

# Multi-Modal NFC for Industrial Sensors

Billy Baker, John Woods, and Martin J. Reed

University of Essex, UK

{bb18655, woodjt, mjreed}@essex.ac.uk

**Abstract**—Near-field communication (NFC) is increasingly being explored for sensing and embedded system applications beyond consumer smartphones, particularly in domains such as smart factories and smart lighting. However, existing NFC deployments are constrained by the limited range, power delivery, and communication reliability of portable readers, restricting their applicability in industrial systems requiring battery-less operation and real-time data exchange.

This paper presents a *Passive-Active NFC* framework for battery-less sensing and embedded applications, enabled by energy-harvesting NFC integrated circuits (ICs) and ultra-low-power microcontrollers. The framework defines four operational states: *Static Passive*, *Static Active*, *Dynamic Passive* (battery-less), and *Dynamic Active*, allowing flexible transitions between sensing, computation, and communication modes. Experimental evaluation is conducted using industrial Type 5 NFC ICs and both handheld and industrial NFC readers, with analysis of power consumption, communication range, reliability, and data integrity.

To support reliable data transfer, a novel NFC Communication Control Protocol is introduced to mitigate corruption during dynamic operation and concurrent communication events. Results demonstrate that industrial NFC readers can extend battery-less operating range up to an order of magnitude compared to consumer devices, while maintaining reliable data acquisition and transmission. The proposed framework enables robust battery-less sensing systems suitable for industrial applications.

**Index Terms**—Near Field Communication, Battery-less Systems, Industrial Electronics.

## I. INTRODUCTION

NFC is widely used in industrial and commercial contexts; however, it is typically limited to applications involving portable readers or powered tags. This paper explores the design, implementation, and evaluation of a Passive-Active NFC system, focusing on key components including NFC ICs, microcontrollers, and antennas. Experimental validation is used to assess operation in industrial environments, analyse the impact of antenna size on communication range, and evaluate power consumption across different microcontroller clock speeds. The introduction of a novel NFC Communication Control Protocol supports dynamic data exchange and mitigates data corruption. This work provides both a practical framework for deploying advanced NFC systems and insight into the associated design trade-offs.

The contributions of this paper are:

- 1) a definition of terminology for the different NFC states of operation;

- 2) introducing an NFC framework that enables transitions between NFC states, including those involving microcontroller operation;
- 3) and, demonstrating and quantifying this framework in a representative industrial use-case.

### A. Near Field Communication Overview

NFC is a short-range wireless communication protocol operating at 13.56 MHz [1] and is a subset of high-frequency (HF) RFID [2]. An NFC system consists of a Reader and a Tag, where the Reader provides both power and data, and the Tag acts as the receiver. Tags may be Passive, relying on harvested energy, or Active, powered by an internal source.

NFC supports five tag types [3]. Types 1–4 operate at ranges of approximately 10 cm under ISO/IEC 14443 [1], while Type 5 tags, based on ISO/IEC 15693, can extend to approximately 100 cm, making them suitable for industrial applications.

A Static Passive Tag typically consists of only an NFC antenna and NFC IC [4], whereas an Active Tag additionally includes a microcontroller and power source.

### B. NFC Terminology and Operating States

To avoid inconsistencies from previous literature, this work defines the following terminology relating to the NFC tag:

**Dynamic** NFC data exchange occurs via both a locally connected system (e.g., microcontroller) and an external NFC reader.

**Static** NFC data exchange occurs only via an external NFC reader.

**Passive** operation occurs without a direct power source and relies on reader energy.

**Active** operation uses an internal power source.

**Battery-less** operation is Dynamic Passive operation where both the tag and microcontroller are powered only when in the reader field.

**Passive-Active NFC** systems are capable of operating across multiple states.

The Passive-Active NFC framework classifies NFC systems along two dimensions: power source (Passive vs. Active) and behaviour (Static vs. Dynamic), as shown in Fig. 1. Passive modes rely on harvested energy, enabling Battery-less operation, while Active modes use internal power. Static states involve predefined behaviour, whereas Dynamic states include microcontroller-driven processing. This framework highlights

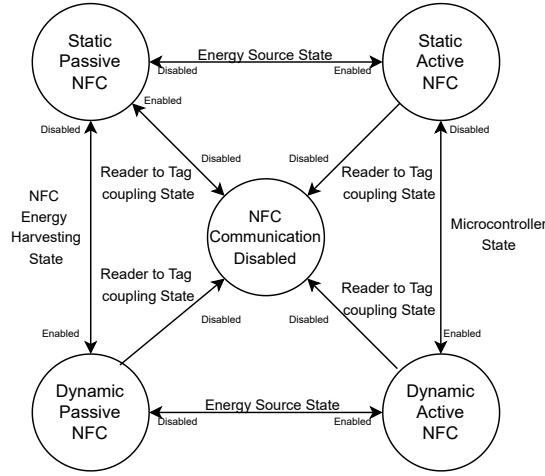


Fig. 1. Passive-Active NFC operational state diagram.

trade-offs between energy consumption, complexity, and functionality, and is particularly relevant for industrial embedded systems.

Within this framework, Static Passive represents the simplest mode, enabling low-power identification and data storage without internal processing. Static Active introduces internal power while maintaining fixed behaviour, improving reliability and range. Dynamic Passive enables Battery-less microcontroller operation using harvested energy, supporting sensing and data exchange with minimal power overhead. Dynamic Active combines internal power with full processing capability, enabling autonomous and complex system behaviour.

Transitions between these states are governed by power availability and system requirements. For example, a Static Passive system may transition to Dynamic Passive when sufficient energy is harvested to activate a microcontroller, while Active systems may switch between Static and Dynamic modes depending on processing needs. This flexibility enables adaptation across applications ranging from simple identification to smart industrial systems.

Battery-less NFC operates in the Dynamic Passive state, where harvested energy powers both the tag and connected circuitry [5]. As shown in Fig. 2, the absence of energy storage limits operation time, computational complexity, and communication range, with some systems operating below 20 mm [6], [7]. Increased power demand further reduces effective range.

A Passive-Active NFC system may combine multiple states, such as Dynamic Active and Battery-less operation or Static Passive and Battery-less operation, within a single system. This enables dynamic mode switching to balance power efficiency and functionality [8], [9].

Typical Battery-less applications include sensor systems such as smart bandages [10] and plant monitoring devices [11], [12]. Beyond sensing, applications such as NFC programming, distributed processing [13], and hybrid communication systems [14] can benefit from the Passive-Active NFC framework.

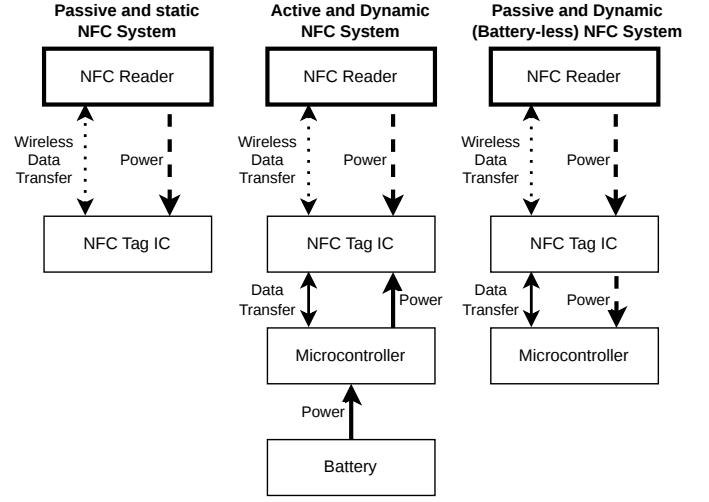


Fig. 2. Functional block diagrams of Static Passive, Dynamic Active, and Battery-less NFC systems.

TABLE I  
COMPARISON OF OTAP, IAP, AND ISP METHODS

| Feature               | OTAP                   | IAP                      | ISP                                     |
|-----------------------|------------------------|--------------------------|-----------------------------------------|
| Update Method         | Wireless               | Wireless Via application | Physical connection                     |
| Usage Scenario        | Factory programming    | Firmware updates         | Factory programming/debugging           |
| Deployment Complexity | Low                    | Medium                   | High                                    |
| Hardware Access       | Not required           | Not required             | Required                                |
| Downtime              | Often requires restart | Minimal                  | Often requires restart and Un-packaging |

### C. OTAP, IAP and ISP Description

In-System Programming (ISP) [15] is a wired method that programs a microcontroller via a preloaded bootloader, typically supplied by the manufacturer. While reliable, ISP requires direct physical access, making it the most complex to deploy, as summarised in Table I.

Over-The-Air Programming (OTAP) [16] enables wireless firmware updates. This requires a bootloader to support reader-to-microcontroller flash communication. OTAP can be implemented using either Passive or Active NFC systems. However, Passive NFC is constrained by limited tag memory, while Active NFC requires an external power source.

In-Application Programming (IAP) [17] provides an alternative approach, allowing modification of configuration data and variables without replacing the full firmware. Although less flexible than OTAP, IAP reduces data transfer requirements and enables efficient runtime updates.

The paper is organized as follows. Section II investigates the relationship between antenna size and programming range. Section III analyses system power consumption and microcontroller trade-offs. Section IV addresses reliability and error mitigation. Section V introduces the proposed NFC programming protocol and compares it with existing methods reported

in Table I. Section VI demonstrates a real-world smart lighting application. Section VII concludes the paper and outlines future work.

## II. THE NFC PROGRAMMING RANGE IN RELATION TO ANTENNA DIMENSIONS

The operational range between an NFC reader and tag represents the primary constraint in passive NFC systems, as it directly depends on both antenna dimensions and power transfer efficiency [18]. For a given operation, the power requirement remains fixed and limited by a defined threshold. Any surplus harvested energy beyond this requirement is dissipated and does not contribute to additional system functionality.

In contrast, active NFC systems are primarily constrained by their communication range and data transfer rate [19]. The communication speed determines how rapidly data transactions or command executions occur, while the duration of communication must align with the reader's operational availability to maintain reliable dynamic interaction. For Battery-less NFC implementations, the interplay between communication speed, range, and power consumption becomes even more critical [19]. Here, power consumption refers to the minimum constant energy required to complete a functional operation, such as a data write or sensor readout, using only the harvested RF energy.

It is important to note that, in active configurations, the amount of power that can be harvested from the RF field is negligible compared to that provided by an internal battery [20]. Typical NFC energy-harvesting circuits generate currents of up to 10 mA at 3.3 V, which restricts the system's ability to sustain prolonged or computation-intensive tasks [21], [22].

Consumer NFC readers, exemplified by smartphone NFC modules, are often portable, intended for single-tag utilisation, and frequently included in multifunctional products. These readers are equipped with miniature antennae, typically measuring less than 10 cm in size [21]. Conversely, industrial NFC readers [22] are designed for multi-tag settings. They utilise larger antennae and increased power outputs, enhancing reliability and reducing dependence on exact tag placement, albeit this compromises portability.

To validate the principles presented in this paper, an industrial use case was implemented on a custom-built system equipped with a low-power STM32 microcontroller, an ST25DV NFC IC, and peripheral circuitry for power measurement. A FEIG LR1002 industrial NFC reader was employed to emulate real-world smart factory conditions, allowing controlled evaluation of programming range, power stability, and communication reliability under varying operational parameters. This setup provided a representative test environment for assessing the effectiveness of the proposed Passive-Active NFC framework in practical industrial applications.

Experimental evaluation of NFC tag antenna types 1, 5, and 6, using an industrial NFC reader (Feig LR1002), is illustrated in Fig. 4 [22]. The experiment replicated a typical battery-less sensor application using a constant 2 k $\Omega$  resistor load.

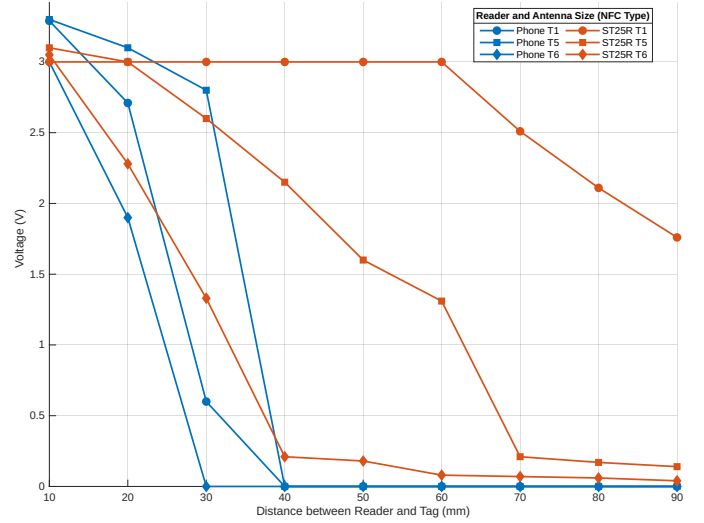


Fig. 3. Communication range of a portable NFC reader versus NFC tag antenna size.

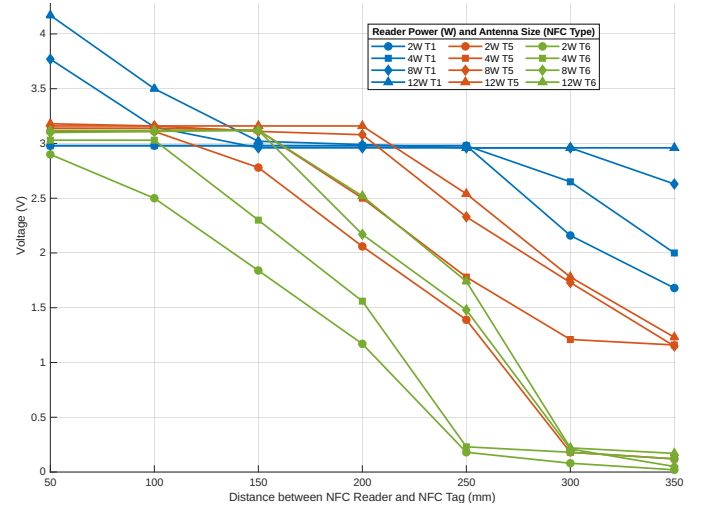


Fig. 4. Communication range of an industrial NFC reader versus NFC tag antenna size.

A Type 1 antenna functioning at 12 W had a communication range beyond 300 mm, but the same antenna at 2 W attained 260 mm. In these systems, the maximum attainable range is determined by the point at which the harvested voltage drops below the minimum threshold necessary for the chosen microcontroller. In this experiment, the base voltage was 2 V.

A good approximation for the relationship between NFC operating parameters and the coupling coefficient  $k(x)$ , at a distance  $x$  between antennas, is given by Finkenzeller [23] for when the radius of the reader antenna,  $r_R$ , is greater than the tag antenna radius,  $r_T$ :

$$k(x) \approx \frac{r_T^2 \cdot r_R^2}{\sqrt{r_T \cdot r_R} \left( \sqrt{x^2 + r_R^2} \right)^3} \quad (1)$$

TABLE II  
TIME REQUIRED FOR NFC READ AND WRITE OPERATIONS

| Clock-Speed       | 16 MHz  | 16 MHz  | 1 MHz   | 1 MHz   |
|-------------------|---------|---------|---------|---------|
| I2C-Frequency     | 400 kHz | 100 kHz | 400 kHz | 100 kHz |
| <b>Write (ms)</b> |         |         |         |         |
| 1 Byte            | 4       | 5       | 6       | 5       |
| 8 Byte            | 13      | 14      | 16      | 16      |
| 16 Byte           | 41      | 44      | 45      | 47      |
| 64 Byte           | 78      | 83      | 85      | 87      |
| 256 Byte          | 294     | 312     | 317     | 326     |
| <b>Read (ms)</b>  |         |         |         |         |
| 1 Byte            | 0       | 1       | 1       | 1       |
| 8 Byte            | 0       | 1       | 2       | 2       |
| 16 Byte           | 1       | 3       | 4       | 5       |
| 64 Byte           | 1       | 6       | 8       | 10      |
| 256 Byte          | 6       | 23      | 31      | 35      |

and when  $r_R < r_T$

$$k(x) \approx \frac{r_T^2 \cdot r_R^2}{\sqrt{r_T \cdot r_R} \left( \sqrt{x^2 + r_T^2} \right)^3} \quad (2)$$

In the case when the antennas have the same radius,  $r_R = r_T = r$ , this simplifies to:

$$k(x) \approx \frac{r^3}{\left( \sqrt{x^2 + r^2} \right)^3} \quad (3)$$

The performance of a consumer/portable NFC Reader was also evaluated as illustrated in Fig. 3. The evaluation shows that the consumer/portable reader has a maximum range that is an order of magnitude less than an industrial reader. The portable reader's lower power consumption and smaller antenna sizes are the reasons for this reduction. Nevertheless, the performance of the reader is significantly influenced by the size of its antenna. The FEIG and ST25R readers both have antennas that are larger than those of Type 1 tags, while the smartphone antenna is comparable in size to the tag antenna. This leads to a range of variations that are contingent upon the proximity of the tag antenna to the reader antenna. The coupling factor is responsible for this effect, which results in a decrease in efficiency when the antenna sizes are not compatible. The data in Fig. 3 is compatible with these observations, which indicate that the Type 5 antenna has lower range than the Type 6 antenna due to the high coupling factor of the Type 6 tag.

### III. MINIMAL VIABLE SYSTEM POWER CONSUMPTION AND ENERGY CONSTRAINTS

Using the experimental configuration described in Section II, Table II displays the measured timings for both block read and write operations at clock speeds of 16 MHz and 1 MHz, with varying Inter-Integrated Circuit (I2C) timings. The read time is significantly reduced at higher clock frequencies, but is also contingent upon the I2C speed. For example, when operating at a 16 MHz clock a change from 100 kHz to 400 kHz gives rise to a fourfold decrease in read time. The I2C speed also influences write time, although the effect is negligible as shown in Table II as the memory write time dominates over processor speed. For all results, read time is significantly shorter than write time, as expected.

TABLE III  
ENERGY CONSUMPTION AND PROCESSING TIME AT DIFFERENT CLOCK FREQUENCIES

| Clock Frequency | Estimated Current (mA) | Measured Current, $I$ (mA) | Processing Time, $t$ (ms) | Calculated Energy, $E$ (mJ) |
|-----------------|------------------------|----------------------------|---------------------------|-----------------------------|
| 16 MHz          | 1.09                   | 2.28                       | 20                        | 0.1368                      |
| 2 MHz           | 0.45                   | 0.75                       | 181                       | 0.40725                     |
| 1 MHz           | 0.31                   | 0.65                       | 430                       | 0.83205                     |

Where  $E$  is derived, at a voltage of 3 Volts as  $E = VIt$

While the power consumption, as presented in Table III offers useful insights for active NFC systems, it is the peak power consumption that becomes the dominant factor in Battery-less NFC designs. In these systems, the absence of any form of energy storage such as capacitors or batteries means that the available energy is limited to the instantaneous power harvested from the NFC field. As a result, even brief current spikes during data transmission or microcontroller operation can interrupt functionality or cause communication errors if the required peak power exceeds the harvested energy.

To maintain stable performance under these constraints, system timing and energy management must be carefully balanced. A higher microcontroller clock frequency can, counterintuitively, improve overall energy efficiency by shortening the execution time of critical tasks, thereby reducing the duration of high-power states. However, this advantage must be weighed against the corresponding increase in instantaneous current demand. Optimal operation, therefore, depends on identifying a clock frequency that provides sufficient processing speed to complete tasks reliably within the available time window, while avoiding excessive peak currents that may lead to data corruption due to power loss. This trade-off underscores the importance of dynamic power management and task scheduling in energy-harvesting NFC systems. Future implementations may benefit from adaptive clock-scaling techniques, where the system dynamically adjusts its processing speed based on available harvested energy, ensuring continuous operation even under fluctuating power conditions.

### IV. NFC RELIABILITY AND DATA INTEGRITY

#### A. Flowchart of Passive-Active Programming

Ensuring reliability and minimising data corruption are among the most critical components of NFC programming and communication. The reliability evaluation followed a write-and-confirm procedure, in which each random data block was first written to the NFC tag memory and then read back by the reader for verification. The returned data were compared with the original transmitted data, and the write operation was considered successful only when the two matched. This procedure is shown in Fig. 5. The NFC tag was programmed, and data integrity was evaluated to ascertain whether any data corruption had occurred. No miswritten bytes were detected in more than 10,000 runs that involved 256-byte writes, over a 7-day duration. This result was achieved under stationary conditions, where the NFC reader and tag remained

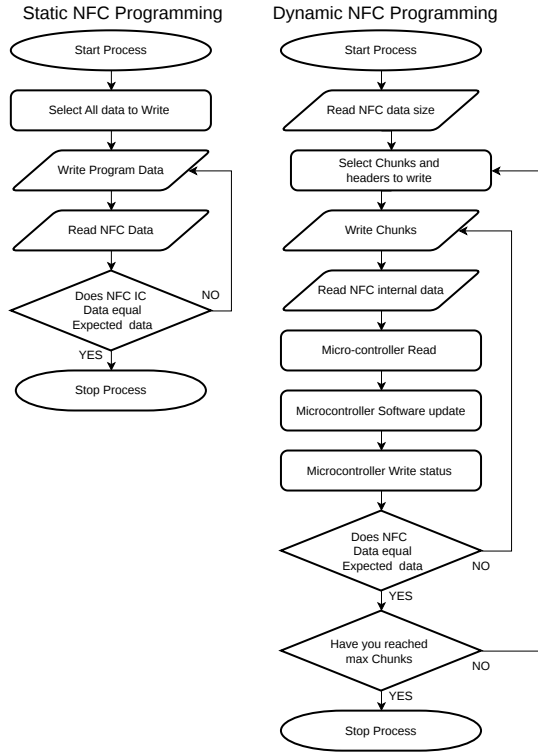


Fig. 5. Flowchart illustrating static and dynamic programming modes in the Passive-Active NFC framework.

fixed in position throughout the experiment. In practical use, movement or misalignment between the reader and tag may introduce additional communication errors.

In the second experiment, reliability over distance was assessed by placing a tag horizontally across the consumer NFC reader (ST25R3911) with a Type 1 antenna at fixed distances of [50,70,90] mm. The purpose of this configuration was to assess the degree of corruption that occurred during the NFC write process as distance increased. When the tag was in the operational range (between 50-70 mm), no data corruption was observed during the write process. A distinct cutoff distance was identified at 90 mm, at which communication ceased completely. The distance of 70 mm marked the maximum reliable operating distance for the system under the tested conditions.

To mitigate the risk of data corruption during Passive NFC write operations, a storage capacitor can be integrated into the circuit to ensure that the system retains enough charge for a sufficient duration following the loss of the external NFC field. This buffer period enables the microcontroller to complete ongoing write processes and gracefully terminate remaining tasks, thereby preventing incomplete data transfers. For example, in the test system described in Section II a minimum hold-up time of approximately 5 ms is required to guarantee a reliable write operation, with additional margin recommended to accommodate variations in load and supply voltage. The power consumption of the system is inherently linked to the clock frequency, and this relationship informs

TABLE IV  
OVERALL TIME REQUIRED FOR OTAP, IAP, AND ISP OPERATIONS  
(INCLUDING SETUP TIME)

| Feature             | OTAP   | IAP  | ISP  |
|---------------------|--------|------|------|
| Initial programming | N/A    | N/A  | Slow |
| Configuration       | Medium | N/A  | Slow |
| Updating            | Medium | Fast | Slow |

the calculation of the required storage capacitor for stable operation.

Under conservative conditions, the system must remain operational for the total duration of a multi-block transaction. For example, in a worst-case scenario for the test system described in Section II: maintaining power for 384 ms allowed multiple write cycles ensuring completion of the entire data exchange without corruption, although an added safety overhead is sensible. This design consideration is particularly critical in Battery-less NFC systems, where continuous power availability cannot be guaranteed, and reliable energy buffering is essential for consistent performance. However, even with a properly designed temporary energy storage failure can still occur and this needs to be considered as briefly described in Section V.

## V. NFC PROGRAMMING PROTOCOL

### A. OTAP, IAP vs ISP

Table IV compares OTAP, IAP, and ISP across initial programming, configuration, and updating. ISP is inconvenient for initial programming due to required physical access (i.e. overall slower), while OTAP and IAP rely on pre-existing firmware and are not typically used at this stage.

For reprogramming, OTAP enables wireless updates with moderate performance, whereas IAP is limited to configuration changes. ISP remains reliable but inefficient for large-scale deployment due to manual processes. During updating, IAP provides the fastest performance with minimal downtime, OTAP offers moderate performance due to flash reprogramming, and ISP is the slowest due to hardware access requirements. All methods require failure mitigation, typically reverting to a *known-good* state. OTAP and ISP present higher risk during failure and require robust bootloader recovery.

While OTAP and IAP can operate in Passive and Active NFC states, Passive NFC is constrained by limited memory, particularly for OTAP. Active NFC removes this constraint but increases deployment complexity due to external power requirements.

The Passive-Active NFC framework with Battery-less operation enables programming without external power connections beyond reader interaction, supporting scalable industrial NFC systems. In summary, IAP is optimal for updates, OTAP for flexible reprogramming, and ISP for reliable but less scalable operation.

### B. NFC Protocol Architecture and Message Structure

Figures 6 and 7 illustrate the protocol developed in this paper for NFC communication and programming. The primary

|     | Byte 1                              |                     | Byte 2          | Byte3  | Byte 4              |
|-----|-------------------------------------|---------------------|-----------------|--------|---------------------|
| 1   | Version                             | Type                | CHUNK AMOUNT    |        |                     |
| 2   | Password/Location information       |                     |                 |        |                     |
| 3   | Password/Location information       |                     |                 |        |                     |
| 4   | SYSTEM                              | LOCATION            | Memory Location | Status |                     |
| 5   | SYSTEM                              | CHUNKS Communicated |                 |        |                     |
| 6   | Location of next chunk (Block rows) |                     |                 |        |                     |
| 7   | Location of last chunk (Block rows) |                     |                 |        |                     |
| 8   | Last Chunk Loaded in memory         |                     |                 |        | Status              |
| 9   | CHUNK ID                            |                     |                 |        | Memory verification |
| 10+ | Payload .....                       |                     |                 |        |                     |

Fig. 6. Message Structure for the NFC Protocol.

motivation behind this protocol is to facilitate dynamic communication, addressing the limitations of existing protocols such as NDEF [24]. NDEF is not well-suited for dynamic communication as it does not provide application-level control for embedded programming, memory targeting, chunk tracking, status reporting, or verification. In contrast, the proposed *NFC Communication Control Protocol* has a message structure that extends the NFC exchange into a task-oriented protocol by adding versioning, message type, system/location fields, chunk management, memory location, status flags, and verification information. The status flag allows the NFC reader and embedded node to track the current state of the operation, such as whether the node is ready, busy, has loaded the last chunk into memory, completed verification, or encountered an error. Therefore, NDEF can be considered the transport or container format, while the proposed structure provides the higher-level control required for reliable NFC-based programming and diagnostics. Additionally, the new protocol is designed to optimize communication and is specifically built to function in memory-constrained environments. It operates with a minimum message length of 96 bytes, featuring a 32-byte header and 64-byte payload. In the experimental configuration, described in Section II, this approach requires 119 ms for a simple write operation.

The protocol structure outlined in Figures 6 and 7 is designed for Passive-Active NFC communication and stands in contrast to the NDEF protocol [24], which is optimized for the communication of any data type. A critical challenge in Battery-less communication systems is managing the prioritization of communication between the microcontroller and the reader. In most NFC systems, internal communication takes precedence over external communication. However, this can lead to data corruption if simultaneous communication occurs. To address this issue, a time-based or action-based system can be implemented to ensure orderly communication using the status field for coordination.

Figure 7 illustrates the three different message sequences for each of the operational states of NFC communication. It is evident that Static Passive NFC represents the simplest mode, as it operates without interruptions during communication. However, as previously mentioned, the data transfer in Passive NFC is constrained by the size of the NFC chip memory. In contrast, Active NFC ensures that the microcontroller remains powered, allowing for predictable communication timings. Nonetheless, interruptions can still occur, leading to delays and potential data corruption if not properly managed.

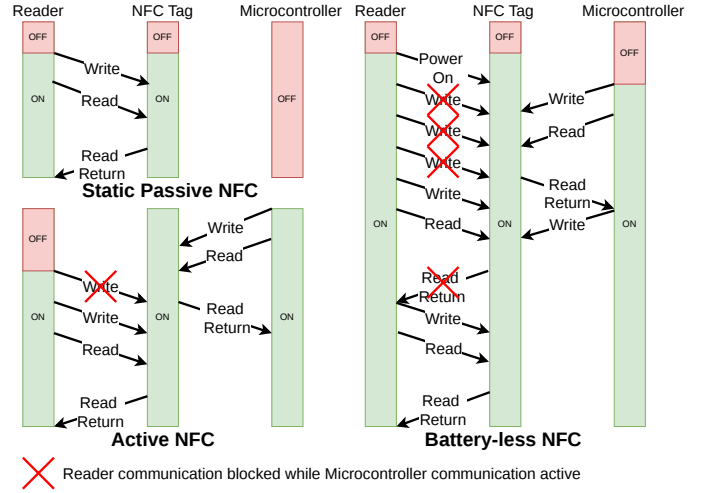


Fig. 7. Message sequence chart for NFC communication

The advantage of Active NFC is its ability to transfer and process data larger than the NFC memory, with the added benefit of predictable power consumption and the flexibility to adjust clock speeds, thus enhancing efficiency. However, a significant limitation is the requirement for an energy storage element, which may gradually discharge even when NFC communication is not taking place. Battery-less NFC is the most complex communication mode, requiring 100% uptime during communication and introducing unpredictability in the microcontroller's state in real-world scenarios. This presents challenges in maintaining the communication timing seen in Active systems. Nevertheless, the benefit is the ability to process data similar to an Active system while retaining the simplicity of hardware comparable to a Passive system.

A key challenge in Passive-Active communication is determining the system's mode, as distinguishing between Active and Battery-less states can be problematic. One potential solution is to use an internal measurement of the battery voltage, to determine whether the system is in Active or Battery-less mode. Some NFC chips are equipped with built-in NFC detection, which could enable switching between Battery-less and Active operational state. This approach implies that internal and external communications cannot occur independently. To mitigate this, a read operation can be used to determine the status of the communication, with write operations only allowed if the status flag is set and no interruptions occur. Prioritizing the read operation is important due to its faster communication speed, minimizing the time it takes to interrupt the NFC memory.

The specifications of NFC ICs vary significantly, but optimization can enhance communication speeds. However, there are limits to how fast communication can occur, based on factors such as NFC memory size, antenna coupling, and internal communication speed. NFC memory is typically constrained by the specifications of the chosen NFC IC, while antenna coupling influences both the range of communication and the relative sizes of the reader and tag antennas. Internal

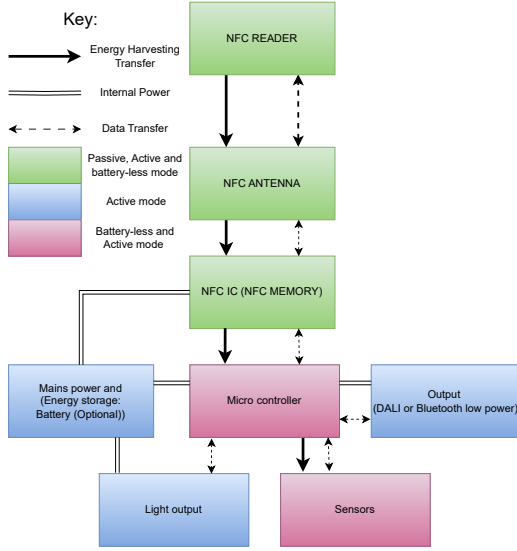


Fig. 8. Block diagram of an example multi-modal Passive-Active NFC system for an industrial lighting system.

TABLE V  
TYPICAL TASK COMPLETION TIMES FOR A PASSIVE-ACTIVE NFC  
LIGHTING SYSTEM

| Use-Case                             | Static Pas-<br>sive NFC (s) | Dynamic<br>Active NFC<br>(s) | Dynamic<br>Passive /<br>Battery-less<br>NFC (s) |
|--------------------------------------|-----------------------------|------------------------------|-------------------------------------------------|
| Firmware update                      | N/A                         | 3.14–12.74                   | 0.64–10.240                                     |
| Over-the-air pro-<br>gramming        | N/A                         | 12.74–53.70                  | 10.24–51.20                                     |
| Diagnostics                          | 0.13–2.05                   | 2.63–12.74                   | 0.13–10.24                                      |
| Inventory track-<br>ing              | 0.76–12.29                  | 3.17–14.79                   | 0.77–12.29                                      |
| Sensor reading                       | N/A                         | 13.38–63.94                  | 10.88–61.44                                     |
| Low-power<br>hybrid<br>communication | N/A                         | N/A                          | 10.88–61.44                                     |
| Hybrid communi-<br>cation            | N/A                         | 13.38–63.94                  | N/A                                             |
| Security update                      | 0.76–12.29                  | 13.38–63.94                  | 10.88–61.44                                     |
| Lighting control                     | 0.76–12.29                  | 3.17–14.79                   | 0.77–12.29                                      |

communication speed depends on the microcontroller's clock speed and the communication bus (e.g., I2C or SPI) between the microcontroller and the NFC IC.

As demonstrated by previous experiments, higher peak power availability leads to more efficient communication. The most effective way to increase peak power is outlined in Section III, which recommends increasing antenna size or reducing the minimum range between the reader and tag. Antenna coupling directly impacts overall power consumption.

## VI. REAL-WORLD INDUSTRIAL CASE STUDY: SMART LIGHTING

Passive-Active NFC can be used to expand into many industrial use cases, for example firmware updates in smart factories or for Passive-Active configuration/programming of

products; further examples are shown in Table V. Figure 8 shows an abstract block diagram for a real-world Passive-Active system. One of the unique features of this work is that the system can include all four NFC states – Static Passive, Static Active, Dynamic Active, and Battery-less – in a single system.

Table V estimates task completion time from the required NFC transfer size with a write time of 5 ms per byte and a read time of 1 ms per byte (Table II). Dynamic Active NFC includes an additional 2.5 s delay for powered processing, which increases the total completion time. Dynamic Passive, or battery-less NFC, is limited by harvested energy, so smaller tasks use 128–2048 byte transfers, while larger tasks may require 2048–10240 bytes depending on the application. Table V therefore compares the suitability of each Passive-Active NFC state for different lighting-system tasks.

An experiment was conducted to evaluate the performance and versatility of the Passive-Active NFC system within a smart lighting setup, using the configuration described in Section II. The test involved a prototype lighting module equipped with all four NFC states (Static Passive, Static Active, Dynamic Active, and Battery-less) integrated into a single control unit and an NFC IC with 2048 bytes of memory. The system was tested in both factory and end-user site environments across several real-world tasks, including firmware updates, diagnostics, lighting control, and sensor data retrieval. A mobile NFC reader and a standard NFC-enabled diagnostic tool were used to initiate interactions under different power conditions. The results of this testing are summarised in Table V, showing the estimated real-world time per task for the Passive-Active NFC lighting module. The use cases vary widely across both factory and customer premises. Table V shows how NFC can be used in a smart factory for inventory and/or OTAP, or firmware updates. In the factory setting, where bulk changes are often required for products, time to complete a task is critical; consequently, Active NFC is discouraged due to the time required to add external power, whereas Battery-less and Static Passive do not require external power.

In summary, the real-world testing showed that Static Passive NFC was most effective for quick, low-power tasks like inventory checks, while Battery-less NFC provided a balance between power independence and data throughput for tasks like diagnostics and sensor readings. Active NFC was used for high-data operations, such as firmware updates and over-the-air programming, although it required additional setup time due to external power needs. The experiment confirmed that a multi-state NFC system significantly enhances flexibility and efficiency in smart lighting applications. This is particularly true where products may require updates or customisation across their lifecycle that could span from multi-device configuration in the factory to in-service firmware updates or simple diagnostic checks.

The available NFC state(s) and power requirements restrict the capability of NFC in a particular use case. For example, simple security tasks, such as security token updates, can be

performed using Static Passive; whereas, for more complex security fixes, such as firmware updates, one of the Active NFC states is required. Power consumption, as stated previously, does not affect Active NFC; however, Battery-less is restricted by the sensor and output required with the maximum power consumption around 10 mA in the test system described above. One of the interesting findings from the industrial lighting use case is that the industrial lighting control system, DALI [25], can be used in a Battery-less NFC state as the bus is typically externally powered, meaning commands and diagnostics can be achieved in Battery-less mode, bypassing both the battery and mains-supplied power circuits for critical failure conditions.

## VII. CONCLUSION AND DISCUSSION

This work developed a Passive-Active NFC framework bringing together four operational states: Static Passive, Battery-less (Dynamic Passive), Static Active and Dynamic Active. The study addresses range limitations, showing that careful antenna design and the use of industrial readers can greatly extend communication distance, particularly for Battery-less and Static Passive modes, enabling reliable operation well beyond typical consumer NFC reader performance.

Energy usage analysis of a real-world experimental system revealed that, while higher microcontroller clock speeds increase instantaneous current, they can improve overall efficiency in Battery-less operation by reducing task duration; i.e., time-to-complete is as important as average power. Reliability testing confirmed that a Passive-Active NFC can achieve error-free data transfers, even when physical alignment is imperfect.

A new NFC Communication Control Protocol was introduced to manage large and dynamic data exchanges more reliably than conventional NDEF, by prioritising read/write operations and reducing corruption risks. Real-world evaluation in an industrial smart lighting product demonstrated the strengths of each state: Static Passive for quick, low-power tasks; Active for high-data operations; Battery-less for sensing and diagnostics without batteries.

Together, these advances show that integrating all four NFC states yields a Passive-Active system that is more flexible, efficient, and reliable than single-mode designs, with strong potential in a wide range of Industrial use-cases including, healthcare, industrial automation, industrial lighting, inventory management and smart factories.

## REFERENCES

- [1] *ISO/IEC 14443: Cards and security devices for personal identification*, International Electrotechnical Commission Std., 2018.
- [2] *ISO/IEC 18000-3: Information technology — Radio frequency identification for item management*, International Electrotechnical Commission Std., 2004.
- [3] *ISO/IEC 15963: Information technology — Radio frequency identification for item management*, International Electrotechnical Commission Std., 2020.
- [4] A. Lazaro, R. Villarino, and D. Girbau, "A survey of NFC sensors based on energy harvesting for IoT applications," *Sensors*, vol. 18, no. 11, p. 3746, 2018.
- [5] M. Boada, A. Lazaro, R. Villarino, and D. Girbau, "Battery-less NFC sensor for pH monitoring," *IEEE Access*, vol. 7, pp. 33 226–33 239, 2019.
- [6] A. Lazaro, M. Boada, R. Villarino, and D. Girbau, "Color measurement and analysis of fruit with a battery-less NFC sensor," *Sensors*, vol. 19, no. 7, p. 1741, 2019.
- [7] B. Baker, J. Woods, M. J. Reed, and M. Afford, "A survey of short-range wireless communication for ultra-low-power embedded systems," *Journal of Low Power Electronics and Applications*, vol. 14, p. 27, 2024.
- [8] G. Moloudian, M. Hosseinifard *et al.*, "RF energy harvesting techniques for battery-less wireless sensing, Industry 4.0, and Internet of things: A review," *IEEE Sensors Journal*, vol. 24, pp. 5732–5745, 2024.
- [9] K. M. Chaffai, R. Berenguer, A. Rezola, J. Diaz, H. Solar, and A. Berain, "Exploring dual-frequency implementation for semi-passive RFID tags," in *2024 39th Conference on Design of Circuits and Integrated Systems (DCIS)*. IEEE, 2024, pp. 1–6.
- [10] P. Escobedo, M. Bhattacharjee, F. Nikbakhtnasrabadi, and R. Dahiya, "Smart bandage with wireless strain and temperature sensors and batteryless NFC tag," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 5093–5100, 2021.
- [11] M. Boada, A. Lazaro, R. Villarino, and D. Girbau, "Battery-less soil moisture measurement system based on an NFC device with energy harvesting capability," *IEEE Sensors Journal*, vol. 18, no. 13, pp. 5541–5549, 2018.
- [12] I. Cappelli, A. Fort, M. Mugnaini, E. Panzardi, A. Pozzebon, M. Tani, and V. Vignoli, "Battery-less HF RFID sensor tag for soil moisture measurements," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–13, 2021.
- [13] C. Peres, M. Emam, H. Jafarzadeh, M. Belcastro, and B. O'Flynn, "Development of a low-power underwater NFC-enabled sensor device for seaweed monitoring," *Sensors*, vol. 21, no. 14, p. 4649, 2021.
- [14] S. Choudhary, H. Singla *et al.*, "A comparative study of NFC and Bluetooth for file transfer applications," in *2024 International Conference on Electronics, Computing, Communication and Control Technology (ICECCC)*. IEEE, 2024, pp. 1–7.
- [15] A. Hussain, M. Hammad, K. Hafeez, and T. Zainab, "Programming a microcontroller," *Int. J. Comput. Appl.*, vol. 155, no. 5, pp. 21–26, 2016.
- [16] K. Arakadakis, P. Charalampidis, A. Makrogiannakis, and A. Fragkiadakis, "Firmware over-the-air programming techniques for IoT networks — a survey," *ACM Computing Surveys (CSUR)*, vol. 54, no. 9, pp. 1–36, 2022.
- [17] T. Ulz, T. Pieber, A. Höller, S. Haas, and C. Steger, "Secured and easy-to-use NFC-based device configuration for the Internet of Things," *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 1, pp. 75–84, 2017.
- [18] N. S. S. Shobha, K. S. P. Aruna, M. D. P. Bhagyashree, and K. S. J. Sarita, "NFC and NFC payments: A review," in *2016 International Conference on ICT in Business Industry & Government (ICTBIG)*. IEEE, 2016, pp. 1–7.
- [19] M. Boada, A. Lazaro, R. Villarino, and D. Girbau, "Read range study of energy-harvested implanted NFC sensors with commercial NFC ICs and smartphones," in *2021 XXXIVth General Assembly and Scientific Symposium of the International Union of Radio Science (URSI GASS)*. IEEE, 2021, pp. 1–4.
- [20] J. I. Cairo, J. Bonache, F. Paredes, and F. Martín, "Reconfigurable system for wireless power transfer (WPT) and near-field communications (NFC)," *IEEE Journal of Radio Frequency Identification*, vol. 1, no. 4, pp. 253–259, 2017.
- [21] M. Boada, A. Lazaro, R. Villarino, E. Gil-Dolcet, and D. Girbau, "Battery-less NFC bicycle tire pressure sensor based on a force-sensing resistor," *IEEE Access*, vol. 9, pp. 103 975–103 987, 2021.
- [22] X. Li, J. Sidén, H. Andersson, and T. Schön, "A paper-based screen printed HF RFID reader antenna system," *IEEE Journal of Radio Frequency Identification*, vol. 2, no. 3, pp. 118–126, 2018.
- [23] K. Finkenzeller, *RFID handbook: Fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. John Wiley & Sons, 2010.
- [24] NFC Forum, "NFC Data Exchange Format (NDEF) Technical Specification," NFC Forum, Tech. Rep., 2026, specifies a common data format for NFC Forum-compliant devices and tags.
- [25] *IEC 62386: Digital Addressable Lighting Interface (DALI)*, International Electrotechnical Commission Std., 2014, standard for digital addressable lighting interface systems.