Connecting the Unconnected: The Unique Power of NFC in IoT Data Acquisition

March 2021

NFC FORUM

Contents

Introduction 3

The Unique Benefits of NFC in IoT Data Acquisition 4

Initializing and Personalizing IoT Sensors with NFC 5

Using NFC to Collect Data from Offline Home Sensors 6

- Use case: NFC-enabled circuit breaker 7
- Use case: Expert bonsai tree care with NFC 7

Using NFC to Collect Data from Health Sensors 7

- Use case: Wearable health sensor patches 9

Using NFC to Collect Data from Legacy Industrial Systems 9

- Use case: Industrial system configuration 10
- Use case: Industrial system maintenance and monitoring 10

Using NFC to Collect Data from Products Across the Cold Chain 10

- Use case: Fine wine cold chain monitoring 11
- Use case: NFC-enabled food packaging, storage, and shipping 11

NFC-Authorized Third-Party IoT Sensor Data Access 12

Meeting the Growing Demand for IoT Data Acquisition 13

Contributors:

Preeti Ohri Khemani, NFC Forum Vice-Chair, Senior Director System Engineering, Infineon Technologies

Vince Coli, Senior Product Manager, Socket Mobile, Inc.

Giuliana Curro, Senior Marketing and Business Development Manager, STMicroelectronics

Erich Reisenhofer, Product Manager for NFC Connected Tag Solutions, NXP Semiconductors

Christian Lesjak, Product Definition Engineer for Embedded Security Solutions, Infineon Technologies

Introduction

The Internet of Things (IoT) promises a future in which businesses and consumers benefit from dramatic increases in efficiency, productivity, ease, and speed. If the predictions become reality, industrial machines will alert companies before they fail, traffic jams will be sharply reduced, homes and offices will be vastly more energy-efficient, chronic health conditions will be better managed and treated, and much more.

However, it must be noted that all of these benefits will only become reality if we can effectively capture, analyze, and report previously-unavailable data from electronic devices – from industrial equipment to smart home appliances.

Companies across industries are already deploying IoT solutions that: uncover insights to inform the product development process; find new revenue-generating opportunities; cut service costs; and more. By 2030, it is estimated there will be 125 billion IoT devices installed and connected to the Internet, up from 11 billion in 2018[1]. Most of those devices will be designed to collect and transmit data in real time or upon request.

By 2030, it is estimated there will be

125 BILLION
IoT devices

installed and connected to the Internet, up from 11 billion in 2018

As manufacturers consider IoT-enabling their products, they must first answer some important questions:

- Internet connection: What is the best way for the device to connect to the Internet?
- Data security: What are the security risks and how can they be mitigated?
- Data privacy: What are the data privacy risks and how can they be minimized?
- Form factor: How will these considerations affect form factor and manufacturing costs?
- Power requirements: What will the impact be on power consumption and battery life?
- Firmware updates: How will firmware updates be performed?
- Network interruptions: What will happen in the event of a network interruption?
- User interface: Will the device require a user interface or could it be controlled via a mobile device?

NFC technology can provide needed answers to these and other questions. NFC supports IoT data acquisition by enabling on-demand Internet connectivity, leveraging smartphone interfaces, reducing power consumption, keeping manufacturing costs under control, and minimizing security risks.

This white paper explores a variety of IoT scenarios and how NFC technology can play a key role in supporting secure, efficient data acquisition.

[1] https://www.dbs.com/aics/pdfController.page?pdfpath=/content/article/pdf/AIO/062018/180625_insights_internet_of_things_the_pillar_of_artificial_intelligence.pdf

The Unique Benefits of NFC in IoT Data Acquisition

The preferred means of data acquisition from IoT devices largely depends on the application and the environment in which it is operating. For example, in an enclosed, fully-wired environment, the most sensible approach is to collect data directly from IoT devices plugged into the facility's Local Area Network (LAN). The network infrastructure already exists and a wired connection is generally stable and reliable.

Other IoT applications involve longer distances and/or more changeable, complex, or uncontrolled environments, thereby making wireless technologies, such as Bluetooth and Wi-Fi, or even longer-range connection technologies, such as Lora, Sigfox, SubGHz, NB-IoT, more appropriate for data acquisition.

However, in some situations, these long-range wireless technologies alone are not sufficient – especially in case of an issue. That's when NFC can act as a vital complementary solution for IoT data acquisition. These situations include:

- **When downlink or uplink communication performance or topology issues result in the loss of data from certain IoT nodes.** NFC enables users to retrieve data directly from the IoT node via an NFC-enabled smartphone or reader.
- **When power to the IoT node is switched off or the battery is dead.** Unlike other technologies, NFC is capable of retrieving 100% of the data in these situations, due to its ability to supply power wirelessly via electromagnetic induction.
- **When the local network fails.** Using an NFC-enabled smartphone, users can capture the data from the IoT device and transmit it via the phone's mobile network.

NFC also provides the only practical data acquisition solution for certain IoT use cases. These include:

- **When the IoT device is not within range of a local network.** Many IoT applications – for example, sensors monitoring railroad tracks – are located far from the nearest local network. NFC does not need to be connected to the local network.
- **When security concerns demand that an IoT device only maintains its connection to the network while transmitting or receiving data.** A device that is always active on the network is more vulnerable to hacking. With NFC, it's possible to keep a device offline except for the short time when the user's tap-and-handover action enables data acquisition.
- **When battery life concerns demand that an IoT device does not maintain continuous connection to the network.** If always on, battery-powered IoT devices can quickly drain their power. This can make them costly to operate and maintain over time. With NFC, an IoT device can be used on the network only when necessary and for as long as necessary to conserve energy and prolong battery life.
- **When the IoT device is not self-powered.** Many potential IoT applications need to gather data from devices that have no power supply of their own – for example, moisture, temperature, or pH sensors – NFC's electromagnetic induction can provide all the power necessary to transfer the acquired data.

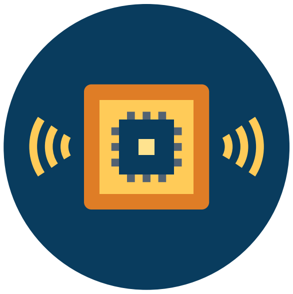
In addition, NFC offers other advantages to make IoT applications easier and more affordable to deploy, implement, and maintain. For example:

- **NFC enables users to perform complex device settings easily using a phone or tablet touchscreen.** NFC can allow a mobile device to serve as the user interface for devices such as heaters, thermostats, and alarm systems. This eliminates the need to add buttons or displays to the IoT device, thereby keeping costs down. Also, some IoT devices may be too small to allow for a user interface; NFC can enable users' mobile devices to provide that interface. Additionally, this allows manufacturers to leverage the power of mobile devices to offer a simpler, faster, more intuitive, or even more customizable user interface.
- **NFC enables users to perform device firmware upgrades via the phone or tablet connection.** Many IoT devices, such as smart home appliances, require periodic firmware upgrades, often for security purposes. Ordinarily, device manufacturers would have to send a technician to each location to perform the firmware upgrade –a costly and labor-intensive effort in many cases. But with NFC, device end users can perform the firmware upgrades themselves – quickly and securely – using their mobile devices.
- **NFC enables users to implement password protection.** Many IoT devices are vulnerable to tampering by hackers. NFC can help address this problem by allowing users to set up and enter strong passwords to enable access.

By addressing these needs and providing such capabilities, NFC makes the deployment and use of IoT devices more versatile, flexible, and secure for both manufacturers and end users.

Initializing and Personalizing IoT Sensors with NFC

NFC-enabled IoT sensors can easily be initialized and configured using NFC mobile phones with just one tap. The NFC Forum Tag NDEF Exchange Protocol (TNEP) enables the bidirectional data exchange and ensures a seamless data exchange between IoT sensors with any NFC Forum-certified mobile device. The sensor itself may even not require an onboard power supply as the required power can be supplied via NFC field. This means battery-free devices can be fully sealed to protect them from dust and moisture and still be connected to the cloud using a mobile device with NFC support.



In addition, the bidirectional communication ability of TNEP allows NFC-enabled smartphones to read the actual state and update the configuration of IoT devices (e.g., showing the title of music being played; enabling adjustment of the device's equalizer setting to suit the type of music being played). Thus, NFC can be used, for example, to configure an audio system, digital camera, lighting system, smart meter, or radiator valve.

Using NFC to Collect Data from Offline Home Sensors

Many of the early IoT devices for home use were online products, such as smart thermostats and security cameras. These products were standalone, easy to install, and designed to operate continuously, so it made sense to have them transmit data via Wi-Fi.

However, as manufacturers seek to IoT-enable more home products, there are many devices that either cannot or should not be continuously connected via Wi-Fi, for the following reasons:

- **Form factor.** Size constraints prohibit the inclusion of a Wi-Fi transceiver or an easy-to-use interface.
- **Installation challenges.** The device needs to fit into existing small or difficult-to-access spaces.
- **Power needs.** The device's power consumption requires AC instead of a battery; or its battery power consumption would require too-frequent battery changes.
- **Security concerns.** A device that is continuously connected via Wi-Fi has a greater vulnerability to hacking.
- **Cost constraints.** IoT-enabling a product as an online device can push its cost higher than what consumers are willing to pay.

Manufacturers who have faced these obstacles but still want to add value and achieve a competitive advantage by IoT-enabling their products can do so by designing their devices with offline sensors that use NFC as their means of data acquisition. With NFC, manufacturers can:

- **Overcome form factor limitations.** Equipping a device with an NFC-based offline sensor requires very little additional space and the user interface can be supplied by the NFC-enabled device that acquires and transmits the data.
- **Enable easier installation.** An NFC-enabled device can be installed virtually anywhere.
- **Supply power.** Many NFC-enabled devices use little or no power. An offline sensor can use power supplied by an NFC-enabled device through electromagnetic induction to perform all data acquisition/transmission tasks. This eliminates the need for batteries or AC power.
- **Reduce security concerns.** An offline sensor is only online during the brief time when data is being transmitted. The short operating range of NFC makes man-in-the-middle attacks[2] very unlikely.
- **Meet manufacturing cost targets.** NFC-enabled sensors and tags are affordable, and many of these use cases take advantage of NFC-enabled devices such as smart phones that users already have.

[2] https://en.wikipedia.org/wiki/Man-in-the-middle_attack

In addition to these benefits, NFC's one-tap paradigm is simple, intuitive, and reliable, thereby eliminating training requirements and reducing customer service and call center costs.

Use case: NFC-enabled circuit breaker

A global leader in electrical equipment manufacturing recently introduced a smart circuit breaker that includes onboard Ethernet communications and active power metering. It is able to self-diagnose problems and send instructions to facilities managers to maximize uptime. While Bluetooth is the primary wireless communication means, the circuit breaker also includes NFC so that facilities managers can monitor the device's condition even in a power outage.

Use case: Expert bonsai tree care with NFC

Bonsai trees can notoriously difficult to grow, requiring regular and careful monitoring, watering, fertilization, and pruning. However, a solution has been developed that uses NFC to enable expert care. A battery-free NFC device is embedded in the bonsai pot, capturing key measurements of soil and temperature conditions. The user holds an NFC-enabled smartphone to the tag to provide power and capture the data. The data is then uploaded to a web application in the cloud, which analyzes the data to provide the user with care instructions.

As these use cases demonstrate, NFC offers significant benefits to both manufacturers and consumers. With NFC:

- More products can be IoT-enabled.
- More valuable data can be collected, analyzed, and acted upon.
- Consumers gain a better understanding of what's going on in their homes.
- Consumers gain more power to control their homes and improve efficiency.

Using NFC to Collect Data from Health Sensors

Home health monitoring is a growing trend as consumers become more health-conscious, the population ages, the incidence of chronic conditions increases, and healthcare costs rise.

Fortunately, technology developments have made it possible for patients to track their own health measurements and share information remotely with their doctors. The Remote Patient Monitoring (RPM) market is projected to grow 6.2% annually over the next five years[3] as more patients use home health monitoring devices to capture measurements such as body temperature, weight, blood pressure, and glucose levels to better control heart disease, obesity, diabetes, and more.

[3] https://www.mordorintelligence.com/industry-reports/global-remote-patient-monitoring-system-market-industry

In addition to ensuring device accuracy, manufacturers of RPM products have two non-negotiable needs:

- **Data integrity.** The effectiveness of "telehealth" systems depends on protecting the integrity of the RPM data as it travels from the device to the care provider for storage, review, and analysis.
- **Privacy.** Laws such as HIPAA in the US and GDPR in Europe have mandated that healthcare providers take steps to maintain the confidentiality of patient information.

For these reasons, any manufacturer of home health monitoring devices must consider data security a high priority in the design and engineering of their products. One way manufacturers can help maintain data security is by making their devices offline sensors. Sensors that are continuously online are more vulnerable to hacking from bad actors, while an offline sensor is only online during the brief time when data is being transmitted.

RPM device manufacturers also need to consider:

- **Cost.** Solutions that provide accurate readings at the lowest cost have a competitive advantage.
- **Power requirements.** A solution that requires no onboard power supply is preferable to one that requires batteries or external power.
- **Ease of use.** If patients are to perform their own health monitoring, the solution has to be fast, easy, and intuitive to use.

NFC technology can address all of these needs, in the following ways:

- **Ensuring explicit user intent.** Unlike other "always-on" technologies, NFC's touch paradigm is intended to explicitly indicate intent. A user has to take an action (tapping their NFC-enable device) for data transmission to occur. And because NFC supports offline sensors, it only provides connectivity when it is needed, thereby safeguarding confidential patient data.
- **Supporting data security.** NFC operates across a very short range, greatly reducing the threat of man-in-the-middle attacks. NFC also allows for the use of digital signatures to authenticate the source of data, and permits the use of hardware-based security controllers as security anchors.
- **Controlling costs.** NFC keeps costs down because NFC tags are small and inexpensive and can be embedded in disposable sensors. With no need for onboard power, manufacturing costs are lower.
- **Eliminating power requirements.** NFC tags need no power supply of their own, so no battery or external AC power is required. Instead, power is supplied through electromagnetic induction by the NFC-enabled device reading the tag (typically, a smartphone or tablet).
- **Ensuring ease of use.** NFC is an intuitive technology that operates with a simple tap; there are no instructions or training required.

In addition to these benefits, NFC is designed to work with home health devices. The NFC Forum's Personal Health Device Communication (PHDC) Technical Specification provides an openly-defined standard for the exchange of personal health data between devices conforming to the ISO/IEEE Std. 11073-20601 Optimized Exchange Protocol and NFC Forum specifications.

Use case: Wearable health sensor patches

A US-based manufacturer offers a broad line of wearable, disposable self-adhesive health sensor patches that are no thicker than ordinary adhesive bandages but include health monitoring technologies and NFC tags for data acquisition. For example, an NFC-enabled diabetes patch performs accurate and pain-free monitoring of blood glucose levels, and a fitness-monitoring version can measure a variety of fitness biomarkers, including heart rate, temperature, hydration, sweat, lactic acid, and electrolytes.

In the future, as wearable health sensors become ubiquitous, NFC will increasingly become the de facto standard for communicating with these devices.

Using NFC to Collect Data from Legacy Industrial Systems

An estimated 50% to 75% of legacy industrial systems are not yet network-attached. These unconnected machines have no means of sharing or transmitting their data and no intuitive user interfaces. This prevents organizations from gathering and analyzing the data for decision-making and from deploying new IoT-based services, such as remote support, diagnostics, and maintenance.

This problem is compounded by the fact that many industrial systems have long lifespans – up to 25 years – and the only way to provide connectivity has been to redesign the machines, a long and costly process.

Fortunately, solutions exist to IoT-enable any existing electronic system with an embedded processor and a debug port using NFC – and without modifying its initial design.

One solution is based on using a connectivity module containing a co-processor that supports NFC and the direct connection of the module to the debug port of a system's microcontroller. (Modules with Bluetooth Low Energy and Wi-Fi support are also available.) The connectivity module plugs into the microcontroller debug port of a product's embedded electronic system.

The connectivity module is complemented by a mobile phone app that supports the NFC interface connectivity. Developers and third parties can create their own IoT applications for particular use cases.

NFC provides easy one-tap connectivity between the connectivity module and the user's smartphone, enabling the collection of machine data and, if desired, uploads that data to the cloud.

To ensure secure data acquisition and transmission, the solution supports local security measures at the module level, including the definition of user profiles and the encryption of the smartphone-to-module communication channel.

The overriding benefit of this approach is that it enables the creation of IoT solutions while protecting the existing capital investment in industrial machines. At the same time, it is easy to implement, saves energy, and reduces data collection errors.

Use case: Industrial system configuration

System installers can leverage the smartphone interface or app to quickly and easily create a specific machine configuration. With the configuration parameters set in the smartphone app, the installer taps the NFC tag and maintains the connection while the configuration data is transferred to the machine.

The installer then launches a verification app that confirms the coherence and validity of the configuration. The history of these actions is transferred back to the manufacturer with the installer's credentials via the smartphone's Internet connection. Back-end systems stock all relevant information and trigger the start of the customer's guarantee and service contract.

Use case: Industrial system maintenance and monitoring

In this use case, the machine is authorized to connect to a monitoring network. The maintenance technician uses NFC and the smartphone to make the connection and validate the machine. Then the software wakes up, configures and opens a long-range, low-power interface, which is then used for permanent monitoring of machine status and alarms.

When an alarm is detected, the technician uses NFC to connect to the correct machine, signs the machine out of the monitoring network, corrects the problem, and verifies correction via the NFC interface. When everything checks out, the technician returns the machine to the monitoring network. All information about the intervention is sent to the cloud via the smartphone's cellular network.

Using NFC to Collect Data from Products Across the Cold Chain

To ensure their quality, many products – such as fine wines, perishable foods, and certain pharmaceuticals – need to be kept at a consistent temperature as they travel through the supply chain from the distribution center to their final destinations. However, until recently, companies had no effective way of monitoring their products' temperatures while in transit.

This meant there was no way to assure customers of product quality and performance, to identify problems in the cold chain, or to ensure accountability for any problems.

This would seem like an ideal opportunity for an IoT solution, but there is no reliable, consistent network access while products are in transit.

However, NFC enables an array of IoT solutions that allow product temperatures to be monitored, recorded, collected, and transmitted across the cold chain.

Here's how it works:

1. A small smart label equipped with a temperature sensor, timer, and NFC chip is inserted inside the shipping container.
2. Optionally, another smart label can be attached to the outside of the container to monitor the environment in which it is being shipped (such as inside a tractor trailer).
3. The smart sensors measure and record the temperature data throughout the cold chain.
4. The data can be captured and transmitted via cellular networks at any point in the cold chain by tapping an NFC-enabled device to the smart label.

These solutions offer benefits for everyone:

- Customers are assured that the products they have purchased have not deteriorated in transit.
- Manufacturers and distributors have hard data to prove that proper temperatures were maintained.
- Companies can collect data to identify and remediate problems.
- Companies can optimize their shipping methods to ensure top quality, performance, and customer satisfaction.

Use case: Fine wine cold chain monitoring

A producer of fine Italian wines puts an NFC-enabled smart label in each case of wine before shipping. The label is programmed to record a temperature history at defined intervals during transit. Upon arrival (or at any point en route), temperature data can be uploaded to the cloud via NFC. The result is that both wine consumers and wine producers gain the assurance that the wine has maintained its quality in transit so that the consumer can fully enjoy it as it was meant to taste.

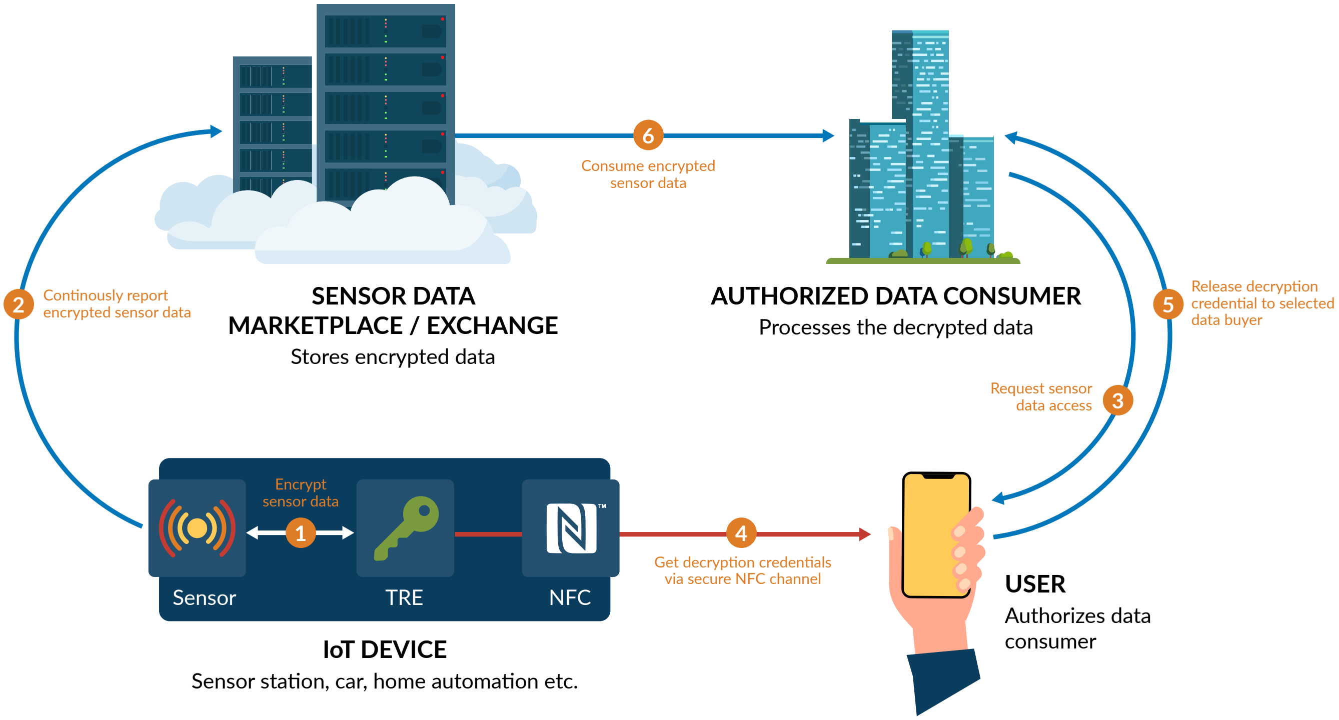
Use case: NFC-enabled food packaging, storage, and shipping

A manufacturer in Poland uses NFC-enabled data loggers and NFC-connected boxes for customizing and monitoring temperatures in its food-based cold chain packaging, storage, and shipping business. Using an NFC-enabled phone or device, a user can scan the manufacturer's label on a fridge or on an NFC-connected box to receive information about current and historical temperature for this specific location.

NFC-Authorized Third-Party IoT Sensor Data Access

As the number of devices connected to the IoT grows into the tens of millions, the risk of losing data to hackers or unauthorized data consumers has increased dramatically. NFC can be used:

- to protect and authenticate IoT data
- for user-controlled access to IoT data
- for (eventually) monetization of IoT data


6
Consume encrypted sensor data
2
Continously report encrypted sensor data
SENSOR DATA MARKETPLACE / EXCHANGE
Stores encrypted data
AUTHORIZED DATA CONSUMER
Processes the decrypted data
5
Release decryption credential to selected data buyer
Request sensor data access
3
Encrypt sensor data
1
Sensor
TRE
NFC
4
Get decryption credentials via secure NFC channel
USER
Authorizes data consumer
IoT DEVICE
Sensor station, car, home automation etc.

Here's how it works:

1. Data acquired by a connected IoT device is protected, such as encrypted and authenticated, using mechanisms of a connected Tamper-Resistant Element (TRE).
2. The encrypted data is continuously transferred to a cloud service, called the Sensor Data Marketplace/Exchange. For example, a smart home sensor collects and relays encrypted sensor data to a smart home cloud; or a connected automobile collects data about road conditions and transmits this data to the road infrastructure database. In either case, the data is encrypted before transmitting it to the cloud.
3. Interested parties can only become Authorized Data Consumers if the user who generated the data actively procures user credentials for these parties. The user is in control of the terms and conditions for access to the data.
4. The user grants access to the encrypted data by reading out the decryption credentials using their mobile device via the NFC interface of the IoT device.
5. The user provides the decryption credentials, under user's terms and potentially in exchange for money or credits, to the Authorized Data Consumer.

6. The Authorized Data Consumer consumes the encrypted IoT device data and decrypts it for further processing.

In this way, NFC provides user control over IoT data, while improving security and making data sharing and authentication easy and secured.

> *Note: The important security primitive for this use case is encryption. This, of course, does not rule out the use of additional protective measures, such as data or user authentication, which may also be based on the IoT device's cryptographic credentials in the TRE, and which may also be read out conveniently via the NFC interface. State-of-the-art cryptographic schemes provide system designers with a broad toolbox of options, depending on specific use case needs.*

Meeting the Growing Demand for IoT Data Acquisition

IoT is still in the early stages of its projected explosive growth. Supporting technologies, such as micro-sensors and 5G networks, will only increase its momentum. As businesses and consumers reap more of the benefits of IoT, demand for new, innovative IoT solutions will only grow.

Developers creating IoT solutions will need to consider how best to connect IoT devices to acquire and transmit data. By offering a solution that requires no continuous power supply, reaches areas beyond easy Internet access, enables expressed user control, and takes advantage of the millions of smartphones already in use around the world, NFC will continue to be the IoT data acquisition technology of choice.

The NFC Forum is committed to serving the evolving needs of the IoT ecosystem. To learn more, visit nfc-forum.org.