

Wireless BMS Architecture for Secure Readout in Vehicle and Second life Applications

Fikret Basic, Claudia Rosina Laube, Patrick Stratznig, Christian Steger

*Institute of Technical Informatics
Graz University of Technology
Graz, Austria
{basic, steger}@tugraz.at*

Robert Kofler

*R&D Battery Management Systems
NXP Semiconductors Austria GmbH Co & KG
Gratkorn, Austria
robert.kofler@nxp.com*

Abstract—Battery management systems (BMS) are becoming increasingly important in the modern age, where clean energy awareness is getting more prominent. They are responsible for controlling large battery packs in modern electric vehicles. However, conventional solutions rely only on a wired design, which adds manufacturing cost and complexity. Recent research has considered wireless solutions for the BMS. However, it is still challenging to develop a solution that considers both the active in-vehicle and the external second-life applications. The battery passport initiative aims to keep track of the batteries, both during active and inactive use cases. There is a need to provide a secure design while considering energy and cost-efficient solutions. We aim to fill this gap by proposing a wireless solution based on near-field communication (NFC) that extends previous work and provides a unified architecture for both use cases. To provide protection against common wireless threats, an advanced security analysis is performed, as well as a system design analysis for the wake-up process that reduces the daily power consumption of the stored battery packs from milli- to microwatts.

Index Terms—Battery Management System, Wireless, Security, Cyber-physical, RFID, NFC, Second life, Vehicle, Battery.

I. INTRODUCTION

Battery management systems (BMS) represent one of the most important building blocks of modern electric vehicles (EV). They are responsible for ensuring safe and reliable use of large battery packs [1]. Since they are one of the main driving forces of an EV, any problem that occurs with the batteries can directly affect the entire vehicle and also the driver's safety, leading to various hazards such as thermal runaway [2]. Modern BMS are deployed in several topologies where different modules are responsible for tasks ranging from battery cell sensor data acquisition to their transmission.

One challenge with modern EV battery systems is the reuse of used batteries at the end of their life cycle. Even if the batteries no longer meet the needs of a vehicle, they may be able to be used for other applications. This battery state is referred to as second life [3]. The battery's state of health (SoH), state of charge (SoC), and other diagnostic information must be tracked during its lifetime [4]. A BMS controller would track this information in an active EV use case through its internal communications, but if the batteries are stored in a warehouse, for example, the battery packs may only be accessed through an interface with a battery pack controller (BPC) using an external reader. BMS communication services

can therefore be viewed from two angles: (i) internal - for communication between different sensors and bridge modules, and (ii) external - for diagnostic and monitoring purposes read from outside the system. There are several legislations underway aimed to introduce battery tracking via battery passports and even distributed monitoring in the cloud using electronic passports [5], [6]. It is important to find an affordable system design that allows flexible and fast readout with respect to both communication approaches. However, currently, there is no unified design that considers different BMS topologies.

Another challenge that is common with BMS is the use of cables for communication. The use of cables is associated with higher assembly cost, weight, complexity, limited scalability, and maintenance [7]–[9]. However, they also provide fast and reliable transmission between modules, which is important for systems such as BMS. An alternative would be to use wireless technologies, but here it is important to assess which technology should be used. There is currently no clear answer to this, with several works proposed ranging from the use of BLE [8], [10], Wi-Fi [11], [12], ZigBee [13], and other technologies [7]. Using multiple technologies in one system is not practical and can lead to increased costs and radio interference. Our goal is to present a design that unifies different use cases under the same wireless technology. We aim to achieve this through the use of radio-frequency identification (RFID), specifically accessible and low-cost near-field communication (NFC).

The BMS and batteries are vital components in modern EVs that also require adequate protection. Any vulnerable system component should be authenticatable and provide protection against tampering and even eavesdropping to protect user privacy [14]–[16]. NFC offers advantages from a security perspective because it enables short-range communication that is difficult to be exploited remotely. However, there are still many vulnerabilities in BMS and NFC that need to be addressed to provide a fully secure design [16]–[18].

In response to the aforementioned challenges, we present in this paper a complete design for wireless BMS internal and external data communication based on NFC. To extend on the previous work in this area, we unify two separate designs, one targeting internal sensor readout from battery packs and the other targeting external status and diagnostic readout in a BMS system design [19], [20].

Contributions. We extend the security architecture by presenting and formally verifying a complete authentication and session establishment protocol for the external readout use case. We also investigate the important wake-up readout cycle for other use cases and propose two different system designs. Summarized, our main contributions are:

- A system architecture that enables wireless internal and external readout of battery sensor data for various cases.
- Proposal of two methods for the wake-up process.
- Extending the existing security solution and its proof.

II. BACKGROUND AND RELATED WORK

A. Battery management systems (BMSs)

A BMS is responsible for controlling a large number of battery cells connected either in series or in parallel to ensure safe and reliable operation [1]. There are several BMS topologies, with distributed systems being the most common [21]. Here, a powerful main BMS controller is responsible for controlling and relaying information to the outside world. The controller communicates with several BPCs that are responsible for intermediate operations and data collection from a group of battery cells. We call this group of elements a battery pack.

B. Near field communication (NFC)

NFC is a short-range wireless technology defined in the ISO 18092 NFC standard, which builds on the ISO 14443 RFID standard. It operates at a radio frequency (RF) of 13.56 MHz with a range and data rate of up to 10 cm and 848 kbit/s, respectively [22]. Today, it is used for fast terminal controls, payments, and applications that benefit from energy harvesting. NFC can operate in three main modes, reader/writer mode, peer-to-peer mode, and card emulation mode [22]. In our work, we rely on the reader/writer mode for all use cases. Here, devices are divided into an active and a passive class. In the context of BMS, NFC suffers from a short range compared to other wireless technologies [7], but it provides an advantage when considering interference, security concerns and accessibility with NFC-enabled devices [19]. It is also capable of generating electromagnetic fields through an active device to power the passive devices via energy harvesting [23].

C. Second life for batteries

A common problem with the use of batteries in EVs is the problem of battery recycling. When the maximum battery capacity falls below a certain threshold (around 80%), the current batteries need to be replaced with new ones. However, the high recycling cost and pollution make this process undesirable. Instead, it is proposed to maximize the potential use of a battery by reusing it for other uses that are not constrained by the same customer criteria as with EVs [3].

Second-life battery use is an ongoing discussion within the European Union (EU). A concept of "battery passports" is being discussed, which aims to track batteries throughout their lifetime, from manufacturing to recycling [5], [6]. The tracking and identification of batteries would be performed via QR codes. However, QR technology is limited in terms of

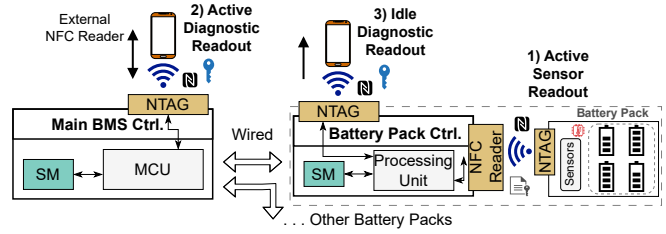


Fig. 1. Wireless NFC BMS architecture considering three different use cases, extending basis design with secure modules (SM) and NFC tags and readers.

TABLE I
OVERVIEW OF THE PROPOSED USE CASES AND DEPLOYMENT SCENARIOS.

Use case	Deploy. scenario	Comm. direction	Readout data
Active sensor	internal; deployed	Batt. pack → BPC	sensor data
Idle diagnostic	external; stored	BPC → Ext. reader	status & sensor data
Active diagnostic	external; deployed	BMS ↔ Ext. reader	status & diagnostic

functionality, scalability, services and security. In this work, we propose an alternative lightweight design that aims to fill these drawbacks with minimal additional overhead. The use of battery passports is also of interest with respect to the new concepts related to the BMS service extension to the cloud environment, as shown in the work of Li et al. [24], Taesic et al. [9], and Kai et al. [25]. This cloud shift provides additional power for SoC and SoH computations and enables machine learning or digital twin models, and extra security verification.

III. THE NOVEL BMS DESIGN FOR WIRELESS READOUT

By relying only on NFC, we are able to provide a solution for three different scenarios that extend the BMS functionality, as described in Table I.: (i) active readout of internal sensors [19], (ii) idle state scenario considered for off-vehicle use cases, and (iii) active diagnostic readout [20].

The system architecture is shown in Figure 1. For both diagnostic readouts (active and idle), both devices are first authenticated before a secure channel is established. The data link communication layer is handled with NDEF records. The data storage depends on the reader application, either storing it offline or online in a database as proposed for battery passports [5]. Elements of the design and its implementation were handled in a recent master's thesis [26].

Diagnostic readout for active and idle states differentiate on the devices used and the data direction. In both cases, communication takes place with an external NFC reader. The active diagnostics use case is intended for situations where BMSs are already deployed in a neighbouring system. In this case, the BMS controller is able to provide the current diagnostic data. The idle readout is intended for the storage of battery packs during their second life transfer [3]. Here,

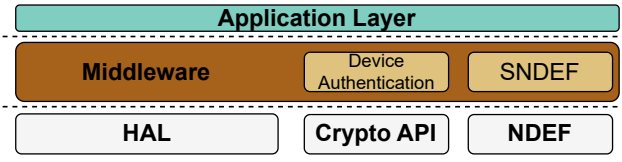


Fig. 2. Proposed wireless BMS software layer stack.

it is considered beneficial to occasionally check the batteries' SoH to determine that no hazards have occurred. In the case of active diagnostic readout, the application data is first formatted before being transferred from the BMS host controller to the NFC reader. The proposed lightweight structure is shown in Figure 3. The BMS is expected to first collect the data from each BPC before forwarding it to the NFC reader. However, BMS topologies need to also be considered. The following considerations must be made for other topologies [21]:

- Centralized: consists of one main BMS control unit and no intermediate modules. Requires one NTAG and NFC reader. The idle diagnostic use case is considered unfeasible unless the controller is also stored.
- Modulated: multiple modules, with one main module and multiple followers. The main module enables the external interface, but each follower module also needs to include an NTAG and NFC reader for all use cases.
- Distributed: similar to the modulated design, but with a clearer separation between the central BMS controller and the battery packs. The architecture is shown in Figure 1.
- Decentralized: consists of multiple BMS subsystems. Considers linear growth of required NFC interfaces based on the topology of the underlying BMS subsystem.

Software architecture. The software architecture is generalized and is shown in Figure 2. It consists of three main layers. At the bottom is the hardware abstraction layer (HAL). It is vendor-specific and contains the driver components, e.g., for interfaces, clock, etc. The cryptographic application programming interface (API) is considered an independent entity that can be connected either directly to the HAL or to a separate security module. NDEF messages are controlled by the NFC driver. Their payload contains the components of the higher SNDEF data set located at the middle layer, i.e., the middleware. Independent of the SNDEF, the middleware is also responsible for device authentication. This means that no other access to the application layer is possible unless it has first been verified, confirmed, and processed by the middleware. Since the middle layer imposes no restrictions on the data format, the application layer can be freely defined by the developer.

IV. SECURITY MODEL

To protect against common threats, a security model needs to be introduced for both internal and external communication. Several BMS threat analysis models have been created, each highlighting important vulnerabilities [9], [14], [15]. We aim not to invent a new protocol that could be susceptible to

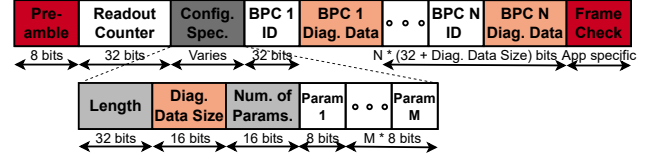


Fig. 3. Application packet structure for the active diagnostic use case.

untracked attacks, but rather to adapt simple, yet effective solutions. The security model needs to answer to the current known BMS and NFC threats and fulfil the following requirements:

- Mutual device authentication
- Use of secure channels: encryption and tamper-proof
- Lightweight models with minimal performance overhead

A. Securing battery pack internal readout

Because battery packs are enclosed, any form of physical attack would directly damage the components and would therefore be infeasible or too costly for the attackers. Similarly, an external attack would also likely be difficult or impossible, although further research is needed to confirm these claims. This leaves the protection of reading the battery packs based on the proposal by Basic et al. in [19] sufficient, i.e., authentication protection based on either symmetric or asymmetric cryptography with previously embedded keys. Hence, on the device-level protection, two key strategies can be employed: (i) authentication; symmetric with pre-shared keys, or asymmetric with originality signatures, and (ii) authorization, with password-controlled read and write access.

B. Security protocol for external BMS readout

The protocol is based on symmetric, rather than asymmetric cryptography, to account for the potential performance or hardware limitations. If the master key is leaked, all past and future sessions could be compromised. Therefore, it is of utmost importance to secure the location of the master key with an SM. We rely on the use of SNDEF records [20].

The security design for external readout, which considers the idle state and active diagnostics use cases, is based on the lightweight security design for authentication and data exchange proposed in [20]. We formalize the protocol in Figure 4. and extend the solution to consider some additional security vulnerabilities that may arise from the original design. It consists of two phases, the authentication phase and the newly added session key possession confirmation phase. During the session key confirmation phase, previous messages are appended, to confirm session key ownership for both parties.

$$1) N_R \rightarrow M_N : N_R, ch_r \quad (1)$$

$$2) M_N \rightarrow N_R : M_N, ch_t, \{\{M_N, ch_r\}_{K_M}\}_{K_M} \quad (2)$$

$$3) N_R \rightarrow M_N : \{\{N_R, ch_t\}_{K_M}^{-1}\}_{K_M}^{-1} \quad (3)$$

$$4) M_N \rightarrow N_R : \{M_N, X\}_{K_S} \quad (4)$$

$$5) N_R \rightarrow M_N : \{N_R, X'\}_{K_S} \quad (5)$$

From the protocol; N_R : NFC reader id., M_N : BMS ctrl. id., ch_r : challenge nonce request from N_R , ch_t : challenge

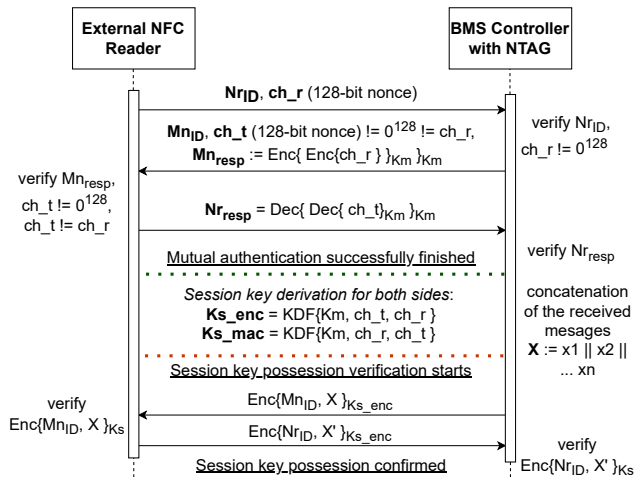


Fig. 4. Security protocol sequence diagram for the external BMS readout.

nonce request from M_N , K_M : pre-embedded master key, K_S : session key, X : concatenated previously received messages from N_R , X' : concatenated received messages from M_N .

The double key encryption is used to fend off an oracle attack that could expose the vulnerabilities of the CMAC if used in the key derivation function (KDF) when based on the CBC-MAC computation. In addition, a nonce cannot be zero or equal to another. Another important point is that the underlying ciphers are not identical, i.e., in our case, BPC encrypts, while the external NFC reader decrypts the challenges, to protect against “chosen challenge oracle” attacks.

V. WAKE UP MODEL DESIGN

Previous works mainly investigated system design and communication with NFC. There are no clear design specifications for interaction with BMS controllers. The wake-up application is important for the idle state use case. Since a BPC is stored along with battery cells, it is not necessary to keep the controller on during the entire storage period. By controlling the wake-up of the BPC, it would be possible to minimize the total power consumption during the time the battery cells are stored and provide power during a communication period with an external NFC reader. Therefore, we want to propose a design that meets the following two main requirements:

- 1) Low power consumption through mode switching
- 2) Fast wake-up time

We propose two approaches to wake-up system design based on the different characteristics of BPC and NTAG: (i) with *event detection* (ED) and (ii) with *energy harvesting* (EH). They are evaluated based on total wake-up time and power consumption, as well as design requirements and HW/SW design considerations. Figure 5. shows the flowchart, with separate steps for both designs. Both rely on the use of I^2C for data transfer, but the difference is in how the wake-up events are triggered and how the power states are managed.

Wake-up with event detection. This method uses the event detection (ED) function on modern NTAG boards, where the ED pin acts as an event pin that can respond to different events,

TABLE II
OVERVIEW OF THE PROPOSED WAKE-UP SYSTEM DESIGN APPROACHES.

Model	Prerequisites	Pros / Cons
Event Detection (ED)	NTAG needs to have an event pin; requires a constant power source	[+] wake-up is possibly faster, [-] needs constant power source, [-] higher power consumption
Energy Harvest. (EH)	NTAG’s EH needs to be specially configured; the reader has to have EH enabled	[+] NTAG is powered off in idle, [+] after wake-up, BPC can supply the NTAG, [-] wake-up takes longer

specifically here, the presence of an NFC field. When an RF field is detected, the ED pin is set to logic high. During idle time, the NTAG remains in the standby state and is constantly powered by the host BPC. The lowest theoretical consumption that can be achieved is if the host BPC uses a very low power state (VLPS) that can still power the NTAG and respond with the wake-up, with the NTAG being in standby mode.

Wake-up with energy harvesting. In this method, the NTAG can be completely shut down and the BPC can be put into a VLPS mode, as with the ED method. This results in lower power consumption, but may also result in a slightly longer wake-up time since the board wake-up depends on energy harvesting. The NTAG is put into EH mode, where energy is harvested from the RF field in close contact with the antenna. Since the BPC does not power the NTAG at all during the sleep phase, unlike the ED method, the NTAG must remain powered on after energy harvesting has triggered its wake-up. Thus, after the BCP wakes up and during the open communication session, it draws power from the battery cells for its normal operating mode and now also powers the NTAG.

VI. EVALUATION

For the evaluation, we use the NCx33xx series of products from NXP as the NTAG and NFC Reader. They are NFC forum-compliant automotive-graded components that provide several benefiting features for testing [27]. The S32K144 microcontroller board was chosen as both the main BMS controller and the BPC. It is widely used in automotive and industrial applications, and it offers a ready BMS diagnostic application [28]. We evaluate the design on the security aspects both with informal and formal protocol analysis and on the real-device performance analysis by investigating the application overhead of the wake-up process.

A. Security informal analysis

The goal is to protect three main assets: (A1) hardware integrity, (A2) software integrity, (A3) transmitted data. To protect the integrity of (A2) and (A3), the protocol uses AES as the encryption algorithm and CMAC for tag verification. This is done to increase usability on different devices and

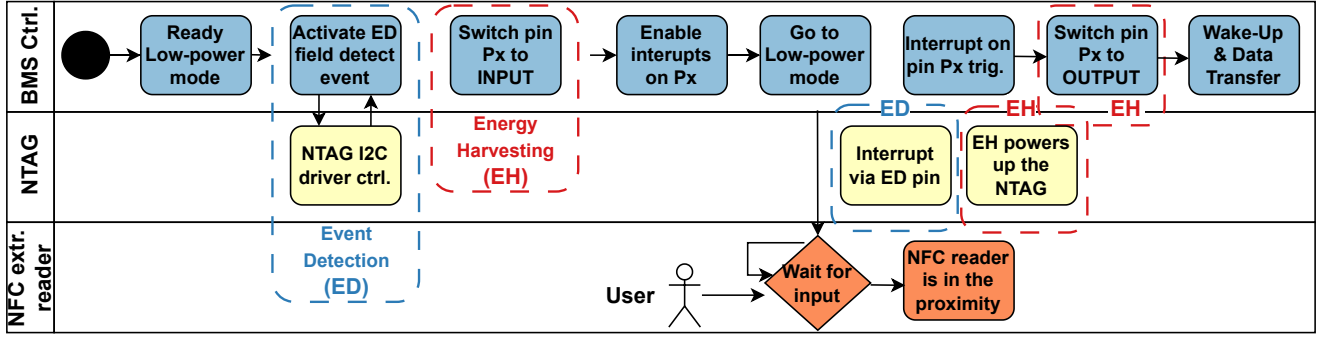


Fig. 5. Wake-up process flowchart: in dashed (ED) blocks steps are shown for the event detection, whereas in (EH) they are shown for the energy harvesting.

improve performance. The operation mode is CBC in Encrypt-then-MAC mode, as it provides higher security than other operation modes. It is important to use a different key between the AES and CMAC computation because using the same key would allow the attacker to forge the tags if they had access to an encryption oracle where they could query the values of the last CMAC computation block. Additionally, to protect against forms of replay attack, tag chaining was implemented. Tag chaining considers appending the previous tag into the buffer of the newly received message to calculate the total tag value, i.e., the MAC value, by using the following structure:

$$MAC_{buffer} := sec_data \mid IV \mid add_data \mid previous_tag$$

(A1) is guaranteed by performing device authentication on the battery pack as described in Section IV-A, and by mutual authentication when communicating with an NFC reader.

B. Security formal analysis - BAN logic

A formal protocol analysis was done on the mutual authentication and session establishment protocol presented in Section IV-B. It uses the BAN logic and its postulates [29].

Idealized protocol. We use the protocol from Section IV-B:

$$1) \text{ all plaintext} \quad (6)$$

$$2) M_N \rightarrow N_R : \{\{ch_r, N_R \xleftrightarrow{K_M} M_N\}_{K_M}\}_{K_M} \quad (7)$$

$$3) N_R \rightarrow M_N : \{\{ch_t, N_R \xleftrightarrow{K_M} M_N\}_{K_M}\}_{K_M} \quad (8)$$

$$4) M_N \rightarrow N_R : \{X, N_R \xleftrightarrow{K_S} M_N\}_{K_S} \quad (9)$$

$$5) N_R \rightarrow M_N : \{X', N_R \xleftrightarrow{K_S} M_N\}_{K_S} \quad (10)$$

Initial assumptions. The following assumptions are made. Firstly, both devices regard the sent nonces to be fresh:

$$N_R \equiv \#(ch_r), M_N \equiv \#(ch_t) \quad (11)$$

Both sides believe in the use of the shared master key:

$$N_R \equiv N_R \xleftrightarrow{K_M} M_N, M_N \equiv N_R \xleftrightarrow{K_M} M_N \quad (12)$$

Goals. We want to make sure that both parties are mutually authenticated and know that the other side trusts that as well:

$$G1.1) N_R \equiv M_N \equiv N_R \xleftrightarrow{K_M} M_N \quad (13)$$

$$G1.2) M_N \equiv N_R \equiv N_R \xleftrightarrow{K_M} M_N \quad (14)$$

For the second-order goals, we want to make sure that both parties trust that the other party has the correct session key:

$$G2.1) N_R \equiv M_N \equiv N_R \xleftrightarrow{K_S} M_N \quad (15)$$

$$G2.2) M_N \equiv N_R \equiv N_R \xleftrightarrow{K_S} M_N \quad (16)$$

Verification. We will start first with G1.1 and G1.2 goals. To verify, we will apply the rules described in the BAN logic [29]. On Eq. 7 we first apply the *message-meaning rule*:

$$\frac{N_R \equiv N_R \xleftrightarrow{K_M} M_N, N_R \triangleleft \{\{ch_r\}_{K_M}\}_{K_M}}{N_R \equiv M_N \mid \sim (ch_r, N_R \xleftrightarrow{K_M} M_N)} \quad (17)$$

We use the *freshness rule* for the nonce and key statement:

$$\frac{\#(ch_r)}{\#(ch_r, N_R \xleftrightarrow{K_M} M_N)} \quad (18)$$

Then, on (18) & (17) we can apply the *nonce verification rule*:

$$\frac{N_R \equiv (18), N_R \equiv M_N \mid \sim (ch_r, N_R \xleftrightarrow{K_M} M_N)}{N_R \equiv M_N \equiv (ch_r, N_R \xleftrightarrow{K_M} M_N)} \quad (19)$$

Finally, to verify the goal G1.1, we can take the *belief rule*:

$$\frac{N_R \equiv M_N \equiv (ch_r, N_R \xleftrightarrow{K_M} M_N)}{N_R \equiv M_N \equiv N_R \xleftrightarrow{K_M} M_N} \quad (20)$$

The verification of goal G1.2 is symmetrical to G1.1, and thus also proved. For the second-order goals, we set additional assumptions. Since X, X' from (9) and (10) are composed out of ch_r and ch_t , we assume by *freshness rule* that:

$$\frac{N_R \equiv \#(ch_r), M_N \equiv \#(ch_t)}{N_R \equiv \#(X), M_N \equiv \#(X')} \quad (21)$$

Now, using the *belief rule* we get the important statements that both sides believe the session key possession:

$$\frac{N_R \equiv (X, N_R \xleftrightarrow{K_S} M_N)}{N_R \equiv N_R \xleftrightarrow{K_S} M_N} \quad (22)$$

$$\frac{M_N \equiv (X', N_R \xleftrightarrow{K_S} M_N)}{M_N \equiv N_R \xleftrightarrow{K_S} M_N} \quad (23)$$

To finalize the verification of G2.1 & G2.2, we use the same line of rules as for the G1.1 & G1.2, i.e., by applying

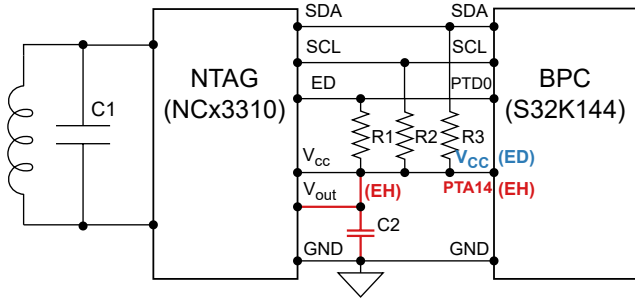


Fig. 6. Hardware design for the BPC that considers the wake-up use cases.

the message-meaning rule, then the freshness rule, non-verification and finally the belief rule. Here, G2.2 is also symmetrical in verification to G2.1.

C. Wake-up process evaluation

A real-world implementation was made using the components based on the hardware design presented in Figure 6. To test the design of ED, the NCx3310 is placed in standby mode with the S32K144 using the VLPS mode. For the idle phase, this results in $29.8 \mu A$ from the S32K144 and $5.9 \mu A$ from the NCx3310, for a total of $35.7 \mu A$ as theoretical current consumption and power consumption of $117.81 \mu W$. In the EH design case, the NTAG is completely disabled, which means that all power consumption comes only from the BPC, resulting in a theoretical current consumption of $29.8 \mu A$ and power consumption of $98.3 \mu W$ for our devices. While the design shows a working and usable test implementation, in a real application a level shifter should be considered to compensate for the potential cross currents that can occur on the connections between I2C, the return signal port, V_{cc} and V_{out} . Depending on the use case, both methods can be applied, but if the overall goal is to reduce power consumption, the method with EH is proposed. In this mode, the BPC remains in power-saving mode while the NTAG draws no power because it is completely powered down.

VII. CONCLUSION

In this work, we have presented a novel design for the wireless deployment of BMS using NFC as an enabling technology, extending previous work. We have considered both internal and external system readouts, as well as active and inactive use cases. We show that it is feasible to use the BMS with NFC for both current active in-vehicle applications and second-life applications. An NFC interface is useful here as it allows flexible readout of the stored battery packs. Here, the security model was extended and evaluated using both informal security analysis and BAN logic. In addition, two wake-up system designs have been proposed and evaluated. For future work, further investigation of the wake-up method is planned, as well as investigation of other potential RFID options focused on lightweight applications, such as a fast readout of the ID of the stored battery packs.

ACKNOWLEDGMENT

This paper is supported by the OPEVA project that has received funding within the Key Digital Technologies Joint Undertaking (KDT JU) from the European Union's Horizon Europe Programme and the National Authorities (France, Belgium, Czechia, Italy, Portugal, Turkey, Switzerland), under grant agreement 101097267. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or KDT JU. Neither the European Union nor the granting authority can be held responsible for them.

REFERENCES

- [1] X. Hu *et al.*, "State estimation for advanced battery management: Key challenges and future trends," *Renew. & Sustain. Energy Reviews*, 2019.
- [2] M. Hartmann and J. Kelly, "Thermal Runaway Prevention of Li-ion Batteries by Novel Thermal Management System," in *IEEE ITC*, 2018.
- [3] W.-C. Lih, J.-H. Yen, F.-H. Shieh, and Y.-M. Liao, "Second Use of Retired Lithium-ion Battery Packs from Electric Vehicles: Technological Challenges, Cost Analysis and Optimal Business Model," in *IS3C*, 2012.
- [4] R. Xiong *et al.*, "Critical Review on the Battery State of Charge Estimation Methods for Electric Vehicles," *IEEE Access*, vol. 6, 2018.
- [5] "Proposal for a regulation of the European Parliament and of the Council concerning batteries and waste batteries, repealing Directive 2006/66/EC and amending Regulation (EU) No 2019/1020," <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0798>, 2020.
- [6] K. Berger, J.-P. Schögl, and R. J. Baumgartner, "Digital battery passports to enable circular and sustainable value chains: Conceptualization and use cases," *Journal of Cleaner Production*, vol. 353, 2022.
- [7] A. Samanta and S. S. Williamson, "A Survey of Wireless Battery Management System: Topology, Emerging Trends, and Challenges," *Electronics*, vol. 10, no. 18, 2021.
- [8] F. A. Rincon Vija *et al.*, "From Wired to Wireless BMS in Electric Vehicles," in *17th MSN*, pp. 255–262, 2021.
- [9] T. Kim *et al.*, "Cloud-Based Battery Condition Monitoring and Fault Diagnosis Platform for Large-Scale Lithium-Ion Battery Energy Storage Systems," *Energies*, vol. 11, no. 1, 2018.
- [10] C. Shell *et al.*, "Implementation of a Wireless Battery Management System (WBMS)," in *IEEE I2MTC*, pp. 1954–1959, 2015.
- [11] T. Gherman *et al.*, "Smart Integrated Charger with Wireless BMS for EVs," in *44th IECON*, pp. 2151–2156, 2018.
- [12] X. Huang *et al.*, "Wireless Smart Battery Management System for Electric Vehicles," in *IEEE ECCE*, pp. 5620–5625, 2020.
- [13] A. Rahman, M. Rahman, and M. Rashid, "Wireless Battery Management System of Electric Transport," *IOP Conference Series: Materials Science and Engineering*, vol. 260, nov 2017.
- [14] S. Sripath *et al.*, "Vulnerabilities of Electric Vehicle Battery Packs to Cyberattacks on Auxiliary Components," *ArXiv*, vol. 1711.04822, 2017.
- [15] M. Cheah and R. Stoker, "Cybersecurity of Battery Management Systems," *HM TR series*, vol. 10, no. 3, p. 8, 2019.
- [16] S. Plosz *et al.*, "Security Vulnerabilities and Risks in Industrial Usage of Wireless Communication," in *IEEE ETFA*, pp. 1–8, 2014.
- [17] N. A. Chattha, "NFC — Vulnerabilities and Defense," in *CIACS*, 2014.
- [18] E. Haselsteiner and K. Breitfuss, "Security in Near Field Communication (NFC) Strengths and Weaknesses," in *Workshop on RFID Security*, 2006.
- [19] F. Basic, M. Gaertner, and C. Steger, "Secure and Trustworthy NFC-Based Sensor Readout for Battery Packs in Battery Management Systems," *IEEE Journal of Radio Frequency Identification*, vol. 6, 2022.
- [20] F. Basic *et al.*, "A Novel Secure NFC-based Approach for BMS Monitoring and Diagnostic Readout," in *IEEE RFID*, pp. 23–28, 2022.
- [21] A. Reindl, H. Meier, and M. Niemetz, "Scalable, Decentralized Battery Management System Based on Self-organizing Nodes," in *ARCS*, 2020.
- [22] "Standards - ISO 14443, ISO 15693, NFC-Forum und NDEF," <https://www.nfc-tag-shop.de/info/nfc-entwicklung/standards-iso-14443-nfc-forum-und-ndef.html>, 2017. Accessed: 16.01.2023.
- [23] M. Bouklachi *et al.*, "Energy Harvesting of a NFC Flexible Patch for Medical Applications," in *IEEE WPTC*, pp. 249–252, 2019.
- [24] W. Li *et al.*, "Digital twin for battery systems: Cloud battery management system with online state-of-charge and state-of-health estimation," *Journal of Energy Storage*, vol. 30, 2020.

- [25] K. Li *et al.*, “Battery life estimation based on cloud data for electric vehicles,” *Journal of Power Sources*, vol. 468, p. 228192, 2020.
- [26] C. Laube, “Design and implementation of secure NFC-based logging for stationary battery management systems,” Master’s thesis, TUG, 2022.
- [27] NXP Semiconductors, “Ntag 5 link - NFC forum-compliant I2C bridge.” NTP53x2, Rev. 3.3, 2020.
- [28] NXP Semiconductors, “S32k1xx data sheet.” S32K1XX, Rev. 14, 2021.
- [29] M. Burrows, M. Abadi, and R. Needham, “A Logic of Authentication,” *ACM Trans. Comput. Syst.*, vol. 8, p. 18–36, feb 1990.