance backbone where wiring is complex and costly — as in a factory deployment. In that case, support of autonomous delivery vehicles on the shop floor, could apply, but as a

complementary application. Some verticals may adopt 5G sooner as a response to the current COVID-19 pandemic, driven by cost optimization, resiliency and automation concerns.

Volkswagen is reported to plan 5G private deployments in 122 German factories in 2020.

An early implementations example is: BMW Brilliance Automotive (BBA, BMW's JV in China) claims complete 5G coverage in all of its factories.

User Advice: Enterprises looking to deploy 5G PMN should:

- Seek out quotations not only from CSPs but also other possible providers such as large equipment vendors and smaller specialist
- Consider SIs and consultancies for design, deployment and managed services.
- Consider licensed and also unlicensed/shared spectrum options where available (for example 5G was approved for use in CBRS in February 2020 such as CBRS; German regulator Bundesnetzagentur [BNetzA] has allocated spectrum in the 3.7 GHz to 3.8GHz band for industrial local 5G).
- CSPs offering Private 5G to industrial buyers need to work with IT service providers that have the required industry skills (and knowledge of other technologies) to provide a value proposition of how 5G supports a specific use case or business KPI to justify the additional investments required to make existing infrastructure 5G ready. For example, in manufacturing 5G is seen as a platform that combines connectivity with security and AI capabilities.

Business Impact: While 5G standard are defined by 3GPP, other bodies are contributing in order to improve applicability to connected industrial applications, for example 5G-ACIA (Alliance for Connected Industries and Automation). 5G PMN can offer enterprises improved security and independence and enable efficiency gains in several manufacturing and industrial processes.

An early implementations example is: BMW Brilliance Automotive (BBA, BMW's JV in China) claims complete 5G coverage in all of its factories.

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Athonet; Ericsson; Huawei; Nokia

Recommended Reading:

"4 Hype Cycle Innovations That Should Be on the Private Mobile Networks Roadmap for 5G Security, CSP Edge and Slicing"

"Market Impact: How CSPs Can Rebuild Resilience and Business Continuity During Disruption"

"Cool Vendors in Communications Service Provider Network Operations"

UL 2900

Analysis By: Santhosh Rao

Definition: The UL 2900 is a set of standards published by UL, a safety and security certification company. The standards cover software cybersecurity requirements for network-connectable products (UL 2900-1), medical and healthcare systems (UL 2900-2-1), industrial control systems (UL 2900-2-2), and security and life safety signaling systems (UL 2900-2-3).

Position and Adoption Speed Justification: UL currently operates in more than 143 countries across 20 industries and has a credible history of helping companies deliver secure, high-quality products. It has also established global standards for emerging technologies. Adoption of the UL 2900 is nascent but rapidly growing, as UL continues to create awareness by educating and advising both the vendor community and consumers of IoT technology. Large enterprises embarking on complex IoT projects often partner with UL for UL 2900 certification of vendor IoT products. However, for the UL 2900 and other such standards to be adopted globally and consistently, UL must work more closely with vendors, regulatory authorities and industry consortia. Given the increasing need for standards, the UL 2900 and other such standards are expected to have a high impact on product design.

User Advice: Enterprises evaluating IoT technologies must ensure vendor products adhere to security standards laid out by standards organizations such as UL. This will reduce the degree of exposure to unforeseen security risks. IoT hardware and software vendors that deliver embedded devices, IoT gateways, networking technologies and IoT platforms must follow the guidelines laid out by certification bodies such as UL. This will ensure the consistent and quality delivery of products, with minimal interoperability issues between multiple vendors and technologies.

Business Impact: The UL 2900 standard becomes particularly relevant as a result of the widespread use of the Internet of Things and associated technologies. With a large number interconnected products and associated complex hardware and software stacks proliferating the market, it is imperative that vendors adhere to the appropriate cybersecurity standards. The UL 2900-1 ensures better interoperability between IoT products and enforces that the right testing/ development methodologies and the right security controls are incorporated in the product design phase. This reduces the overall security risks associated with the product.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: UL

Recommended Reading: “Market Guide for Industrial IoT Gateways”

“Market Guide for Edge Computing Solutions for Industrial IoT”

Wi-Fi 7 (802.11be)

Analysis By: Tim Zimmerman; Mike Toussaint; Bill Menezes

Definition: IEEE 802.11be is the next amendment proposal to IEEE 802.11 for advances in WLAN. The amendment builds upon the existing IEEE 802.11ax standard and potentially will be called Wi-Fi 7.

Position and Adoption Speed Justification: IEEE, the standards body of 802.11-based technologies, started the Extremely High Throughput (EHT) Working Group in September 2018. The new amendment will use the unlicensed spectrum newly allocated at 6 GHz to create more efficient use of noncontiguous spectrum and allow 320 MHz bandwidth and 16 spatial streams. This will boost theoretical performance with higher speeds upward of 30 Gbps, increase WLAN capacities, and lower latency while maintaining backward compatibility with existing 802.11 standards. Since the amendment is using existing technical functionality but allowing for more spatial streams to coexist and wider bandwidth for higher performance, we expect to move through the Hype Cycle much faster than other amendments.

User Advice:

- Clients must review their use cases as 802.11ac Wave 2 or 802.11ax capabilities can support the vast majority of enterprise use cases.
- Advanced use cases for immersive technologies such as virtual reality and 8K video streams are expected to proliferate over the next three to five years.
- The amendment is only in the IEEE Working Group.
- End users are advised to follow the progress of the standard, but products will not be available for another 12 to 18 months.

Business Impact: Wi-Fi 7 (802.11be) will focus on the deployment of video traffic and the throughput requirements for 4K and 8K video streams, though many applications may be addressed using Wi-Fi 6. New high-throughput, low-latency immersive applications such as virtual or augmented reality will continue to be developed for the enterprise market.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

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

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

“Critical Capabilities for Wired and Wireless LAN Access Infrastructure”

At the Peak

Project Connected Home over IP

Analysis By: Bill Ray

Definition: Project Connected Home over IP is a collection of standards being promoted as the perfect combination to enable home automation. The project is backed by Amazon, Apple, Google, Comcast, and the Zigbee Alliance, with members including IKEA, Signify and Samsung SmartThings.

Position and Adoption Speed Justification: The project was launched in December 2019 and is intended to combine the best features of existing smart home standards into a single (royalty free) standard. This standard will operate over Internet Protocol (IP) connections, initially on Wi-Fi and Thread (itself carried over 802.15.4). Bluetooth will be supported, using IP over Bluetooth low energy (BLE).

As it will work over any IP bearer the standard will quickly be extended to operate over Ethernet, cellular or other broadband technologies. The choice of bearer will be up to the product vendor, but as IP is a common layer, basic interoperability should be assured.

While still a young standard, the backing of such big names warrants an advanced position on the Hype Cycle as it uses existing semiconductors and there's an expectation of fast development. The Peak of Inflated Expectations can be expected with the first product offerings, so this year the profile has been placed just before the peak with an expected time to plateau of two to five years.

User Advice: Adoption should only be considered after careful consideration — it is far from certain that Project Connected Home over IP will become the dominant standard for home automation. While it is being backed by some very big brands it's worth noting that all of them have backed previous standards, and many of them are also members of competing consortia.

In the absence of a published standard, companies that chose to invest in Project Connected Home over IP should consider building compliance through adoption of the existing standards that will be coopted to form the new one. Principally this means Dotdot and Thread, with Dotdot providing the application layer and Thread providing the mesh networking capability. Hardware with support for 802.15.4 (perhaps using Zigbee) should be able to transition to the new standard through a software upgrade.

Such companies should also note that Bluetooth will provide a competitive platform, given that IP over BLE is unlikely to be a desirable carrier for the new standard.

Business Impact: Project Connected Home over IP is really about the desire to use IP communications for home automation. IP has many advantages — being easy to program and robust in deployment. But it lacks some key features that make it less friendly to end users. Bluetooth, the chief competitor in this market, has a robust service delivery protocol (SDP), which permits a device (or a user) to quickly and easily browse through local wireless devices to pick

connections. IP has no equivalent capability, and previous attempts to build one on top of the IP layer have floundered.

Extending IP to every part of the connected home will speed application development, but it risks making the technology more difficult for end users to adopt when compared to the simple discovery process created by the Bluetooth.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Amazon; Apple; Google

Recommended Reading: "Market Insight: The Move From the Connected Home to the Intelligent Home"

"Market Trends: Connected Home Adoption in the U.S. and the U.K."

Ultrasound

Analysis By: Bill Ray

Definition: High-frequency sound, beyond the range of human hearing, can be used for IoT beaconing and communications. Smartphones can often use ultrasound without modification, using their existing microphone and speakers.

Position and Adoption Speed Justification: Ultrasound can be used for point-to-point communications, between smartphones or from beacons. It has also been embedded in piped music to provide broadcast data (across a shop or shopping center) and/or location information (where separate ultrasound streams can be sent to each speaker).

The ability to interact with an unmodified smartphone remains important, and ultrasound (using a smartphone app) has become a significant payment mechanism in South Korea (notably in taxis, but also in general retailers with Lotte L.pay). However, a complete lack of industry standard continues to prevent wider adoption. Google's Nearby API can use ultrasound, though most implementations rely on Bluetooth beacons, which are a competitive technology.

In February 2020, Sonos acquired market leader Chirp, reflecting renewed interest in the seen among smartphone and technology vendors. The technology has, therefore, been moved toward the Peak of Inflated Expectations and is expected to plateau within five years.

User Advice: The ability to operate without a standard, within a specific application, may keep ultrasound communications alive, but the lack of standard means that anyone considering ultrasound should hire a development company with off-the-shelf code available. Vertical applications in radio-free, or high-security, environments may find ultrasound useful, but in most cases, Bluetooth beacons will be a better alternative.

The ability to embed ultrasound into broadcast media remains a point of differentiation. It is also possible that ultrasound will resurface embedded in broadcast media, to synchronize smartphone (or smart speaker) applications. This would depend on privacy concerns being allayed, which currently seems unlikely.

Business Impact: For short-range payments or interaction with vending machines ultrasound can be practical but will always compete with the more-standardized NFC protocol. Similarly, Bluetooth beacons will be the most-significant competitor to ultrasound and may have gained enough market share to prevent ultrasound building a sustainable market share.

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Early mainstream

Sample Vendors: CUE; Dansolplus; DOV-E; Sonos

Recommended Reading: "Market Guide for Indoor Location Application Platforms"

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

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

eSIM

Analysis By: Pablo Arriandiaga

Definition: The embedded SIM (also called eSIM or eUICC) is a programmable subscriber identity module (SIM) that is physically embedded into a mobile device. It is designed to remotely manage multiple CSPs profiles and be compliant with GSMA specifications. An eSIM is provisioned over-the-air (OTA) with operator credentials, giving users the ability to change providers. eSIMs should not be confused with “soft” SIMs (iSIMs or virtual SIMs) that store operator secret credentials in software. These are not included here.

Position and Adoption Speed Justification: GSM Association (GSMA) standards’ work, first in IoT and later with consumer sectors, has increased potential innovation for OEMs and other players. More than 200 MNOs worldwide support eSIM and adoption is accelerating, mainly in consumer devices, driven by cases such as wearables, trackers or tablets where size and/or placement,

mobility, update frequency, and life cycle are important. In consumer devices, the increasing support of main OEMs for eSIMs in their new 4G and 5G smartphones will also act as a trigger for accelerating adoption.

In IoT, the main driver is the connected car, but other areas such as utilities and logistics are also driving adoption as well. In IoT most use cases are using eSIM as insurance to avoid future lock-in. However, MNOs are reporting low use compared to their IoT installed base. Additional challenges are that GSMA needs to evolve the standards to solve battery problems for NB-IoT that are required for use cases such as utilities as an alternative to 2G networks.

User Advice: Enterprises using IoT solutions need to evaluate the eSIM service offer by CSPs or IoT MVNOs acting as prime contractors by assessing MNOs supporting each by country including version of the standard supported, and interoperability with other eSIM subscription management platforms. In 3GPP LPWA IoT solution users need to understand the impact of updating profiles OTA on the battery life and the feasibility of doing it using the data throughputs that those technologies support. Other solutions such as iSIM or nuSIm (not covered in this profile) could be an alternative if providers show commitment to support future standardize versions.

OEMs should continue to promote eSIM in designs where its advantages are attractive, for example use cases swapping cellular providers regularly across countries and with big amounts of data. OEMs should also work with the GSMA and CSPs to present end users with a superior solution and a balanced playing field for new and innovative offers.

CSPs must craft an evolution plan to efficiently support the shift to eSIM and take advantage of emerging opportunities leading to competitive differentiation. Leverage the flexibility of eSIM to attract new customers with superior service offerings that also motivate existing users to stay (for example, by eliminating per-device fees and instead bundling in content, wearables and more).

CSPs must ensure that their eSIM technology is compatible with a variety of different handset manufactures and eSIM vendors, to ensure they can support multiple download and activation methods. In addition, evolve their billing support systems with advanced eSIM management capabilities.

Business Impact: Businesses with a large number of mobile devices used by their employees will also benefit from the convenience of eSIM for minimizing roaming tariffs when roaming. eSIM can deliver a streamlined user experience for managing cellular connectivity, enabling IT teams to provision and deploy new devices in a rapid and convenient fashion.

For OEMs, eSIM uses less space and is cheaper than traditional SIM technology. This means that mobile connectivity can now be introduced into hardware where it was previously not feasible due to cost or space restrictions.

CSPs can gain new business opportunities from a world of intelligently connected services and devices, reduce the logistical costs associated with handling traditional SIM cards and retain existing SIM security. In addition, eSIM is the vital enabler for the future growth of the IoT market allowing CSPs and IoT MVNOs to provide local connectivity worldwide in a cost-effective way and move from a pure connectivity play to a platform play.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Apple; Arm; EMnify; Ericsson; Gemalto; Giesecke+Devrient; IDEMIA; Samsung Electronics; Sierra Wireless; Truphone

Recommended Reading: "Magic Quadrant for Managed IoT Connectivity Services, Worldwide"

"Critical Capabilities for Managed IoT Connectivity Services, Worldwide"

"3 Automotive Hype Cycle Innovations That Should Be on Your Connected Vehicle Roadmap"

"Market Guide for Internet of Things Mobile Virtual Network Enablers"

NB-IoT

Analysis By: Kosei Takiishi

Definition: Narrowband-Internet of Things (NB-IoT) is a low-power wide-area (LPWA) wireless connectivity protocol designed to coexist with LTE and 5G networks. It is a 3GPP standard, first standardized on its Release 13 in 2016; its key features include bidirectional communications and throughput of several tens of Kbps using licensed spectrum. Officially known as "LTE Cat NB1," it enables more-economical module cost and a greater maximum power efficiency than LTE-M Cat M1. This analysis of the technology also covers further Cat NB specifications.

Position and Adoption Speed Justification: NB-IoT, along with Long Term Evolution for machine-type communications (LTE-M; also known as "LTE Cat M1"), is the 3rd Generation Partnership Project's (3GPP's) effort to address the emerging LPWA market for supporting use cases for IoT in a WAN setting.

As with other LPWA technologies, its key focus areas include low data rate, low power consumption and low module cost. This is because the target use case is for connected devices that typically have a long life, low data rate and volume, together with a sporadic transmission frequency.

One of the advantages of NB-IoT is that it can use the existing LTE spectrum that mobile network operators (MNOs) have been allocated. In addition, NB-IoT can mainly be rolled out via a simple software upgrade on existing LTE infrastructure. LTE Cat NB2 is also standardized by 3GPP Release 14 in 2017. Major upgrades from Cat NB1 include peak data rate improvement up to 120 Kbps, supporting positioning and single-cell multicast and energy/latency optimization. Cat NB2 enhancement is covered by 3GPP Release 15 in 2018 by adding new wake-up signal to decrease power consumption and TDD support. Globally, 93 CSPs have already commercialized NB-IoT based on GSMA as of January 2020. Among them, China is moving much faster in terms of NB-IoT adoption than the rest of the world. Given the size of the Chinese market, this affects the global overall speed of adoption as well.

User Advice: Product leaders in mobile CSPs should:

- Focus LPWA efforts on NB-IoT and LTE-M. Though it is worth noting that NTT DOCOMO in Japan shut down its NB-IoT service in 2020, so there is a need to observe major CSPs' decisions carefully.
- Test NB-IoT for more-demanding industrial use cases, as NB-IoT supports authentication (which is supported by the SIM card on mobile devices in 3GPP) and also boasts high reliability, which a licensed spectrum operation supports better than unlicensed alternatives.
- For IoT deployments involving the Chinese market, give NB-IoT a high priority in the near term.
- For deployments outside of China, use NB-IoT on the basis that investing in the standard will be a long-term play but a low-risk strategy — while planning for continuous evolution (such as 5G massive machine-type communications [mMTC] and Cat NB2).

Business Impact: No IoT connectivity protocol is necessarily better than another, but each caters to a different set of business requirements. Among LPWA alternatives, NB-IoT will address the needs of use cases with higher requirements for reliable connectivity, higher SLAs and robust 3GPP security. The main difference between NB-IoT and other fully or partially proprietary LPWA technologies (such as long-range [LoRa] and Sigfox) is that NB-IoT is a 3GPP standard. It will be deployed in a majority of mobile CSPs, which will benefit from the stronger and richer 3GPP ecosystem; though it is worth noting that interoperability is not guaranteed as different network operators are deploying NB-IoT in different frequency blocks. Finally, as an extension of LTE, NB-IoT will be deployed within mature networks, with established operational and customer experience management key performance indicators (KPIs) and practices, along with mature systems such as self-organizing networks (SONs) and IT support systems.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Arm; China Mobile; Ericsson; Huawei; Nokia; Qualcomm; Quectel; u-blox; Vodafone; ZTE

Recommended Reading: "Market Trends: CSPs Must Focus on NB-IoT and LTE-M for Their LPWA Strategies"

"Exploit LPWA Networks Now — 5G Won't Change Them"

Thread

Analysis By: Bill Ray

Definition: Thread is a royalty-free networking protocol designed to run on top of 802.15.4 to provide connectivity with IPv6 support for the Internet of Things (IoT). The standard is managed by the Thread Group and has recently been adopted by Project Connected Home over IP.

Position and Adoption Speed Justification: Thread provides IPv6 networking (by using 6LoWPAN), allowing individual endpoints to be addressed directly from anywhere on the internet (subject to firewalls and security protocols). This direct addressing opens Thread-connected endpoints to internet developers and cloud-based controls without the need for a local management hub.

Thread uses 6LoWPAN, which, in turn, uses the IEEE 802.15.4 wireless protocol with mesh communication, to extend range and provide robust communications. The standard is provided royalty-free and an open-source version (under the BSD license), branded OpenThread, is available from Google Nest. This makes Thread silicon very inexpensive, and the lack of an application layer reduces the processing required, to further reduce costs.

The standard has seen some adoption in industrial deployments, attracted by the simplicity of IP development, but projects are few and far between. Thread is an integral part of Project Connected Home over IP, which has the backing of companies including Google, IKEA, Amazon, Apple and Samsung Electronics, so the future of the protocol is largely dependent on the success of that standard. Therefore, we have moved this technology along the Hype Cycle.

User Advice: Be aware that the future of Thread is in the hands of the 182 companies making up the Thread Group. Many of these companies were already making 802.15.4 semiconductors, while others are also supportive of Bluetooth low energy — the primary competitor. Samsung Electronics, Google and OSRAM are all members of the Bluetooth Special Interest Group (SIG), along with most of the silicon providers involved.

Bluetooth low energy (BLE) offers comparable functionality with the additional capability of being able to interface with mobile phone handsets and other existing products. Bluetooth may be marginally more expensive, and the Bluetooth mesh protocol is less efficient where messages are being addressed to specific endpoints. If there is any doubt, then combination chips (supporting both 802.15.4 and Bluetooth) are available, allowing the network selection to be made in software.

Business Impact: Thread could still become a significant provider of consumer connectivity depending on the success of Project Connected Home over IP. If the project members actively back that standard, then Thread will be carried along and may spread into enterprise and industrial applications from that base.

However, without significant investment from Google, Apple, IKEA and Amazon, Thread will be relegated to a small number of vertical markets, where its addressed mesh and lower cost would make it preferable to Bluetooth.

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Adolescent

Sample Vendors: Arm; Google Nest; Samsung Electronics; Yale

Recommended Reading: "Market Insight: Bluetooth and Wi-Fi Will Dominate the Connected Home by 2021"

"IoT Technology Disruptions: A Gartner Trend Insight Report"

Sigfox

Analysis By: Aapo Markkanen

Definition: Sigfox is a proprietary low-power wide-area (LPWA) technology owned and commercialized by a company of the same name. It has been designed for the use of ultra-low-throughput IoT applications, enabling a payload of 12 bytes. The Sigfox radio link uses unlicensed industrial, scientific and medical (ISM) radio bands. The exact frequencies can vary according to national regulations, but in Europe, the 868MHz band is widely used, the U.S. 902MHz, Japan 923MHz and Australia 920MHz.

Position and Adoption Speed Justification: As a network technology, Sigfox targets IoT applications that use low-cost, battery-powered devices in areas such as tracking, monitoring, security and connectivity fallback. Sigfox is the simplest available LPWA standard to implement, and the underlying business model involves giving away the license to semiconductor and other hardware makers. The business model used by Sigfox (the company) is based on subscription charges the end users pay for connectivity, as well as commercial licensing agreements that the company as the IP holder has with its country-level and regional network operator partners. Sigfox provides local partners with exclusive country-level rights to encourage network rollouts, and the company itself also serves as the network operator in a number of strategic markets, such as France and the U.S. Besides the available public networks, the technology is available also to be deployed as separate private enterprise networks. As of May 2020, there were operational Sigfox networks in 73 countries. In February 2020, Sigfox confirmed that across the networks it had 15.5 million active registered devices; the average price of chipsets across the installed base was approximately US$2. The installed base remains modest for this kind of technology and Gartner is yet to see evidence of the growth trajectory trending considerably upward in the near future. Consequently, in the Hype Cycle, Sigfox is nearing the Trough of Disillusionment territory.

User Advice: Organizations needing to deliver low-bandwidth IoT solutions to widely distributed objects in a cost-efficient manner today should explore Sigfox IoT network options available in their regions. Sigfox has several partners in its ecosystem that can be utilized in its clients' use cases. As its key benefits, Sigfox enables lower device and connectivity costs than competing technologies. It is also capable of providing a basic geolocation functionality, without an extra cost. On the downside, Sigfox is still a relatively unproven venture, and from the end user's point of view, it represents a certain degree of supplier risk related to its financial performance and venture financing, as well as in the long-term the viability of its network-operator partners. The vendor lock-in associated with the Sigfox model makes the supplier risk particularly pressing. In addition, the use of Sigfox's technology is strictly constrained by spectrum regulations. Most importantly, enabling downlink communications remains a challenge, and we therefore advise that end users

consider Sigfox mostly for application concepts that do not rely on a reliable downlink. For instance, over-the-air firmware updates are highly challenging to deploy over a Sigfox network due to the technical limitations. Possible regulatory changes related to spectrum would impose further technical risks.

Business Impact: IoT networks as a whole will be relevant to a wide range of industries and applications communicating with IoT assets distributed over a large area. Sigfox's value proposition makes it relevant to a number of low-cost and technically simple applications, and its arrival has in part pushed mobile communications service providers (CSPs) to accelerate the deployment of their own LPWA alternatives, especially NB-IoT. End-user organizations should review their technology choices regularly as new connectivity options become available in their markets, and for the time being consider Sigfox one of the options for lost-cost, low-bandwidth deployments. The most important technologies competing with Sigfox are NB-IoT and LoRa.

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: adeunis; Kyocera; ON Semiconductor; Sigfox; STMicroelectronics; Thinxtra; WND Group

Recommended Reading: "Unlock the Innovation Potential of Future Location-Sensing Technologies"

"SWOT: Sigfox, LPWA, Worldwide"

Dotdot

Analysis By: Bill Ray

Definition: Dotdot is a network-independent protocol for negotiating communication between IoT endpoints and gateways. It emerged from the Zigbee Alliance to provide an interoperable language for service discovery and delivery across the IoT, and is now part of Project Connected Home over IP.

Position and Adoption Speed Justification: Dotdot was launched in January 2017 and has gained from being based on the preexisting ZigBee Cluster Library. Dotdot is designed to operate over IP networks, and can be carried over Wi-Fi or wired networks, as well as Google's Thread and Zigbee itself (the latter not using the IP communication layer).

Dotdot is competing with a wide range of alternatives but gains from the experience of the Zigbee Alliance as well as support of its membership (though it should be noted that many Alliance members are also members of the competing Bluetooth SIG). Despite limited adoption, Dotdot will gain from being part of Project Connected Home over IP — an alliance which will incorporate Dotdot and counts several industry giants as members. Before said inclusion, Dotdot had already gained some interest from developers who appreciate being able to use standard IP development

environments, yet promotion via such an important project will be significant. Hence, Dotdot has moved along the Hype Cycle curve and will likely accelerate to plateau within the next two years.

User Advice: Dotdot competes with other protocols, such as IoTivity, which enjoys broad industry backing and an open-source pedigree. Where interoperability across networks or integration with third-party cloud services is desired, IoTivity will represent a better option. However, users creating a stand-alone project may gain from the advantages of IP development and managed interoperability offered by Dotdot.

While Dotdot can, and does, work over Zigbee, it's designed to be agnostic to the networking layer and excels on networks which lack a default application layer (such as Thread). Some networking protocols, such as Bluetooth, offer a comprehensive application layer that renders Dotdot redundant, but anyone deploying a network which lacks such functionality should consider Dotdot.

Business Impact: Standards will be essential to the growth of the IoT, but at the moment there are too many of them and the industry will need to settle on fewer standards if interoperability is to be achieved. While the Bluetooth SIG controls the application stack from the hardware upward, Dotdot is dependent on networking and hardware layers underneath it. A single standard for IoT service discovery and delivery would be enormously beneficial to the IoT industry, but it seems unlikely that (in the long term) that standard will be Dotdot.

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Project Connected Home over IP; Zigbee Alliance

Recommended Reading: "Market Insight: The Move From the Connected Home to the Intelligent Home"

"Market Trends: Connected Home Adoption in the U.S. and the U.K."

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"

Wi-SUN

Analysis By: Sylvain Fabre

Definition: Wireless Smart Ubiquitous Networks (Wi-SUN) is based on IEEE 802.15.4g, a meshed Field Area Network (FAN) standard developed to address the needs of low-power, long-range, peer-to-peer FANs, mostly used in the utility industry. The FAN specification uses IEEE 802.1X enterprise-level security, IETF IPv6 protocols (UDP/TCP and IPv6 over low-power wireless personal-area networks [6LoWPANs]), and Routing Protocol for Low-Power and Lossy Networks (RPL).

Position and Adoption Speed Justification: The standard was approved in March 2012. The Wi-SUN Alliance was set up in April 2012 to promote the technology. As of June 2020, it includes more than 230 members (227 a year ago) in 26 countries (25 a year ago) with over 95 million devices rolled out (91 million a year ago).

There is limited scale potential in Internet of Things (IoT) implementations for the utility industry, as adoption slowed. The rise of competing cellular and LPWA IoT solutions will limit longer term Wi-Sun applicability.

Wi-SUN has many deployments and is a promising approach for utilities — its open standard FAN specification, which enables ecosystem growth, was released in May 2016, with a FAN Certification program started in Oct 2018. Vendor operability is essential in any ecosystem, and the certification program is a useful addition.

Examples of deployments include:

- Power utility Tokyo Electric Power Company (TEPCO) in Japan uses Wi-SUN commercial operations for B-route connections between smart meters and home energy management (HEM) system controllers.
- City of Copenhagen (DK) has a Wi-Sun network with smart street lights, also interconnecting sensors which optimize traffic signals in real time.
- ESB Telecoms, Ireland has a nationwide Wi-SUN mesh IoT network.

Wi-SUN may struggle to gain scale as there are several LPWA alternatives; LoRA is the main competition to Wi-SUN, and is trying to move industrial users away from existing mesh solutions (such as Zigbee and Wirepas).

User Advice:

1. Target Wi-SUN primarily at use cases for utility applications; Street lighting and other smart cities IoT application stand to gain from the technology.

2. Consider alternatives that have a more proven potential for scale, such as Narrowband Internet of Things (NB-IoT) and Long Term Evolution for machine-type communications (LTE-M). Wi-SUN is entering an already very crowded space, with additional existing and future competitors fighting for recognition (including also minor variants, such as long-range [LoRa] and low-power and so forth). While some deployments will seek to avoid proprietary flavors, some connectivity alternatives will be just as standardized as Wi-SUN.

3. Test feasibility of wider-scale Wi-SUN deployments. For example, applying a mesh architecture over a wide area (such as a city) could compromise long battery life on nodes that are part of the mesh transmitting signals on behalf of other nodes — a challenge for all mesh systems. Leaf nodes' battery life is not affected, however.

4. Consider regulation and the availability of frequencies. Although Wi-SUN was developed and initially deployed in Japan — using the ISM 920MHz unlicensed band, which is available in Japan but not in Europe or the U.S. — frequencies now supported include:

- 902MHz to 928MHz for the U.S. and multiple other regions
- 920MHz in Japan
- 863.6MHz in Europe
- 865MHz to 867MHz in India

This can assist in its international deployment potential and address the higher hardware costs. Wi-SUN uses sub-2.4GHz spectrum, 900MHz ISM bands, with data rates between 50 Kbps to 1 Mbps. The typical range between nodes is about 1 km.

5. Consider Wi-SUN as a standards-based approach for use cases that require strong security and faster data rates (e.g., for firmware update in utilities), which are key differentiators with other proprietary low-power wide-area network (LPWA) technologies, such as LoRa or Sigfox.

6. Compare cost of ownership with other alternative technologies. Wi-SUN's lower chipset cost was an initial advantage relative to some LPWAs, such as NB-IoT, but this is not the case any longer — so factor in operating costs if managed services are required.

Business Impact: There are varieties of connectivity alternatives to choose from when it comes to IoT. Wi-SUN has the advantage of being part of the technology group based on an open standard, thereby avoiding some pitfalls inherent in proprietary approaches, with higher throughput and increased security compared with other non-3GPP alternative LPWAs.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Agilent; Analog Devices; Itron; Landis+Gyr; Nissin Systems; OMRON; Panasonic; Renesas Electronics; Rohde & Schwarz; ROHM

LoRa

Analysis By: Bill Ray

Definition: LoRa is a low-power wide-area network (LPWA) specification, which defines a communication protocol and network system architecture that enables the cost-effective, long-range connection of objects (multiple kilometers), with a long battery life. It can be deployed as a public or private network. LoRa is most often deployed using the LoRaWAN networking layer, but it can also utilize other networking layers.

Position and Adoption Speed Justification: LoRa was designed to work in unlicensed radio spectrum. Initially in the 900MHz band, but the standard has recently been extended to support the 2.4GHz band which offers global availability. LoRa is owned by Semtech, which licenses out the standard. Semiconductors are available from Microchip and STMicroelectronics as well as Semtech. LoRa offers an alternative to 3rd Generation Partnership Project (3GPP)-based LPWA technologies, such as NB-IoT and LTE-M, which are designed to be deployed by CSPs in the licensed spectrum.

For use cases that do not require the predictability afforded by licensed spectrum operations, LoRa represents an alternative with good availability today. Access points can be obtained for very low cost ($200 or less) and provide campus coverage (stretching 5 km or more, depending on the environment).

The standard has been deployed by more than 120 mobile network operators, including several CSPs in Europe. In China, Alibaba and Tencent are deploying public LoRa networks, but the major

growth, globally, is in private networks. Recent innovations include the aforementioned extension into the 2.4GHz band, and support for broadcast OTA updates. Reflecting these changes we have moved LoRa along the Hype Cycle, and reduced the Time to Plateau to less than two years.

User Advice: Service providers need to:

- Include LoRa in your evaluations of proprietary LPWAs, but prioritize 3GPP variants if available, such as NB-IoT.
- Consider LoRa where available as spectrum bands may limit NB-IoT interoperability over contiguous markets (such as European countries or U.S. states).
- Use LoRa for deployments targeted at vertical industries or specific applications.

End users need to consider that:

- Enterprises can also deploy LoRa as a private enterprise network, either entirely in-house or with a system integrator. In fact, private enterprise networks are the areas where LoRa currently appears to be enjoying the most significant traction.
- LoRa and other non-3GPP-based variants have been deployed and operated commercially for some years now to address enterprise and industrial use cases.

Business Impact: The key business impact is operating expenditure (opex) savings from object connectivity. LoRa infrastructure enables the long-range connection of objects with both limited bandwidth requirements and low-traffic communications, thus enabling very low power consumption and a battery life of a decade or more, using unlicensed spectrum. Over the longer term, LoRa will be a viable technology for specific use cases.

LPWAs are already offering connectivity outside the traditional cellular networks, both in terms of pricing and business model. LoRa can be deployed as a public or private network.

LPWA hardware (both the infrastructure and the endpoints) is less expensive than cellular systems. The increased range of LPWA technologies means fewer base stations, further reducing costs.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Actility; Kerlink; KPN; Microchip Technology; MultiTech; Orange Business Services; Semtech; Senet; STMicroelectronics

Recommended Reading: “Market Trends: CSPs Must Focus on NB-IoT and LTE-M for Their LPWA Strategies”

“Market Insight: LoRa Is a Valid Option for CSPs in Selected Low-Power, Low-Bandwidth Use Cases”

Autonomous Vehicles

Analysis By: Jonathan Davenport

Definition: Autonomous vehicles use various onboard sensing and localization technologies, such as lidar, radar, cameras, GPS and map data, in combination with AI-based decision making, to drive without human intervention. This Innovation Profile does not cover ADAS features that require humans to supervise vehicle operations. While self-driving cars are getting most of the attention at present, the technology can also be applied to nonpassenger vehicles for transportation of goods.

Position and Adoption Speed Justification: There have been a number of signs of autonomous driving moving into the Trough of Disillusionment during the past year. Drive.ai and Starsky Robotics failed, Cruise cut 8% of its workforce, and Zoox is looking for a buyer, Continental has delayed AV investments after Q120 earnings plummeted and Audi has abandoned its plans to introduce the Level 3 traffic jam pilot feature into its A8 vehicles, which it had originally announced back in 2017. Likewise, Ford Motor Company made the decision to shift the launch of its self-driving services to 2022 to evaluate the long-term impact of COVID-19 on customer behaviors.

But there has been increased investment too. For example, Intel's Mobileye has acquired Moovit and is developing an autonomous mobility as a service (MaaS) solution for the emerging robotaxi market. This plan shifts Intel from being a supplier of chips and self-driving systems for the automotive industry and places it in direct competition with automakers' own mobility ambitions and the likes of Waymo, Baidu and Yandex. Likewise, autonomous vehicle pilots and trials have continued to be undertaken, though most continue to be supported by safety drivers. To overcome regulatory issues, many autonomous shuttle buses have been demonstrated on private road networks, such as at airports.

The efforts of automobile manufacturers and technology companies to develop autonomous vehicles have been prominently featured by mainstream media, leading to unrealistic and inflated expectations for the technology. Artificial intelligence (AI) is a critical technology for enabling autonomous vehicles, and development of machine learning algorithms for autonomous vehicles has accelerated. Key challenges for the realization of autonomous vehicles continue to be centered on cost reductions for the technology and industrialization. However, the challenges increasingly include regulatory, legal and societal considerations, such as permits for operation, liability, insurance and the effects of human interaction.

Continued advancements in sensing, positioning, imaging, guidance, mapping and communications technologies, combined with AI algorithms and high-performance computing capabilities, are converging to bring the autonomous vehicle closer to reality. However, in 2020, complexity and cost challenges remain high, which is impacting reliability and affordability requirements, as well as hindering the ability for companies to get regulatory approval.

User Advice: The adoption of autonomous vehicle technology will require increasing levels of technical sophistication and reliability that rely less and less on human driving intervention. Automotive companies, service providers, governments and technology vendors (for example, software, hardware, sensor, map data and network providers) should collaborate on joint research

and investments to advance the required technologies, as well as work on legislative frameworks for self-driving cars.

Furthermore, consumer education is critical to ensure that demand meets expectations once autonomous vehicle technology is ready for broad deployment. Specific focus must be applied to the transitional phase, where autonomous or semiautonomous vehicles will coexist with an older fleet of nonautonomous vehicles.

Look for use cases, such as mining, agriculture or airports, where autonomous vehicles can operate in restricted areas safely without regulatory restrictions. Use these implementations to drive early revenue and gather data and insights to improve the performance of self-driving systems.

Autonomous vehicles will have a disruptive impact on some jobs, such as bus, taxi and truck drivers. Develop policies and programs to train and migrate employees who will be affected by automation to other roles.

Business Impact: The main implications of self-driving vehicles will be in the economic, business and societal dimensions. Automotive and technology companies will be able to market autonomous vehicles as having innovative driver assistance, safety and convenience features, as well as being an option to reduce vehicle fuel consumption and improve traffic management. The interest of nonmobility companies (such as Intel, Waymo, Apple and Baidu) highlights the opportunity to turn self-driving cars into mobile computing systems. These systems offer an ideal platform for the consumption and creation of digital content, including location-based services, vehicle-centric information and communications technologies.

Autonomous vehicles are also a part of mobility innovations and new transportation services that have the potential to disrupt established business models. For example, autonomous vehicles will eventually lead to new offerings that highlight mobility-on-demand access over vehicle ownership by having driverless vehicles pick up occupants when needed. Autonomous vehicles will deliver significant societal benefits, including reduced accidents, injuries and fatalities, as well as improved traffic management, which could impact other socioeconomic trends.

When autonomous driving enters the Trough of Disillusionment, it might be a good opportunity for new market entrants.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Audi; AutoX; Daimler Group; General Motors; Mobileye; Pony.ai; Tesla; Uber; Waymo

Recommended Reading: “Market Trends: Monetizing Connected and Autonomous Vehicle Data”

“Forecast Analysis: Autonomous Vehicle Net Additions, Internet of Things, Worldwide”

“Utilize Partnerships to Secure a Winning Position in the Autonomous Driving Ecosystem”

"Market Insight: Use Situationally Aware Platforms to Enable Safe Autonomous Vehicle Handovers"

"Maverick* Research: Autonomous Mobile Structures Will Fuel the Sharing Economy"

Hardware-Based Security

Analysis By: Neil MacDonald; Tony Harvey

Definition: Hardware-based security uses chip-level techniques for the protection of critical security controls and processes in host systems independent of OS integrity. Typical control isolation includes encryption key handling, secrets protection, secure I/O, process monitoring and unencrypted memory handling.

Position and Adoption Speed Justification: Adoption is increasing and becoming mainstream, as hardware-based isolation capabilities are becoming standard in most hardware devices and cloud-based IaaS offerings. These approaches strongly isolate parts of the system (and typically its security controls) from a breach of the application or OS. Interest in strong isolation techniques has risen in the face of ongoing disclosures of new types of side-channel attacks. Another driver is the desire to use IaaS providers in potentially hostile parts of the world and protect these workloads from virtual machine and memory snapshotting. However, disillusionment remains as methods vary wildly among vendors, and some strong isolation capabilities such as Intel Software Guard Extensions (SGX) require applications to be rewritten and are incompatible with techniques used by AMD. Abstraction layers, such as Asylo, may help but add another layer of complexity and are not widely adopted.

Multiple implementations are appearing across vendors, OSs and chipsets:

- Samsung's Knox security hypervisor, where a supervisory process monitors the OS kernel for aberrant behavior. The supervisory process runs at a higher privilege level than the OS and cannot be compromised.
- Intel SGX provides a new privilege level for running code, which can be set up in a user-level process but excluded from operating system or hypervisor access. Multiple public cloud providers now support SGX including Alibaba Group, IBM and Microsoft.
- AMD has a similar set of technologies for protecting memory against physical and system software-based attacks: Secure Memory Encryption (SME), Transparent Secure Memory Encryption (TSME) and Secure Encrypted Virtualization (SEV).
- In 2018, Intel introduced chip-level Threat Detection Technology (TDT) that was further improved in 2019 and is now supported by multiple security offerings, including Microsoft Windows Defender.
- Microsoft uses hardware-based virtualization features in Windows 10 and Windows Server 2016 to create a protected code execution space for monitoring the OS and providing security features with Device Guard and Credential Guard.

- VMware built AppDefense — a way to monitor and protect applications from the hypervisor layer, outside of the workload, protected by virtualization-enabled hardware.
- Apple has developed and shipped its iOS Secure Enclave processor to protect sensitive operations and monitor kernel integrity.
- Google has developed a custom chip, Titan, for hardware-based root of trust and is deployed throughout their data centers. This chip binds a strong identity to each server, verifies the integrity of firmware and software, and creates a nonrepudiable audit trail of all changes to each machine.
- Amazon Web Services (AWS) uses a custom-designed Nitro Controller on its Nitro-based systems that includes a special micro-controller for security isolation and integrity measurements called the Nitro Security Chip. This becomes the foundation for its confidential computing offering called Nitro Enclaves, although this isolation uses the Nitro Hypervisor.

User Advice:

- Hardware-based security is strong, but may potentially still be broken by software flaws, or side-channel attacks such as Spectre and Meltdown. Patch and remain vigilant for unexpected breaches.
- Most systems will include hardware-rooted isolation and integrity capabilities by default. Make strong isolation of sensitive code and security controls a mandatory part of IT systems procurement, including IaaS.
- For systems under direct enterprise control, implement a BIOS-level patching strategy to deal with exposures that require BIOS-level remediation.
- For systems that move to public cloud infrastructure, evaluate the need for confidential computing capabilities only for the most critical applications to protect sensitive operations such as key management and sensitive intellectual property.
- Although the SGX approach is compatible with hypervisors, there may be unanticipated interactions. For example, it may not be possible to snapshot, suspend and restore a partition with a protected process. Understand limitations of hypervisor-based functionality before implementing SGX.
- Before activating Windows 10 virtualization-based security, check for compatibility issues with third-party approaches that also use virtualization techniques.
- Hypervisor-based approaches with security rooted in hardware virtualization techniques are another way to achieve similar levels of strong isolation (for example, Hysolate and Bitdefender have offerings that use this approach).
- None of these mechanisms are interoperable, so plan different strategies for different devices and server platforms.

Business Impact: If an operating system is compromised, its security controls can be disabled and sensitive data in memory stolen; hardware-based security can prevent this. Hardware-based security can significantly reduce attack surfaces across computing devices, but require that

operating system software and system management software be able to make use of it. Upgrading to most recent versions of software that can use hardware features and using cloud systems with advanced security, can materially increase system security.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: Amazon Web Services (AWS); Apple; Bitdefender; Fortanix; Google; Hysolate; Intel; Microsoft; Samsung Electronics; VMware

Recommended Reading: "Market Guide for Cloud Workload Protection Platforms"

"How to Make Cloud More Secure Than Your Own Data Center"

"Security Leaders Need to Do Seven Things to Deal With Spectre/Meltdown"

"How to Mitigate Firmware Security Risks in Data Centers, and Public and Private Clouds"

"Key Management as a Service Exposes Different Risks to Data in Public Clouds"

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”

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

OPC UA

Analysis By: Anushree Verma

Definition: Open Platform Communications Unified Architecture (OPC UA) is platform-independent, vendor-independent, service-oriented architecture which expands on the functionality and security found in OPC Classic. OPC Classic has been the backbone for connectivity in industrial automation devices and applications.

Position and Adoption Speed Justification: OPC UA's latest update was in 2018, (OPC UA v1.04). It is typically used in the industrial automation and energy markets and supports two protocols:

- A binary protocol that employs minimal resources
- A web service protocol (SOAP) that uses HTTP/HTTPS ports

Data types and structures are defined in profiles, thereby enabling the data to be used for information modeling. In the past year, advancements have been made in transport mapping of OPC UA to Time-Sensitive Networking (TSN), enabling deterministic exchange between UA applications. This will help in synchronization of machinery on the plant floor or within device communications, establishing a holistic communication infrastructure from the sensor to the cloud. Hence, this technology has been moved closer to the plateau to reflect its increased use and maturity.

User Advice: OPC UA is essential for connectivity in manufacturing facilities and will be the de facto communications technology for Industrie 4.0. Identify the ways it can be combined with existing fieldbus standards to gradually adopt it, starting with vertical communication, followed by communication between machines and then gradually at the field level.

Business Impact: OPC UA is being used in industrial automation and automotive applications. The interoperability, extensible data stack and flexibility of OPC UA permit vendors to promote service as a solution via manufacturing execution systems to drive plant efficiencies. Interoperability and openness will enable manufacturers to transform and thus create effective solutions which will enhance productivity.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Bosch Rexroth; ICONICS; Microsoft Azure; Mitsubishi Electric; NI; NTT Communications; Schneider Electric; Siemens

Recommended Reading: "Market Guide for Industrial IoT Gateways"

LTE-M

Analysis By: Kosei Takiishi

Definition: Long Term Evolution for machine-type communications (LTE-M) is aimed at providing a cellular communications infrastructure that is able to support the Internet of Things (IoT). It is specified by the 3rd Generation Partnership Project (3GPP) standards, first developed and published in 3GPP Release 13 (2016). The first specification is so-called LTE Cat M1 and has added capabilities with new 3GPP releases. This analysis of the technology also covers further LTE-M specifications.

Position and Adoption Speed Justification: Standards-compliant LTE-M devices are now being produced and improvements continue in power consumption, cost and performance.

Following LTE-M, IoT wide-area connectivity standards continued to be developed with the emergence of narrowband-IoT (NB-IoT) as an alternative technology choice that has lower bandwidth capability, but a wider area coverage, lower device power consumption and potentially, lower device cost. Differentiators for LTE-M are bigger throughput, supporting limited to full mobility and voice communication by VoLTE.

Cat M2 is also standardized by 3GPP Release 14 in 2017. Major upgrades from Cat M1 include peak data rate improvement up to 2.5 Mbps, enhanced mobility and half-duplex voice, supporting positioning and single-cell multicast. Cat M2 enhancement is covered by 3GPP Release 15 in 2018 by adding new use cases, including support for higher UE velocity, a lower UE power class and TDD support. Globally, 36 CSPs have already commercialized LTE-M based on GSMA as of January 2020.

User Advice: Communications service providers (CSPs) planning to expand their IoT communications services business should consider incorporating LTE-M into their LTE networks alongside alternatives such as standards-based NB-IoT or long-range WAN (LoRaWAN).

Business Impact: Attention to LTE-M has mainly been based in North America, while CSPs in Asia/Pacific are tending to favor the alternative NB-IoT standard (also supported in 3GPP Release 13), which uses a much smaller slice of spectrum. Europe is split between LTE-M, NB-IoT and LoRaWAN. It remains to be seen how LTE-M will compete with the industrial, scientific and medical (ISM) band solutions such as LoRaWAN.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Ericsson; Huawei; Nokia; Sierra Wireless; ZTE

Recommended Reading: “Exploit LPWA Networks Now — 5G Won’t Change Them”

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 Nanomsg/NNG. 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"

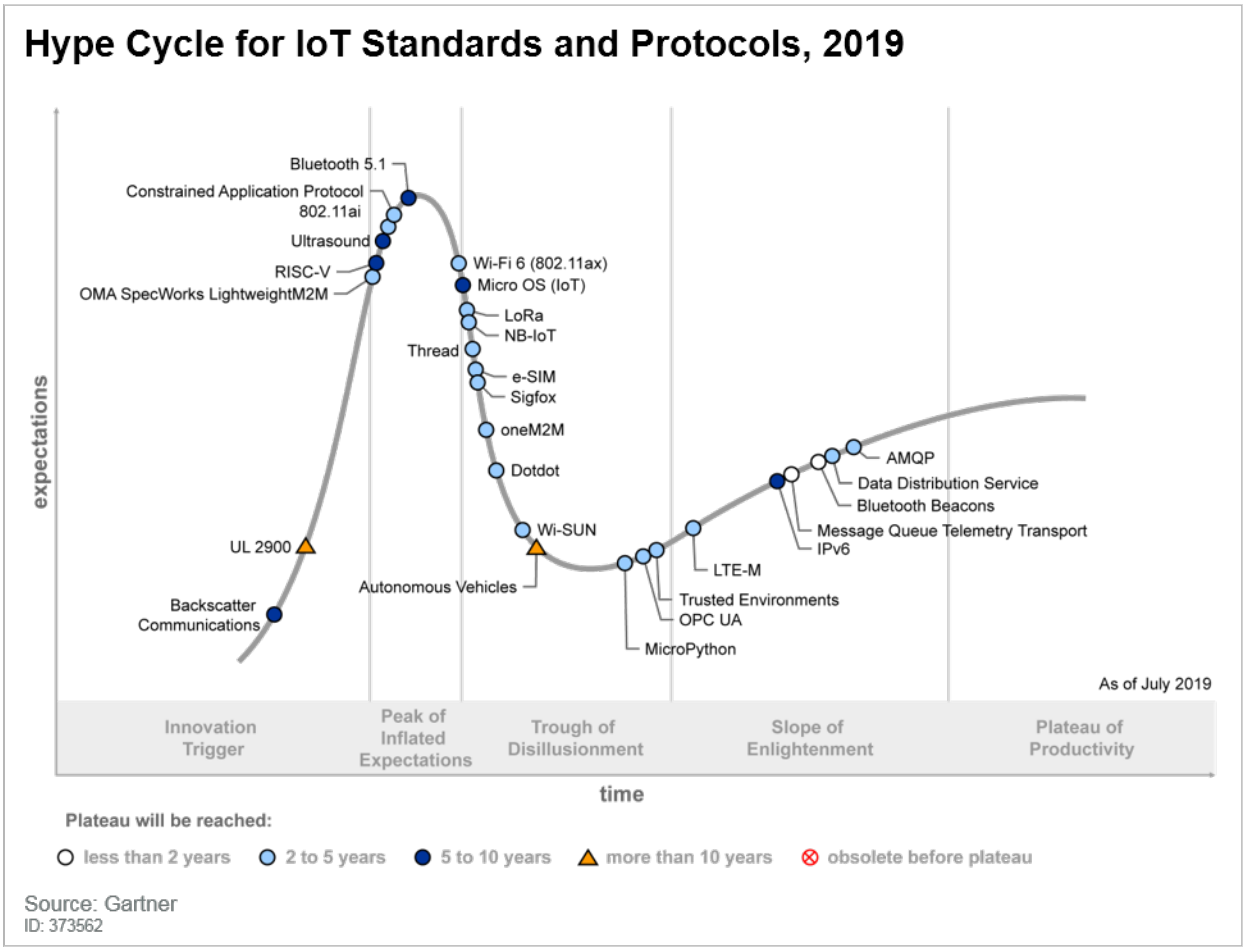
"Market Guide for Industrial IoT Gateways"

"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"

Appendixes

Figure 3. Hype Cycle for IoT Standards and Protocols, 2019



Source: Gartner
ID: 373562

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 (June 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 (June 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-the-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 (June 2020)

Gartner Recommended Reading

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

Understanding Gartner's Hype Cycles

Critical Capabilities for Managed IoT Connectivity Services, Worldwide

5 Key Technologies and Trends for Tech CEOs Planning Their IoT Roadmaps

Market Guide for Industrial IoT Gateways

2019 Internet of Things (IoT) Trends Barometer

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