Retail Therapy

Wireless tech is rejuvenating the shopping experience for both retailer and consumer
The McKinsey Global Institute, an economics research firm, has estimated that by 2030 the IoT could enable $5.5 trillion to $12.6 trillion in value globally, including the value captured by consumers and customers of IoT products and services. However, from where we are today to the IoT of 2030 is not a straightforward path. The wireless tech underpinning the IoT is complex to build, deploy and maintain. Nordic’s strategy has always been to make things easier by providing engineers with end-to-end solutions—not just silicon, but software, development tools, services and technical expertise. Dealing with a single supplier allows developers to focus on innovative applications. Nordic’s end-to-end strategy is coming to fruition for cellular IoT. The LPWAN is becoming the dominant solution for secure and reliable long-range connectivity for the IoT. Our comprehensive cellular IoT platform includes support for DECT NR+, the world’s first non-cellular 5G technology standard. Comprising new products based on nRF91 Series SiPs, this massive IoT offering means vendors can access chipsets, modules, software and services designed, controlled and supplied by a single company. (See pg10.)

Nordic is also pursuing an ambitious product roadmap for other IoT technologies. We’ve just announced the nRF54H20, an incredibly powerful SoC sporting multiple Arm Cortex-M33 processors and multiple RISC-V coprocessors. We’ve also announced our second Wi-Fi companion IC, the nRF7001, a low-cost solution for low-power Wi-Fi products requiring 2.4 GHz single band connectivity only. If the IoT is to reach the potential forecast by McKinsey, it will need a comprehensively engineered foundation. Together with our innovative customers, Nordic is among the leaders in making sure those foundations are built to last.

Wireless Quarter is contract published on behalf of Nordic Semiconductor by Ecritech Media

Editor
Steven Keeping sk@ecritech.media
Assistant Editor
Chris Williams cw@ecritech.media
Contributing Editor
Kalon Huett kalon@ecritech.media
Production Editor
Andrew Widen-King awk@ecritech.media
Creative Director
Sam Grimmer sam@ecritech.media
Prepress
Nathan Gargent
Print & Distribution
Printech Europe

To subscribe to WQ visit www.nordicsemi.com/wqmag

The Bluetooth word mark and logos are registered trademarks owned by the Bluetooth SIG, Inc. and any use of such marks by Nordic Semiconductor is under license.

© Nordic Semiconductor 2023

To view this edition online, visit www.nordicsemi.com/wqmag
Nordic introduces fourth generation low power wireless SoCs

Nordic Semiconductor has announced the nRF54 Series, its fourth generation of wireless SoCs. The first chip in the nRF54 Series, the nRF54H20, is ideal for disruptive IoT applications demanding high processing power, excellent energy efficiency and state-of-the-art security.

The nRF54 Series follows Nordic’s award winning nRF51, nRF52 and nRF53 Series, and introduces an innovative new hardware architecture. The nRF54H20 belongs to the ‘H’ branch of the wider nRF54 Series. Capable of supporting Bluetooth 5.1 and future Bluetooth specifications, like LE Audio, Bluetooth mesh, Thread, Matter and more, the nRF54H20 will be the foundation for a new wave of revolutionary IoT end-products.

“Decades of ultra low power wireless expertise have come together to form the nRF54 Series,” says Svend-Forre Larsen, Nordic’s CEO. “Our first SoC from the fourth generation of Bluetooth LE solutions, the nRF54H20, not only represents a significant milestone for Nordic, but also allows Nordic’s customers to build end products far more advanced and efficient than they were yesterday.”

“A disruptive product like the nRF54H20 happens through a long-term commitment to R&D, and Nordic has been willing to commit that commitment,” says Sven-Egil Nielsen, Nordic’s CTO/ EVP R&D and Strategy. “The SoC’s high level of integration will enable developers to shrink their designs by replacing multiple components—for example application microprocessor, external memory and wireless SoC—with just one highly compact device. In addition to advanced wearables, smart home, medical and LE Audio applications, the nRF54H20 SoC is an ideal solution for applications demanding complex machine learning (ML) and support for sensor fusion at the edge.

“The ground-breaking nRF54H20 is a major technical achievement,” adds Kjetil Halstad, EVP Product Management at Nordic. “It is a truly worthy successor to our nRF53, nRF52, and nRF53 Series, and we expect our nRF54 Series to again disrupt the low power wireless segment.”

Smart tape measure records accurate measurement data

U.S. based REEKiton has released a digital wireless tape measure for use on building sites, providing users with accurate, recorded measurement data via the associated smartphone app.

The T1 Tomahawk Digital Tape Measure features an absolute optical encoder and magnetic angular position sensor that together provide a measurement accuracy within 0.5 mm, according to the company.

When a measurement is taken it is immediately appears on the device’s built in OLED display for alive view by the user. With the press of a button the data is saved. The data is then relayed using Bluetooth LE connectivity to the ROCK iOS and Android app.

“REEKiton believes in reducing waste on job sites through error reduction,” says Kostas Dikanopoulos, CTO at the firm. “The T1 Tomahawk achieves this by providing accurate and robust measurement.”

When a measurement is taken it is immediately appears on the device’s built in OLED display for alive view by the user. With the press of a button the data is saved. The data is then relayed using Bluetooth LE connectivity to the ROCK iOS and Android app.

“The ground-breaking nRF54H20 is a major technical achievement,” adds Kjetil Halstad, EVP Product Management at Nordic. “It is a truly worthy successor to our nRF53, nRF52, and nRF53 Series, and we expect our nRF54 Series to again disrupt the low power wireless segment.”

Pallet Tracking

A range of asset trackers designed for use in transport pallets has been launched by U.K.-based tech firm System Loco. The Locotrack HC4A and RM2Track are embedded in composite pallets during manufacture, for use by Pallet as a Service (PaaS) providers.

The devices include both an ambient temperature sensor and an accelerometer, allowing them to transmit the location of the pallet only when it starts or stops moving. This helps conserve battery life. The sensors are overseen by Nordic Semiconductor’s nRF52840 SoC, using its powerful Arm Cortex M4 processor with floating point unit (FPU).

Locotrack HC4A and RM2Track employ a combination of location technologies including GNSS, Wi-Fi, cellular and Bluetooth LE. Once the location data has been collected, it can be transmitted to the Cloud based LocoAware web platform. From there, owners can easily manage and configure large portfolios of devices and track the location of their pallet fleet.

“The logistics industry moves from tracking vehicles to pallets to individual packages, our asset trackers provide complete visibility of the location and integrity of goods from in-bound transit, through warehousing and when dispatched to the end customer,” says Daniel Essed, CTO at System Loco. “It is also common for millions of these pallets to go missing each year, with them often ending up in landfill. Our technology helps to prevent this type of waste, allowing for recovery and reuse of pallets, as well as recycling at end-of-life.”

Canadabased IQonboard has developed a Bluetooth LE beacon tag that creates what is claimed to be the world’s first self-loading digital manifest. The T1tag has been field tested for remote operations across wildlife, mining and personnel transport applications.

The IQonboard system comprises the patent pending T1 Tag beacon tag, a small (5.3 by 1.3 cm), lightweight (22 g), IP67-rated crushproof wearable using Nordic’s SoC, nRF52832 SoC, based on the SiYEST Blend Nano module—an SoC that is associated with the IQonboard app for iOS, smartphones and tablets.

Once allocated and attached to clothing or cargo, each T1tag can be quickly configured and programmed to broadcast the name and weight of respective crew, cargo and passengers to the onboard app using the Bluetooth LE connectivity. This provides real time visibility of who is boarding the transport, taking the guesswork out of weight and balance calculations for pilots and dispatchers. The automatically generated flight manifests are also made visible to ground operations.

“Canadabased IQonboard has developed a Bluetooth LE beacon tag that creates what is claimed to be the world’s first self-loading digital manifest. The T1tag has been field tested for remote operations across wildlife, mining and personnel transport applications. The IQonboard system comprises the patent pending T1 Tag beacon tag, a small (5.3 by 1.3 cm), lightweight (22 g), IP67-rated crushproof wearable using Nordic’s SoC, nRF52832 SoC, based on the SiYEST Blend Nano module—an SoC that is associated with the IQonboard app for iOS, smartphones and tablets.

Once allocated and attached to clothing or cargo, each T1tag can be quickly configured and programmed to broadcast the name and weight of respective crew, cargo and passengers to the onboard app using the Bluetooth LE connectivity. This provides real time visibility of who is boarding the transport, taking the guesswork out of weight and balance calculations for pilots and dispatchers. The automatically generated flight manifests are also made visible to ground operations. The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”

The IQonboard solution is designed to enhance aviation safety and reduce pilot workload. For example, the solution could be used when helicopters are hired for emergency response activities like wildfire fighting, where the full manifest of the aircraft for each and every leg of a flight must be communicated to the dispatch center.

“Canadabased IQonboard has developed a Bluetooth LE beacon tag that creates what is claimed to be the world’s first self-loading digital manifest. The T1tag has been field tested for remote operations across wildlife, mining and personnel transport applications. The IQonboard system comprises the patent pending T1 Tag beacon tag, a small (5.3 by 1.3 cm), lightweight (22 g), IP67-rated crushproof wearable using Nordic’s SoC, nRF52832 SoC, based on the SiYEST Blend Nano module—an SoC that is associated with the IQonboard app for iOS, smartphones and tablets.

Once allocated and attached to clothing or cargo, each T1tag can be quickly configured and programmed to broadcast the name and weight of respective crew, cargo and passengers to the onboard app using the Bluetooth LE connectivity. This provides real time visibility of who is boarding the transport, taking the guesswork out of weight and balance calculations for pilots and dispatchers. The automatically generated flight manifests are also made visible to ground operations. The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”

The IQonboard solution is designed to enhance aviation safety and reduce pilot workload. For example, the solution could be used when helicopters are hired for emergency response activities like wildfire fighting, where the full manifest of the aircraft for each and every leg of a flight must be communicated to the dispatch center. The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”

The IQonboard solution is designed to enhance aviation safety and reduce pilot workload. For example, the solution could be used when helicopters are hired for emergency response activities like wildfire fighting, where the full manifest of the aircraft for each and every leg of a flight must be communicated to the dispatch center. The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”

The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”

The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”

The IQonboard solution is designed to enhance aviation safety and reduce pilot workload. For example, the solution could be used when helicopters are hired for emergency response activities like wildfire fighting, where the full manifest of the aircraft for each and every leg of a flight must be communicated to the dispatch center. The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”

The IQonboard solution is designed to enhance aviation safety and reduce pilot workload. For example, the solution could be used when helicopters are hired for emergency response activities like wildfire fighting, where the full manifest of the aircraft for each and every leg of a flight must be communicated to the dispatch center. The system provides a real time view... which helps improve communications and decrease reliance on radio, [while] eliminating the need for manual calculations,” says Vincent Hoag, CEO, IQonboard. “Manifest reporting becomes an operational advantage.”
Wearable knee support joins joint injury recovery

NZ-based OPUM Technologies has developed an orthopaedic remote patient therapeutic monitoring solution and digital rehabilitation platform for joint injury recovery. The core of the technology is an instrument for precisely measuring medical data including skin movement. The device is made of titanium with a unique, biocompatible surface finish. It can be built for use with a wide range of orthopaedic practices, such as the Digital Knee wireless goniometer. A Nordic nRF52840-powered sensor device that continuously measures the range of motion of the knee. The goniometer—an instrument for the precise measurement of angles—requires no calibration and is accurate to less than one degree. Moreover, the solution integrates advanced digital data analytics including machine learning (ML)-powered activity recognition and posture recognition, as well as traditional sensors and accelerometers. The integrated Nordic nRF52840 SiP based on the Wafer Level Chip Scale Package (WLCSP) integrates the main application processor for the Digital Knee sensor, performing all data capture activities and running a number of proprietary algorithms and ML classifications. Using Bluetooth LE connectivity provided by the nRF52840 SiP, the data is sent from the sensor to a user’s smartphone, where it is stored on the device and a partnership with the challenge sponsors and Wevolver. Entries will be judged by experts from the research community, as well as representatives from partnering companies and organizations. The grand prize winner will receive $20,000 in sponsorship, a one-year subscription to nRF Cloud Services for up to 500 devices, and a partnership with the challenge sponsors and Wevolver. The research community will be able to submit projects as part of the Connect for Good Challenge on the nRF9160 SiP for cellular IoT connectivity. The product weighs only 76 g and can be entirely powered by LTE signals, while using the smartphone as a receiver that detects Bluetooth signals, which are then modified into reflected Wi-Fi signals. The smartphone then becomes an RFID reader, the Wafer Level Chip Scale Package (WLCSP) version of Nordic Semiconductor’s nRF52840. The nRF52840 SiP enabled Bluetooth LE connectivity allows real-time health data to be relayed wirelessly from the device to the user’s smartphone, from where an app provides real-time insights to the user. The app includes an alarm system to alert the user when the system detects anomalies. The device is designed to be used as a digital twin of the user’s health, tracking their recovery journey, including rehabilitation therapy and surgical plans, and share data and compliance with their care teams. The device can be used to provide real-time insights for patients performing their prescribed activities and assessments. Through the app, patients can also build a digital twin of their knee to deliver a continuous holistic picture of knee health, track their recovery journey, receive and track prescribed therapy and surgical plans, and share data and compliance with their care teams. The solution is designed to be energy efficient, helping to fight against food waste and improve sustainability. The device also comprises software, electronic health services for up to 500 devices (valued at $3,000), Soracom connectivity for each device and a partnership with the challenge sponsors to accelerate project development.

Digital knee sensor, performing all data capture activities and running a number of proprietary algorithms and ML classifications. Using Bluetooth LE connectivity provided by the nRF52840 SiP, the data is sent from the sensor to a user’s smartphone, where it is stored on the device and a partnership with the challenge sponsors and Wevolver. Entries will be judged by experts from the research community, as well as representatives from partnering companies and organizations. The grand prize winner will receive $20,000 in sponsorship, a one-year subscription to nRF Cloud Services for up to 500 devices, and a partnership with the challenge sponsors and Wevolver. The research community will be able to submit projects as part of the Connect for Good Challenge on the nRF9160 SiP for cellular IoT connectivity. The product weighs only 76 g and can be entirely powered by LTE signals, while using the smartphone as a receiver that detects Bluetooth signals, which are then modified into reflected Wi-Fi signals. The smartphone then becomes an RFID reader, the Wafer Level Chip Scale Package (WLCSP) version of Nordic Semiconductor’s nRF52840. The nRF52840 SiP enabled Bluetooth LE connectivity allows real-time health data to be relayed wirelessly from the device to the user’s smartphone, from where an app provides real-time insights to the user. The app includes an alarm system to alert the user when the system detects anomalies. The device is designed to be used as a digital twin of the user’s health, tracking their recovery journey, including rehabilitation therapy and surgical plans, and share data and compliance with their care teams. The device can be used to provide real-time insights for patients performing their prescribed activities and assessments. Through the app, patients can also build a digital twin of their knee to deliver a continuous holistic picture of knee health, track their recovery journey, receive and track prescribed therapy and surgical plans, and share data and compliance with their care teams.
Animal Tracking

Pet tracker uses machine learning to detect animal health problems

Norwegian-based tech company, Lilbit, has launched a smart wearable that tracks pet location and health metrics. The small and lightweight device attaches to the pet’s collar, and once paired to a smartphone, ensures an easy way to monitor and record their location and movements. The collar uses Bluetooth LE connectivity provided by Nordic’s nRF5180 SIP. If the dog or cat moves beyond Bluetooth LE range, the device can detect and report the animal’s position using LTE-M/NB-IoT connectivity and GPS trilateration enabled by Nordic’s nRF9160 SIP. The Lilbit development kit includes an integrated inertial measurement unit (IMU)—with accelerometer, magnetometer and gyroscope—records the animal’s movements and, with the support of proprietary machine learning (ML) algorithms, can, over time, associate these movements with particular behaviors and health issues. The combination of the nRF9160’s Arm Cortex-M33 application processor and the nRF52811’s Arm Cortex-M4 processor, provides Lilbit with the processing power to comfortably handle these complex and processor intensive communications. From the IMU and Andriod Ligoil or Lcat app, the owner can track the pet’s location and location history, but also review the animal’s activity data, as well as its temperature, behavior and any health issues.

Internet of Things

‘Traffic cop’ algorithm keeps robots on task

Multiple robots simultaneously relaying time sensitive information over a wireless network can lead to a traffic jam of data, while even information that manages to get through might be too old for an up-to-date report. Drones searching a disaster zone, for example, rely on recent data to locate survivors or report potential hazards. Now Massachusetts Institute of Technology engineers have developed a solution. This method allows any wireless network to handle high load of time sensitive data coming from multiple sources. This approach, called WiSlow—a scheduling algorithm that can run on a centralized computer—configures a wireless network to control the flow of information from multiple sources while ensuring the network is relaying the freshest data by allowing a fast in, first out protocol rather than the RF firmware,” says Morten Saether, CEO of Lilbit.

Smart Agriculture

Irrigation sensor detects water leaks

Norwegian company T5 Sense has launched a cellular IoT irrigation sensor for water leak detection and location monitoring for sprinkler carts. The T5Sense Irrigation Sensor Gen IIis used on farms and can be easily retrofitted to almost any type of legacy irrigation system. Alerts and notifications about water leaks, the sprinkler’s location, speed and estimated finish time are transmitted to the Cloud via Nordic’s nRF9160 SIP. From there, the information can be sent to the farmer’s smartphone for viewing on an app. The nRF9160’s application processor provides the necessary computational power for the sensor to monitor and analyze the micro vibrations in the water pipe. Changes in these vibrations indicate a flow imbalance.

Smart Home

Home sensors support Amazon Sidewalk

Brownian Communications has launched its latest line of IoT sensors with support for Amazon Sidewalk, a secure, free-to-connect community network designed to provide low-cost connectivity for billions of devices. The multifunction smart home sensors integrate Nordic Semiconductor’s nRF52840 Bluetooth LE SOC and a Semtech SX1262 transceiver to extend the sensors’ working range at home and beyond the front door (see WQ Issue 1 2023, pg 91). “Amazon Sidewalk makes it possible to install our IoT sensors at the edge of a home network,” says Mohammed Alhennawi, Sales Director at Brownian Communications. “Our objective is to design wireless sensors that are safe, easy to set up, and use daily. We achieved this by incorporating the nRF52840 Bluetooth LE SOC from Nordic, which provides the most reliable maintenance free connectivity.”

Smart Health

Humidity sensor enables respiration monitoring and smart diapers

Researchers have developed an electrode sensor solution to alert parents and carers when a baby’s diaper needs changing. The sensor is based on a hand-drawn electrode created using a pencil, drawn on paper to treated with a sodium chloride solution. The device takes advantage of the way paper naturally reacts to changes in humidity. As water molecules are absorbed in the paper, the sodium chloride solution becomes ionized and current flows through the graphite depositing the pencil. If setting off the sensor. The hydration sensor is highly sensitive to changes in humidity and provides accurate readings from 5.6 percent to 90 percent relative humidity. For wireless applications the pencil drawing is connected to a lithium battery which powers data transmission to a smartphone using Bluetooth LE connectivity. The researchers integrated four humidity sensors between the absorbent layers of a diaper to create a smart version capable of detecting wetness and changing reminders. For respiration monitoring, the co-authors from Penn State University, Hebei University of Technology and Tianjin Tianzhong Yimai Technology Development drew the electrode directly on a solution-treated mask. The sensor differentiated mouth breathing from nose breathing and was able to classify three breathing states—deep, regular and rapid. “Different types of disease conditions result in different rates of water loss [from the skin],” explained researcher Huangyu ‘Larry’ Chang, Associate Professor of Engineering Science and Mechanics at Penn State University. “The skin will function differently based on these conditions, which we will be able to flag and possibly characterize using the sensor,” says Cheng.

By the Numbers

Global cellular IoT module shipments grew 14 percent YoY in 2022 to register record annual volume, according to Counterpoint’s latest Global Cellular IoT Modulator and Chipset Tracker report. The analyst ascribed the growth in demand for IoT modules to a number of factors including smart meter implementation, retail POS upgrades, intelligent asset tracking, and growth in connected cars due to progress in electrification and autonomous capabilities. The research showed that during 2022, NB-IoT remained the most popular LPWAN IoT connectivity technology.

Kaleido intelligence reports that smart home sensors sold for almost $5 billion in culture IoT connectivity revenue in 2022, a CAGR of 36.7 percent from an expected $7.2 million in 2023. According to the firm, this growth comes from an increasing level of automation in maintenance, alongside a significant expansion of real time video use. The research found the manufacturing industry will transmit nearly 220 petabytes of data over cellular channels by 2028.

The global wireless charging market will exceed $6.7 billion by 2023, up from $7.7 billion in 2022 and $5.6 billion in 2021, according to a new report by Markets and Markets. Increasing market demand for wireless charging products due to convenience and safety in various sectors like healthcare, consumer electronics and the automotive industry are key factors anticipated to boost the market growth of wireless charging.
News Extra

Nordic introduces end-to-end cellular IoT solution with DECT NR+ support

New SiPs combine with software, Cloud services and technical support for a complete design and deployment solution for cellular IoT and NR+

Designing, installing and maintaining cellular IoT products is challenging. And it has been made harder by supply chain fragmentation. In the worst case, an OEM might have to deal with individual suppliers of chipsets, development tools, software, development kits, modules and Cloud services.

Nordic Semiconductor’s strategy is to consolidate the supply chain by bringing together all the elements needed for the successful launch and implementation of an IoT product under one roof. The company’s Bluetooth LE solutions, for example, include SiCs, proven stacks, module partners, comprehensive design and development tools, prototype platforms and reference designs. And after deployment in the field, Bluetooth LE end products can be regularly updated with over-the-air software downloads.

Now Nordic has followed the same strategy to become the first company to offer a fully inclusive, world-class massive IoT solution. The offering forms a comprehensive, end-to-end cellular IoT platform with support for DECT NR+ (NR-1). Comprising new products based on nRF91 Series SiPs this massive IoT offering brings simplicity, stability and cost efficiency to cellular IoT design, manufacture and deployment. For the first time, vendors can access SiPs, software, and services designed, controlled, and supplied by a single company.

“Today’s announcement positions Nordic Semiconductor as the pre-eminent supplier of massive IoT solutions,” says Svein-Tore Larsen, Nordic’s CEO. “I’m very proud to declare that the company is the first to offer a comprehensive cellular IoT solution that will save our customers considerable time, money, engineering resources, and frustration that result from dealing with fragmented supply chains. This integrated cellular IoT solution follows the same unified platform strategy we have implemented for our class-leading Bluetooth LE, Thread and Wi-Fi products.”

Extending the nRF91 Series

Nordic’s cellular IoT solution with support for NR+ comprises two new nRF 91 Series SiPs, the nRF9161 and nRF9131, evaluation and development tools, development software, and IoT Cloud services, plus world-class technical support and advice.

The nRF9161 is a complete, targeted globally pre-certified SPI that makes it possible to use a single device to select either cellular IoT, or NR+ for massive, ultra-reliable private 5G networking. (See column opposite The tech behind massive IoT.)

The tech behind massive IoT

Massive IoT describes a future network of trillions of IoT connected devices. Such a network will support applications that require a large volume and density of devices with widespread coverage. Examples include smart utility meters, smart streetlights and asset trackers.

To meet its promise, massive IoT must be based on a networking technology that supports scalability and versatility. Deployment densities of one million devices per square kilometer will be possible.

Moreover, the network will demand robust and secure bidirectional end-to-end communication with the Cloud without the need of a gateway.

Cellular IoT is an ideal technology for massive IoT. It uses cellular infrastructure to connect massive IoT devices to the Cloud. The tech is an LPWAN technology that can connect over kilometers, supports many IoT devices, and doesn't require much battery power.

Key advantages include Internet Protocol (IP) inter-operability which enables a bidirectional link between end-devices and the Cloud without expensive and complex gateways. Further advantages include future-proofing, scalability, security and high quality of service (QoS). NB-IoT and LTE-M are the two underpinning technologies supporting cellular IoT. NB-IoT is primarily designed for energy efficiency and for penetration into buildings and other areas that are otherwise challenging to reach. It is not based directly on LTE (4G) technology but does include many aspects of cellular technology. Latency ranges from one to 15 seconds.

LTE-M is based on a streamlined form of LTE technology, and supports secure communications, ubiquitous coverage and high system capacity. Its ability to operate over a relatively large bandwidth improves latency and throughput compared with NB-IoT.

The technology is suitable for secure end-to-end IP connections, and mobility is supported by LTE cellular handover techniques.

Companies building products for tomorrow’s IoT can work with a single supplier, safe in the knowledge all platform parts will be perfectly optimized.

Deployed customer end-devices based on the new SiPs will be supported by Nordic’s nRF Cloud. nRF Cloud is optimized for seamless and power-efficient operation with Nordic’s IoT products and offers a connectivity platform and Cloud services solution for massive IoT deployments from onboarding to decommissioning.

The HIGHLIGHTS:

- Understanding DECT NR+: The first non-cellular 5G standard
- Designing Secure IoT Products

Combo Power from nRF5340 SoC with range from nRF21540 FEM, using module from Laird

Catch all the latest Nordic webinars on-demand

WATCH NOW

webinars.nordicsemi.com/videos

HIGHLIGHTS

Understanding DECT NR+: The first non-cellular 5G standard
Designing Secure IoT Products

Combined Power from nRF5340 SoC with range from nRF21540 FEM, using module from Laird

WATCH NOW

webinars.nordicsemi.com/videos
Auracast broadcast audio could revolutionize audio sharing

By allowing an audio source device to broadcast to an unlimited number of receivers, Auracast can change how people consume content and interact with their environment.

Auracast broadcast audio is a specific and unified implementation of broadcast audio for personal audio sharing and broadcasting audio in public spaces.

Auracast allows an audio source device like a smartphone, laptop, TV, PA or sound system to broadcast one or several audio streams to an unlimited number of Bluetooth audio receivers. The broadcast would use the Bluetooth 5.2 specification’s Isochronous Channels to transmit signals to things like headsets, True Wireless Stereo earbuds or specialized products like hearing aids.

“Auracast broadcast audio is a specific and unified implementation of broadcast audio for personal audio sharing and broadcasting audio in public spaces,” explains Chuck Sabin, Senior Director of Market Development at ABI Research.

Auracast assistant and headset device to tune into the Auracast broadcast audio of a particular screen at a venue where televisions are installed but no audio is provided, or where the audio is hard to hear, such as gyms or bars. Longer term, one-to-one or counter-based assistive listening applications could emerge in retail and other service environments.

A growing market

According to ABI Research, by 2030 there will be nearly 2.6 million Auracast deployments across venues such as libraries, social or meeting venues, recreational facilities, entertainment and culture, as well as airports and transportation hubs. Public assembly use cases will account for nearly 42 percent of those deployments. Air travelers, for example, would be able to select the Auracast broadcast for their specific terminal, filtering out unnecessary announcements. Places of worship, restaurants and hotels are also places that could potentially benefit from Auracast.

Silent TV screens, assistive listening and multi-language support applications are expected to become increasingly prevalent over time. And as the market develops and the installed base of Auracast devices grows, new use cases are likely to emerge. However, it will take some time for the ecosystem of LE Audio transmitting and receiving devices to develop, says ABI Research.

The firm expects the “major inflection point” to occur around 2025: “When the technology will be more familiar, transmitter devices will be more readily available, and the installed base of LE Audio-enabled devices will have reached a critical mass.”
In Short

Despite predictions of the decline of physical retail in the wake of the pandemic, the sector is healthy and growing with the help of IoT tech.

Wireless solutions are impacting the entire retail value chain from warehouse to delivery, helping retailers in pricing, staffing, and maintenance. Retail lighting systems have become crucial in delivering on this promise.

Wireless tech is improving the retail experience for everyone, maximizing profits for the retailer and delivering value added convenience for customers.

RETAIL’S CHANGING FACE

It is a widely held misconception that COVID-19 precipitated the downfall of the physical retail store. While the pandemic undoubtedly changed the face of bricks and mortar retail, rumors of its demise have been greatly exaggerated (see State of Play: Why physical retail still rules).

According to U.S. Department of Commerce data, ten years ago e-commerce accounted for 8 percent of retail purchases, today that’s 20 percent. After significant pandemic-powered growth in online sales in 2020, by 2021 physical retail was growing just as fast, and at a much higher base. By 2022, e-commerce in the U.S. topped $1 trillion for the first time, but total retail sales were a shade under $5 trillion. There is life in physical retail just yet.

“Physical retail is not disappearing, it’s changing,” says Lorenzo Amicucci, Business Development Manager – Retail at Nordic Semiconductor. “Success comes from embracing new tech that can enhance the customer experience and offer something complementary to online purchases. The future of retail isn’t online or offline – it’s both.”

The advent of multichannel retail has raised the stakes on logistics. If one in five customers want to buy online, then it’s imperative retailers can meet this demand. But some consumers want things ‘now’, not even tomorrow and definitely not next week or next month. This instant gratification is why physical retail retains its dominance. Yet, the success of e-commerce has been the ability of retailers to close the gap between desire and delivery. Amazon set the bar with the promise of same- or next-day delivery. Other retailers have followed, and IoT technology is now essential in the warehouse to improve the visibility of physical assets across a floor space that in the case of Amazon’s assets across a floor space that in the case of Amazon’s...
A brief history of retail tech

The first form of retail is believed to have begun around 8,000 years ago in the 7th millennium BCE, somewhere in the Middle East. Bartering and chewing were the earliest examples of commerce, but trading above a bartering for wheat for an animal skin was an inexact science, so the invention of money around 5,000 years ago allowed for greater precision to the retail exchange.

The first form of retail as we know it today began in earnest. Fast forward to 1883 and inspired by a machine he saw on a ship which counted the number of times the propellers completed a revolution, bar owner James Ritty invented the cash register, allowing him to keep an accurate track of sales and at the same time making it harder for light-fingered employees to pocket the takings. Come the 1940s, two further inventions proved hugely profitable to retailers, the shopping trolley and the credit card. The shopping trolley evolved from wire-hand baskets as a solution to shoppers having to carry their heavy groceries, but also allowing them to buy much more than their previous basket’s capacity. And they did. Meanwhile credit cards meant people could pay for their purchases without having to withdraw money from the bank. Happily, retailers quickly noticed people spent more money when they used a credit card rather than cash.

In 1974 barcodes were introduced, and a pack of wheat for an animal skin was an inexact science, but that the appearance of machines and freshness of the slushie on offer often acted as a deterrent to purchase. Nearly empty reservoirs kill sales because consumers think the beverage inside is old and stale – even if that is not the case. “Consumers haven’t fallen out of favor with... slushies, they’ve fallen out of favor with a poor customer experience,” says Kyle Freebairn, CEO of Freezal. To address declining sales the company partnered with Norwegian IoT tech company, 7Sense, to develop a low-cost circuit board based on Nordic’s silicon. Once retrofitted to existing slushie machines the board enabled remote NB-IoT monitoring of frozen beverage machines. “With the cellular IoT enhancement, our customers won’t even have to phone us for most issues; if they have a problem, we’ll know before they do,” says Freebairn. The result was sales growth at 70 times the industry average, that more than offset the cost of moving to cellular IoT.

Together with other innovations such as self-checkouts, self-scanning and contactless payment, tech helps retailers cut labor costs, while maximizing sales and consumer experiences.

HIGH MAINTENANCE

Throughout history people have quickly realized that bad food can make you sick, but before the advent of commercial refrigeration at the turn of the 20th century, food safety standards weren’t always as rigorous as they are today. Despite much improved practices and multi-level governance for regulation and enforcement, food safety incidents still occur, and the fines for the negligent can be eye-watering. Back in 2020, Chipotle Mexican Grill agreed to pay a $25 million criminal fine for a foodborne illness outbreak that made over a thousand people sick. A faulty or broken refrigerator in a supermarket could at best result in thousands of dollars of spoiled stock, or worse cause illness in a customer that could not only incur a hefty fine but catastrophically damage a business’ hard-earned reputation. Wireless IoT solutions are now widely deployed to mitigate against such risks by early detection of food inventory spoilage and automatic activation of previously manual temperature measurements. For example, last year Canadian company Stratusware launched its Tampscan, a solution comprising temperature sensor beacons and a Bluetooth LE to Wi-Fi gateway both integrating Nordic’s nRF9160 SiP. The beacons measure the ambient and surface temperature of front- and back-of-house equipment, and relay the data to a cloud platform for round-the-clock monitoring of a potentialissu.

A useful tool in the last year was the SECO Embedded Sensor smart plug, developed by German IoT solutions company Lemonbeat, that detects a range of energy parameters and allows the user to remotely assess whether their commercial chillers or freezers require maintenance. The smart plug employs a sensor to record energy, voltage, power and current variables, and can be retrofitted to any 230 V-powered device. The device then uses an nRF9160 SiP to relay data to a cloud-based platform. “With a highly granular monitoring of energy parameters, it is possible to detect patterns... about the health status of the chiller or freezer and whether it needs maintenance or not,” says Lemonbeat CEO, Oliver van der Monds. “This means SECO is able to schedule a service only when it is actually needed.” Such solutions may not be new, but what is new is the communication infrastructures that can be leveraged for this purpose. One of the most promising is Thread, where sensors can be added to create a mesh network to collect data from around the shop. Thread networks support low power devices ensuring they operate efficiently and securely, making them ideal for battery powered
Physical retail is not disappearing. Its changing — and the key to success is to embrace new technologies.

REDRESSING GRUEN’S TRANSFER

The release of LE Audio and Auracast broadcast audio capabilities by the Bluetooth SIG (see pg12), will introduce retail into the customer experience. “This enables exactly the type of hybrid online-offline retail experience consumers have come to demand,” says Amicucci. “The introduction of Bluetooth Direction Finding [also enhanced the customer experience by] providing the basis for precision-positioning and... helping both customers and employers find products faster and easier.”

These wireless technologies have taken the evolution of retail full circle, away from the deliberate and coercive manipulation of the consumer’s senses described by the Gruen transfer, and back towards Victor Gruen’s original idea of retail experience based on ease and efficiency.

As Gruen knew, at its essence, successful retail isn’t about the retailer getting one over on the customer. The art of a successful retail exchange is to ensure a satisfactory outcome for both parties. Today, wireless tech is improving the retail experience for everyone, maximizing profits and reducing costs for the retailer, and delivering value added convenience to customers.

Tech Check: Revolutionizing Retail

COVID-19 might have delivered a huge shot in the arm for e-commerce, but bricks-and-mortar retail still dominates, in the U.S., four out of every five dollars spent on shopping are spent in a physical store, as consumers still enjoy the instant gratification and ability to see and touch things that online shopping can’t provide. Meanwhile a range of wireless technologies are reinventing the retail experience, making it both more convenient for the consumer, and profitable for the retailer.

Contactless payment saves time and can improve the overall security of payment systems. Both Bluetooth LE and NFC have roles to play. NFC offers the inherent security of very short range communication making a hacker’s eavesdropping attack very difficult. Bluetooth LE offers more versatility even making electronic payments possible when the terminal’s connection to the Internet is disrupted.

Bluetooth LE electronic shelf labels connected to a Cloud gateway allow retailers to automatically update pricelabels from a central point across multiple stores or in certain geographic locations. The smart labels can also be used as beacons for targeted marketing via a consumer’s phone proximity.

LED electronic shelf labels can be used as beacons for targeted marketing. These wireless technologies have taken the evolution of retail full circle, away from the deliberate and coercive manipulation of the consumer’s senses described by the Gruen transfer, and back towards Victor Gruen’s original idea of retail experience based on ease and efficiency.

Scann-and-go lanes in supermarkets allow consumers to avoid the long checkout queues by using their smartphone to scan and pay for items as they move around the store. When they reach the exit gate, shoppers can scan their receipt code at the dedicated terminal, and once payment is authorized, the gate will automatically open.

The ONE shopping mall in Hong Kong has no fewer than 24 hours of mixed retail and restaurant space, an easy environment in which to get lost or separated from your friends. Shopping centers employing Bluetooth Direction Finding beacons provide a reliable real-time location system (RTLS) solution, helping consumers use their smartphone to navigate indoors with sub-meter accuracy.

More than two million shopping carts go missing in the U.S. each year, many of them stolen. Replacing a lost cart can cost retailers up to $250, so they are turning to technology to combat the problem. Some retailers are using wheels that lock if taken off site, or QR code and NFC based systems. In future cellular IoT devices paired with GNSS and NFC Cloud location Services, could allow retailers to track, monitor and quickly retrieve any purified shopping carts.
Secure by Design

The IoT Industry is coming together to fight the threat of cyber-attacks by adopting standardized approaches that build security into connected devices by default.
In a wide range of scenarios, this was made clear by the attack described at the beginning of this article. Known as the ‘Dyn attack’, it remains one of the most prominent cyber-attacks involving IoT. In another infamous IoT attack, hackers stole a U.S. casino’s high roller database by exploiting a vulnerability in a fish tank thermometer in the casino’s lobby. Other IoT threats illuminate the high stakes for safety. Security researchers have long raised hacking fears involving connected medical devices such as pacemakers and insulin pumps. In 2015, Fiat Chrysler was forced to recall 1.4 million vehicles after a software security flaw was discovered in a Jeep Cherokee. Video baby monitors and home security cameras have also been subject to compromise due to security failings.

**CHEAP BUT EXPOSED**

Attacks on the IoT appear to be on the rise. According to cybersecurity provider Kaspersky, the first half of 2021 saw 15 billion attacks on IoT devices, a doubling from the previous six months. In truth, concerns about the state of security in IoT devices have persisted for some time, among both security researchers and advocates — the latter fearful about the impact security concerns might have on general consumer confidence in the IoT as a whole.

According to McKinsey, only about 30 percent of providers of IoT solutions consider digital trust to be critical, compared with approximately 60 percent of buyers. While complicity may once have played a role, the increase in successful attacks on IoT devices could also be a result of their inherent characteristics. “IoT devices have much more limited resources in terms of computing power, memory, energy, and also sometimes lack hardware and software security features to protect against various threats,” says Tiago Monte, Developer Marketing Manager at Nordics Semiconductor. “This can lead to simplified or lightweight security implementations on IoT devices, which can be more vulnerable to attacks.”

The physical accessibility of IoT devices — often deployed within reach in publicly accessible locations, as is the case with smart city deployments — also increases their exposure to physical attacks and tampering, says Monte. Remote attacks are equally a threat as they are for any networked device, including those in enterprise computing contexts.

The nature of the IoT supply chain presents its own challenges. Researchers have long understood that cyber attackers love complexity — the more layers or nodes of equipment, the more software integrations or third parties involved, the more likely there will be a gap or loophole that can be exploited. By their nature, IoT deployments involve several vendors, components and points of integration, creating greater risk. This vulnerability emphasizes the importance of having individual components and devices that are themselves inherently secure. Incentives and the allure of easy connectivity have also played their role. In recent years, the IoT’s potential to deliver benefits including efficiency, innovation and enhanced customer experience has become better known just as the costs of chips fell, making the economic case for turning any product into a connected device somewhat irresistible. “The price of turning a dumb device into a smart device [can be as low as] 10 cents,” renowned security expert Mikko Hyppönen told a European conference recently. “It’s going to be so cheap that vendors will put the chip in any device, even if the benefits are only very small.”

Unfortunately, security costs, so the business case for working to protect these devices didn’t follow as readily, resulting in the development and rollout of many connected devices that had poor or even non-existent standards of security.

**PROTECTED BY DEFAULT**

But in the wake of heightened awareness to cyber-attacks the tide is now turning. Public expectations of IoT devices have also clearly shifted. A survey by the U.K. government in 2020 found nine out of ten people now expect smart devices to have basic embedded features to protect user privacy and security. Nordic’s Monte believes the imperative for IoT security is even more fundamental than meeting emerging consumer buying preferences. “Security breaches of individual IoT products threaten not only the prosperity of companies making vulnerable products, but they also impact entire product categories by giving them a reputation for being insecure,” he says. As a result of the wide-scale reputational impacts, securing the IoT is now becoming a serious mission for companies involved across the sector, from chip vendors through to device makers. The journey towards good IoT security has been long, but ultimately positive. Despite good intentions, early approaches were somewhat “half-baked” and “inconsistent,” says Monte. At a time when security was still not a priority, well-meaning manufacturers were left to do their best with minimal guidance about what was best practice. Security was also often left to the end of the design process, added either as an afterthought or only after the discovery of security issues that would have prevented a product being released. The approach of ‘retrofitting’ security late in the development process not only creates more vulnerable outcomes. “In many cases, it also makes the solution more expensive,” according to a Deloitte report.

Happily, we are now seeing a shift in thinking towards making IoT devices that are both ‘secure by design’ and ‘secure by default’, says Monte. In the former, security needs are considered and addressed in the early stages of product design, in the same way a designer might consider functional and non-functional requirements such as battery life or user interface, he says.

---

**State of Play**

**Why are criminals so interested in the IoT?**

Experts say 2021 was the year of ransomware, but things changed in 2022 as the bad guys realized the estimated 17 billion IoT devices in 2022 to be a result of their inherent characteristics. “IoT devices...” says Tiago Monte, Developer Marketing Manager at Nordics Semiconductor. “This can lead to simplified or lightweight security implementations on IoT devices, which can be more vulnerable to attacks.”

The physical accessibility of IoT devices — often deployed within reach in publicly accessible locations, as is the case with smart city deployments — also increases their exposure to physical attacks and tampering, says Monte. Remote attacks are equally a threat as they are for any networked device, including those in enterprise computing contexts.

The nature of the IoT supply chain presents its own challenges. Researchers have long understood that cyber attackers love complexity — the more layers or nodes of equipment, the more software integrations or third parties involved, the more likely there will be a gap or loophole that can be exploited. By their nature, IoT deployments involve several vendors, components and points of integration, creating greater risk. This vulnerability emphasizes the importance of having individual components and devices that are themselves inherently secure. Incentives and the allure of easy connectivity have also played their role. In recent years, the IoT’s potential to deliver benefits including efficiency, innovation and enhanced customer experience has become better known just as the costs of chips fell, making the economic case for turning any product into a connected device somewhat irresistible. “The price of turning a dumb device into a smart device [can be as low as] 10 cents,” renowned security expert Mikko Hyppönen told a European conference recently. “It’s going to be so cheap that vendors will put the chip in any device, even if the benefits are only very small.”

Unfortunately, security costs, so the business case for working to protect these devices didn’t follow as readily, resulting in the development and rollout of many connected devices that had poor or even non-existent standards of security.

But in the wake of heightened awareness to cyber-attacks the tide is now turning. Public expectations of IoT devices have also clearly shifted. A survey by the U.K. government in 2020 found nine out of ten people now expect smart devices to have basic embedded features to protect user privacy and security. Nordic’s Monte believes the imperative for IoT security is even more fundamental than meeting emerging consumer buying preferences. “Security breaches of individual IoT products threaten not only the prosperity of companies making vulnerable products, but they also impact entire product categories by giving them a reputation for being insecure,” he says. As a result of the wide-scale reputational impacts, securing the IoT is now becoming a serious mission for companies involved across the sector, from chip vendors through to device makers. The journey towards good IoT security has been long, but ultimately positive. Despite good intentions, early approaches were somewhat “half-baked” and “inconsistent,” says Monte. At a time when security was still not a priority, well-meaning manufacturers were left to do their best with minimal guidance about what was best practice. Security was also often left to the end of the design process, added either as an afterthought or only after the discovery of security issues that would have prevented a product being released. The approach of ‘retrofitting’ security late in the development process not only creates more vulnerable outcomes. “In many cases, it also makes the solution more expensive,” according to a Deloitte report.

Happily, we are now seeing a shift in thinking towards making IoT devices that are both ‘secure by design’ and ‘secure by default’, says Monte. In the former, security needs are considered and addressed in the early stages of product design, in the same way a designer might consider functional and non-functional requirements such as battery life or user interface, he says.

---

**Special Report: Cyber Security**

About 30 percent of providers of IoT solutions consider digital trust to be critical, compared with approximately 60 percent of buyers.
The shift towards ‘secure by default’ is clear. The wireless protocols used in the IoT have evolved from having security as optional, to having security built into the specifications by default. And it’s not just at the data exchange level, but at the device level too, with features such as secure boot and firmware updates. Companies like Nordic have identified a set of basic security objectives that are built into its products by default, and which Monte says ought to be part of any IoT product. These features include ensuring only authorized software can be executed and updated on a device, separating trusted and untrusted services on devices, and secure storage to ensure confidentiality and integrity of data and assets.

DELIVERING STANDARDIZED SECURITY

Despite this recent progress, a persistent challenge for IoT security is the lack of standardization, which translates into fragmented, inconsistent and ultimately inadequate levels of security of IoT deployments as a whole. The fragmentation is compounded by the existence of a broad spectrum of IoT products, and vastly inconsistent security expectations across these product categories. For instance, while medical devices must often meet stringent security requirements, for many consumer IoT devices, for example toys, there are no mandatory security requirements.

More recently, the IoT ecosystem appears to have realized standardization is necessary for more consistent, better security outcomes. Ninety-six percent of respondents to a survey by IoT industry consortium PSA Certified expressed interest in industry-led guidelines for IoT security best practices. In response, PSA Certified has brought together major stakeholders to consolidate fragmented security approaches into a standardized approach for the IoT. It developed a four-stage framework that guides developers through the steps necessary to implement the right level of security for an end product, providing guidance and technical resources and access to an ecosystem of certified and standardized components. Nordic’s Monte points to an ever-growing list of IoT products that have PSA certification as a sign of the framework’s positive impact on the security ecosystem. Nordic itself has aligned with the framework.

Standards and expectations are also being pushed at a national policy level, with regulators in several countries outlining expectations and establishing minimum security standards for IoT products. In the EU, lawmakers recently introduced security standards that require Internet-connected products to have “appropriate levels of cybersecurity.” In the U.S., recent Executive Orders on cybersecurity have led to the development of IoT security standards by respected standards body the National Institute of Standards and Technology (NIST), in much the same way as the European Telecommunications Standards Institute (ETSIs) has done in Europe.

Collective efforts are also being directed at improving consumer awareness and trust. Until now, the inability for consumers to distinguish a secure IoT device from an insecure one undermined confidence in IoT devices. Now, several security labeling schemes for IoT devices are in train. According to the U.S. White House, which announced a labeling program last October, such schemes will provide consumers with “peace of mind that the technology being brought into their homes is safe” and incentivize manufacturers to make secure devices. Similar schemes are either in place or under development in Singapore and Australia. (See pg.6)

UNLOCKING THE VALUE OF THE IOT

The benefits of a more secure IoT accrue in many places, not least the businesses that incorporate better security into their products. A survey of businesses by PSA Certified found having security in their products had positive impacts to the bottom line of 96 percent of survey respondents. The same survey found having better IoT security reduced costs and insurance premiums and supported the ability to charge more for products based on their enhanced security features. It also found customers were willing to pay such a premium.

Improved security can also help developers of IoT solutions unlock stronger customer relationships, especially in contexts where confidence and reliability are critical. A prime example is the Wireless Flex Dimming Receiver.lighting solution from Illumination company Fluence, which is built using Nordic’s nRF52840 SoC and is PSA Certified. The products are targeted at the agriculture sector and enables growers to maximize their yield and produce quality by optimizing lighting conditions. Given the precision with which plants need to be exposed to light, smart lighting solutions such as these must be resilient to disruptions or outside interference. With these priorities in mind, customers likely feel greater trust and confidence because of the product’s inherent security features.

Beyond benefits for individual manufacturers, it’s in the impact on the IoT ecosystem at large where we may see the full return on investment from enhanced security. McKinsey says executives would increase their spending on the IoT by 20 to 40 percent if “cybersecurity concerns were completely managed.”

It’s also worth remembering previous McKinsey projections that the IoT could enable between $5.5 trillion to $5.2 trillion in value globally by 2030. As some have observed, many such projections about the growth of IoT have yet to materialize. One of the reasons for this is that, in a world of fast-evolving and highly destructive cyber threats, the very feature at the heart of IoT’s promise—its ability to unite large numbers of connected devices to work together in a fully integrated ecosystem—is also the very thing that “creates the risk of vulnerabilities that could have catastrophic consequences”, in McKinsey’s words. But now, as wireless IoT suppliers like Nordic, industry consortia like PSA Certified and regulators around the globe work in unison to prioritize the incorporation of security into IoT products, these risks could be mitigated. With a united commitment to ensure better security, we may finally see the injection of trust that unlocks the full value of the IoT.
Planet Bluetooth
Bluetooth’s spread and evolution continue and suppliers of the omnipresent tech are innovating across applications once unimaginined

Delivering in-depth analysis of fitness and performance levels to amateur and professional athletes on the run. Sending, alerts and precise locations of potentially dangerous incidents to emergency contacts who can respond accordingly. Providing medical grade assessments of an individual’s health without a health practitioner in sight.

These are just some of the many scenarios in which near ubiquitous wireless tech is making everyday life simpler, safer and healthier for billions. And as ambitious developers take advantage of evolving technologies, connected devices with smaller form factors will do even more using even less power.

An infection point in the remarkable rise of wireless innovation carved back a quarter of a century to the emergence of an interoperable protocol that formed a standard, alongside an open specification for hardware and software. That technology came to be known as Bluetooth, which now spans across a networked segment of the connected world ever since. Within two years of Ericsson, Nokia, IBM and Toshiba creating the Bluetooth Special Interest Group (SIG) in May 1998, the Bluetooth 1.0 Specification had been launched and the first Bluetooth cellphone and wireless headset developed. From there the rate of adoption accelerated impressively. The Bluetooth 5.2 and beyond specification, which in its various forms has powered a significant innovation can be traced back a quarter of a century to the Bluetooth SIG’s launch in 1998. Today’s high end wearables represent just the latest shifted paradigm—a figure expected to climb to 7 billion by 2026. Today we are all in the Connected World – smart homes, smart cities and even smart devices changing the way we live on Planet Bluetooth. The release of the standard drove impressive growth, but things really got going with the release of an energy efficient version, Bluetooth LE, in 2010 as a hallmark element of Bluetooth 4.0 Specification. Bluetooth LE was born out of a 2001 Nokia venture to deliver a wireless technology which would operate from coin cell batteries and allow peripherals such as heart rate monitors to connect to the Finnish company’s handsets. It was further developed with partners including Nordic Semiconductor—a company that was already a renowned pioneer in ultra low power, high performance wireless connectivity. Nordic’s technology enabled, among other applications, a heart rate belt to wirelessly connect to a Nokia phone. Nokia’s initiative was eventually released to the public in October 2006 under the brand name Wibree – and it soon attracted the attention of the Bluetooth SIG.

Crucially, although it was a leader in proprietary intellectual property (IP) to the Bluetooth SIG. It proved a masterstroke; the low power wireless market exploded, with Nordic’s share making it a global market leader.

Bluetooth LE was a game changer because its ultra low power consumption meant data could be gathered from sensors without requiring frequent battery recharge or replacement. And because handset makers were familiar with the original Bluetooth technology, it rapidly adopted the low power version in their new models. That was the catalyst for a huge market in ‘appcessories’, wirelessly linked peripheral devices such as fitness bands that leveraged the smartphone’s computational horse power. Today’s high end wearable represent just the latest chapter of this story.

The rise and rise of Bluetooth
The expansion of Planet Bluetooth has been built on both constant enhancements to the Bluetooth Core Specification—the technical name for the document that details how to build Bluetooth devices—and the powerful Bluetooth SoC’s with their associated application software that power increasingly sophisticated applications.

“The Bluetooth SIG member community is dedicated to delivering innovations that improve the capabilities of Bluetooth technology and help shape new market trends,” said Mark Powell, CEO, Bluetooth SIG, in a statement. For example, the introduction of Bluetooth 5 in mid 2016 added some key capabilities to Bluetooth tech, notably increased range or higher data throughput. Bluetooth 5 sensors removed some of the barriers to retrieving data across longer distances, improving functionality across a gamut of wireless applications from smartwatches to smart agriculture.

The July 2017 release of the Bluetooth mesh 1.0 specification—as the name suggests, a mesh networking technology—expanded the capabilities of Bluetooth LE for the first time allowing devices within a network to communicate using radio packets relayed via other nodes without recourse to a central hub device. Bluetooth mesh provides vital functionality for applications in smart lighting, predictive maintenance, asset tracking and positioning among others. In 2019, a further update to the Bluetooth Specification, Bluetooth 5.1, brought another powerful application of the technology to the fore—the direction finding. Designed to enhance location services where previously Received Signal Strength Indication (RSSI) offered limited precision, Bluetooth Direction Finding offered new and improved use case for real-time location systems (RTLS) such as indoor asset tracking. The feature yields an improvement in location accuracy from meters to centimeters, opening up new possibilities for accurate indoor positioning of both assets and people. It’s anticipated that smartphones supporting Bluetooth Direction Finding will enable scenarios like locating lost personal items and wayfinding in large spaces such as airports and hospitals. There will be a total of 178,000 Bluetooth RTLS implementations by the end of 2023, with 262 million Bluetooth Location services device shipments anticipated this year, according to data by analyst ABI Research.

In the lucrative audio market, Bluetooth tech described as the ‘future of wireless sound’ now allows engineers to enhance the sound quality and power consumption of wireless audio products. Bluetooth 5.2 added capabilities to the specification that support LE Audio. (See pg. 5) In 2022, 1.36 billion Bluetooth audio streaming devices—including headsets, headphones, speakers and earbuds—were shipped globally.

Bluetooth tech is also the radio of choice for commissioning smart home devices. While smart home device manufacturers can select from several low power wireless protocols such as Thread or Zigbee, Bluetooth’s unique advantage is its interoperability with smartphones and tablets. And with its inclusion in Matter, Bluetooth tech’s place in the smart home is now cemented as its competitive advantage from the biggest tech companies in the world, including Nordic Semiconductor. Matter stands to revolutionize the smart home by uniting disparate ecosystems and bringing the world of smart devices closer together.

Pioneer becomes leader
Nordic has been part of Bluetooth LE’s success since its joint venture with Nokia’s Motiongage initiative in 2001. Being a pioneer of a technology doesn’t guarantee a company will become a leader. Nordic’s engineering teams have worked hard to establish the company at the forefront of Bluetooth LE tech. The firm built its early ultra low power wireless experience to become one of the first companies to launch a Bluetooth SoC—a highly-integrated chip including radio, microprocessor, memory and other functionality—with its nRF51 Series in 2012. The SoC concept had since been copied by virtually every Bluetooth LE supplier. Fast-forward over a decade and today, Nordic’s award-winning, high-performance, yet easy to design-in-
By the Numbers

3.5 billion
Bluetooth peripheral devices to ship in 2023

686 million
Bluetooth smart home devices to ship in 2023

635 million
Bluetooth wearables shipped annually by 2027

1.67x growth for Bluetooth data transfer device shipper

ENDLESS APPLICATIONS

Like the capability of its products, the performance of applications enabled by Nordic’s low power wireless tech continues to improve. For example, a high-end Bluetooth sportwatch monitors the wearer’s heart rate, heart rate variability, blood oxygen saturation, sleep data, strain and skin temperature. The data is relayed to a smartphone via Bluetooth LE. The C406 Pro satellite GPS bike computer can record over 100 different items of riding data across 13 categories as well as support up to eight peripherals.

What’s in a name?

The Bluetooth brand is universally recognized, but few could immediately explain the origin of the name. Given the level of innovation it’s associated with, Bluetooth doesn’t sound particularly quirky. It’s not an acronym, nor does it refer to a form of RF modulation. So where does it come from? Surprisingly, the name dates back more than a millennium to King Harald Bluetooth...
Transportation

Enua Charge

This cellular IoT powered smart portable EV charger, allows EV owners to charge their vehicles at multiple locations.

The U.S. government is aiming to make electric vehicles (EVs) half of all new vehicles sold by 2030, while Berg Insight forecasts there will be nearly 10 million EV charging points in Europe by the end of next year. Reliable, secure wireless connectivity to EV charging stations is essential if these projections are to be realized, and cellular IoT is predicted to dominate.

The Enua Charge device employs Nordic Semiconductor’s nRF9160 SiP with integrated LTE-M/NB-IoT modem and GNSS to provide Cloud connectivity. The connectivity enables an EV to be charged remotely and securely, for example, only activating during times of the day when electricity is at its cheapest. The charger also integrates a parking sensor, allowing parking operators to remotely monitor when a car is parked in a reserved charging spot but is not charging.

The Enua Charge can be mounted to any Enua WallMount and easily detached and taken with the driver on their journey. This way, only a single EV charger is required if an Enua WallMount is installed in multiple locations, such as at home or the office. NFC communication between the charger and the wall mount identifies the charger, allowing the charger to precisely measure energy consumption in more than one location, for instance, when used with company cars visiting different office facilities.

While most commercial EVs can travel between 300 and 500 km on a single charge, Californian automaker Proterra set the record for distance covered back in 2017 with its Catalyst E2 Max bus. The heavy vehicle was fitted with a 660 kWh battery pack which enabled it to cover 1,772.2 kilometers before the battery pack ran out of energy and the bus ground to a halt. The heavy vehicle charging system meant it only needed a few hours to fully charge and be ready for another day of operation.

EVs are not a modern invention. The first full-sized EV was actually created by Scottish inventor Robert Anderson as far back as 1832. The crude prototype was powered by non-rechargeable primary power cells, the first human-carrying EV with its own power source was tested and driven in Paris in 1881 by French inventor Gustave Trouvé. He failed to patent the vehicle instead focusing his attention to marine propulsion, adapting the invention to propel small watercraft, in so doing inventing the outboard motor.

Enua Charge

Transportation

Motoring enthusiasts like to hear the roar of a V8 engine when they are behind the wheel, which is one reason why many EV makers add fake engine noise to otherwise silent electric vehicles. Sometimes called enhanced engine noise, it uses powertrain data to simulate the engine noise and then pushes it through internal and external speakers. The artificial noise also helps remind drivers of their own rapid acceleration, and warns pedestrians of the car’s presence. Car makers are also exploring the idea of adding engine vibrations to add yet more authenticity.

Tech Check

In addition to the nRF9160 SiP, the Enua charger employs Nordic’s nRF52840 SoC, providing Bluetooth LE wireless connectivity between the charger and the Enua app on the user’s smartphone. From the app, users can configure the charger to suit their individual requirements, unlock the charger, select predefined charging profiles, view the charging status of their EV, receive notification when charging is complete, as well as implement linked smart home functionality.
Agricultural sensor saves water on the smart farm

The Nordic nRF9160 SiP-powered 7Sense water sensor helps track sprinkler carts and notifies farmers of irrigation leaks

Solving the irrigation issue

Farmers typically irrigate during the night in cooler, more favorable conditions from 9 p.m. to 5 a.m., explains Tangen, as it interrupts valuable sleep. “It’s a never-ending hassle during the summer,” he says. “One hot summer when we travelled around talking to farmers, the irrigation issue came up time and again. We started to realize how... occupied farmers are with the irrigation process. It became clear to us that they needed a high-tech solution.”

Need to Know

Nordic nRF9160 SiP features both LTE-M and NB-IoT, allowing it to accurately relay the position of assets. It can also communicate with Cloud services to receive cellular base station coordinates to determine position, offering a signal to your points of interest. Developed specifically for the irrigation market, the solution uses the GNSS and cellular localization capabilities of Nordic’s nRF9160 cellular IoT SiP and 7Sense’s proprietary Cloud service to provide the user with insights and notifications about the sprinkler cart’s location, speed and the expected finishing time of the irrigation circuit. This data can be transmitted to the Cloud via the nRF9160 SiP’s multimode LTE-M/NB-IoT modem. From there, the data can be sent to the farmer’s smartphone. Using the 7Sense iOS/Android app, agriculture workers can view sprinkler cart locations, receive alerts for leaks and manage their fleet of carts. It also provides a map view of irrigation routes for better management. By notifying farmers when carts pass certain points the service allows for more efficient irrigation management and planning. Farmers can also receive notifications if a cart has overturned or stopped moving, when previously they would have to manually locate a cart that failed to complete its route to identify any issues.

Leak detection capabilities

The wireless sensor can be easily retrofitted to almost any type of existing irrigation system. Using 7Sense’s patented non-intrusive flow detection, the device can immediately sense any loss of water in order to alert the farmer. The device can analyze micro vibrations in the water pipe to detect changes in flow, which may indicate leaks, using the nRF9160’s powerful ARM Cortex-M33 application processor. The 7Sense Irrigation Sensor Gen II boosts a battery life of up to two years, thanks in part to the class-leading low power consumption of the nRF9160 SiP. “This low power consumption was a major drawcard for the nRF9160 SiP,” adds Tangen. “However, we also needed an application processor that was powerful enough to provide leak detection calculations, as well as reliable tracking. The Nordic SiP delivered on all counts.”

Considering 3.2 billion liters of water are lost through leakage every day in the U.K. (according to water management specialist Aquacare), fixing any leaks as soon as possible is critical. Moreover, water leaks can be incredibly expensive for farmers in terms of the cost of the water, as well as the time, energy and resources required to locate and fix them – in addition to the cost of any damage to crops in the event of a flood. “The 7Sense exemplifies a hands-off approach to water management, allowing everything to be done remotely,” says Tangen. “It not only reduces water waste, but also means that manual resources can be reallocated from monitoring irrigation systems to more productive tasks.”

The 7Sense exemplifies a hands-off approach to water management, allowing everything to be done remotely.
A Nordic powered edge intelligence solution for the electric vehicle (EV) value chain has been developed by India-based tech company Intellcir. The company manages data across batteries, swap stations, charging infrastructure, and vehicles, making it possible for anyone to build solutions on top of the data and Intellcir’s edge intelligence hardware and software stack. The solution can be used by automotive OEMs, battery manufacturers or battery energy-as-a-service companies, as well as for last-mile solution providers.

Intellcir’s edge intelligence hardware, Flashy, is powered by Nordic Semiconductor’s nRF52833 SoC. In addition, the gateway integrates a cellular modem for device-to-Cloud data transmission, allowing the user to send over-the-air device firmware updates (OTA-DFUs), as well as deploy edge analytics to their remote assets.

In addition to the nRF52833’s powerful processor and the cellular modem, Flashy incorporates a GPS module, accelerometer, multi sensor interface and edge processor. This enables customers to deploy edge analytics on their assets. The Nordic SoC provides seamless Bluetooth LE wireless connectivity for off-line diagnostics of the Flashy, and for connecting assets and data to the Cloud in the absence of cellular coverage. The solution also offers end-to-end data security while maintaining ultra low power consumption.

Intellcir’s software stack supervises the devices to ensure reliable data delivery. This, combined with Intellcir’s edge intelligence hardware, as well as a solid infrastructure setup for data storage on a scalable Cloud infrastructure, provides the user complete flexibility across the full stack.

In-Depth look at Nordic’s wireless solutions

**Telematics & Transport**

A Nordic powered gateway forms heart of smart vehicle ecosystem

A Nordic powered edge intelligence solution for the electric vehicle (EV) value chain has been developed by India-based tech company Intellcir. The company manages data across batteries, swap stations, charging infrastructure and vehicles, making it possible for anyone to build solutions on top of the data and Intellcir’s edge intelligence hardware and software stack. The solution can be used by automotive OEMs, battery manufacturers or battery energy-as-a-service companies, as well as for last-mile solution providers.

Intellcir’s edge intelligence hardware, Flashy, is powered by Nordic Semiconductor’s nRF52833 SoC. In addition, the gateway integrates a cellular modem for device-to-Cloud data transmission, allowing the user to send over-the-air device firmware updates (OTA-DFUs), as well as deploy edge analytics to their remote assets.

In addition to the nRF52833’s powerful processor and the cellular modem, Flashy incorporates a GPS module, accelerometer, multi sensor interface and edge processor. This enables customers to deploy edge analytics on their assets. The Nordic SoC provides seamless Bluetooth LE wireless connectivity for off-line diagnostics of the Flashy, and for connecting assets and data to the Cloud in the absence of cellular coverage. The solution also offers end-to-end data security while maintaining ultra low power consumption.

Intellcir’s software stack supervises the devices to ensure reliable data delivery. This, combined with Intellcir’s edge intelligence hardware, as well as a solid infrastructure setup for data storage on a scalable Cloud infrastructure, provides the user complete flexibility across the full stack.

**Connected Home**

Bluetooth LE and Wi-Fi power advanced Matter designs

Arizona-based hardware and firmware engineering firm Fanstel has launched a series of dual Bluetooth LE and Wi-Fi modules. The WT02C40C with on-chip Bluetooth LE and Wi-Fi, and the WT02V40V with vertically-mounted chip antennas for Bluetooth LE and Wi-Fi, allow the modules to be easily integrated into consumer electronics, automotive and medical devices.

**Nordic Partner Program**

Goliath, KYOCERA AVX and SODAQ expand Nordic Partner Program

IoT Cloud services provider Goliath (solution partner), IoT engineering design specialist SODAQ (solution partner) and advanced antenna manufacturer KYOCERA AVX (design and solution partner), have joined Nordic Semiconductor’s rapidly expanding Nordic Partner Program (NPP).

KYOCERA AVX provides active and passive antenna solutions for industrial IoT, consumer electronics, automotive and medical applications. The company has prototyping and testing facilities worldwide to support customers during the design and development phases of their products. KYOCERA AVX provided RF and antenna development support to IoT technology company Digital Matter, during development of its Oyster 3 asset tracking and management solution which used Nordic’s nRF9160 SiP and nRF5580 SoC.

The collaboration ensured optimum wireless performance for the end customer.

For cost-optimized designs requiring 2.4 GHz single band connectivity

**World-Friendly™ IoT**

The collaboration ensured optimum wireless performance for the end customer.
Today’s IoT isn’t as secure as it could be because many devices have been built with protection as an afterthought. This ‘last-minute’ approach leads to unforeseen vulnerabilities that can be exploited. According to the PSA Certified 2023 Security Report, the number of cyber attacks on smart devices have tripled since 2021. IoT security by reaches range from the loss of personal data from a hacked wearable to a risk of illness or even death due to compromised medical devices such as pacemakers and insulin pumps. Fortunately, the electronics industry is not standing still. Regulations and standards are being adapted to set a baseline for IoT security. In many markets there is a need for security to be considered at the earliest stages of design. One standard, which is helping developers achieve this is PSA Certified. Spearheaded by microprocessor IP vendor, Arm, and some global independent test labs, PSA Certified offers an IoT security framework that implements trusted protection for silicon, software, services and end-products. Nordic’s nRF9160 and nRF5340 are PSA Certified Level 2 and the nRF52840 to Level 1 which demonstrates they implement PSA-Root of Trust (RoT). The system software for example, a real time operating system (RTOS) uses this PSA-RoT to implement its own security.

Building products based on PSA Certified devices makes it simpler to gain end-product certification. There are three levels of certification covering chips, system software and end-products. Nordic’s nRF9160 and nRF5340 are PSA Certified Level 2 and the nRF52840 to Level 1 which demonstrates they implement PSA-RoT of Trust (RoT). The system software for example, a real time operating system (RTOS) uses this PSA-RoT to implement its own security. The developer can then build the end-product using the certified silicon and system software.

Technical Briefing

A Security First Approach to IoT Product Design

IoT devices are becoming the focus for cyber attacks. But the PSA Certified IoT security framework is helping developers build products with stronger defenses.

A Key Requirement Underpinning Many International Regulations is Security to be Considered from the Very Earliest Stages of IoT Product Design

Greater security can be achieved by isolating areas that need to be secure from those that can or need less sensitive information. Leaving less critical areas with low protection reduces the overall cost of security without increasing risk. Information can be extracted from the secure area via an application programming interface (API), but no security critical information is accessible via the API. For example, a non-secure processing environment (NSPE) may utilize APIs to encrypt data without ever having access to the encryption keys or the underlying cryptographic implementation resources of the secure processing environment (SPE). The device might also feature secure storage for security critical data and assets. (See Panel Using trusted firmware to protect critical data.) Every IoT product should be uniquely identified and provide evidence it is the device it claims to be. Such identification prevents unauthorized devices joining a network and opening up a vulnerability. Moreover, each device should be able to run the cryptography needed for secure communication without the information being exposed to the application software when it could be exploited by an attacker. Finally, it’s important security is considered at all stages of a product’s lifecycle – not just when it’s in the field. Examples include debugging, commissioning and configuration.

A Four Step Approach to Security

From a developer’s perspective security can be seen as complex and expensive. Adding security considerations to a project schedule can also be seen as a threat to extend time to market.

The framework simplifies a secure-by-design strategy by dividing it into four steps: threat modeling and security analysis (‘architect’), implementation of firmware source code (‘implement’), and independent testing (‘certify’).

To illustrate how the framework works, let’s consider a threat modeling process. The first step is to identify the assets that need protecting – these are things like encryption keys, identification certificates and data. Next the developer should think about how the assets could be attacked, for example, through an attack on the network, or a direct attack through a chip interface. The third step is a risk analysis (impact x probability). The items or data under the greatest risk of attack are those that should be tackled first. Finally, there’s mitigation – what the developer needs to do to protect against attack.

The developer might, for example, consider his or her assets to be firmware, credentials and data. For the firmware, the security requirement is integrity, and the threat is tampering. The vulnerability might be a malware, a software bug, a weakness in the main storage, an insecure ITAG interface or lack of protection during a device firmware update. The effect of exploiting any of these vulnerabilities is the opportunity to store malware and then launch a distributed denial of service (DDoS) attack. One way to mitigate against such an attack would be to implement a secure bootloader. Such software would ensure that even malware has installed via a vulnerability it wouldn’t run.

The threat modeling is completed the developer must specify hardware and software that can support the desired protection against the threats identified during the exercise. So, for example, if the threat modeling reveals a need for a cryptographic accelerator, secure storage and isolation a suitable solution could be to use product line Nordic’s nRF9160 or nRF5340 (which are PSA Certified security best-practice devices and offer these capabilities).

Gaining Certification

Building products based on PSA Certified devices makes it simpler to gain end-product certification. There are three levels of certification covering chips, system software and end-products. Nordic’s nRF9160 and nRF5340 are PSA Certified Level 2 and the nRF52840 to Level 1 which demonstrates they implement PSA-RoT of Trust (RoT). The system software for example, a real time operating system (RTOS) uses this PSA-RoT to implement its own security. The developer can then build the end-product using the certified silicon and system software.

OEMs building their devices on certified silicon and system software can inherit their certifications for the end-products. PSA Certified aligns with the standards and regulations demanded by international markets such as European Telecommunications Standards Institute’s (ETSI) EN 300 440 and National Institute of Standards and Technology’s NIST 8259A. Such alignment helps when applying for end-device certification by reducing engineering overhead and speeding up time to market.

Protecting the IoT against malicious attack can only be assured by building in security during the earliest stages of design. PSA Certified assures Nordic’s silicon incorporates standard proven and trusted protection. That makes it easier for developers to ensure their products are also protected.

A Nordic webinar entitled Designing Secure IoT Products is available from bit.ly/43L.Fyay.
## Nordic Product Guide

This handy summary describes all of Nordic's IoT solutions.

### RF SoCs and SiP

<table>
<thead>
<tr>
<th>SoC/MCU</th>
<th>Series</th>
<th>Package</th>
<th>Pinouts</th>
<th>Features</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>nRF9160</td>
<td>nRF916x</td>
<td>TQFP64</td>
<td>64 pins</td>
<td>BLE, Wi-Fi, GER, 6LoWPAN, NFC, GPS</td>
<td>Industrial, smart home, IoT, audio</td>
</tr>
<tr>
<td>nRF52840</td>
<td>nRF52x</td>
<td>QFN48</td>
<td>48 pins</td>
<td>Bluetooth LE, Thread</td>
<td>Industrial, smart home, IoT, audio</td>
</tr>
<tr>
<td>nRF52833</td>
<td>nRF52x</td>
<td>QFN32</td>
<td>32 pins</td>
<td>Bluetooth LE, Thread</td>
<td>Industrial, smart home, IoT, audio</td>
</tr>
<tr>
<td>nRF52820</td>
<td>nRF52x</td>
<td>WLCSP94</td>
<td>94 pins</td>
<td>Bluetooth LE, Thread</td>
<td>Industrial, smart home, IoT, audio</td>
</tr>
<tr>
<td>nRF52811</td>
<td>nRF52x</td>
<td>WLCSP94</td>
<td>94 pins</td>
<td>Bluetooth LE, Thread</td>
<td>Industrial, smart home, IoT, audio</td>
</tr>
<tr>
<td>nRF52810</td>
<td>nRF52x</td>
<td>WLCSP94</td>
<td>94 pins</td>
<td>Bluetooth LE, Thread</td>
<td>Industrial, smart home, IoT, audio</td>
</tr>
</tbody>
</table>

### Power Management ICs

<table>
<thead>
<tr>
<th>IC</th>
<th>Features</th>
<th>Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>nPM1300</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>nPM1000</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>nPM6001</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

### Range Extender

**nRF21540**

**Description:** The nRF21540 is an RF front-end module (FEM) that improves range and connection robustness for Nordic nRF70 Series ICs.

**Applications:** As a Wi-Fi range extender, it can be used with Nordic’s extended temperature-qualified nRF5340, nRF92833, and nRF92820 SoCs in industrial applications.

**Tech Spec**

- **Output power:** Adjustable in small increments up to +2 dBm
- **Receive gain and noise figure ratings:** 15 dB receive gain, 2.1 dB noise figure
- **Input supply:** 1.7 to 5.5 V
- **Package:** 40x4 mm QFN21

**Development tools:** nRF21540 DK and nRF21540 SoC. It is a shield house with nRF52 and nRF53 Series ICs.

### Cloud Services

**nRF Cloud Services**

**Description:** nRF Cloud Services are optimized for Nordic’s low power IoT Devices. nRF Cloud Services support Device-to-Cloud, Cloud-to-Cloud, and Cloud-to-Cloud. In the former, the device connects directly to nRF Cloud. In the latter, connection is to a customer’s Cloud that then connects to nRF Cloud’s REST API.

**Services:** nRF Cloud Services are offered by nRF Cloud and include GPS, cell-based and Wi-Fi assistive locationing. The product supplies accurate, real-time data for IoT devices. The A-GPS service reduces time-to-first-fix. The result is lower latency and lower power consumption.

**Additional features:** Supports Cloud-to-Cloud connections via device provisioned to a customer Cloud provider. Supported products include nRF53 Series ICs and nRF70 Series ICs.

### Tech Spec

- **Location services:** Assisted GPS, Assistive GPS, Single-Cell (SCELL), Multi-Cell (MCCELL), Wi-Fi
- **Efficiency:** Supports Cloud-to-Cloud connections via device provisioned to a customer Cloud provider.

**Support:** The nRF Cloud Services are offered as a service hosted by non-Nordic products.

**Applications:** Tracking, RTLS, and other applications requiring location data.

**Tech Spec**

- **Compliance:** IEEE 802.11a/b/g/n (Wi-Fi 4), IEEE 802.11ac (Wi-Fi 5), and Bluetooth LE
- **Features:** Low power, good coexistence with Bluetooth LE, and high throughput

**Development tools:** nRF21540 DK and nRF21540

**Applications:** Smart tracking, smart home, industrial, military, and more.
nRF54H20 SoC

Superior processing power
Generous amount of memory
Best-in-class radio
State-of-the-art security
All integrated into one compact ultra low power SoC