WQ

WIRELESS QUARTER

Issue 2, 2023

SECURE BY DESIGN: FIGHTING THE THREAT OF IoT CYBER ATTACKS

PLANET BLUETOOTH: THE NON-STOP EVOLUTION OF BLUETOOTH TECHNOLOGY

Retail Therapy

Wireless tech is rejuvenating the shopping experience for both retailer and consumer

NORDIC LAUNCHES 4TH GENERATION SOCs

AURACAST TRANSFORMS AUDIO SHARING

SAVING WATER DOWN ON THE SMART FARM

NORDIC SEMICONDUCTOR

Welcome

Geir Langeland
EVP Sales & Marketing

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.

> "The wireless technology 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

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 Woolls-King *awk@ecritech.media*

Creative Director
Sam Grimmer *sam@ecritech.media*

Prepress
Nathan Sargent

Print & Distribution
Printech Europe

NORDIC SEMICONDUCTOR

nordicsemiconductor NordicSemi nordic-semiconductor @NordicTweets devzone.nordicsemi.com

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

Contents

WQ WIRELESS QUARTER
Issue 2, 2023
SECURE BY DESIGN: FIGHTING THE THREAT OF IoT CYBER ATTACKS
PLANET BLUETOOTH: THE NON-STOP EVOLUTION OF BLUETOOTH TECHNOLOGY
Retail Therapy
Wireless tech is rejuvenating the shopping experience for both retailer and consumer
NORDIC LAUNCHES 4TH GENERATION SOCs
AURACAST TRANSFORMS AUDIO SHARING
SAVING WATER DOWN ON THE SMART FARM
NORDIC

News

The latest developments from Nordic Semiconductor

Internet of Things

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 5.4 and future Bluetooth specifications, plus 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 Svenn-Tore 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 those we see today."

"A disruptive product like the nRF54H20 happens through a long-term commitment to R&D, and Nordic has been willing to make that commitment," says Svein-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 Holstad, EVP Product Management at Nordic.

"It is a truly worthy successor to our nRF51, nRF52, and nRF53 Series, and we expect our nRF54 Series to again disrupt the low power wireless segment."

Building & Construction

Smart tape measure records accurate measurement data

U.S. based REEKON Tools 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 immediately appears on the device's built in OLED display for a live 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 T1 Tomahawk uses Nordic's nRF52832 SoC for wireless connectivity between the tape measure and a smartphone while providing ample memory for data storage.

The unit can store over 1000 readings.

From the ROCK app users can view their stored measurements. These can be further edited into material optimizations, layouts and external program exports.

"REEKON Tools believes in reducing waste on job sites through error reduction," says Kostas Oikonomopoulos, CTO at the firm. "The T1 Tomahawk achieves this by providing accurate and robust measurement."

Logistics & Transport

Beacon tag creates wireless manifest for helicopter crews

Canada based IQonboard has developed a Bluetooth LE beacon tag that creates what is claimed to be the world's first self loading digital manifest. The IQtag has been field tested for remote operations across wildfire, mining and personnel transport applications.

The IQonboard system comprises the patent pending IQtag beacon tag—a small (5.3 by 1.3 cm), lightweight (22 g), IP67-rated crushproof wearable using Nordic Semiconductor's nRF52832 SoC based I-SYST Blyst Nano module—along with the associated IQonboard app for iOS smartphones and tablets.

Once allocated and attached to clothing or cargo, each IQtag 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 and what is onboard 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," explains Vincent Hoog, 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.

Asset Tracking

Pallet trackers provide location updates and environmental data

A range of asset trackers designed for use in transport pallets has been launched by U.K. based tech firm System Loco. The LocoTrack HGC4 and RM2Track are embedded in composite pallets during maufacture, 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 HGC4 and RM2Track employ a combination of location technologies including GNSS, Wi-Fi, cellular IoT 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.

"As 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 Essafi, COO 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 re-use of pallets, as well as recycling at end-of-life."

In Brief

NETWORK-BASED WEATHER FORECASTING

Telco leader Vodafone is opening up its network to a rainfall monitor, underpinned by technology from Spanish network monitoring and optimization specialist Wireless DNA. The meteorological technology analyzes network data and the behavior of wireless signals—which are sensitive to atmospheric conditions and can be disrupted by precipitation—and takes into account the many factors that influence signal quality to measure rainfall across a vast area. The service is expected to be used to better project extreme weather instances and help prevent floods, wildfires and other natural disasters.

IN-CAR BLUETOOTH HIGHLY RATED BY DRIVERS

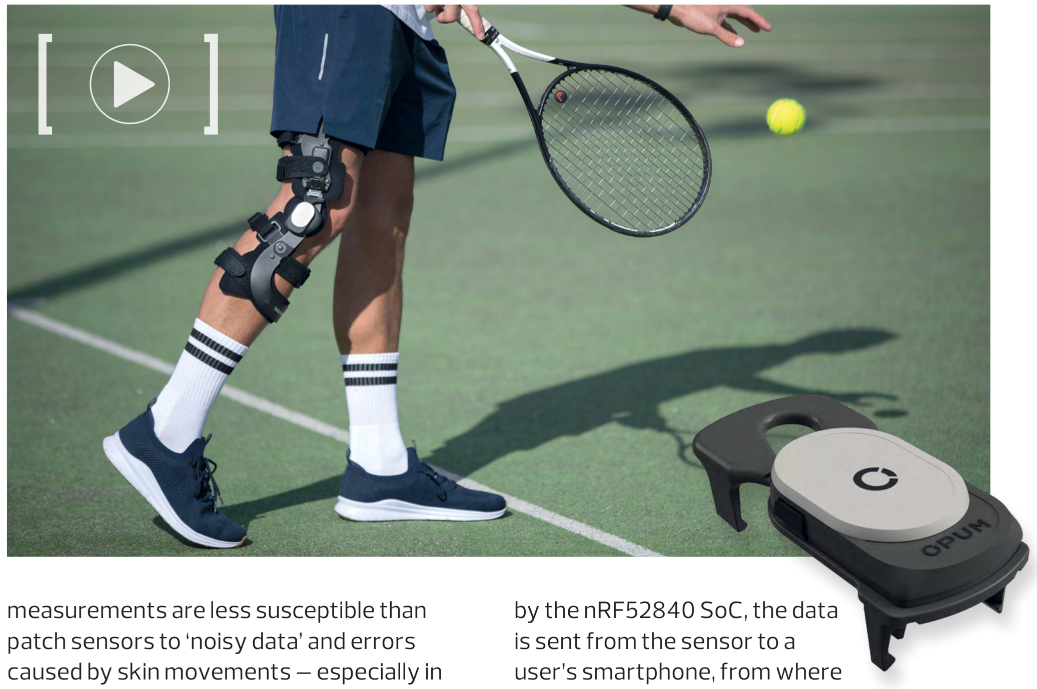
A survey of 2000 British motorists by U.K. car dealership Motorpoint found in-car Bluetooth was the top item of modern car technology drivers could not live without. Bluetooth rated ahead of LED lights, keyless entry, smartphone integration and adaptive cruise control. The survey rated in-car Bluetooth the tenth most important driving innovation ever. In top spot was multiple airbags, with GPS satellite navigation, reversing cameras, power steering and parking sensors taking out the top five positions. Among inventions rated less important than Bluetooth, were electric windows, blind spot alarms, and autonomous vehicles.

AUDIO TRANSMITTERS MAKE ENTERTAINMENT EASY

Avantree Corp. has launched another Nordic nRF52832 powered wireless audio transmitter solution following last year's release of Quartet. Quartet enabled multiple sets of headphones to be wirelessly connected to a single source. The new Avantree Shift solution includes two audio transmitters and two sets of headphones, allowing transmitters to be placed in separate rooms with multiple TVs, set to a specific channel. Headphones can easily be connected to either transmitter by selecting the corresponding channel, enabling users to move from room-to-room and switch the audio source streaming to their headphones.

Sports & Fitness

Wireless knee supports 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 turnkey solution—which also comprises software, electronic health record integration and clinical monitoring for orthopaedic practices—is the Digital Knee wireless goniometer, a Nordic nRF52840 powered sensor device that continuously measures the range of motion of the joint.

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 clinical data analytics including machine learning (ML)-powered activity and posture recognition and tracking.

Digital Knee clips on to wearables including therapeutic braces. It can be used as a standalone goniometer when bracing is not needed, such as post knee replacement.

"[When] anatomically aligned on the affected limb, [the product] ensures the measurements are less susceptible than patch sensors to 'noisy data' and errors caused by skin movements – especially in patients with excess soft tissue," explains Paul Mallinson, CTO, OPUM Technologies.

The integrated Nordic nRF52840 SoC based Raytac MDBT50Q-1MV2 module acts as 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 SoC, the data is sent from the sensor to a user's smartphone, from where the associated app provides 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.

Sustainability

Breakthrough fights food waste

Wireless tech developed by the University of California San Diego allows users to check which items in their fridge are about to expire saving costs and reducing waste.

The technology combines a chip integrated into product packaging and software for a smartphone. The smartphone then becomes capable of identifying objects based on signals the embedded chip emits. The smartphone equipped with the software can also be used as an RFID reader.

The work harnesses technical breakthroughs in so-called backscatter communication, which uses signals already generated by a smartphone which are then directed back to the device in a format it can understand.

The tiny custom chip requires so little power that it can be entirely powered by LTE signals, using RF energy harvesting.

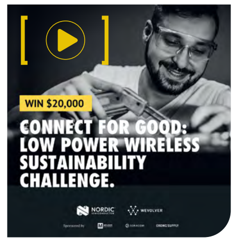
"This approach enables a robust, low-cost and scalable way to provide power and enable communications in an RFID like manner, while using smartphones as the devices that both read and power the signals," says Patrick Mercier, a professor in the Department of Electrical and Computer Engineering at the University of California in San Diego.

The researchers achieved this breakthrough by harvesting power from LTE smartphone signals and buffering this power onto an energy storage capacitor. This in turn activates a receiver that detects Bluetooth signals, which are then modified into reflected Wi-Fi signals. The software update for the mobile comprises a bit sequence that turns the Bluetooth signal into something that can be more easily turned into a Wi-Fi signal.

The device has a range of one meter. Adding a battery would boost range, but increase costs.

Sustainability

Connect for Good Challenge tackles sustainability issues



Nordic Semiconductor and the Connect for Good: Low Power Wireless Sustainability Challenge is inviting organizations, engineers, start-ups and students to submit a project that uses low power wireless tech to solve issues related to the UN's Sustainable Development Goals (SDGs). All entries will incorporate Nordic's nRF9160 DK - a single-board development kit for evaluating the nRF9160 SiP for cellular IoT connectivity.

Nordic partnered with sponsors Mouser Electronics, Soracom and Crowd Supply to launch the Connect for Good Challenge on the Wevolver platform. Competition entries close on October 12, 2023.

"The winning design will be an innovative product that is energy efficient, helps fight climate change, protects ecosystems, or is beneficial to society," says Geir Langeland, Nordic's EVP Sales and Marketing. "We are excited to have the support of industry leading sponsors committed to encouraging engineering innovation for the future."

The challenge entries will be reviewed by a five-person judging panel from Nordic, the sponsors and Wevolver. Entries will be judged based on the technical and commercial feasibility, the level of innovation and the potential impact on the selected SDGs.

The grand prize winner will receive $20,000 along with a year's subscription to nRF Cloud 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.

Smart Health

Smart breast pump tracks pumping sessions

Swiss company Medela has launched a smart breast pump that uses Nordic's nRF52832 to wirelessly track pumping sessions. The Freestyle Hands-free Breast Pump uses the wireless connectivity enabled by the SoC to connect with the user's smartphone. From the mobile, users can view their session data, monitor the device's battery life, and record and view their freezer supply of milk.

The product weighs only 76 g and can fit discretely inside the user's bra. The system—including the pump—weighs less than 450 g, making it one of the lightest in-bra systems on the market, according to the company. The device is comprised of the pump, two collection cups, four breast shields in two different sizes (21 and 24 mm) and two membranes.

Connected Health

Ear worn pulse oximeter enables continuous monitoring

A wireless, non intrusive, ear worn pulse oximeter for medical grade, continuous oxygen monitoring and low oxygen alerts has been developed by U.S. based health tech start-up OxiWear. The device is designed to support the more than 10 percent of the global population at risk of hypoxia. The disease can result in various organs being damaged.

Worn on the ear, OxiWear accurately monitors a user's oxygen levels in real time. By using the device, individuals can better manage hypoxia, helping to avoid hospitalizations and medical testing.

"OxiWear is ... ideal during physical activity when the user's hands might otherwise be preoccupied," says George Beckstein, the firm's CTO.

The OxiWear device features an integrated optical sensor for photoplethysmography (a light source and a photodetector used to measure volumetric variations in blood circulation) and an accelerometer for motion detection. These sensors are overseen by the Wafer Level Chip Scale Package (WLCSP) version of Nordic Semiconductor's nRF52840.

The nRF52840 SoC enabled Bluetooth LE connectivity allows real time health data to be relayed wirelessly from the device to the user's smartphone, from where an accompanying app displays the blood oxygen (SpO_2) and heart rate information.

OxiWear also employed Nordic's Power Profiler Kit II (PPK2) to identify parts of the design that were increasing power consumption, allowing the battery life to be optimized and extended.

In Brief

DIGITAL TECH TRANSFORMS PUBLIC SERVICES

As part of the Mobile World Congress 2023 exhibition's 'Accelerating Digital Transformation of Public Services' session, global telco Huawei launched the Inclusive Connectivity 2.0 Solution. The solution facilitates network construction in remote areas with complex factors. It combines datacom, optical networks and wireless products, designed to bring connectivity to remote mountainous areas. The ultimate goal is to achieve inclusive and equitable digital services. The integrated Cloud and network architecture enables the public sector to easily and securely exchange data across networks and regions, offering one-stop services for citizens.

GROWTH FOR ACCESS CONTROL MARKET

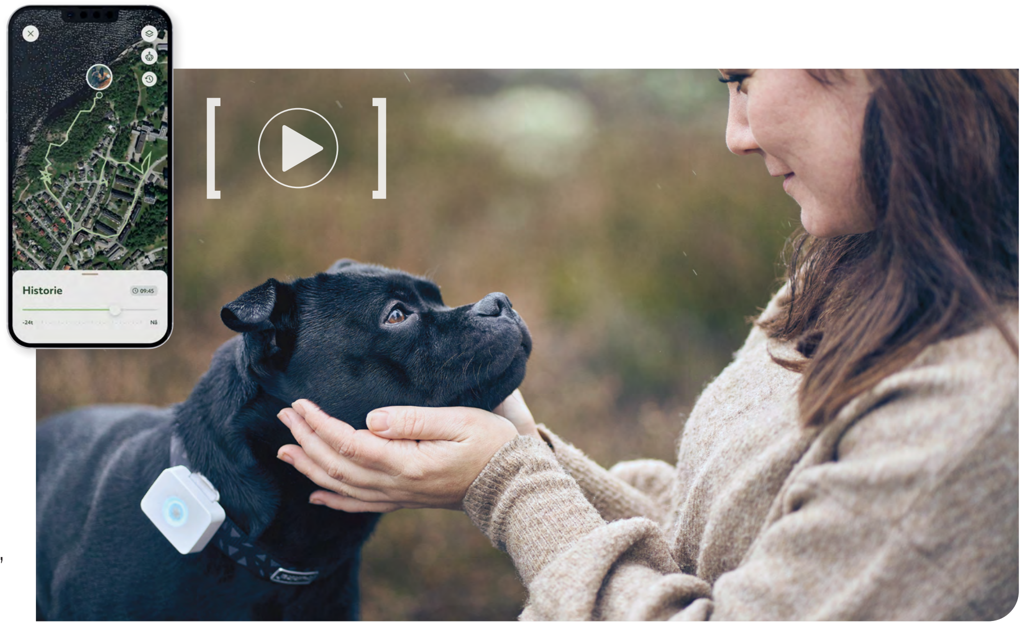
The global access control market size is projected to grow from $9.9 billion in 2023 to $14.9 billion by 2028, according to a new report, *Global Access Control Market by Offering*. The market is expected to grow at a CAGR of 8.4 percent from 2023 to 2028. Security smart cards and biometric access systems play an important role in preventing minor security risks in offices. These systems control the access of individuals in offices and monitor their attendance. The research suggests increased use of Cloud-based services will create lucrative opportunities for suppliers. North America holds the largest share of the global access control market.

ASSISTIVE LISTENING DEVICE CUTS OUT NOISE

A universal assistive listening device developed by U.K. based AudioTelligence helps those with hearing difficulties hear more clearly in noisy settings with or without hearing aids. According to the company, the compact and portable Orsana device will add hearing enhancement to any brand of LE Audio enabled hearing aids, or improve their ability to hear through background noise by connecting wirelessly with the low latency required for face-to-face conversations. The device also has the ability to combine with the new Bluetooth LE Audio broadcast capability, Auracast, enabling several people to connect to one device.

Animal Tracking

Pet tracker uses machine learning to detect animal health problems



Norway 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 nRF52811 SoC. 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 device's integrated inertial measurement unit (IMU)—with accelerometer, magnetometer and gyroscope—records the animal's different 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 computations.

From the iOS and Android Lildog or Lilcat 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. The device employs a 500 mAh Li-Po battery, which can last up to six days between charges, thanks in part to the ultra low power characteristics of the Nordic solutions.

"The nRF9160's Arm processor made it possible to integrate our advanced machine learning functionality while Nordic's comprehensive development environment and nRF Connect SDK enabled us to focus on our application code and use of sensors rather than the RF firmware," says Morten Sæthre, CEO of Lilbit.

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 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 by the paper, the sodium chloride solution becomes ionized and current flows through the graphite deposited by the pencil, 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 tiny 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 alerting parents.

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 Huanyu 'Larry' Cheng, Associate Professor of Engineering Science and Mechanics at Penn State University.

"The skin will function differently based on those underlying conditions, which we will be able to flag and possibly characterize using the sensor," says Cheng.

Internet of Things

'Traffic cop' algorithm keeps robots on task

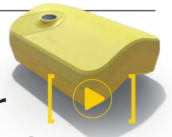
Multiple robots simultaneously relaying time sensitive information over a wireless network can lead to a traffic jam of data, while even information that manages to get through might be too old for an up-to-date report. Drones searching a disaster zone, for example, rely on recent data to locate survivors or report potential hazards.

Now Massachusetts Institute of Technology engineers have developed a solution. The method tailors any wireless network to handle a high load of time sensitive data coming from multiple sources. This approach, called WiSwarm—a scheduling algorithm that can be 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 observing a 'last in, first out' protocol. Rather than attempting to take in data from every source at every moment, the algorithm determines which node of a network should send data next.

The team used their method to tweak a Wi-Fi router, demonstrating that the tailored network could act like an efficient 'traffic cop' – able to prioritize the freshest data to keep multiple vehicle-tracking drones on task. This offers a practical way for multiple units to communicate over Wi-Fi without needing to carry bulky equipment onboard.

Smart Agriculture

Irrigation sensor detects water leaks



Norwegian company 7Sense has launched a cellular IoT irrigation sensor for water leak detection and location monitoring for sprinkler carts. The 7Sense Irrigation Sensor Gen III is 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 change in flow and potential leaks.

Smart Home

Smart home sensors support Amazon Sidewalk

Browan Communications has launched its latest line of MerryIoT sensors with support for Amazon Sidewalk, a secure, free-to-connect community network designed to provide reliable 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, pg10.*)

"Amazon Sidewalk makes it possible to install our IoT sensors at the edge of a home network," says Mohammed Alhennawi, Sales Director at Browan 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."

The MerryIoT smart home sensors provide air quality, motion and water leak detection, as well as indicating open doors and windows. Each device also integrates up to three additional sensors for temperature, humidity, tilt or tampering, as well as an 80 dB alarm.

To simplify the development of Amazon Sidewalk-enabled products, developers can use Nordic's nRF Connect SDK, a scalable and unified software development kit for building products based on all the company's nRF52, nRF53 multiprotocol, nRF70 Wi-Fi and nRF91 Series cellular IoT devices.

By the Numbers

14% growth in shipments

Global cellular IoT module shipments grew 14 percent YoY in 2022 to register record high annual volume, according to Counterpoint's latest *Global Cellular IoT Module 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.

$4.9 billion by 2028

Kaleido Intelligence reports that smart manufacturing will generate almost $5 billion in cellular IoT connectivity revenue by 2028, a CAGR of 36.7 percent from an expected $772 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.

$63.7 billion by 2032

The global wireless charging market will exceed $63.7 billion by 2032, up from $7.7 billion in 2022 and $9.6 billion in 2023, according to a new report by Market.us. Increasing market demand for wireless charging solutions 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.

Massive IoT

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 SoCs, 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+'). 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 Svenn-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 nRF91 Series SiPs, the nRF9161 and nRF9131, evaluation and development tools, development software, and nRF Cloud services, plus world-class technical support and advice.

The nRF9161 is a complete, targeted globally pre-certified SiP 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.*) New features introduced in the nRF9161 SiP modem firmware and on nRF Cloud help customers further reduce power consumption making the SiP ideal for use cases demanding long battery life. The new product also boasts enhanced GNSS and cell-based location performance. The nRF9131 SiP is a feature-compatible alternative to the nRF9161 measuring half the size and offering greater flexibility in design and sourcing for high-volume businesses. By integrating the SoC and RF Front End in a mini-SiP, the nRF9131 eliminates major RF risks and simplifies the manufacturing process compared to the traditional use of chipsets in high-volume designs. The two SiPs are currently available for sampling to key customers.

Nordic's end-to-end cellular IoT solution will accelerate the roll out of massive IoT deployments

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

Development with the new SiPs is through Nordic's unified and scalable nRF Connect SDK. The nRF Connect for Desktop software also offers unique cellular IoT tools for optimizing power consumption and evaluating, monitoring and debugging network connectivity.

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.

Two new sets of services, nRF Cloud Security Services and nRF Cloud Device Management, offer secure remote provisioning, cryptographic identity authentication, device state monitoring and protocol-agnostic connectivity options.

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) interoperability 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 underlying 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 communication, 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.

LE Audio

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

The next generation of Bluetooth audio technology, LE Audio, was created to address the shortcomings of Classic Audio, while making it easier to develop lower complexity, non-proprietary audio products, and ultimately deliver on the promise of high quality audio streaming. In the push towards commercialization, the new audio standard takes advantage of new features which will bring superior sound, support lower latency, reduce power consumption, enhance interoperability and ease the development of new audio device types (*see WQ Issue 1, 2022 pg26*).

Now LE Audio is primed to play an increasingly central role in the way people listen to content and engage with their environment. A report compiled by ABI Research on behalf of the Bluetooth Special Interest Group (SIG), forecasts three billion LE Audio-enabled devices will be shipped in 2027. That figure was 115.5 million in 2022.

One of the most significant new capabilities enabled by the release of LE Audio is Auracast broadcast audio – a location-based broadcast application with a user interface similar to Wi-Fi hotspots. Auracast broadcast audio is a specific set of requirements that uses the Public Broadcast Profile (PBP) specification for a universal format and availability of a public broadcast.

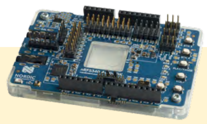
Auracast allows an audio source device like a smartphone, laptop, TV, PA or sound system to broadcast one or several audio streams to an unlimited number of Bluetooth audio receivers. The broadcast would use the Bluetooth 5.2 specification's Isochronous Channels to transmit signals to things like headphones, 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 the Bluetooth SIG. "Following both the LE Audio specification and the Auracast requirements ensures all Auracast transmitters and receivers will interoperate together, globally."

Opening new opportunities

Auracast can create new ways of consuming content and interacting with the environment. With ABI Research suggesting 57 percent of users plan to increase the time they spend using their audio devices, Auracast enables new market opportunities to attract consumers with both public and private broadcast use cases.

The Bluetooth SIG has identified five of these audio use cases. The primary promoted use case for Auracast is for it to become a high-quality, lower cost augmented and assistive listening technology in venues where PA or hearing loop infrastructure is currently deployed. Thanks to the connectionless broadcast capabilities of LE Audio, any number of users will be able to effectively tune into various public audio streams using their own devices. Such a use case opens up wider accessibility for over 1.5 billion people (nearly 20 percent of the global population) living with hearing loss. This is a group the World Health Organization anticipates will grow to 2.5 billion by 2050.



Tech Check

Nordic Semiconductor's nRF5340 Audio DK contains everything needed to start LE Audio development and supports all Auracast features. The kit is configurable and can function as a USB dongle to send or receive audio data from a PC. It can also function as a business headset or a True Wireless Stereo earbud

Auracast can also enable multi-language audio streams in locations that support simultaneous translation services. Users will be able to tune into a relevant stream for their preferred language. Typical use cases include audio broadcast in theaters or cinemas.

A more niche use case enables people to join audio tour systems within venues such as museums, stadiums and tourist attractions. Elsewhere, in addition to TV streaming using LE Audio in the home, individuals could use their Auracast assistant and headset device to tune into the 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 2.5 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."

Bjørn Kvaale
Product Marketing Engineer,
Nordic Semiconductor

Global standards strengthen the IoT

Without standards there's no way to guarantee component parts of a network will work seamlessly together

Nordic Semiconductor is an enthusiastic advocate for wireless standards. Mainstream adoption of wireless technology has consistently been proven to be greatly accelerated if customers can see it is internationally backed and there's a healthy ecosystem of competing suppliers.

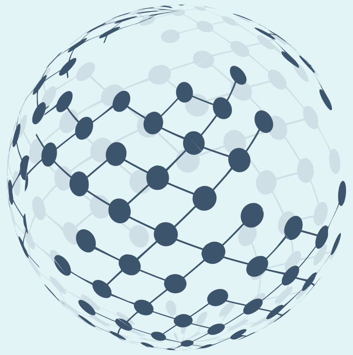
Moreover, standards adoption gives customers confidence the technology will thrive, and they are not subject to the whims of a single supplier. They are also reassured that a device compatible with a given standard will seamlessly interoperate with other devices built to the same standard from a range of different suppliers.

> Nordic is an active and enthusiastic participant in several organizations that are developing standards for the IoT

Bodies such as the Institute of Electrical and Electronic Engineers (IEEE) develop, maintain, and administer specifications that detail how wireless tech should be built. The IEEE, for example, produces a standard that details how the Wi-Fi media access control (MAC) and physical layer (PHY) must be designed. The WLAN standard, IEEE 802.11, encompasses a suite of other standards including 802.11ax (Wi-Fi 6), and is itself part of IEEE 802, a set of LAN standards. (*See WQ Issue 1, 2023 pg36*.) Elsewhere, the 3rd Generation Partnership Project (3GPP), the group originally set up to define standards for 3G networks, is today mapping out 5G and 6G standards. These include those for cellular IoT specifications such as LTE-M and NB-IoT.

Nordic is an active and enthusiastic participant in several organizations developing standards for the IoT. As far back as 2006, the company contributed core expertise in ultra low power wireless design to the Bluetooth LE standard. Bluetooth LE subsequently became one of the fastest growing wireless technologies in history. And more recently, Nordic played a key role in developing the Matter specification (*see WQ Issue 4, 2022 pg10*). Nordic's nRF52 and nRF53 Series SoCs meet the requirements of the Bluetooth v5.3 specification. Similarly, the nRF9160 cellular IoT SiP complies with the 3GPP's latest LTE-M and NB-IoT standards and the nRF7002 complies with IEEE's Wi-Fi 6 standard.

Wireless standards have ensured the best engineering minds work towards the same objective, even if they are employed by competing companies and live in different countries. That makes for rapid advances in IoT technology while ensuring wireless end-products are robust, reliable and interoperable.



Retail Therapy

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

In Short

Despite predictions of the demise 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 to filling shelves, pricing, staffing and maintenance

Retail lighting systems can host connected sensor networks based on Thread or Bluetooth mesh, monitoring equipment, temperature, lighting and people

You might think today's monolithic shopping malls are by design a monument to human convenience, the truth is they are anything but. Their layout is intentionally confusing, designed to make you lose track of your original intentions, and more susceptible to making impulse buys. It's not a theory, it's a scientifically-proven psychological phenomenon known in the retail business as the 'Gruen transfer', named after pioneering shopping mall architect Victor Gruen.

Disorientating shoppers and presenting them with lots of things to buy brings the 'transfer', the moment you stop shopping for something in particular, and start just shopping in general. It's why our most commonly bought items—milk and bread—are usually at the furthest corner of the supermarket, not conveniently at the front.

The irony is Gruen hated such design. His vision was for an efficient shopping mall experience, not one disrupted by bright lights, diversion tactics and illogical floor plans. If Gruen were still with us he might appreciate that today wireless technology is disrupting that disruption, working hard for both retailer and consumer, and completely reinventing retail at every level and in every way.

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 from 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 has become crucial in delivering on this promise.

"It's more important than ever to track goods across the entire value chain in 'real time' - from production to warehouse to customer," says Amicucci. "Accurate data not only helps retailers get products to the consumer faster, it also mitigates against losses."

Bluetooth LE has proved a reliable tech for tracking and monitoring products in transit. For example, wireless devices equipped with thermocouples and accelerometers can be placed in refrigerated and fragile cargoes to monitor temperatures and impacts. They can ensure cold chain deliveries remain within temperature tolerances, and allow remedial action if an excursion occurs. When paired with cellular IoT technology, data can be sent directly to the Cloud, allowing remote monitoring without the need for a smartphone or gateway, and enabling a more holistic view of a supply chain through web-based logistics platforms.

Just-in-time e-commerce has also demanded online retailers' warehouse operations significantly improve their performance. 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 new warehouse near Ontario, California, will sprawl to 371,000 square meters and dispatch 125 million packages a year. Wireless sensors, connected networks, location services and machine learning (ML) will combine to ensure consumers' unpredictable buying patterns, and smaller yet more frequent orders across many and varied product lines, continue to be met with the same or next day delivery promise. (*See WQ Issue 1 2023, pg22.*)

THE DEMAND FOR DIGITAL

It's not only online retailers who have been forced to embrace technology to improve the customer experience, physical stores have also had their digital epiphany (see sidebar *A brief history of retail tech*). Consumers may still prefer the face-to-face retail experience but they expect all the benefits of online shopping.

"Physical stores are becoming more digital as customers expect a similar experience as online shopping," says Amicucci. "Retailers have to be able to respond to the requirements of today's consumer or risk losing them online, or to a digital savvy store. Consumers want to use their smartphones as part of the in-store experience. They may want to know the specific details of a product, compare pricing, or read reviews. If they are a loyal customer, they might expect a special price."

Pricing is both art and science, influenced by factors such as demand, competitor pricing, market conditions and economic trends. Dynamic pricing is one of the most effective ways of increasing sales, because it adjusts prices based on the willingness of customers to make purchases. Airlines and Uber are two examples of businesses that employ 'surge pricing' to dynamically raise prices based on holiday seasons, the time of the week or location. For bricks-and-mortar retailers that required changing price labels. But wireless tech has now transformed dynamic pricing for physical retailers.

Smart shelf labeling systems enable retailers to automatically update products from a central point across multiple stores and branches—or in certain geographic locations—to enhance the customer experience and retailer profitability.

For example, Minew ESL (Electronic Shelf Label), developed by China tech firm Shenzhen Minew

Tech Check

The Minew ESL smart shelf labeling system enables retailers to automatically update individual shelf price labels across multiple stores or locations from a central point

Stratosfy's Tempgenie assists with the early detection of food inventory spoilage and attaining regulatory compliance

The SECO Energy Sensor smart plug employs a sensor to record energy, voltage, power and current variables and keep refrigeration equipment safely humming

Technologies, allows retailers to improve price visibility, reduce both pricing errors and labor costs, as well as offer promotions in near real time. Comprised of a Cloud platform, gateways and Nordic Bluetooth LE-powered shelf labels, pricing commands can be sent wirelessly from the web-based dashboard to store-located gateways, from which point commands are relayed to the smart labels using Bluetooth connectivity. The smart labels can also be used as beacons for marketing to consumers in close proximity via compatible smartphone apps, and for reporting back to the gateway and the Cloud platform, allowing retailers to remotely monitor and manage their stock.

For those in any doubt that smart labeling systems are the future, U.S. retail behemoth Walmart has entered an agreement with a digital retail solution company for the provision of 60 million digital shelf labels across 500 locations over the next 12 to 18 months, leveraging the Bluetooth Special Interest Group's (SIG) new standard for ESL.

STACK 'EM HIGH, WATCH 'EM FLY

If pricing is important, then making sure there are products to sell in the first place is fundamental. There is no bigger retail turn-off for a customer than empty shelf space, but keeping shelves brimming is labor-intensive. Behind the cost of inventory, a retailer's next highest operating expense is payroll. Maximizing both staff efficiency and stock availability requires careful planning.

Rather than relying on an army of stackers to constantly monitor shelf inventory, tech-savvy retailers are now deploying Wi-Fi-connected shelf cameras as well as cellular IoT-based remote monitoring to ensure shelves and products remain well stocked. Combined with Cloud-based AI models to identify empty space, staff can be focused on replenishing shelves only when required.

One company that has embraced cellular IoT wireless technology for remotely monitoring its retail assets is U.S. based frozen drinks company Freezing Point, parent company of consumer 'slushie' brand, Frazil. The company recognized one of the key reasons the 50-year old slushie industry was suffering from sluggish growth wasn't that consumers had lost interest in frozen drinks, 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 hadn't fallen out of favor with ... slushies, they'd fallen out of favor with a poor customer experience," says Kyle Freebairn, CEO of Frazil. To address declining sales the company partnered with Norwegian IoT tech company, 7Sense, to develop a low-cost circuit board based on Nordic Semiconductor's nRF9160 SiP. 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 10 times the industry average, that more than offset the cost of moving to cellular IoT. Together with other innovations such as self-checkouts and contactless payment, tech helps retailers contain 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-won reputation. Wireless IoT solutions are now widely deployed to mitigate against such risks by early detection of food inventory spoilage and automation of previously manual temperature measurements. For example, last year Canadian company Stratosfy launched its Tempgenie solution comprising temperature sensor beacons and a Bluetooth LE to Wi-Fi gateway both integrating Nordic's nRF52840 SoC. 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 potential issue.

Also launched last year was the SECO Energy 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 Mond. "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 are 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

Tech Check

The nRF9160 SiP with integrated LTE-M/NB-IoT modem and GNSS employs an Arm Cortex-M33 as a dedicated application processor, and has 1 MB of flash and 256 kB of RAM. It can support a wide range of retail use cases

A brief history of retail tech

The first form of retail is believed to have begun around 9,000 years ago in the 7th millennium BCE, somewhere, historians believe, in the Middle East. Bargaining and bartering were the earliest examples of commerce, but trading a bushel of wheat for an animal skin was an inexact science, so the invention of money around 5,000 years ago brought greater precision to the retail exchange.

Despite the advent of cash and the obvious need to buy and sell goods, it wasn't until the 1600s that permanent shops with regular trading hours replaced *ad hoc* markets. Even then, the retail experience was unlike anything we would recognize today. Before 1700, the typical retail store had no counter, display cases or changing rooms, they were really walk-in workshops selling a wide variety of goods made on site. It wasn't until the 18th century that shop owners started to get the hang of retail and embrace their customers, allowing them to browse merchandise, as well as touch and feel products.

Thereafter the technology-led revolution in retail 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 allowed 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 chewing gum in a supermarket in Ohio became the first item in the world to have its barcode scanned. The technology meant not only could customers move through the checkout process much faster than before, but inventory tracking methods were also vastly improved.

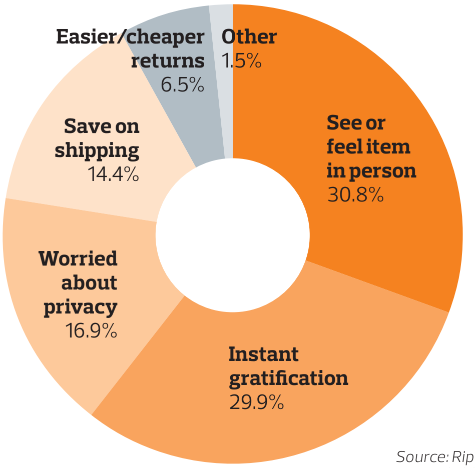
Twenty years later and QR codes were invented, enabling at least 20 times as much data storage as the barcode, and finally—in theory—consigning the price gun and price sticker to history.

State of Play

Why physical retail still rules

Despite the enormous surge in online shopping accelerated by the pandemic, e-commerce has a long way to go before it kills off the high street shop or the shopping mall. Four-out-of-five retail dollars are still spent in a bricks and mortar retail outlet rather than via a web browser. While e-tailers are doing all they can to close the gap and address the digital divide, there are still five key reasons we purchase items in-store instead of online, according to a poll of more than 1200 U.S. shoppers.

What would make you most likely to purchase an item in-store instead of online?



Source: Ripen ecommerce LLC, 2021

and sensor based retail applications such as monitoring refrigeration equipment," says Nordic's Amicucci.

And it's not only refrigeration equipment that can benefit. As many retailers are discovering, their lighting is the perfect conduit for introducing connectivity. Lighting is everywhere in the retail environment, and importantly it is not reliant on battery power. By connecting sensors to a Thread or Bluetooth mesh network in the lighting system, not only can condition monitoring and predictive maintenance applications be supported, but HVAC and the lighting itself can also be optimized. For example, the lighting or store temperature can be automatically regulated to provide comfortable conditions for customers.

Lighting infrastructure can also host occupancy or presence sensors, allowing illumination to be adjusted based on the number of people in parts of the store. The sensors can also be used to track the movement of customers, creating heatmaps to help retailers understand where they spend the most time to optimize store layout.

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 and 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 employees 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 a 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.

> Physical retail is not disappearing, its changing … and the key to success is to embrace new technologies

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

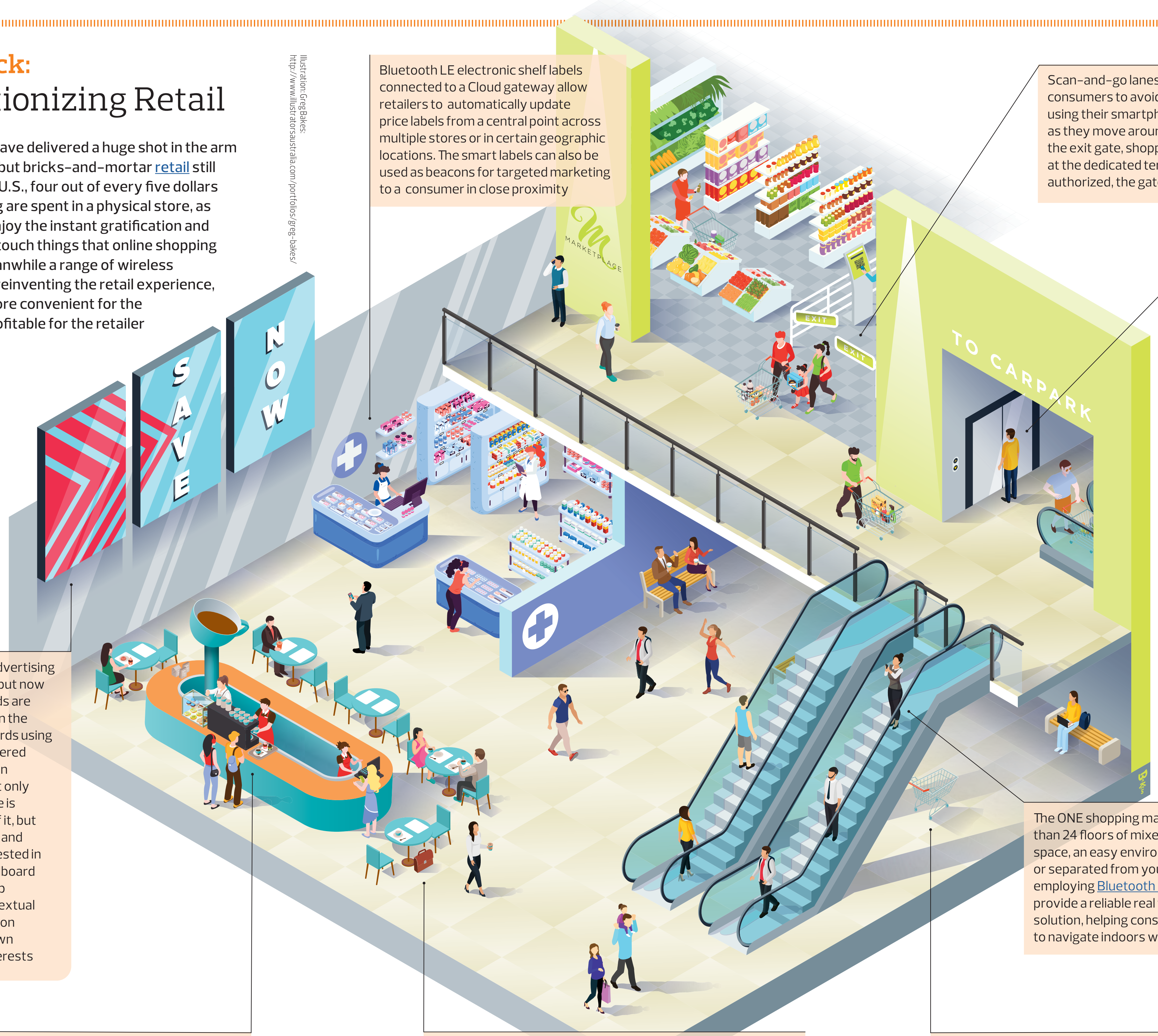


Illustration: Greg Bakes: http://www.illustratorsaustralia.com/portfolios/greg-bakes/

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

Scan-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

With an abundance of valuable merchandise in storerooms, shopping malls demand a high level of security to ensure stock safety. Bluetooth LE and cellular IoT-based systems can ensure only authorized staff gain access to stockrooms and other secure locations. Wireless systems can also log entry and exit data to record who accessed a secure location and when. This data can be reported to the Cloud for further analysis

Highly-targeted advertising is common online, but now electronic billboards are playing catch-up. In the near future, billboards using Bluetooth LE-powered sensors and beacon technology will not only identify if someone is standing in front of it, but who that person is and what they're interested in purchasing. The billboard could then serve up personalized, contextual information based on that person's known preferences or interests

The ONE shopping mall in Hong Kong has no fewer than 24 floors 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

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 attacks very difficult. Bluetooth LE offers more versatility even making electronic payments possible when the terminal's connection to the Internet is disrupted

Shopping centers are big and busy places. The Dubai Mall sprawls for more than one million square meters, so recovering lost possessions can be tricky. A Bluetooth LE asset tag attached to a laptop or bag allows users to locate lost items via an app if within Bluetooth LE range. If out of range, other users' smartphones in a network can also notify the owner if they find the missing item

More than two million shopping carts go missing in the U.S. each year, many of them stolen. Replacing a lost cart can cost a retailer 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 member ID systems. In future cellular IoT devices paired with GNSS and nRF Cloud Location Services could allow retailers to track, monitor and quickly retrieve any purloined 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 Short

Cyber threats are on the rise, including an increase in attacks on IoT devices

IoT devices face particular security challenges based on their characteristics, physical deployment and placement in supply chains

Traditional approaches to IoT security are now shifting, with greater emphasis on integrating security into early design phases

For a short period of time in 2016, the Internet went dark for users of the world's best-known websites. Twitter, Netflix, Reddit, *The New York Times* and dozens of other high-profile sites suddenly went offline, all at once. Millions were left inconvenienced, the result of a cyber security attack several publications later described as having "broken the Internet".

The devastating outage was soon traced to an unexpected source – home security cameras, baby monitors, thermostats and scores of other everyday home appliances. More specifically, hundreds of thousands of these home appliances that were connected to the Internet had been compromised and then effectively taken over by cyber attackers. In what might be the ultimate show of vandalism for our digital times, the attackers unleashed this newly acquired army of connected devices on a critical system that supported many of the world's biggest websites, flooding it with internet traffic until it became overwhelmed and the websites that relied on it became inaccessible.

Unsurprisingly, such a sudden and devastating blackout of a large chunk of the Internet would become a catalyst for global conversations about cyber security. These conversations not only focused on the resilience of the many global businesses and services that had been affected, but—given the attack source—drew attention specifically to the state of security in the emerging world of connected devices, the IoT.

Almost a decade on and many high-profile cyber-attacks later, and with IoT devices even more pervasive in our digital world, getting security right for connected devices is high on the agenda for policymakers, device manufacturers and consumers. Happily, a deeper understanding of the threats to the IoT, combined with the emergence of clearer guidance, standards and regulation, is helping the industry move closer to its mission of embedding security into the fabric of IoT devices by default. The result could be a more trusted and resilient ecosystem that makes it much harder for the bad guys to break in.

RISKY BUSINESS

Most businesses today operate in an environment of heightened cyber risks. Key factors in this increase have been the growing reliance by companies on digital technologies and the simultaneous explosion in the creation and accumulation of data. Both these situations generate attractive targets for maliciously motivated cyber attackers – the former because it offers the potential to cause widespread disruption and the latter because of the financial value of stolen data, which can now be traded on the dark web or used in extortion campaigns.

Cyber attackers have also grown rapidly in number, and evolved and enhanced their capabilities. This is true both technologically through capabilities like artificial intelligence (AI), and organizationally, with attacks coming from a wide range of diverse, well resourced and highly coordinated sets of actors including state sponsored groups, financially motivated cybercriminal gangs and ideologically driven activists.

By 2025, the cost of cybercrime is predicted to reach $10.5 trillion annually, according to research firm, Cybersecurity Ventures. Staggering as that figure may be, the truth of the heightened threat environment is perhaps better reflected in the steady stream of news items about major data breaches and disruptive cyber-attacks affecting everyday businesses and well-known brands. These include major banks, telcos, retailers, hotel chains, medical facilities, charitable organizations and more. Customers of these organizations are often the true victims of these attacks, suffering everything from breaches of their private information, large-scale financial losses or being prevented from accessing critical services.

CONNECTED DEVICE VULNERABILITY

For cyber analysts, a particularly concerning recent trend has been the increased targeting of critical infrastructure. These are operators of services that governments deem essential for society to function, and typically include organizations in sectors like health, energy, food, water and communications.

The most devastating attacks on critical infrastructure are those that have targeted key critical connected components or smart devices; these often form part of complex industrial control systems such as electricity distribution grids or water pipelines. (*See WQ Issue 2, 2021 pg22.*) But for many observers, the broader takeaway from this trend has been the severe vulnerability of connected devices generally, and the need to do more to secure them.

It's a massive challenge: By 2025, there will be almost 42 billion IoT devices, according to analyst firm IDC. This growth in the volume of connected devices means an expanding target for cybercriminals, for several reasons. Firstly, the more connected devices the larger the so-called 'attack surface', or number of potential vulnerable targets an attacker can seek to exploit. Secondly, the large volumes of data generated by and transferred between connected IoT devices is itself a rich target for interception.

Like the attacks on critical infrastructure, disruptive attacks on the IoT can result in serious consequences

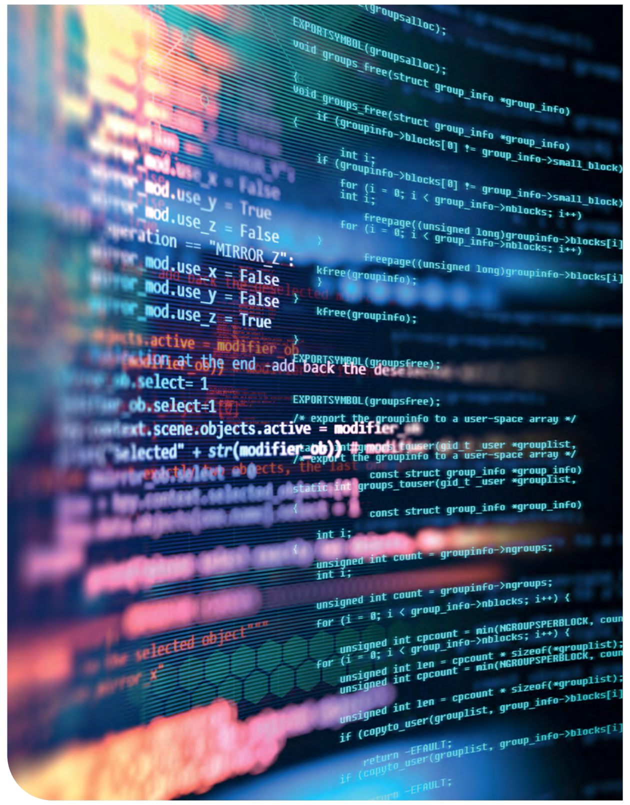
By the Numbers

$10.5 trillion
The cost of cybercrime by 2025
(Source: Cybersecurity Ventures)

1.5 billion
Attacks on IoT devices in the first half of 2021
(Source: Kaspersky)

48%
Number of OEMs viewing the fragmentation of standards and regulations as the top IoT security challenge
(Source: PSA Certified)

> "The most devastating attacks on critical infrastructure are those that have targeted key critical connected components or smart devices



> About 30 percent of providers of IoT solutions consider digital trust to be critical, compared with approximately 60 percent of buyers

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 1.5 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 IoT 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 complacency 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 Nordic 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 lure 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.

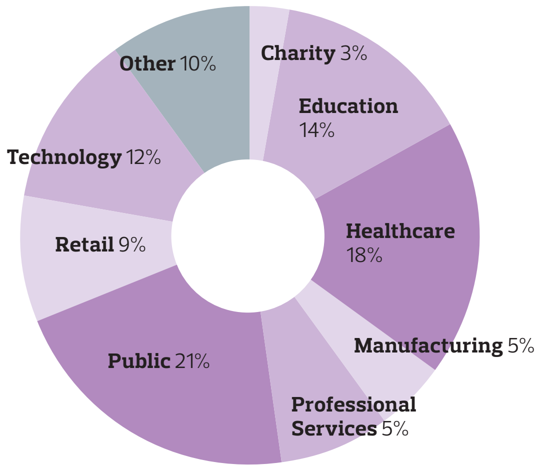
> Security breaches of IoT products threaten not only the prosperity of companies, but also impact entire product categories by giving them a reputation for being insecure

State of Play

Why are criminals so interested in the IoT?

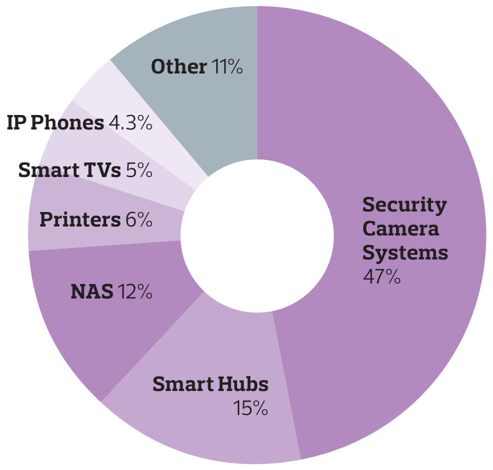
Experts say 2021 was the year of ransomware, but things changed in 2022 as the bad guys realized the estimated 17 billion IoT devices represent juicier pickings. While IT hardware and software security has dramatically improved, the same cannot be said of IoT devices. According to U.S. media company CNBC, IoT devices with minimal defences represent entry points for attacks on critical infrastructure, or the device itself can be the specific target due to the data contained therein. This is one of the reasons why security cameras are an enticing prey. A weakness that's now being addressed is a mechanism to make it easier to download regular software updates to provide security patches.

Security incident by sector 2022



Source: IT Governance

Most hacked IoT devices 2019



Source: Devopedia

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 secure 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, and 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 a 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 (ETSI) 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 pg36.*)

psacertified™

Need to Know

The PSA Certified IoT Security Framework guides developers in securing connected devices, from analysis through to security assessment and certification. It provides standardized resources to help resolve the growing fragmentation of IoT security

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 resilience 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 product is targeted at the horticulture 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 $12.6 trillion in value globally by 2030. As some have observed, many such predictions 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 consortiums 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.

> "The IoT ecosystem appears to have realized that standardization is necessary for more consistent, and better, security outcomes

Ten dollars to rein in a monster

One of the most devastating and notorious cyber-attacks in history was thwarted by $10 and a stroke of luck.

In 2017 the WannaCry ransomware swept across the globe, seizing up hundreds of thousands of computer systems in dozens of countries. Among the most prominent victims of the attack were healthcare systems in the U.K., affecting people seeking medical care, along with telecommunications companies in Spain, manufacturers in France and train services in Germany.

The ransomware worked by exploiting a vulnerability, or security hole, in Microsoft Windows that had been originally developed by the U.S. National Security Agency and then stolen by a hacker group called ShadowBrokers, who then passed it on to the hacker community.

The cybercriminals behind WannaCry would come to use the vulnerability to infect scores of computers, encrypting their key files and demanding extortion payments of about $300 to unlock the files.

As chaos and panic spread around the world, the cyber security community began to step up efforts to contain the attack. Microsoft released patches to protect some of its products from the attack. Other security researchers frantically tried to reverse engineer the code behind the ransomware, in the hope it might offer some clues on how to contain it.

One researcher, Marcus Hutchins, better known in the cyber security community as 'MalwareTech' would prove to be an accidental hero. Deep within WannaCry's code, Hutchins found a reference to a hidden website URL, which was not a live webpage. Curious about why the code would reference the URL, Hutchins shelled out $10 to register the website domain.

Once the URL became active, WannaCry suddenly shut itself down and ceased spreading. Hutchins had inadvertently discovered the ransomware's 'kill switch'.

Experts later told *Wired* magazine the feature had likely been deliberately built into the ransomware by its creators in case they ever needed "to rein in the monster they'd created".

While 'Hutchins' actions didn't help those whose organizations and systems were already infected, for those not yet affected it bought valuable time to apply patches and other protective measures.

Planet Bluetooth

Bluetooth's spread and evolution continue and suppliers of the omnipresent tech are innovating across applications once unimagined

In Short

In a quarter of a century Bluetooth technology has become ubiquitous

The introduction of Bluetooth LE in 2010 dramatically expanded the technology's range of applications

Bluetooth LE now encompasses mesh networking, indoor location services, high quality audio, and smart home interoperability

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 concerns 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 inflection point in the remarkable rise of wireless innovation can be traced 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 in its various forms has powered a significant segment of the connected world ever since. Within two years of Ericsson, Nokia, Intel, 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 SIG's membership skyrocketed and last year over 5 billion Bluetooth-enabled devices were shipped worldwide – a figure expected to climb to 7 billion by 2026.

Today wearables are universal, while smart homes, smart industries and even smart cities are transforming life 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 the Bluetooth 4.0 Specification. Bluetooth LE was born out of a 2001 Nokia venture to develop 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 wireless tech, Nordic took the decision to back the open standard—just as it has with cellular IoT, DECT NR+ and Wi-Fi in more recent times—ceding much of its hard-won 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 tech, they 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 horsepower. Today's high end wearables 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 SoCs 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—extended 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 – 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 is 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.

> "The Bluetooth SIG member community is dedicated to delivering innovations that improve Bluetooth technology and help shape new market trends

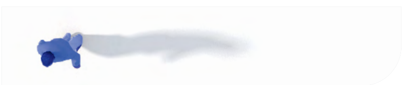
In the lucrative audio market, Bluetooth tech described as the 'future of wireless sound' now allows engineers to enhance the sound quality and power consumption of wireless audio products. Bluetooth 5.2 added capabilities to the specification that support LE Audio. (*See* WQ *Issue 1, 2022* *pg26*.) The tech enables audio developers to meet increasing consumer performance demands and drive continuous growth across the audio peripheral market. It also enables Auracast broadcast audio and will standardize the implementation for Bluetooth audio in hearing aids. (*See pg12*.) 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. With support 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 it joined Nokia's Wibree initiative in 2006. However, 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 on 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 shipments over the next five years

Source: ABI Research – 2023 Bluetooth Market Update

Bluetooth LE solutions are used by the world's leading brands in myriad products, including PC peripherals, gaming, sports and fitness, mobile phone accessories, consumer electronics, toys, healthcare and industrial automation. All Nordic solutions are advanced and power efficient, but offer different feature sets and memory configurations. The company ships more than one million Bluetooth LE SoCs every day. According to Bluetooth SIG data compiled by DNB Markets, Nordic had a market share of 39 percent of new design certifications in the Bluetooth LE market in 2021. A total of more than 1,100 new designs were certified in 2022, of which 446 had Nordic inside.

Since the introduction of the nRF51 Series, Nordic's chips have evolved in performance—primarily based on the use of more advanced semiconductor manufacturing tech, more generous memory, more processing power and speed, and more embedded cores—through successive product introductions. Each new generation has allowed developers to push the boundaries of innovation without making major sacrifices in power consumption.

In late 2019, Nordic Semiconductor announced the launch of the nRF5340 as the latest flagship in its Bluetooth LE SoC family. The nRF5340 is the world's first wireless SoC based on an Arm Cortex-M33 dual-processor hardware architecture. A high-performance application processor combined with a fully programmable, ultra low power network processor, enables the former to look after advanced processing such as machine learning while the latter supervises the wireless protocol. In addition, the highly integrated SoC has advanced security features, making it ideal for advanced wearables, professional lighting and industrial automation applications.

"Developers are already working on implementing the more complex applications required for the commercial products of tomorrow," says Bjørn Åge "Bob" Brandal, Nordic Semiconductor, VP of Sales and Marketing, Asia Pacific. "These applications require greater computational power and high security, but with the energy efficiency for which Nordic solutions have become renowned. The nRF5340 meets these needs, and together with our design tools will make complex applications much easier and simpler to implement."

Earlier this year, Nordic Semiconductor announced the first SoC in its nRF54 Series, extending the company's pioneering approach in Bluetooth LE. The nRF54H20 SoC boasts multiple Arm Cortex-M33 processors and multiple RISC-V coprocessors making it ideal for disruptive IoT applications demanding high processing power, excellent energy efficiency and state-of-the-art security. Capable of supporting Bluetooth 5.4 and future Bluetooth specifications, plus LE Audio, Bluetooth mesh, Thread, Matter and more, the nRF54H20 will be the foundation for a new wave of revolutionary IoT end products. In addition to next-gen 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. (*See pg4.*)

The Nordic nRF52840 SoC-powered WHOOP 4.0 wearable lasts up to five days between charges with continuous physiological data monitoring

Magene's C406 Pro is a multifunctional GPS bike computer that can record over 100 different types of riding data as well as support up to eight peripherals

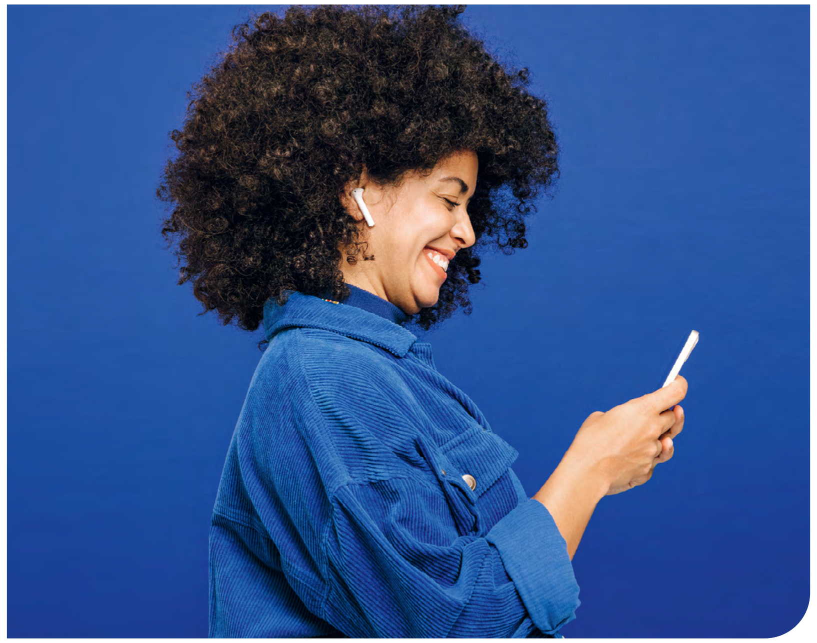
"Decades of ultra low power wireless expertise have come together to form the nRF54 Series," says Svenn-Tore Larsen, CEO, Nordic Semiconductor. "Our first SoC from the fourth generation of Bluetooth LE solutions, the product not only represents a significant milestone for Nordic, but also allows Nordic's customers to build end products far more advanced than those we see today."

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 health monitoring wearable launched by U.S. based human performance company, WHOOP, can perform continuous physiological data monitoring for up to five days without requiring recharge. "With [a] breakthrough battery design and extremely low power consumption enabled by the nRF52840 SoC, we can deliver up to five days of continuous physiological data monitoring before needing a recharge," says Brian Martins, Group Lead Electrical Engineering at WHOOP.

The WHOOP 4.0 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 using the Nordic SoC and made accessible via an app where members can get health insights, see improvements and irregularities, as well as download their health records.

Meanwhile, intelligent technology company Magene's multifunctional GPS bike computer can record over 100 different items of riding data across 13 categories as well as support up to eight peripherals. The C406 Pro uses satellite positioning to accurately record and display a range of data such as speed, mileage, time, temperature and altitude on its 2.4-in (61 mm) LCD screen. The integration of Nordic's multiprotocol nRF52840 SoC allows the bike computer to support sensor devices such as heart rate monitors, power meters, speed and cadence sensors as well as electronic shifting systems and the company's L508 Radar Tail Light. The SoC also supports the ultra low power ANT+ wireless protocol which allows the bike computer to be simultaneously linked with complementary ANT+ Magene and third party devices. "As a brand, Nordic has mature market experience, an enormous number of customer success stories, and timely technical support," says Fanbin Kong, CTO of Magene.

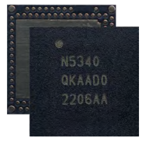


Elsewhere, Anglo-American fitness equipment manufacturer, WaterRower, has developed rowing machine performance monitors to provide users with 'real time' access to motivational programs and data-driven incentives to train smarter and keep fit. The machine uses an nRF52811 to send the user's data to a smartphone app.

And in the industrial sector, China based OctoNet's Bluetooth positioning gateway uses the direction finding capabilities of Nordic's nRF52833 SoC to keep track of high value hospital equipment and the whereabouts of staff in hospitals. "The excellent performance, stability and reliability of Nordic's products are the best in the industry," says Xin Zhang, CTO at Jiangsu OctoNet Technology. "In addition, Nordic's sales engineers and technical support engineers showed great professionalism and enthusiasm when providing support."

These examples stand out, but the list of similarly advanced applications employing Nordic enabled Bluetooth LE wireless connectivity is truly extensive.

Bluetooth LE technology is now synonymous with the connected lifestyle across the globe. Bluetooth LE devices are helping people in a smart home in Los Angeles to those working on an outback ranch in remote Australia and everywhere in between. Whether a dedicated athlete, an intrepid adventurer, a patient with an acute medical condition, or simply a typical consumer in the developed world, we're all citizens of Planet Bluetooth.



Tech Check

The nRF5340 is Nordic's current flagship Bluetooth LE SoC and is the world's first with two Arm Cortex-M33 microprocessors. One is a dedicated application processor while the other is a low-power network device. The just announced next-generation SoC, the nRF54H20, will feature multiple Arm M33 and RISC-V microprocessors

What's in a name?

The Bluetooth brand is universally recognized, but few could immediately explain the origins of the name. Given the level of innovation it's associated with, 'Bluetooth' doesn't sound particularly geeky. 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' Gormsson, who was well known for two things: Uniting Denmark and Norway in 958, and his dead tooth, which was a dark blue/grey color, earning him the nickname Bluetooth.

Fast forward to 1996, three industry leaders—Intel, Ericsson and Nokia—met to plan the standardization of a short-range radio tech to support connectivity and collaboration between different products and industries. During this meeting, Jim Kardach from Intel suggested Bluetooth as a temporary code name. "King Harald Bluetooth ... was famous for uniting Scandinavia just as we intended to unite the PC and cellular industries with a short-range wireless link," Kardach later explained.

Bluetooth was only intended as a placeholder until marketing could formally name the nascent technology. Around this time, a number of different companies in the Special Interest Group (SIG) were each developing their own names. The leading contenders were IBM's proposal, "PAN" (Personal Area Networking), and Intel's proposal, "RadioWire". PAN was the frontrunner until an exhaustive search discovered it already had tens of thousands of hits across the Internet, while a full trademark search on RadioWire couldn't be completed in time for launch. This left Bluetooth as the last option standing. And before the name could be changed it had gathered the industry's attention, quickly becoming synonymous with short range wireless technology – to the extent the SIG originally had its application for a U.S. trademark rejected on the basis of Bluetooth already being synonymous with short range radios. As for the Bluetooth logo, it represents a 'bind rune' merging the symbols for Kings Harald's initials.

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

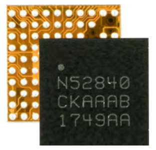
EVs are not a modern invention. The first full-sized EV was actually created by Scottish inventor Robert Anderson as far back as 1832. The crude prototype was powered by non-rechargeable primary power cells. The first human-carrying EV with its own power source was tested along a Paris street in April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

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 hefty 660 kWh battery pack which enabled it to cover 1,772.2 kilometers before its battery pack ran out of energy and the bus ground to a halt. The bus' high speed charging system meant it only needed an hour to return to full charge and be on its way

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

Motoring enthusiasts like to hear the roar of a V8 engine when they are behind the wheel, which is one reason 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

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 smartly, 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



Tech Check

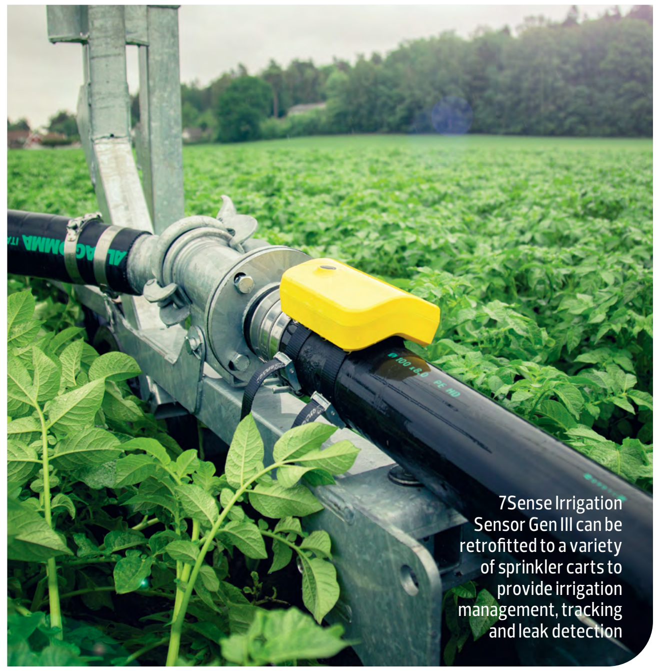
In addition to the nRF9160 SiP, the EV charger employs Nordic's nRF52840 SoC, providing Bluetooth LE wireless connectivity between the charger and the Enua app on the user's smartphone. From the app, users can configure the charger to suit their individual requirements, unlock the charger, select predefined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

Smart Agriculture

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

> The 7Sense exemplifies a hands-off approach to water management, allowing everything to be done remotely



7Sense Irrigation Sensor Gen III can be retrofitted to a variety of sprinkler carts to provide irrigation management, tracking and leak detection

Our poorest and most vulnerable communities desperately need sustenance. The World Bank has found that 205 million people worldwide are dangerously malnourished. And as the global population continues to grow and the amount of arable land remains static, resources are being stretched even thinner. The solution is to use technology to enhance yields from the world's existing farms.

But even with tech, the situation is challenging, particularly as water supplies are under immense strain. Agriculture is the largest water user worldwide, accounting for 70 percent of total freshwater withdrawals on average. While these amounts vary greatly between countries in some developing nations agriculture water use can reach as high as 95 percent.

"Improving agricultural productivity, while conserving and enhancing natural resources, such as water, is an essential requirement for farmers to increase global food supplies on a sustainable basis," the UN's Food and Agriculture Organization (FAO) said in a statement. Yet data from analyst High Tide Technologies shows 40 percent of the water used in agriculture is wasted due to poor irrigation and management.

"Traditional irrigation systems in agriculture are labor-intensive and require constant manual monitoring," says Max J. Tangen, CEO at 7Sense Agritech, a Norwegian agricultural technology company that has developed an innovative irrigation control system to help reduce water waste. "They often consist of hundreds of meters of hoses, pipes and connectors, where many components can—and do—malfunction. Any failure could potentially lead to enormous water losses, as well as damage to fields and crops."

Solving the irrigation issue

Farmers typically irrigate during the night in cooler, more favorable conditions. However, this is far from ideal, explains Tangen, as it interrupts valuable sleep. "It's a never ending hassle during the summertime," he says. "One hot summer when we travelled around talking to farmers, the irrigation issue came up time and time 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."

Armed with this information, 7Sense set about developing its 7Sense Irrigation Sensor Gen III – a system designed to automatically detect water loss, protect crops and free up time for farmers. The solution uses the GNSS and cellular locationing 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 effective 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.

Need to Know

Nordic's nRF9160 SiP features built-in GNSS, allowing it to accurately relay the position of assets. It can also communicate with Cloud services to use cellular base stations to determine position, offering a less precise but more battery-friendly locationing solution

Leak detection capabilities

The wireless sensor can be easily retrofitted to almost any type of existing irrigation system. Using 7Sense's patent pending, 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 III boasts 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 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."

Mike Williston
Co-Founder & CEO, Satellite Displays, Inc.

Assistive tech provides accessibility and inclusivity

Helping people with hearing loss is vital in the era of mask wearing

Technological advancements have opened the door to many solutions that help improve the lives of those who are deaf or hard of hearing. As nearly 2.5 billion people globally will have some level of hearing loss by 2050, it is imperative we innovate to create solutions that are affordable, accessible and easy to use.

The challenge with hearing loss is that it's an invisible disability. If you have crutches, it's very easy for somebody to understand that you need help up the stairs. But when I walk in with hearing loss, it may not be immediately obvious if I need assistance. This has become even truer in the age of COVID-19. I, like many hard of hearing people, quickly realized I could not hear as well as I thought because voices were muffled and lips were covered by masks. It got to a point where I wouldn't even want to go into a store because of how difficult it was to communicate. That is why we developed Badger, the world's first closed captioning smart badge.

> It is imperative we innovate to create solutions that are affordable, accessible and easy to use

The smart badge converts the wearer's speech to text, then transmits it via Bluetooth LE to the Badger smartphone app which provides voice-to-text captioning and translation into more than 50 languages.

The captions are then relayed back to the badge where they appear on the E-Ink display enabling anyone to easily understand what the wearer is saying.

The device can be used anywhere communication is important, but it is aimed mainly at use in healthcare contexts. The technology makes it easier and more cost effective for medical facilities to meet the requirements of the Americans with Disabilities Act—and equivalent laws worldwide—to help people who are deaf or hard of hearing, and help create more inclusive environments.

A sector in growth

In my opinion, the assistive tech sector will only continue to expand. As we all know, when we age we tend to become more in need of help, and people are living longer, so it is critical for tech companies to continue to innovate in the assistive technology space. For those companies, ourselves included, the biggest challenges are low cost, readily affordable materials, and making the technology easy to implement for users. We have to make assistive tech affordable to people who need it, and we have to make the user experience great, otherwise no one will use it.

That said, in the next three to five years I believe the assistive tech sector is going to explode, and the catalyst for that change will be that people will actually be looking for new tech that will improve their lives as they age to provide more inclusion in society.

As an early stage start-up it is empowering to believe what we are doing will improve the lives of many people, but ultimately we are also just creating pretty cool technology.

[Tech Zone]

An in-depth look at Nordic's wireless solutions

The EdgeTrak 4S can be fully configured remotely and deployed at scale

Cellular IoT

Industrial connectivity solution enables Cloud-based operations monitoring

An industrial connectivity solution from equipment management company, Rulo, is helping users simply and securely connect equipment to the Cloud to monitor, control and manage operations. The Nordic nRF9160 SiP-powered Rulo EdgeTrak 4S controllers feature flexible, user-configurable inputs and outputs that enable connection to equipment and systems.

The EdgeTrak 4S can be fully configured remotely and deployed at scale, and allows industrial organizations to supervise and control machines and processes using 'real time' data. Benefits of the solution include edge processing capabilities and detailed custom reports via dashboards on the accompanying web-based platform.

The EdgeTrak 4S is designed primarily for non-road mobile and stationary applications, with target markets including oil and gas, water, asset tracking and construction. For example, a U.S. oil and gas company, Rimrock, deploys EdgeTrak 4S to optimize well management. The EdgeTrak 4S controllers are used to monitor and send out alerts on a range of parameters including wellhead pressures, compressor data and tank levels to avoid any unnecessary downtime.

"Previously, Rimrock field personnel were required to visit well sites every day, multiple times a week, or once weekly – depending on the well," says Brian Barton, VP Sales and Marketing, Rulo. "Now ... EdgeTrak 4S can relay performance data to the Cloud remotely, allowing field personnel to make better use of their time by putting an end to routine visits and relying on alerts instead."

At the heart of the EdgeTrak 4S, the Nordic nRF9160 SiP's powerful application processor with generous memory is responsible for the core processing of machine and process data, while the LTE-M cellular IoT connectivity enabled by the nRF9160's modem ensures reliable coverage to relay data from the device to the Cloud.

Smart Home

Module enables Matter over Thread

Nordic design partner HooRii Technology has launched a Matter, Lightweight Machine-to-Machine (LwM2M) and Open Connectivity Foundation (OCF) over Thread compatible module for use in space-constrained smart home and lighting applications. The Thread 1.3.0 certified HRN71 module is available in two different versions, one with a PCB antenna measuring 10 by 12 by 2.6 mm, the other with support for an external antenna in a 10 by 10 by 2.6 mm form factor.

The module is powered by Nordic's nRF52840 multiprotocol SoC. The SoC is a Thread certified component.

For Matter applications the module uses the nRF52840's Thread connectivity for transport and Bluetooth LE connectivity for commissioning new devices. Matter over Thread prototyping is supported by Nordic's nRF52840 DK single-board development kit for the nRF52840 SoC. The module runs on the HooRiiOS operating system, which provides development-free Matter firmware.

Nordic Partner Program

Golioth, KYOCERA AVX and SODAQ expand Nordic Partner Program

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

Golioth offers an IoT platform that makes it easy to link Cloud services to IoT devices. The platform seamlessly integrates with Nordic's nRF9160 low power SiP and the company's nRF53 and nRF52 Series multiprotocol SoCs. This integration makes it easy for Nordic customers to measure, monitor and manage their IoT end devices at scale. The Golioth product is also being extended to Nordic's other IP interoperable solutions such as the nRF7002 Wi-Fi companion IC and Thread SoCs.

SODAQ designs and creates unique hardware solutions in projects for large corporate IoT departments and manufactures products for companies who want to deploy tracking and sensing devices in their logistics chain. In addition to off-the-shelf products, SODAQ offers custom hardware, embedded software, RF, antenna and security design as a service.

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 nRF9160 DK. The collaboration ensured optimum wireless performance for the end customer.

Logistics & Transport

Telematics 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, Intellicar. 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 Intellicar'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 first/last mile solution providers.

Intellicar's edge intelligence hardware, Flashμ, is powered by Nordic Semiconductor's nRF52833 SoC. In addition, the gateway integrates a cellular modem for device-to-Cloud data transmission, together enabling 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, Flashμ 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 Flashμ, 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.

Intellicar's software stack supervises the devices to ensure reliable data delivery. This, combined with Intellicar'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 WT02E40E Series modules integrate both Nordic Semiconductor's nRF5340 advanced multiprotocol SoC, and nRF7002 Wi-Fi 6 companion IC.

The modules offer multiple antenna options to meet different applications. Options include the WT0E40E with u.FL connectors for Bluetooth LE and Wi-Fi 6 antennas, the WT02C40C with on-chip Bluetooth LE and Wi-Fi 6 antennas, the WT02V40V with vertically-mounted chip antennas for Bluetooth LE and Wi-Fi 6, the WT02E40C with a u.FL connector for a Wi-Fi 6 antenna and an on-chip Bluetooth LE antenna, and the WT02E40F with a u.FL connector for a Wi-Fi 6 antenna and a Bluetooth LE PCB antenna.

Tech 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

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 breaches 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 adopted to set a baseline for IoT security. In many markets this baseline will be a mandatory requirement. While the global approach is fragmented there are emerging common requirements. For example, there are similarities between the EU's Radio Equipment Directive, Cyber Security Act, and Cyber Resilience Act, and similar U.S., U.K., Singapore, Finnish, and Australian regulations. (*See pg20.*)

A requirement underpinning many of these regulations is for security to be considered from 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 nRF5340 SoC and nRF9160 SiP are PSA Certified Level 2 with the nRF52840 certified to Level 1.

Security is a balance

Protection costs, and even with high expenditure, no product can be guaranteed completely secure. With enough time, money and motivation, any IoT system can be breached. That makes security a balance between cost and risk. Implementing security for an IoT application requires a specific engineering skillset, additional chip resources, and a secure production environment. These are all things that add dollars. But this expense must be balanced against the risk (where risk = impact x probability) of a successful attack. For example, an attack will have a high impact if it involves a loss of confidential personal data, while it might also have a high probability because that data is of interest, and the device is inherently simple to breach. In this case good security measures should be considered to reduce the risk because the cost of security is lower than the cost of a successful attack.

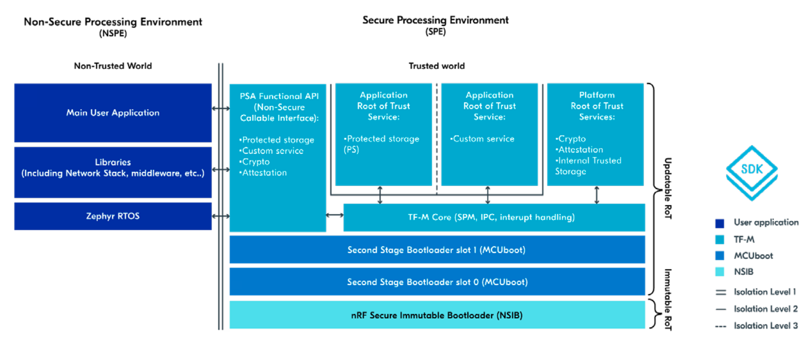
But even low risk products shouldn't be left defenseless. Simple protection such as secure-boot and -update with anti-rollback is a good start. Secure boot ensures the device verifies that its original software, and any subsequent update, is authorized and is safe to run. Anti-rollback prevents an older (and potentially vulnerable) version of the firmware being reinstated.

> "A key requirement underpinning many international regulations and standards is for 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 more secure from those that contain 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 utilise an API 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 where 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.

Using trusted firmware to protect critical data


Non-Secure Processing Environment (NSPE)
Secure Processing Environment (SPE)
Non-Trusted World
Trusted world
Main User Application
Libraries (Including Network Stack, middleware, etc..)
Zephyr RTOS
PSA Functional API (Non-Secure Callable Interface):
•Protected storage
•Custom service
•Crypto
•Attestation
Application Root of Trust Service:
•Protected storage (PS)
Application Root of Trust Service:
•Custom service
Platform Root of Trust Services:
•Crypto
•Attestation
•Internal Trusted Storage
TF-M Core (SPM, IPC, interupt handling)
Second Stage Bootloader slot 1 (MCUboot)
Second Stage Bootloader slot 0 (MCUboot)
nRF Secure Immutable Bootloader (NSIB)
Updatable RoT
Immutable RoT
SDK
User application
TF-M
MCUboot
NSIB
Isolation Level 1
Isolation Level 2
Isolation Level 3

Trusted Firmware-M (TF-M) is a secure processing environment which runs on Arm TrustZone enabled hardware such as that on Nordic's nRF9160 SiP. TF-M isolates critical security services and data from non-secure user applications. It also provides PSA-Root of Trust (RoT) and secure services such as cryptography and secure storage.

Nordic's unified and scalable software development kit, nRF Connect SDK, supports IoT product development with TF-M, and offers a reference implementation of a secure processing environment (SPE). When using the SDK for development, the non-secure processing environment (NPSE) hosts things such as the main user application, libraries (such as network stacks and middleware) and the Zephyr real time operating system (RTOS).

The SPE is home to functions that need to be protected. It provides multiple levels of isolation. The first level is between the NSPE and SPE. The second level of isolation provides additional protection for the Application RoT Service within the SPE. The third level of isolation protects some Application RoT Services not only from the rest of the SPE, but also from other Application RoT Services. In practice this means each Application RoT Service is sandboxed and can only use its own allocated resources.

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 threaten to extend time to market. PSA Certified IoT security framework addresses these concerns by offering a standardized approach to IoT security from design through to certification.

The framework simplifies a secure-by-design strategy by dividing it into four steps: threat modeling and security analysis ('analyze'); hardware and firmware specification ('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 logs. For the firmware, the security requirement is integrity, and the threat is tampering. The vulnerability might be malware, a software bug, a weakness in the mass storage, an unsecure JTAG 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 if malware has installed via a vulnerability, it wouldn't run.

Once 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 base the product on Nordic's nRF9160 or nRF5340 (which are PSA Certified security best-practice devices and offer these capabilities).

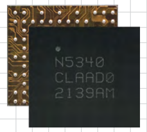
Gaining certification

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 devices. Nordic's nRF9160 and nRF5340 are PSA Certified Level 2 and the nRF52840 is 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. 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 303645 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/43LFyay



Need to Know

Nordic's nRF5340, the world's first dual-core Arm Cortex-M33 wireless SoC, has been designed with security in mind. For example, the SoC's Arm TrustZone provides trusted execution by implementing a division between secure and non-secure Flash, RAM, peripherals and GPIOs. The SoC is PSA Certified Level 1

Nordic Product Guide

This handy summary describes all of Nordic's IoT solutions

Full product details at: www.nordicsemi.com/Products

RF SoCs and SiP

		nRF 91 SERIES	nRF SERIES 53	nRF 52 SERIES						
		nRF9160	nRF5340	nRF52840	nRF52833	nRF52832	nRF52820	nRF52811	nRF52810	nRF52805
WIRELESS PROTOCOL	LTE-M	●								
	NB-IoT	●								
	GNSS	●								
	BLUETOOTH LOW ENERGY		●	●	●	●	●	●	●	●
	BLUETOOTH 5.3		●	●	●	●	●	●	●	●
	LE AUDIO		●							
	DIRECTION FINDING		●		●		●	●		
	2 Mbps		●	●	●	●	●	●	●	●
	LONG RANGE		●	●	●		●	●		
	BLUETOOTH MESH		●	●	●	●	●			
	THREAD		●	●	●		●	●		
	MATTER		●	●						
	ZIGBEE		●	●	●		●			
	ANT		●	●	●	●	●	●	●	●
	2.4 GHz PROPRIETARY		●	●	●	●	●	●	●	●
	NFC		●	●	●	●				
TYPE	SYSTEM-ON-CHIP (SoC)		●	●	●	●	●	●	●	●
	SYSTEM-IN-PACKAGE (SiP)	●								
CORE SYSTEM	CPU	64 MHz Arm Cortex-M33	128 MHz Arm Cortex-M33 +64 MHz Arm Cortex-M33	64 MHz Arm Cortex-M4	64 MHz Arm Cortex-M4	64 MHz Arm Cortex-M4	64 MHz Arm Cortex-M4	64 MHz Arm Cortex-M4	64 MHz Arm Cortex-M4	64 MHz Arm Cortex-M4
	FPU	●	●	●	●	●				
	DSP INSTRUCTION SET	●	●	●	●	●	●	●	●	●
	CACHE	●	●	●	●	●				
	MEMORY	1 MB Flash, 256 KB RAM	1 MB Flash, 512 KB RAM +256 KB Flash, 64 KB RAM	1 MB Flash, 256 KB RAM	512 KB Flash, 128 KB RAM	512 KB or 256 KB Flash, 64 KB or 32 KB RAM	256 KB Flash, 32 KB RAM	192 KB Flash, 24 KB RAM	192 KB Flash, 24 KB RAM	192 KB Flash, 24 KB RAM
	CLOCKS	64 MHz / 32 kHz	128 MHz / 64 MHz / 32 kHz	64 MHz / 32 kHz	64 MHz / 32 kHz	64 MHz / 32 kHz	64 MHz / 32 kHz	64 MHz / 32 kHz	64 MHz / 32 kHz	64 MHz / 32 kHz
SECURITY	ARM TRUSTZONE	●	●							
	ARM CRYPTOCELL	310	312	310						
	ROOT-OF-TRUST	●	●	●						
	SECURE KEY STORAGE	●	●							
	AES ENCRYPTION	●	●	●	●	●	●	●	●	●
RADIO	LTE-M/NB-IoT/GPS MODEM	●								
	CERTIFIED LTE BANDS	1-5, 8, 12-14, 17-20, 25-26, 28, 66								
	FREQUENCY	700-2200 MHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz	2.4 GHz
	MAXIMUM TX POWER	23 dBm	3 dBm	8 dBm	8 dBm	4 dBm	8 dBm	4 dBm	4 dBm	4 dBm
	RX SENSITIVITY	-108 dBm (LTE-M), -114 dBm (NB-IoT), -155 dBm (GPS)	-98 dBm (1 Mbps)	-95 dBm (1 Mbps)	-96 dBm (1 Mbps)	-96 dBm (1 Mbps)	-95 dBm (1 Mbps)	-97 dBm (1 Mbps)	-96 dBm (1 Mbps)	-97 dBm (1 Mbps)
	ANTENNA INTERFACE	50 Ω single-ended	Single-ended	Single-ended	Single-ended	Single-ended	Single-ended	Single-ended	Single-ended	Single-ended
PERIPHERALS	HIGH SPEED SPI		●	●	●					
	TWI, SPI, UART	4xTWI/SPI/UART	4xTWI/SPI/UART +TWI/SPI/UART	2xTWI/SPI, SPI, 2xUART	2xTWI/SPI, SPI, 2xUART	2xTWI/SPI, SPI, UART	2xTWI/SPI, UART	TWI/SPI, SPI, UART	TWI, SPI, UART	TWI, SPI, UART
	QSPI		●	●						
	USB		●	●	●		●			
	PWM	4	4	4	4	3		1	1	
	PDM	●	●	●	●	●		●	●	
	I2S	●	●	●	●	●				
	ADC, COMPARATOR	ADC	●	●	●	●	COMP	ADC, COMP	ADC, COMP	ADC
	TIMER, RTC	3, 2	3, 2 + 3, 2	5, 3	5, 3	5, 3	4, 2	3, 2	3, 2	3, 2
	TEMPERATURE SENSOR	●	●	●	●	●	●	●	●	●
CERTIFICATIONS		nordicsemi.com/9160cert	CE, FCC	CE, FCC	CE, FCC	CE, FCC	CE, FCC	CE, FCC	CE, FCC	CE, FCC
OPERATING TEMPERATURE		-40 to 85°C	-40 to 105°C	-40 to 85°C	-40 to 105°C	-40 to 85°C	-40 to 105°C	-40 to 85°C	-40 to 85°C	-40 to 85°C
SUPPLY VOLTAGE RANGE		3.0 to 5.5 V	1.7 to 5.5 V	1.7 to 5.5 V	1.7 to 5.5 V	1.7 to 3.6 V	1.7 to 5.5 V	1.7 to 3.6 V	1.7 to 3.6 V	1.7 to 3.6 V
DEVELOPMENT KITS		nRF9160 DK, Nordic Thingy:91	nRF5340 DK, nRF5340 Audio DK, Nordic Thingy:53	nRF52840 DK, nRF52840 Dongle	nRF52833 DK	nRF52 DK, Nordic Thingy:52	nRF52833 DK	nRF52840 DK	nRF52 DK	nRF52 DK
PACKAGES		10x16x1.04 mm LGA	7x7 mm aQFN94 (48 GPIOs), 4.4x4.0 mm WLCSP95 (48 GPIOs)	7x7 mm aQFN73 (48 GPIOs), 6x6 mm QFN48 (30 GPIOs), 3.5x3.6 mm WLCSP94 (48 GPIOs)	7x7 mm aQFN73 (42 GPIOs), 5x5 mm QFN40 (18 GPIOs), 3.2x3.2 mm WLCSP (42 GPIOs)	6x6 mm QFN48 (32 GPIOs), 3.0x3.2 mm WLCSP50 (32 GPIOs)	5x5 mm QFN40 (18 GPIOs), 2.53x2.53 mm WLCSP44 (18 GPIOs)	6x6 mm QFN48 (32 GPIOs), 5x5 mm QFN32 (17 GPIOs), 2.48x2.46 mm WLCSP33 (15 GPIOs)	6x6 mm QFN48 (32 GPIOs), 5x5 mm QFN32 (17 GPIOs), 2.48x2.46 mm WLCSP33 (15 GPIOs)	2.48x2.46 mm WLCSP28 (10 GPIOs)

Power Management ICs

		nPM FAMILY		
		nPM1300	nPM1100	nPM6001
TYPE	PMIC	●	●	●
FEATURES	BUCK REGULATOR	2	1	4
	BATTERY CHARGER	●	●	
	LDO	2		2
	LOAD SWITCH	2		
CHARGER	TERMINATION VOLTAGE	3.5 to 4.45 V	4.1 to 4.25 V or 4.2 to 4.35 V	
	MAX CHARGING CURRENT	800 mA	400 mA	
	POWER PATH MANAGEMENT	●	●	
	THERMAL PROTECTION	●	●	
	BATTERY COMPATIBILITY	LiFePO4, Li-ion, LiPo	Li-ion, LiPo	
POWER RAILS	INPUT VOLTAGE	4 to 5.5 V	4.1 to 6.7 V	3 to 5.5 V
	USB COMPLIANCE	Type-C	●	
	REGULATED OUTPUT VOLTAGE	1 to 3.3 V	1.8 to 3 V	0.5 to 3.3 V
	MAX CURRENT PER BUCK	200 mA, 200 mA	150 mA	550 mA, 200 mA, 150 mA, 150 mA
SYSTEM MANAGEMENT	ADC	10-bit		
	FUEL GAUGE	●		
	HARD SYSTEM RESET	●		
	TIMED WAKE-UP	●		●
	WATCHDOG TIMER	●		●
	SHIP MODE / HYBERNATE	●	●	●
	BROWN-OUT DETECTOR	●	●	●
	LED DRIVERS, GPIOs	3, 5	2, 0	0, 3
	CONTROL INTERFACE	TWI	Pin-configurable	TWI
REGULATORY COMPLIANCE		CE, JEITA, RoHS	CE, JEITA, RoHS	CE, RoHS
OPERATING TEMPERATURE		-40 to 85°C	-40 to 85°C	-40 to 85°C
EVALUATION KITS		nPM1300 EK	nPM1100 EK	nPM6001 EK
PACKAGE OPTIONS		5x5 mm QFN32, 3.1x2.4 mm WLCSP	4x4 mm QFN24, 2.1x2.1 mm WLCSP	2.2x3.6 mm WLCSP

Range Extender

nRF21540

Description: The nRF21540 is an RF front-end module (FEM) that improves range and connection robustness for Nordic nRF52 and nRF53 Series SoCs. The nRF21540 is a complementary device operating as a 'plug-and-play' range extender with the addition of just a few external components. The nRF21540's 13 dB RX gain and low noise figure of 2.7 dB, coupled with up to +21 dBm TX output power, ensure a superior link budget boosting the range of supported SoCs by between 6.3 and 10x. The RF FEM suits all applications that require increased range and/or robust coverage. In demanding RF environments, or where the application is operating close to the range limit, it can be more energy efficient to use the nRF21540 than continuously resend packets.

Operation: The nRF21540 supports Bluetooth LE, Bluetooth mesh, Matter, Thread, Zigbee and 2.4 GHz protocols. The RF FEM's TX output power is dynamically adjustable and can be set to comply across all geographical regions. The RF FEM can be used with Nordic's extended temperature-qualified nRF5340, nRF52833 and nRF52820 SoCs in industrial applications.

Tech Spec

Output power
Adjustable in small increments up to +21 dBm

Receive gain and noise figure ratings
13 dB receive gain. 2.7 dB noise figure

Input supply
1.7 to 3.6 V

Package
4 by 4 mm QFN16

Development bundle
nRF21540 DK and nRF21540 EK. The EK is a shield for use with nRF52 and nRF53 Series DKs

Applications
Asset tracking, smart home, industrial, toys, audio

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 or Cloud-to-Cloud use. 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 in nRF Cloud and include GPS, cell-based and Wi-Fi assisted locationing. The product supplies accurate, rapid location data for IoT devices. The A-GPS service reduces time-to-first-fix. The result is lower latency and lower power consumption. P-GPS downloads predictive data, extending the validity of assistance data. For Wi-Fi location, the device scans two or more Wi-Fi APs and sends network information to nRF Cloud, where the location is calculated. Cell based services use base stations to predict location. Each location feature has its advantages, so switching between different location services during operation can be useful.

Tech Spec

Location services
Assisted GPS (A-GPS), Predictive GPS (P-GPS), Single-Cell (SCELL), Multi-Cell (MCELL), Wi-Fi

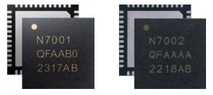
Additional features
Supports Cloud-to-Cloud use cases for devices provisioned to a different Cloud provider

Supported products
nRF9131 SiP, nRF9160 SiP, nRF9161 SiP, nRF9160 DK, Nordic Thingy:91, nRF7002 companion IC

Applications
Industrial, smart appliances, asset tracking, RTLS

Wi-Fi 6 companion ICs

nRF70 Series



Description: The nRF7001 companion IC is a low power Wi-Fi solution for end products requiring 2.4 GHz connectivity only. The nRF7002 can be used in both the 2.4 and 5 GHz bands. The products offer good coexistence with Bluetooth LE devices and feature one Spatial Stream (SS), 20 MHz channel bandwidth, 64 QAM (MCS7), 86 Mbps PHY throughput and OFDMA (downlink and uplink).

Operation: The nRF70 Series companion ICs provide low power, secure Wi-Fi connectivity as well as Wi-Fi assisted locationing based on Service Set identifier (SSID) scanning. The ICs incorporate Wi-Fi 6's Target Wake Time (TWT), a power-saving feature allowing the ICs to negotiate a wake-up schedule with the access point (AP) to which it is connected. The nRF70 Series accompany Nordic's nRF52 and nRF53 Series Bluetooth LE SoCs, and the nRF91 Series cellular IoT SiPs. The nRF70 Series can also be used as companion ICs in applications hosted by non-Nordic products.

Tech Spec

Compliance
IEEE 802.11b (Wi-Fi 1)/a (Wi- Fi 2)/g (Wi-Fi 3)/n (Wi-Fi 4)/ac (Wi-Fi 5) (not the nRF7001)/ax (Wi-Fi 6)

Package
6 by 6 mm QFN

Features
Low power, good coexistence with Bluetooth LE, TWT

Development tools
nRF7002 DK, nRF Connect SDK

Applications
Asset tracking, smart home, industrial