SIGFOX IS EXPANDING THE IoT, 12 BYTES AT A TIME

If it feels like just about everything these days connects to the **Internet of Things (IoT)**, or will soon be IoT capable, you're not wrong. Last year, two separate reports, one from IDC and one from Juniper Research, looked at the IoT, and the message was clear: things are only going to get more connected.

As of early 2020, the total number of IoT connections worldwide had already reached 30 billion. IDC and Juniper both expect that number to exceed 80 billion within the next four to five years. To put that into context, IDC predicts that, by 2025, there will be more than 152,200 devices connecting to the IoT every 60 seconds.

A DIFFERENT KIND OF CONNECTION

Many of these new IoT connections will take advantage of the latest 5G capabilities, to support cutting-edge use cases like self-driving cars, virtual-reality headsets, high-resolution security systems, and autonomous drones.

But there will also be dramatic growth in IoT connections that don't need the kind of advanced performance available with 5G. Small, battery-powered devices – such as sensors, which collect and transmit readings for use in manufacturing, agriculture, healthcare, utility grids, and urban infrastructures, and asset tags, which track and report their whereabouts in the supply chain – deal in very small amounts of data and need only an intermittent connection to the cloud.

Moreover, sensors and asset tags are often deployed in places beyond the reach of Wi-Fi, such as pipelines and agricultural fields, and they often require mobility, for use cases like fleet management, shipping, and supply-chain automation.

To service this segment of the IoT, device-to-cloud connections tend to make use of Low-Power Wide Area Network (LPWAN), a wireless technology that offers low-bandwidth, energy-efficient connectivity, and low bit rates over long ranges.

LPWAN OPTIONS

With LPWAN, the endpoints typically connect directly to common central access points, in much the same way that Wi-Fi is configured. The specific LPWAN protocol chosen depends largely on the use case, but the most popular options are LTE-M, NB-IoT, LoRa, and Sigfox. Each comes with its own set of benefits and tradeoffs:

- **LTE-M and NB-IoT**

  LTE-M (which stands for LTE-Machine Type Communication) and NB-IoT (for Narrowband IoT) are cellular standards defined by the 3GPP. LTE-M offers latency in the range of 100 to 150 ms, making it a good choice for connected vehicles, wearables, trackers, and alarm panels. NB-IoT consumes minimal power and can connect more than 50,000 devices per cell.

  As cellular technologies, LTE-M and NB-IoT offer worldwide coverage and run on networks recognized for their security features. They also use OFDM modulation, to strengthen the signal and increase the link budget, but the complexity of ODFM modules can make the integration effort harder. Also, LTE-M and NB-IoT require a subscription from a Mobile Network Operator, which can add cost if mobile devices are subject to roaming charges or if the operating area requires more than one provider for full coverage.

- **LoRa**

  LoRa (an abbreviation for Long Range) is a proprietary, non-cellular modulation technique. It's based on Chirp pread Spectrum (CSS) modulation, which spreads signals over different frequency channels and data rates. LoRa offers a combination of long battery life and very long range, making it a good choice for things like livestock tracking, pipeline monitoring, and city-wide networks of trash containers, streetlights, and other infrastructure items.

  Technically speaking, LoRa is the physical layer (PHY) only, and is only available in Semtech radio chipsets. Most deployments run LoRa on LoRaWAN, a protocol defined by the LoRa Alliance. LoRaWAN defines the media access layer (MAC), the communication protocol, and the network architecture. The tightly held, proprietary details of LoRa radio chipsets can be a deterrent, since a proprietary solution can raise issues with sourcing and can present challenges for the development roadmap.

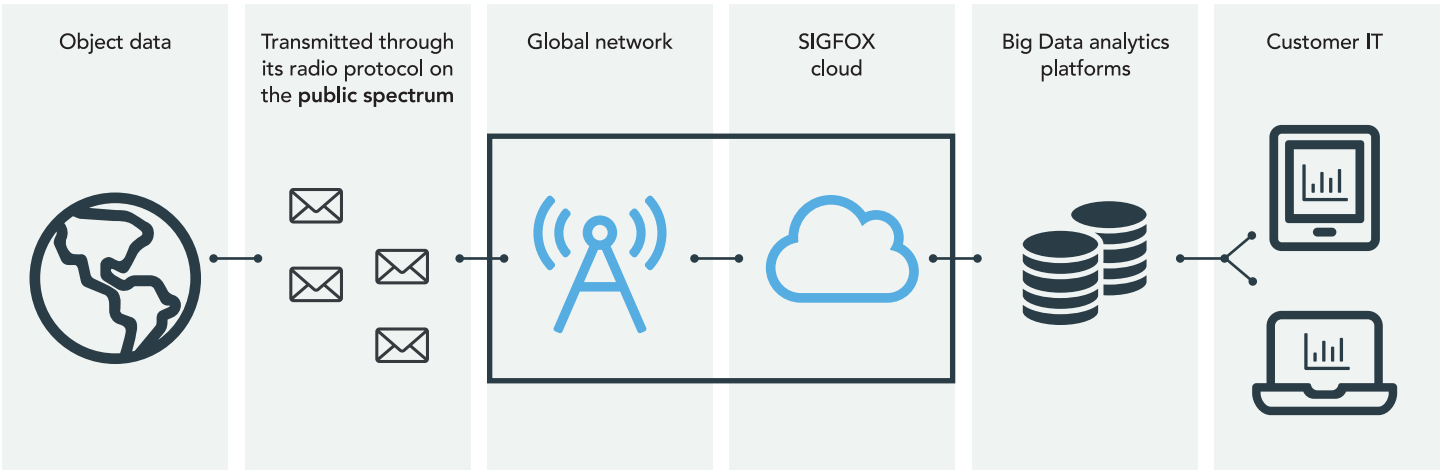
- **Sigfox**

  Sigfox, like LoRa, began life as a proprietary technology, and was created by the French company of the same name. The Sigfox specification is now in the public domain, however, which means developers and manufacturers have a larger, more diverse ecosystem to work with.

  The Sigfox protocol uses Ultra Narrowband (UNB) technology to save energy, and employs shift-keying techniques in the uplink and downlink to reduce interference. The range is about 10-30 km.

  One thing that makes Sigfox stand out is that it restricts both the size and frequency of data signals. Within a 24-hour period, there can be no more than 140 uplink messages, at 12 bytes per message, and no more than four downlink messages, at 8 bytes per message, all traveling at low data rates. Restricting transmission to once every 12 minutes or so, and limiting the size of messages, minimizes power consumption and extends battery life.

  Sigfox devices connect to 0G, which is the company's subscription-based, low-data-rate cellular network. The network offers near global coverage and connects directly to the Sigfox cloud, which collects data and provide interfaces to thrid party cloud services.



The secure Sigfox setup offers simplicity, flexibility, and reliability

SIGFOX IS TAILOR-MADE FOR SENSORS AND ASSET TAGS

The connectivity requirements for sensors and tags are minimal, and the Sigfox protocol, with its intermittent transmission of short messages, is a good fit for several reasons.

- **Simplicity**

  The silicon modules are both cost-effective and simple to use, for easier integration, and are compatible with 2G/3G/4G cellular and Wi-Fi. Working within the Sigfox network means there's no need for pairing or configuration, because all Sigfox devices use the same simple, dedicated link for cloud connectivity.

- **Efficiency**

  Devices stay in sleep mode most of the time, and only transmit in short bursts, so the battery doesn't have to work overtime to support connectivity. The long battery life also means sensors and tags can remain in the field for years at a time without a battery change.

- **Coverage**

  The Sigfox 0G network is now available in 72 countries and regions, covering populations of 1.3 billion people and an area of 5.8 million square km. The company is building out their terrestrial network, and is launching a satellite network. To support supply-chain applications, coverage includes hundreds of ports and airports worldwide. The network is fully managed and offers a high Quality of Service (QoS) rating. Also, there's a single, low-cost subscription for global network usage, so there's no roaming charges and no need to negotiate multiple contracts when operating in different regions.

- **Security**

  Sensors and asset tags need to defend against hacking, which can include attempts to take over control, steal information, or disrupt service. Within the device, Sigfox modules use a tamper-resistant secure element to prevent device cloning and to physically protect the encryption keys used to safeguard transmissions. At the base station, and between the base station and the cloud, Sigfox uses payload encryption for logical security and to prevent data theft. Also, there is the added protection that Sigfox base stations only accept uplinks from Sigfox devices.

- **Reliabilty**

  The spread-spectrum format of Sigfox signaling helps reduce interference and prevent attempts to jam transmissions. Spatial diversity means each message emitted by a device is received by multiple base stations, so any attempt to jam the base station, in order to prevent transmission, requires jamming all relevant base stations at once. The inexpensive handheld jammers typically used to jam 2G/3G/4G signals offer nowhere near the power needed for simultaneous jamming, and as a result fail to disrupt Sigfox transmissions.

SIGFOX FOR INDUSTRIAL AND SUPPLY CHAIN APPLICATIONS

Sensors and asset trackers that use Sigfox for connectivity are compelling options for a wide range of applications, with relevant use cases in industry, transport, logistics, utilities, energy, healthcare, agriculture, and more.

In the supply chain, Sigfox can be used as an extension of any local RFID networks that are used to identify, monitor, and track assets. Sigfox adds mobility, so assets with RFID tags can still be tracked while in transit, and Sigfox base stations can be mounted in partner facilities, such as distribution centers, where there may not be an RFID infrastructure. Participation in the supply chain is one of the reasons why seaports and airports have been a priority for Sigfox as they expand their network.

WHERE NXP FITS IN

NXP plays a vital role in LPWAN technologies and offers highly integrated Sigfox options. The NXP OL2385 is a System-on-Chip Sigfox solution that combines hardware and software to deliver excellent RF performance with a low BoM cost. The OL2385 is pre-loaded with Sigfox modem software and is part of a Sigfox-approved reference design.

The OL2385 is also supported by NXP's IoT Development Platform, which makes it easy to explore Sigfox functionality next to Zigbee, Bluetooth Low Energy (BLE), Wi-Fi, GPS, and more. Developers can quickly create a proof-of-concept design before committing to a specific hardware configuration, and can gain insights into Sigfox communication before investing in a full-on deployment.

To learn more about Sigfox and how NXP is expanding the options for LPWAN connectivity in the IoT, visit **www.nxp.com.**

Thomas Lorbach, Product Manager with NXP Semiconductors

Thomas has been working in the semiconductor industry for 20 years in various roles in engineering, and joined NXP Semiconductors in the UK as Product Marketing Manager for ZigBee/IEEE802.15.4 solutions in 2007. Since 2015, Thomas has been a part of NXP's Advanced Analog business based in Hamburg where he is responsible for the company's automotive and industrial sub-GHz products.