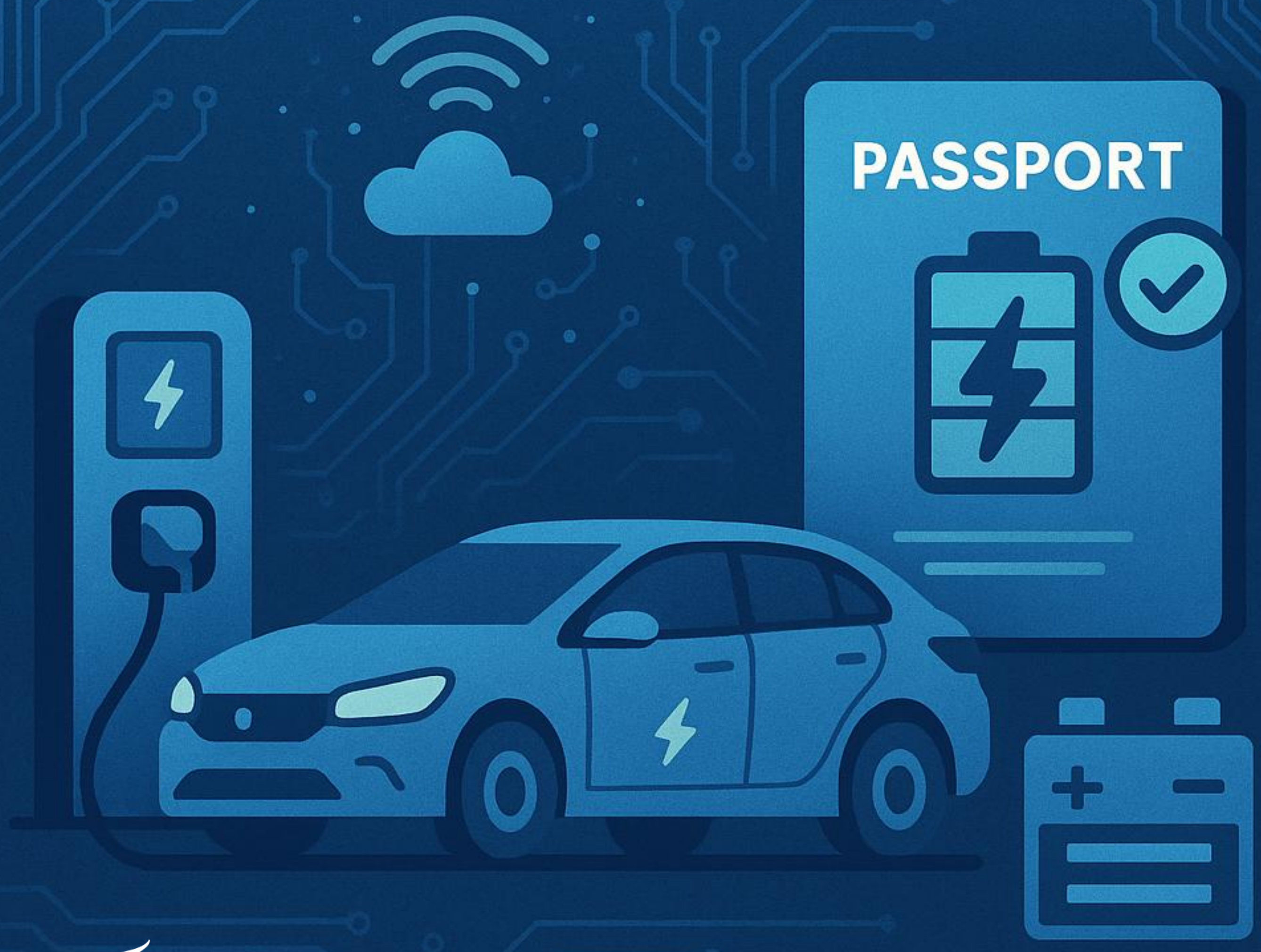
IoT-DRIVEN DIGITAL PRODUCT PASSPORT FOR EV BATTERIES

A thesis on evaluation framework for potentials and challenges



TU Delft

IOT-DRIVEN DIGITAL PRODUCT PASSPORT

FOR EV BATTERIES

An Evaluation Framework for Potentials & Challenges

A thesis submitted to Delft University of Technology
in partial fulfilment of the requirement for the degree of

MASTER OF SCIENCE

in Management of Technology

by

Quoc Khanh Ma
Student number: 6006507

To be defended publicly on 26th August, 2025

Thesis Committees

First Supervisor & Chairperson:	Dr. A.Y. (Aaron) Ding	TU Delft
Daily Supervisor:	Dr. Boriana Rukanova	TU Delft
Second Supervisor:	Dr. Merla Kubli	TU Delft
Advisor:	Prof. dr. Yao-hua Tan	Tu Delft

Acknowledgment

This thesis represents the final requirement to obtain my Master's degree in Management of Technology and the concluding chapter of my academic journey at TU Delft. I would like to take a moment to express my gratitude to my first supervisor and chairperson, Dr. Aaron Ding, for his continuous support, insightful feedback, and academic guidance throughout this thesis journey on such a complex yet amazing research topic. I am also sincerely thankful to my daily supervisor, Dr. Boriana Rukanova, for her invaluable mentorship, constructive critiques, and timely support. Her ability to challenge my assumptions and guide me toward clarity and rigor in my thinking has significantly enriched the quality of this work.

Furthermore, I would like to thank my second supervisor, Dr. Merla Kubli, for her thoughtful feedback and care for details that pushed me to explore the broader perspectives for this study, as well as for my writings. A special thank you to Prof. dr. Yao-hua Tan, whose advice and insights during key stages of this research were greatly appreciated. I am grateful to have such diverse and supportive committees for my research.

To all the experts who participated in the interviews and graciously contributed their time and remarkable insights, I deeply appreciate your support for my study. Your efforts will always be remembered since it was you who made this study possible, enriching this study’s findings from diverse perspectives. To all the friends I made along the journey, you are the ones who made the last two years of my life unforgettable. The struggles, laughter, and cherished memories we had together will forever stay in my heart. To Phuong, thank you for the support whenever I need it the most. All the distance cannot stop your presence.

And lastly, to my family, the ones who provided unconditional love and support for whatever I do and wherever I go. I would like nothing more than to share this achievement, this journey, with you. To my parents, your upbringing, your sacrifices, and your love are my biggest motivation that has shaped me as I am today, tomorrow, and many years to come.

Quoc Khanh Ma

Delft, July 2025

Executive Summary

Background. In pursuit of a circular and sustainable economy, the European Union has introduced the Digital Product Passport (DPP) as a regulatory tool to enhance product transparency and lifecycle accountability. For electric vehicle (EV) batteries, DPPs are mandated under Regulation (EU) 2023/1542 and aim to record critical information such as composition, state of health, safety events, and usage history. These records will support environmental compliance, facilitate reuse and recycling, and enable data-driven product stewardship.

Problem. While the DPP concept is promising, its implementation in the EV battery sector presents complex challenges. Specifically, EV batteries generate vast amounts of dynamic data—such as temperature, state of charge (SoC), and charge/discharge cycles—which require continuous monitoring, secure storage, and traceable transmission. Translating regulatory data requirements into actionable technical system design remains an underexplored issue. Furthermore, stakeholders such as OEMs (Original Equipment Manufacturers) and second-life recyclers lack practical tools to evaluate whether existing IoT architectures can meet these emerging obligations. The need to understand and overcome these barriers resulted in the main question of this research:

"How can a suitable evaluation framework be developed to assess the potentials and challenges of IoT-driven Digital Product Passports for EV batteries?"

Research Approach. This thesis adopts a Design Science Research (DSR) methodology to develop a framework that helps decision-makers evaluate the suitability of different IoT system architectures for DPP implementation. The study focuses exclusively on dynamic data, recognizing IoT as a critical enabler for real-time sensing, processing, and data transfer in EV battery management systems (BMS). Literature reviews, technical standards (e.g., DIN DKE SPEC 99100), and EU pilot projects (e.g., Battery Pass, CIRPASS) were analyzed to extract the key regulatory, technical requirements and create a knowledge base for this study.

Analysis. The analysis began with mapping key dynamic data attributes required by the DPP—such as SoC, temperature, charge cycles, and accident logs—to specific layers of IoT architecture. This revealed how data is generated at the perception layer, processed in the middleware, and reaches the end-user via the application layer. From this foundation, a set of evaluation dimensions was developed to translate technical and regulatory requirements into comparable system capabilities. These dimensions—covering some functions such as sensing accuracy, real-time event detection, and data format—form the basis of the evaluation matrix and trade-offs table, enabling structured comparison and system-level design.

Framework Design. The framework developed in this study centers on two practical tools: an evaluation matrix and a trade-off table. The evaluation matrix enables a structured comparison of different IoT architecture profiles based on their ability to support DPP requirements in EV batteries. It guides decision-makers in identifying the strengths and limitations of each configuration using operational and regulatory criteria. The trade-off table complements this by highlighting key interdependencies—such as how increased sensing accuracy may burden storage and others. These trade-offs help decision makers (OEMs, solution providers) understand the broader implications of system design choices. Together, these tools provide a flexible, decision-oriented framework that supports early-stage planning and encourages system-level thinking in DPP implementation.

Validation. The framework was validated through exploratory and in-depth interviews with eleven experts from different academic disciplines and industrial sectors. The outcome confirmed the framework's logic and relevance, particularly the importance of certain dimensions such as lifecycle updates, sensing accuracy, and stakeholder-specific access control for DPP. Experts strongly supported the trade-off table for surfacing key design tensions, such as edge–cloud processing distribution, latency, and cost–complexity balance. The expert feedback led to refinements in both the evaluation matrix and trade-off table, improving their usability and relevance in different real-life contexts. Overall, the validation process demonstrated that the framework is technically robust, flexible to different organizational contexts, while based on and aligned with regulatory and industry needs, making it a practical decision-support tool for IoT-enabled DPP system design.

Future Research. Several directions are recommended for future research. First, the evaluation framework should be tested in real-world pilot environments to validate its practical applicability and scalability across different OEMs and regulatory contexts. Second, the current framework remains qualitative; future studies could develop quantitative benchmarks for each evaluation dimension, such as minimum sensing resolution or acceptable latency thresholds based on other existing standards/regulations. Third, further investigation into deciding criteria for key trade-offs, for example, the edge–cloud trade-off, particularly to support decision-making on where to process lifecycle data. Fourth, the translation to business impact—such as cost-performance trade-offs and service value realization—would enhance the framework's strategic relevance for industry stakeholders. These research directions would further strengthen the relevance, technical and regulatory soundness of this study for DPP implementation.

Table of contents

Acknowledgment i
Executive Summary ii
Table of contents iv
List of Figures vi
List of Tables vii
Acronyms viii
1. Introduction 1
   1.1 Background & Motivation 1
   1.2 Problem Statement & Research Gap 3
   1.3 Research Questions 4
   1.4 Research Objectives & Scope 5
   1.5 Thesis Outline 6
2. Literature Review 7
   2.1 Digital Product Passports for Electric Vehicle Batteries 7
   2.2 The Internet of Things 8
   2.3 The Role of IoT in Enabling Digital Product Passports 11
   2.4 Synthesis and Summary 14
3. Methodology 15
   3.1 Framework for Research Design 15
   3.2 Research Methodology 16
4. Evaluation Framework Design 21
   4.1 Analysis: Data and Requirements for DPP 21
   4.2 Analysis: Evaluation Dimensions 26
   4.3 Evaluation Framework: Evaluation Matrix & Trade-off Table 35
5. Validation: Expert Interviews 41
   5.1 Insights from Exploratory Interviews 41
   5.2 Insights from In-depth Interviews 42
   5.3 Summary of Expert Insights 49
6. Result - Refined Evaluation Framework 51
   6.1 Evaluation Matrix 51
   6.2 Trade-off Table 52
7. Discussion 55

7.1 Research Findings 55
7.2 Limitations 56
7.3 Suggestions for Future Research 57
7.4 Contributions 58
8. Conclusion 59
8.1 Conclusion 59
8.2 Reflection 60
8.3 Link to Management of Technology 60
Bibliography 61
Appendix A: Literature Review Strategy 67
Appendix B: Research Diagram 69
Appendix C: Interview Protocols 70
Appendix D: Creating Evaluation Dimensions 72
Appendix E: Key Trade-offs from Expert Interviews 74
Appendix F: Insights Mappings from Analysis 78
Appendix G: Codebook for Thematic Analysis 79

List of Figures

Figure 1: Digital Product Passport concept for EV 2

Figure 2: An Internet of Things taxonomy by Yaqoob et al. (2017) 9

Figure 3: General IoT Architecture by Ahmid et al. (2024) 10

Figure 4: Other IoT architecture representations by Atzori et al. (2017) and Yaqoob et al. (2017) 11

Figure 5: Design Science Research framework adopted from Hevner et al. (2004) 15

Figure 6: Overview of interview protocol 19

Figure 7: Adopted visual models of the RAMI and IIRA reference frameworks 26

Figure 8: Logic behind the evaluation dimensions 30

Figure 9: DPP in EV operation context 31

Figure 10: Overview of discussions for IoT and Required Data Mapping 42

Figure 11: Overview of evaluation dimensions for DPP 44

Figure 12: External factors influencing system design 50

Figure 13: Overview of Required data points 78

Figure 14: Overview of Challenges from expert interviews 78

List of Tables

Table 1: Overview of exploratory participant profiles 18

Table 2: Overview of in-depth participant profiles 20

Table 3: Summary of required dynamic data attributes (DIN DKE SPEC 99100) 21

Table 4: Mapping of Required DPP Data Attributes and IoT Layers 23

Table 5: Full mapping between DPP Dynamic data requirements and corresponding IoT layers 24

Table 6: IoT platform and function gap analysis, adopted from Mineraud et al. (2016) 29

Table 7: Summary of Evaluation Dimensions and affected attributes 33

Table 8: Evaluation Matrix 35

Table 9: Trade-off table for the framework evaluation dimensions 38

Table 10: Evaluation Matrix with architecture profiles 39

Table 11: Ranking of Evaluation Dimensions based on expert interviews 47

Table 12: Refined Evaluation Matrix with dimension importance ranking 51

Table 13: Refined Trade-off table 54

Table 14: Overview of literature search engines 67

Table 15: Overview of Keywords and Search strings 68

Acronyms

API Application Programming Interface

BMS Battery Management System

CMU Cell Monitoring Unit

CIRPASS Collaborative Initiative for a Standards-based Digital Product Passport

DPP Digital Product Passport

EV Electric Vehicle

EU European Union

ESPR Ecodesign for Sustainable Products Regulation

GPRS General Packet Radio Service

GPS Global Positioning System

GSM Global System for Mobile Communications

IoT Internet of Things

IIRA Industrial Internet Reference Architecture

JSON-LD JavaScript Object Notation for Linked Data

LMT Light mean of transport

MQTT Message Queuing Telemetry Transport

OEM Original Equipment Manufacturer

QoS Quality of Service

RAMI Reference Architecture Model Industrie 4.0

RFID Radio Frequency Identification

REST Representational State Transfer

RDF Resource Description Framework

SoC State of Charge

SoH State of Health

SOCE State of Certified Energy

TSCH Time-Slotted Channel Hopping

1. Introduction

This chapter introduces the research context underlying this study. Chapter 1.1 outlines the background and the research motivation within the broader sustainability and policy landscape. Chapter 1.2 identifies the problem statement and highlights current gaps in both academic and practical understanding. Chapter 1.3 formulates the central research question, followed by the sub-questions. Chapter 1.4 presents the research scope and objective. Lastly, Chapter 1.5 provides an outline of the overall thesis structure.

1.1 Background & Motivation

Sustainability has become a global movement with a strategic goal aimed at preserving natural systems while promoting continuous social and economic development. The Brundtland Report defined sustainable development as that which "meets the needs of the present without compromising the ability of future generations to meet their own needs" (World Commission on Environment and Development, 1987). Following this ideology, the European Union (EU) is advancing an ambitious regulatory agenda aimed at accelerating the shift toward a circular and sustainable economy. Under the European Green Deal, various legislative proposals have been introduced to improve resource efficiency, reduce carbon emissions, and encourage responsible product lifecycle management.

The Ecodesign for Sustainable Products Regulation (ESPR) proposal was published as a part of the EU Green Deal. Its main aim is to improve sustainability in products placed on the EU market, with more stringent environmental standards throughout the product lifecycle (European Commission, 2022). To aid the regulatory implementation, the Digital Product Passport (DPP), a key innovation that was introduced by the European Commission within the *ESPR*, which aims to make sustainable products the norm in the EU market (European Commission, 2022). According to the World Economic Forum (2023), DPP is a machine-readable data carrier that stores and communicates essential information about a product's characteristics, lifecycle, and environmental impact, including details such as material composition, carbon footprint, repairability, and recyclability. The primary goals of the DPP are to improve product transparency, enable informed decision-making across the supply chain, and support reuse, repair, remanufacturing, and responsible recycling.

Another major effort toward sustainability is the shift from internal combustion engine vehicles to electric vehicles (EV). EVs offer immediate local emission reductions, particularly in urban environments, and when powered by renewable energy sources, can significantly cut lifecycle emissions. Studies show that EVs can reduce greenhouse gas emissions by up to 60% over their lifetime compared to conventional vehicles, depending on the energy mix used for charging (Transport & Environment, 2020). The rapid transition toward EV is reshaping the global automotive industry. With the EU plans to ban the sale of new petrol and diesel cars by 2035 (European Commission, 2021) and the recent development of battery technology, the EV industry is expected to grow significantly in the coming decade (Cerruti et al., 2024; Weiss et al., 2023). At the heart of this transition lies the EV battery, a critical component that decides the performance of the vehicle and stands out as a high-value commodity. Each EV battery contains substantial quantities of lithium, cobalt, nickel, and graphite—elements that are considered critical raw materials by the European Commission due to their limited availability, geopolitical risk, and environmental extraction impacts (European Commission, 2023). Producing a single EV battery can require 8 kg of lithium, 35 kg of nickel, and 20 kg of manganese, alongside a vast amount of water and energy (Castelvecchi, 2021).

Most EVs nowadays depend on rechargeable lithium-ion batteries, which have a finite life span and degrade gradually over time. In 2022, global e-waste reached 62 million metric tons, with only 17.4%

formally recycled (Global E-waste Monitor, 2024). Improper disposal of millions of decommissioned batteries could cause significant environmental hazards, including toxic waste leakage and pollution of ecosystems. Furthermore, the lack of reliable systems for battery traceability and second-life utilization exacerbates resource inefficiencies and environmental risks. Without robust end-of-life strategies, including reuse, repurposing, and high-yield recycling, the growth of electromobility may trade one environmental problem for another.

Although the DPP concept, as a regulatory tool, provides a potential pathway for capturing these traceability data on EV batteries, operationalizing DPP in real-world settings is far from straightforward. Unlike many other consumer products, EVs—particularly their batteries—generate vast amounts of technical data throughout their lifecycle. To meet the objectives of the EU Battery Regulation, DPPs must accurately capture and maintain both static data (battery composition, manufacturer origin, carbon intensity, material sourcing) and dynamic data (real-time performance indicators such as state of charge (SoC), state of health (SoH), charge cycles, degradation rates, and usage patterns), , as illustrated in Figure 1 (World Economic Forum, 2023).

Static data, such as battery composition, manufacturing origin, and supply chain documentation, is often dispersed across stakeholders in heterogeneous, proprietary formats, leading to persistent integration barriers and siloed data systems (Berger et al., 2022). Simultaneously, dynamic data—including operational parameters like SoC, SoH, and charging cycles—must be continuously captured, processed, and verified throughout a battery's lifecycle. This requires a robust digital infrastructure ensuring secure, reliable, and real-time data transmission (Berger et al., 2023)

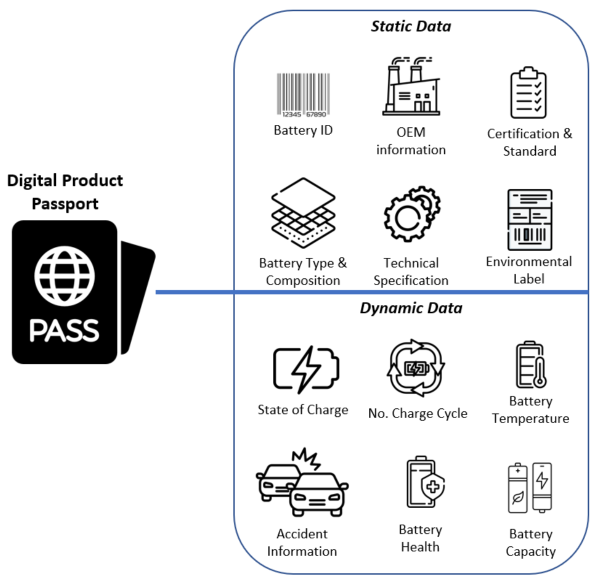


Figure 1: Digital Product Passport concept for EV

Moreover, questions about data ownership, privacy, and access control are highly contested. Stakeholders across the EV ecosystem—original equipment manufacturers (OEMs), regulators, recyclers, and second-life operators—often require access to overlapping but distinct sets of product data, posing governance and architectural challenges (Berger et al., 2023). Without a standardized approach to translating regulatory intent into machine-readable data models, DPP implementation risks being fragmented or non-operational in real-world settings (Berger et al., 2023).

Amid these challenges, the Internet of Things (IoT) emerges as an enabling technology, capable of addressing many previously mentioned limitations. Modern EVs are increasingly equipped with IoT-enabled components—onboard sensors, control units, telemetry modules, and cloud-connected platforms—that monitor and transmit operational data in real time (Singh et al., 2022; Rao et al., 2024). These existing infrastructures offer a technical basis upon which DPP functionality can be layered. However, integrating DPPs with IoT systems is not without difficulties. As more functions are added, it introduces complexities in the architectural designs. Since this is a regulatory tool, it must accommodate both technical requirements and policy expectations for the EV's daily operation. Addressing these gaps requires a structured investigation into how different IoT architectures can serve the operational demands of DPPs in the EV sector.

1.2 Problem Statement & Research Gap

1.2.1 Problem Statement

Despite the growing momentum around DPP, a significant gap persists between the DPP policy and the technical systems to implement it in the context of EVs. While the regulation defines what information must be included and made accessible across the battery’s lifecycle, it does not provide guidance on how this information should be collected, stored, managed, and updated in real time (Uusitalo et al., 2023). This is especially problematic for data that is not fixed at the time of manufacture but changes throughout the product’s use phase, such as battery performance, charging patterns, thermal events, or degradation indicators. These forms of dynamic data are critical for ensuring compliance, enabling second-life applications, and supporting safe recycling — yet they are the most technically demanding to manage (Berger et al., 2023).

During operation, EV batteries generate large volumes of data through the onboard monitoring systems, such as the Battery Management System (BMS), embedded with various IoT components. These existing infrastructures offer a potential foundation on which DPP implementation can be expanded upon (Garrido-Hidalgo et al., 2020). However, converting this raw data into a structured, reliable, and DPP-compliant form requires careful coordination across multiple domains: hardware design, software architecture, cloud infrastructure, cybersecurity, and stakeholder governance (Berger et al., 2023; Uusitalo et al., 2023). Furthermore, the data must be selectively accessible by a range of actors — from manufacturers and service providers to recyclers and regulators — each with different needs and permissions. This makes the design and integration of supporting data systems a highly complex task.

Without clear guidance to evaluate how well existing or proposed IoT architectures meet these multifaceted requirements, OEMs, system integrators, and solution providers are left to make ad hoc decisions that may fall short of compliance or result in overly rigid, costly systems. There is an urgent need for practical decision-support tools that can help assess which architectural approaches are most suitable for enabling dynamic DPP functionality in EV batteries — not only from a technical standpoint, but also considering feasibility, scalability, and operational fit (Garrido-Hidalgo et al., 2020).

1.2.2 Research Gap

While the regulatory vision is well-defined, there is a literature gap in operationalizing DPPs in real-world settings. Stakeholders in the value chain have voiced concerns regarding unclear data formats, interoperability standards, and governance models, which hinder the development of coherent and feasible technical pathways (Berger et al., 2023). Most existing studies provide high-level design principles or focus on policy frameworks but stop short of addressing the technological enablers required for dynamic, cross-platform data flows—particularly those involving real-time operational data from battery systems (da Silva et al., 2023; Berger et al., 2023). Moreover, Langley et al. (2023) and Berger et al. (2023)

highlight the ongoing lack of consensus on governance models and system architectures that can balance data privacy, interoperability, and stakeholder alignment. This tension between the regulatory mandate and the lack of technological readiness and standardizations underscores the foundational gap in the current DPP.

Another key gap in current literature is the integration of IoT technology —particularly those embedded in modern EVs' BMS — for DPP. BMS generates real-time data such as SoC, SoH, and temperature logs, which are the legally required data points for DPP compliance. These data points are also useful for second-life use (Garrido-Hidalgo et al., 2020). While several studies highlight the theoretical value of linking digital technologies with DPPs to improve lifecycle data transparency (Baars et al., 2021; da Silva et al., 2023), few provide concrete frameworks or system architectures to operationalize such integration for EV use cases. Despite the increasing technical capability of BMSs to collect granular data, most research still centers on static information—such as composition or carbon footprint—rather than dynamic, performance-based metrics (da Silva et al., 2023; Berger et al., 2023). This focus limits the potential of DPPs to inform predictive or value-driven reuse and recycling strategies. Without integrating dynamic data, DPPs risk remaining passive records rather than active enablers of circularity. Thus, further research is needed to systematically explore how current BMS with existing IoT architecture can be embedded in DPP frameworks to support actionable lifecycle management (Uusitalo et al., 2022). In addition, the technical readiness of IoT systems for enabling DPP functionality remains underexplored. Although technologies such as edge sensors, cloud storage, and digital twins are discussed conceptually (Garrido-Hidalgo et al., 2020; Langley et al., 2023; Rufino et al., 2024), their integration maturity, interoperability, and deployment constraints are rarely assessed in a systematic manner. Studies tend to focus on theoretical integration without benchmarking readiness or evaluating feasibility at the system level (Weinzerl et al., 2023; Uusitalo et al., 2022). As a result, decision-makers currently lack validated tools to evaluate when, where, and how IoT can support DPPs implementation across different stages of the battery lifecycle.

This research seeks to address these gaps by designing an evaluation framework specifically tailored to integrate IoT technologies within DPP for EV batteries. Applying a Design Science Research (DSR) methodology, this study developed and validated the artifact—an evaluation framework—that assists industry actors, particularly EV OEMs, in understanding and navigating the functional requirements of DPPs. By aligning technological capabilities with stakeholder-specific use cases, the framework aspires to move DPP from conceptual promise to actionable implementation.

1.3 Research Questions

The thesis dives into assessing IoT and their potential use cases to support the implementation of DPP for EV batteries. Bounded by the impending regulation, this research domain is time-critical and underdeveloped, as it is a relatively new concept with an abundance of unclear requirements from a complex stakeholder network. An evaluation framework is required to systematically assess regulatory and technical requirements in the EV context to provide more transparency into the topic. This approach can provide a practical guideline for any relevant parties that partake in the value chain of EV batteries. The following research question captures the nature of this study:

"How can a suitable evaluation framework be developed to assess the potentials and challenges of IoT-driven Digital Product Passports for EV batteries?"

From the main research question, four sub-research questions are derived to organize the research process systematically. As the study adopted the DSR methodology, it focuses on designing a product, here an evaluation framework for IoT that requires the following sub-questions:

Sub-question 1: *What are the key technical, regulatory, and data requirements for DPP in EV batteries?*

The first sub-question aims to establish a clear understanding of the core requirements for DPPs. This step involves conducting and analyzing the literature for theories, frameworks, regulatory documents, and other related consortium projects. The objective is to identify existing challenges and key data requirements that link between regulations and existing EV systems.

Sub-question 2: *What evaluation criteria must be included in the framework to capture the operational context of IoT-Driven DPP?*

Building on the input requirements, the second sub-question focuses on developing a set of evaluation dimensions that serve as the foundation for the framework. The operational context of the EV is analyzed to see which technical functionalities are required for DPPs to be implemented in the day-to-day operational scenario.

Sub-question 3: *What is the structure and design of the evaluation framework for IoT adoption in DPPs?*

The third research question focuses on creating the artifact based on the outcomes of the previous sub-questions. The design artifact – here the evaluation framework and its following components – aims to guide the assessment of potentials and challenges of different IoT architecture profiles for DPP-contexts.

Sub-question 4: *Does the framework address challenges and provide practical guidelines for IoT-Driven DPP adoption?*

Following the artifact development, the fourth research question seeks to validate the framework through practical testing and expert insights. This phase includes conducting interviews with experts in different disciplines to evaluate the robustness and applicability of the framework in addressing the requirements of IoT-driven DPPs.

1.4 Research Objectives & Scope

While the full implementation of a DPP requires the collection of both static and dynamic data attributes across the battery lifecycle, this study deliberately narrows its focus to only dynamic data. Static data—such as manufacturer ID, production site, or component composition—remains unchanged over time. In addition, it does not create any substantial requirements for real-time sensing or processing capabilities. In contrast, dynamic data—including metrics such as SoC, charging cycles, thermal anomalies, and event logs—are subject to continuous variation. Therefore, these metrics demand a more complex infrastructure and capabilities (such as sensing, processing, computing, and transmitting data). These attributes and their technical demands are where IoT technologies play a critical enabling role, making dynamic data the most relevant focus for an evaluation framework.

The framework is intended to support technical decision-makers—particularly for OEMs, system integrators, and solution providers—in selecting suitable IoT architecture profiles that can enable traceable, compliant, and interoperable DPP for EV battery. Furthermore, this research does not propose a fully universal or finalized technical blueprint for DPP implementation. Instead, it offers a flexible evaluation approach, adaptable to evolving regulatory requirements and technological advancements. By limiting the scope to dynamic data attributes and the architectural capabilities that support them, the framework remains focused, actionable, and relevant to early-stage decision-making within OEM environments.

1.5 Thesis Outline

The thesis is divided into seven chapters. Chapter 1 introduces the policy and technological context, outlines the research problem, defines the objectives, and sets the scope of the study. Chapter 2 provides a knowledge base of the relevant domains for this study, including existing literature on DPPs, IoT, and BMS architectures. Chapter 3 explains the methodological and framework approach for this study. Chapter 4 presents the core of this study, through the design process, key analysis of the framework, along with its components. Chapter 5 provides expert interviews and highlights key insights. Chapter 6 presents the refined framework based on expert interviews. Chapter 7 discusses key findings, addresses limitations, and suggests directions for future research. Finally, Chapter 8 concludes the study with a reflection and a link to the Management of Technology study.

2. Literature Review

A literature review is essential to identify the scientific knowledge base and gaps in the research topic. Therefore, this chapter provides the background, key themes, and relevant concepts for this study through the following structure. Chapter 2.1 introduces the concept and policy relevance of DPP, particularly for EV batteries. Chapter 2.2 explains the IoT concept, its development, and its role in industry. Chapter 2.3 explores how IoT can support DPP implementation, particularly for EV case. Finally, Chapter 2.4 provides a summary of the literature review. In addition, the approach to literature review is provided in Appendix A.

2.1 Digital Product Passports for Electric Vehicle Batteries

2.1.1 Definition and Policy Context

As part of the European Union's broader strategy for promoting a circular and sustainable economy, DPP has emerged as a policy-driven tool to enhance product transparency, traceability, and lifecycle accountability. By definition, DPP is a structured set of product-related data linked through a unique product identifier and accessible via electronic means that supports sustainability, circularity, value retention, and compliance verification throughout a product's lifecycle (Regulation (EU) 2023/1542). Specifically for EV batteries, DPPs serve as digital records containing key information on the battery's origin, usage, composition, and environmental impact. This initiative is formally codified in Regulation (EU) 2023/1542, which came into effect in July 2023 and mandates that all EV batteries, industrial batteries over 2 kWh, and light means of transport (LMT) batteries must be accompanied by a digital passport starting from 18th February 2027 (European Union, 2023). The regulation defines the battery passport as a machine-readable, electronic record linked to a unique battery identifier and accessible via a QR code. It is part of the EU's broader eco-design policy, aligning with the goal of embedding digital transparency mechanisms across high-impact product categories. The DPP is not only intended for documentation but also plays a central role in regulatory compliance, enabling authorities and market participants to track a battery's environmental and operational performance over time.

2.1.2 Core functionalities and Stakeholder Requirements

DPP for EV batteries is designed to comprehensively capture and communicate information across all stages of a battery's lifecycle. The data included in the DPP is expected to cover raw material sourcing (including country of origin and certification schemes), manufacturing processes (such as carbon footprint and material composition), in-use diagnostics (including charging patterns and degradation rates), and end-of-life details (such as disassembly instructions, recyclability scores, and recovery efficiency) (Jousse, 2024). This structured dataset enables greater transparency and traceability, allowing various stakeholders to access the specific information they need for their roles in the circular economy.

The requirements for DPPs vary according to stakeholder needs. Regulatory authorities, including market surveillance bodies and customs agencies, use DPP data to monitor compliance with environmental and safety regulations. They benefit from easy access to verified data points such as carbon footprint declarations or sourcing documentation (CIRPASS 2, 2024). OEMs and battery producers utilize DPPs to support quality assurance, warranty management, and secondary use assessments, such as determining whether a battery can be reused in stationary storage applications after its automotive lifecycle ends (CIRPASS, 2024a). Recyclers and remanufacturers rely on DPPs for accurate disassembly guidance, identification of hazardous components, and optimization of material recovery processes (Wenning et al., 2024). Consumers and professional buyers also derive value from DPPs by gaining insights into a battery's durability, environmental footprint, and repair history, which can influence purchasing decisions and build trust in product sustainability.

To address the previously mentioned functions, the CIRPASS (Collaborative Initiative for a Standards-based Digital Product Passport) and Battery Pass are two major EU-funded industrial initiatives strategically developed to facilitate the large-scale DPP deployment of across key sectors such as electronics, textiles, and batteries. Supported under the European Union's Digital Europe Programme, CIRPASS serves as a foundational coordination and support project that brings together over 30 partners, including standardization bodies, digital solution providers, and industry stakeholders. Its primary goal is to develop a harmonized system architecture, identification schemes, and data exchange mechanisms to ensure interoperability of DPP systems across sectors and borders (DPP System Roadmap, 2024). Similar to this effort, the Battery Pass project specifically addresses the regulatory requirements set by the EU Battery Regulation by focusing on a robust DPP framework tailored to electric vehicle (EV) batteries. It emphasizes traceability, lifecycle monitoring, and second-life applications by integrating dynamic IoT-enabled data into the DPP ecosystem (Battery Pass, 2024). Both initiatives are instrumental in operationalizing the European Green Deal and the ESPR, reflecting the EU's commitment to fostering a circular economy through digital innovation and regulatory alignment (Regulation (EU) 2023/1542).

With these ongoing foundational works, DPP systems are being developed with modularity and data governance in mind. Stakeholder consultations within the CIRPASS project highlight the importance of role-based access control and interoperability between systems. For example, access to detailed recycling instructions may be restricted to certified recyclers, while only general sustainability scores are made available to consumers. This targeted data exposure ensures that DPPs remain both privacy-conscious and commercially viable (Jousse, 2024).

2.2 The Internet of Things

2.2.1 Definition and History

The term "IoT", first popularized by Kevin Ashton in 1999, is a growing concept that has developed significantly over the past decades. In its simplest form, IoT refers to a network of interconnected physical devices—ranging from everyday consumer items to industrial machinery—that are embedded with sensors, software, and communication technologies (Atzori et al., 2010). Initially, Kevin Ashton employed Radio Frequency Identification (RFID) to link physical objects to digital systems, and that is one of the first versions of IoT (Atzori et al., 2017). Nowadays, far from the original use, IoT devices are now everywhere, able to collect, transmit, and sometimes act on data over the internet with minimal human intervention (Gupta & Quamara, 2018). Common characteristics found across most definitions of IoT include ubiquitous connectivity, intelligent sensing and actuation, distributed computing, interoperability, and most importantly, the scalability to billions of devices (Gupta & Quamara, 2018; Yaqoob et al., 2017).

Gradually, IoT has advanced over the years, combined with other complementary technologies such as cloud computing, big data analytics, artificial intelligence (AI), and 5G connectivity. IoT finds itself in different domains with various unique use cases. For example, in the healthcare industry, wearable devices have made constant and connected health tracking possible, opening up many possibilities such as health data analytics or remote caring solutions (Baker et al., 2017). In the manufacturing sector, IoT has been widely adopted to provide real-time production tracking and other predictive maintenance solutions. In some cases, it can also be used to exchange information, greatly boosting logistical efficiency and optimizing the supply chain (Caputo et al., 2016). For the EV domain, IoT-based solutions are increasingly incorporated in the different operational aspects. IoT have been used to significantly enhances vehicle management through real-time monitoring of battery health, optimizing battery usage, and prolonging overall battery life (Savari et al., 2020). Moreover, IoT supports advanced driver-assistance systems and autonomous driving features by enabling seamless communication between vehicles and infrastructure (Wang et al., 2021). These applications show that there is a growing number of potential applications for IoT in the EV domain.

2.2.2 IoT Taxonomy and Technological Stack

Since IoT is a broad concept with a growing definition, understanding its taxonomy would offer a structured way to classify the key dimensions that define IoT ecosystems. Figure 2 presents the work from Yaqoob et al. (2017) to categorize IoT according to their applications, enabling technologies, business objectives, architectural requirements, platform types, and network topologies. While the applications and business objectives domains focus more on the real-life usage or business operation goals, other categories, such as enabling technologies, architectural requirements, platform types, and network domains, focus more on the technical aspects of IoT. This can range from very high-level details such as a large-scale, heterogeneous network, to more well-defined characteristics such as scalability, flexibility, interoperability, and security. This category group mainly focus on the technical capabilities and performance aspects of an IoT system. While this taxonomy is useful for understanding the broader functional scope and design variability of IoT systems, it is not granular enough to address system challenges and operational focus. Abstract concepts like "business objectives" are better suited for contextual analysis or planning rather than system modelling or evaluation frameworks.

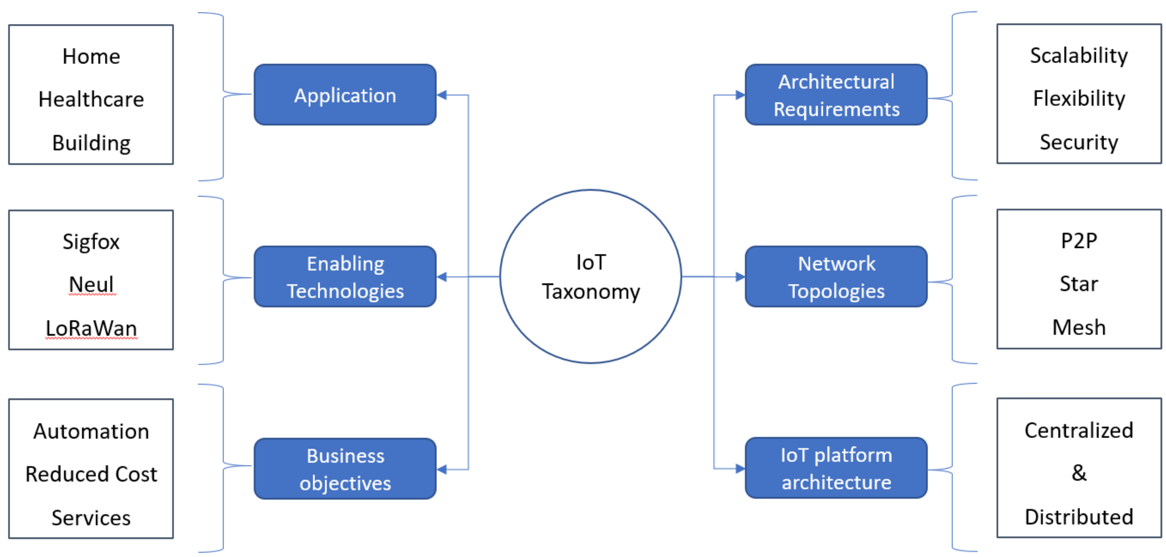


Figure 2: An Internet of Things taxonomy by Yaqoob et al. (2017)

Through reviewing multiple studies, a common architectural pattern has emerged that organizes IoT systems into four distinct layers: Perception, Network, Middleware, and Application. This model is widely adopted across academic and industrial literature due to its clarity and modularity (Ahmid et al., 2024). Figure 3 describes this model, with each layer playing a specialized role in the IoT system:

- **Perception Layer**: The perception layer serves as the foundational interface between the physical world and IoT systems, consisting of sensors, actuators, RFID tags, and embedded devices that capture environmental data or trigger physical actions. It enables real-world interaction but should not be confused with the physical layer of communication models, as it focuses on data acquisition rather than signal transmission (Gupta & Quamara, 2018).

- **Network Layer**: Responsible for data transmission, this layer routes information from the perception layer to the middleware or application layers. Communication can occur over protocols such as 5G, Zigbee, or Wi-Fi, depending on range and bandwidth needs.
- **Middleware Layer**: Acting as the service layer, this part handles data processing, filtering, storage, and service coordination. It often involves cloud computing resources and supports functions such as trust management, service discovery, and API (Application Programming Interface) provisioning (Ahmid et al., 2024).
- **Application Layer**: The topmost layer interacts with users and enterprise systems. It delivers meaningful insights and services—such as battery health visualization in EVs—based on the underlying data flow

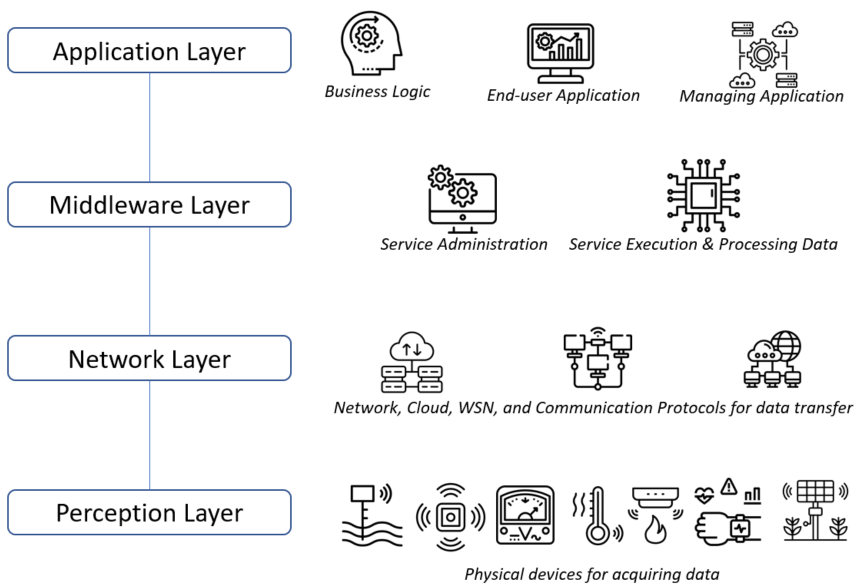
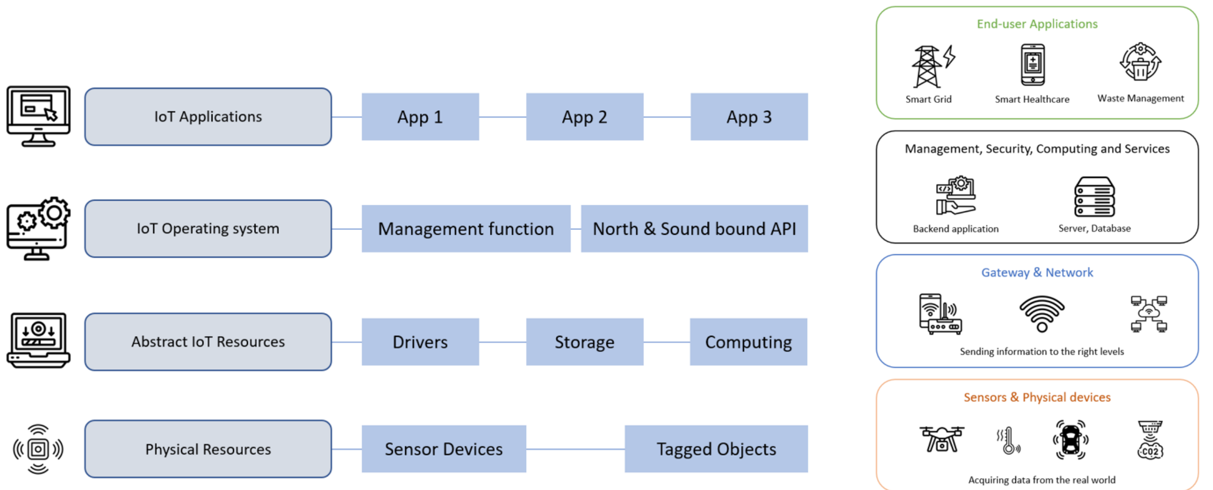


Figure 3: General IoT Architecture by Ahmid et al. (2024)

While the four-layer model is widely accepted, several studies propose alternative IoT architectures that reflect different design priorities or abstraction levels. These models often introduce new layers or reorganize existing ones to specific technological concerns such as virtualization, middleware intelligence, or platform heterogeneity. For example, Atzori et al. (2017) propose a generalized architecture that is less concerned with strict technical layering and more focused on system components and roles. Their model includes three primary elements: IoT applications, which provide services to end-users; the IoT operating system, which coordinates devices and manages system resources; and drivers, which act as abstraction interfaces between physical IoT resources and the operating system. This view highlights the integration of hardware abstraction into the software stack but does not explicitly separate communication or data processing layers.

In another study, Uviase and Kotonya (2018) present a simplified three-layer architecture consisting of a physical sensing layer, an IoT middleware layer, and an application layer. Their emphasis is on the middleware's role in managing communication, data coordination, and interoperability—largely driven by service-oriented architecture (SOA) principles. This model intentionally omits a dedicated network layer, folding communication responsibilities into the middleware, and illustrates the rising importance of cloud-based services and intelligent APIs in contemporary IoT deployment. Yaqoob et al. (2017) introduce yet another variation by identifying four vertically integrated components: smart applications, management and security services, gateway and network infrastructure, and sensors and connectivity. Their focus is not only on the data flow but also on platform-wide services such as trust, authentication, and data privacy. While insightful for mapping system-wide concerns, this framework blends functional domains (like security and management) across what would otherwise be separate technical layers in a traditional architecture.



General IoT architecture by Atzori et al., 2017

General IoT architecture by Yaqoob et al., 2017

Figure 4: Other IoT architecture representations by Atzori et al. (2017) and Yaqoob et al. (2017)

These variations, as shown in Figure 4, reveal that IoT architecture is not monolithic. Different models emphasize different priorities—some focus on enabling technologies and system abstraction (Atzori et al., 2017), others on integration and interoperability (Uviase & Kotonya, 2018), and others still on security and application-level orchestration (Yaqoob et al., 2017). However, they often result in overlapping or loosely defined responsibilities between layers, which can complicate system modularity and make cross-system comparisons more difficult.

2.3 The Role of IoT in Enabling Digital Product Passports

2.3.1 The Choice of IoT

IoT, along with its expanding capabilities over time, offers a promising foundation in enabling DPP. The intrinsic nature of IoT, where physical devices such as sensors, actuators, and embedded systems generate and transmit real-time data, makes it ideally suited to meet DPP requirements, especially those related to lifecycle documentation, performance monitoring, and compliance auditing (Shafique et al., 2020). In the case of EV, IoT has already manifested within the vehicle BMS, which is present in nearly all of modern EV (Geetha et al., 2024). BMS is a critical component in EV, designed to monitor and regulate the operation of battery cells to ensure safe, efficient, and long-lasting performance. It continuously tracks parameters such as voltage, current, temperature, and SoC, protecting the battery from conditions like overcharging, deep discharging, or overheating. Additionally, the BMS supports functions such as cell balancing, fault detection, data logging, and communication with other vehicular or cloud-based systems, forming the core of what is now evolving into Internet-of-Batteries (Li et al., 2023).

BMS is inseparable from EVs because this system oversees critical battery parameters such as SoC, SoH, voltage, temperature, and current. It is also typically embedded with communication modules that allow remote diagnostics, data logging, and in some advanced applications, over-the-air updates (Shafique et al., 2020). As mandated by the EU Battery Regulation (EU) 2023/1542, data on the battery's state of health and remaining lifetime must be made available through the BMS to enable reusability, repurposing, and end-of-life planning (European Union, 2023). This establishes a strong position for IoT as an enabling technology for DPPs through existing BMS infrastructure.

IoT is particularly well-positioned among other candidate technologies due to its modular extensibility and existing deployment base. Other technologies, like blockchain, require heavy validation and infrastructure transformation, focusing on ensuring trust and decentralized control rather than data and connectivity (European Blockchain Observatory and Forum [EUBOF], 2023), or RFID, which provides only point-in-time static identification. IoT systems support continuous data flow, system-wide integration, and context-aware decision-making (Colaković & Hadžialić, 2018). Cloud computing, while crucial for data storage and analytics, lacks the edge-device-level interaction and real-time responsiveness that IoT enables (Al-Dulaimy et al., 2024). These mentioned technologies, rather than being direct competitors, are complementary to IoT rather than replacing it, but they focus on other aspects, such as trust and security, more than the collection of data for the EV itself. Given its existing presence in BMS, the choice of IoT for DPPs is similar to extending their current BMS capabilities, rather than requiring a completely new data infrastructure, hardware, or functions to be developed from scratch.

In summary, IoT offers significant potential as an enabler for implementing DPP systems, particularly in the context of EV batteries. Its technical feasibility stems from its established integration with BMS, which already supports essential sensing and diagnostic functions such as real-time monitoring of temperature, voltage, and usage profiles (Li et al., 2023). Moreover, IoT can help the process in capturing and transmission of dynamic data across the battery lifecycle, aligning with regulatory requirements for traceability and sustainability reporting under the EU Battery Regulation (Li et al., 2023; Regulation (EU) 2023/1542).

2.3.2 Opportunities and Challenges of IoT in DPP system

The use of IoT introduces a substantial opportunity. Key battery parameters, including temperature, voltage, current, and usage history, are often sourced from the existing BMS, which already integrates sensing and diagnostic functionalities within the EV platforms (Li et al., 2023). By expanding these capabilities into broader IoT architectures, their utility can be extended beyond vehicle-centric control to product-centric data sharing within the DPP ecosystem (Shafique et al., 2020).

A distinctive strength of IoT lies in its ability to bridge physical and digital infrastructures through real-time, distributed sensing and communication. Data collected by edge/perception-level sensors is processed by IoT middleware, which filters, aggregates, and formats the information—commonly in lightweight, machine-readable formats such as JSON (JavaScript Object Notation for Linked Data)—before synchronizing it with cloud platforms for persistence and accessibility (Colaković & Hadžialić, 2018). This middleware plays a crucial role in localizing decision-making (e.g., triggering service alerts and critical event logs) (Uviase & Kotonya, 2018), while also supporting global functions such as DPP data updates or regulatory audits. The CIRPASS system architecture embraces this structure by anchoring all DPP data around a unique product identifier and supporting both static and dynamic updates (Wenning et al., 2024), for which IoT can specifically support dynamic operational data.

These functionalities are well-illustrated in CIRPASS user scenarios. In User Story 7 (CIRPASS 2, 2024), a remanufacturer accesses battery history data, updating new information about component replacement and secondary applications. This real-time access to extract, update lifecycle data significantly improves the safety, efficiency, and yield of end-of-life processing (Wenning et al., 2024). Both cases underscore the potential for IoT to meet the data request and support decision-making across circular economy functions, from reuse and repair to recycling and reporting.

Nonetheless, several challenges must be addressed to realize these benefits. Interoperability is a persistent concern in IoT deployments, especially when integrating devices from multiple vendors with differing data protocols and semantics. While there are many initiatives and semantic projects that aim to standardize industrial data exchange, full implementation across stakeholders remains elusive (Dorsemaine et al., 2015). Security and privacy are equally critical. The continuous collection and transmission of operational data raises more concern about how these data are accessed and stored. CIRPASS proposes role-based access models to ensure that only authorized actors can view or modify specific DPP fields, but this adds complexity to the system as the details of such a mechanism are not yet defined (Wenning et al., 2024). From an organizational standpoint, operational context and legacy integration present further barriers. EV manufacturers and other SMEs in the battery value chain may struggle to retrofit their systems with IoT hardware and added functionalities. Every step in which the data is collected, processed, transmitted, and updated presents unique challenges that need to be integrated within the operational context of EV.

Despite these challenges, IoT remains a highly effective enabler for DPPs. Its maturity, modularity, and compatibility with BMS systems already embedded in EVs reduce the implementation burden while offering rich functionality. IoT helps realize the vision of DPPs as living digital records that capture product histories and inform circularity decisions throughout the battery lifecycle.

2.3.3 Existing IoT Architectures for BMS

Several academic studies have proposed IoT-based system architectures for EV battery monitoring, differing in their topological design, data communication strategies, and functional emphasis. These architectures offer valuable insights into how IoT can support DPP implementation, particularly through the collection of dynamic battery data such as voltage, temperature, SoC, and SoH. Due to the limited public availability of proprietary industrial architectures, academic research profiles provide accessible, transparent descriptions that allow for critical analysis and serve as an example for evaluating the applicability and readiness of this study’s framework.

To support the framework development in this study, four academic profiles were selected from peer-reviewed literature and doctoral research. These profiles were chosen for their diversity in system maturity, technical approach, and hardware configurations within the context of BMS design. For example, the selected profiles represent both centralized and decentralized topologies, with varied optimization goals and application scenarios. Although these implementations are not commercial in nature, they provide meaningful and structured examples to explore potential compatibility with emerging DPP requirements.

Profile 1, developed by Wahab et al. (2018), presents a centralized IoT-based battery monitoring system for EVs. Its main strength lies in simplicity and ease of implementation, offering core capabilities such as remote collection of battery voltage and GPS (Global Positioning System) data. While for Profile 2, proposed by Kim et al. (2018), introduces a decentralized wireless BMS architecture leveraging IoT-based networks to enable distributed monitoring and control. Its key strengths include real-time event detection and scalability for dynamic monitoring contexts. Profile 3, described by Le Gall et al. (2022), focuses on optimized network management using Time-Slotted Channel Hopping (TSCH) protocols to enhance communication efficiency in EV BMS. This architecture is well-aligned with DPP criteria related to dynamic data integration and cloud connectivity, though it presents complexity challenges in deployment. Profile 4, a PhD dissertation from Bašić (2023), presents a secure and wireless BMS designed with regulatory compliance in mind, incorporating verifiable credentials and robust data protection mechanisms specifically designed for DPP objectives. While strong in data integrity and lifecycle tracking, it entails greater system development effort and cost. These candidate profiles serve as the comparative cases for applying the evaluation framework developed in this study. Their evaluation is presented in Chapter 4, where each architecture profile is assessed to identify strengths, limitations, and areas for alignment or improvement.

2.4 Synthesis and Summary

The literature reveals that DPP is a central regulatory tool under the EU's sustainability agenda, aimed at improving transparency, traceability, and lifecycle management of products—most urgently for EV batteries under Regulation (EU) 2023/1542. For batteries, the DPP must capture structured data spanning raw material sourcing, manufacturing, in-use diagnostics, and end-of-life processes, serving diverse stakeholder needs from regulators to recyclers. Existing EU-funded initiatives such as CIRPASS and Battery Pass have advanced high-level functional requirements, attribute lists, and user stories, yet they often stop short of defining operational-level evaluation criteria for technical system design.

IoT emerges from the literature as the enabling technology for meeting DPP dynamic data requirements, given its capacity for real-time sensing, processing, and secure transmission. Foundational IoT reference architectures provide structured insights into component roles, interoperability, and integration patterns, while academic BMS-focused IoT designs illustrate concrete implementations. However, most documented systems prioritize either functional coverage or communication optimization, with few explicitly aligned to regulatory traceability goals. Integration of IoT and DPP is shown to be promising but still underdeveloped. Prior studies emphasize that dynamic operational data—such as SoC, thermal anomalies, and event logs—require complex, resilient architectures linking physical sensing layers, middleware, and application services. Gaps remain in translating abstract regulatory requirements into measurable technical performance criteria, as well as in addressing trade-offs between cost, scalability, and compliance.

Overall, the literature highlights a lack of technically actionable, architecture-level evaluation frameworks tailored to EV battery DPP contexts. Addressing this gap requires combining regulatory insights, IoT architectural principles, and EV operational use-case analysis. This study responds to that need by developing an evaluation framework that assesses the readiness and adaptability of IoT-based systems for supporting battery DPPs, aligning design decisions with both technological feasibility and evolving regulatory mandates.

3. Methodology

This chapter explains the approach used to answer the research questions mentioned in Chapter 1. Firstly, Chapter 3.1 describes the research framework that guides this study as the starting point. Then, Chapter 3.2 presents the research methodology along with the data collection process to validate the study result.

3.1 Framework for Research Design

The DSR methodology is a problem-solving research approach that focuses on addressing real-world challenges through creating, developing, and evaluating artifacts and solutions. Originating from the information system field, the DSR method has gained traction and recognition among scholars in various disciplines. These fields share a common characteristic: technological advancements can improve efficiency, competitive advantages, and decision-making processes (Hevner et al., 2004). Unlike traditional science research, which aims to understand and explain phenomena, DSR focuses more on the design and implementation of solutions that can take different forms, such as models, methods, frameworks, software, or even systems (Gregor and Hevner, 2013).

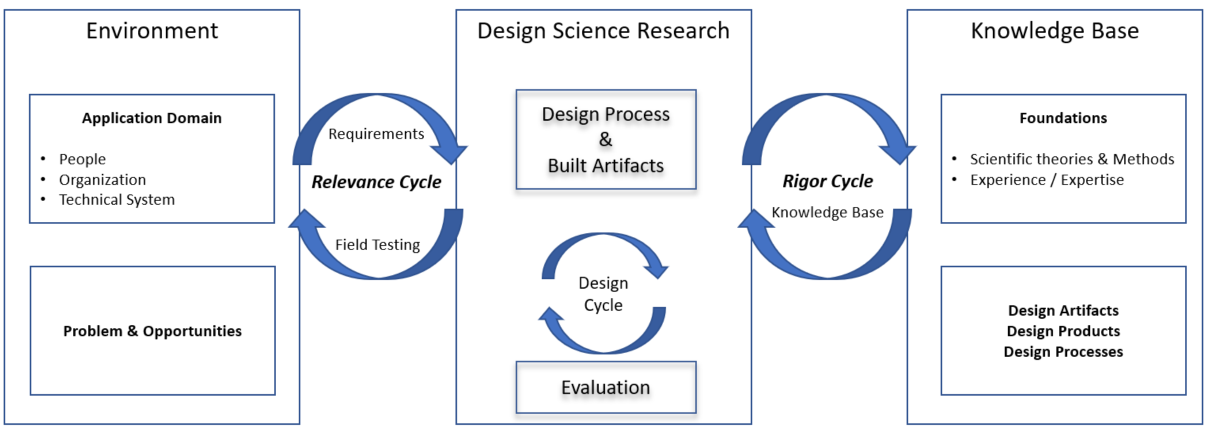


Figure 5: Design Science Research framework adopted from Hevner et al. (2004)

The research topic - IoT-driven DPP for EV batteries – is motivated by a real-world problem (impending Battery Directive starting in 2027). In addition, the topic carries not only technical elements such as dynamic data but also many regulatory pressures. As a result, the development of a usable artifact must integrate stakeholder-specific requirements, system constraints, and policy mandates. Given these characteristics, the DSR methodology was deemed most appropriate for this study. Compared to approaches such as case study research, which focuses on contextual analysis, or grounded theory, which aims to generate theory from observations, DSR emphasizes the artifact creation and iterative evaluation (Gregor & Hevner, 2013). This focus on designing and refining a solution aligns with the study's goal of producing a functional, evaluative framework for assessing IoT-based architectures for DPP compliance. DSR also allows integration of both theoretical grounding (through the rigor cycle) and real-world validation (through expert feedback), which is particularly valuable in addressing a complex, multi-stakeholder problem that is still under development (Hevner et al., 2004). Adopted the three-cycle model from Hevner et al. (2004), as shown in Figure 5, the research was organized as follows:

1. Relevance cycle

A structured review of regulatory texts (e.g., EU Battery Regulation), relevant policy documents, and existing DPP pilot project reports identified the precise data types, update frequencies, and requirements for real-time tracking of battery health and lifecycle events. The document analysis process ensured that the artifact responds to current compliance demands and stakeholder expectations for dynamic data. This helps the study answer the first sub-research question related to the key technical, regulatory, and data requirements for DPPs in EV batteries.

2. Rigor cycle

A comprehensive literature review surveyed the latest IoT architectures, classifications, reference models, and industrial frameworks. The purpose of this step was to create a solid knowledge base in the research domains. Gathered insights inspired the artifact development process and served as a guideline to avoid some common gaps in current designs. On the other hand, operational contexts of EV battery use—derived from proposed user stories and system-architecture scenarios— were studied to show how the DPP requirements can fit when an EV operates with its intended use. The required DPP data was mapped onto these EV technological capabilities and functions to see where the data originates from or how it is processed. The purpose of this step was to establish the DPP-required functionalities and design constraints for the DPP framework, hence answering the second sub-research question related to evaluation criteria to capture the operational context of IoT-Driven DPPs.

3. Design cycle

From the findings in the Relevance and Rigor cycles, the DPP evaluation framework and its components were constructed as the artifacts. Along with the framework, the process of how to use the framework was also introduced with examples constructed from the literature review earlier. This step helps answer the third sub-research question related to the structure of the evaluation framework. Subsequently, a preliminary interview was conducted with two objectives: (i) to validate the design logic behind the framework (ii) to explore if there are any ambiguities, insights, and modifications needed.

With this exploratory feedback, the framework was consolidated for roll-out for other experts in the next rounds of in-depth interviews. The goal of this interview round was to assess whether the artifact sufficiently addresses the research questions. The focal points of this round were the application of the framework in different expert contexts. Hence, the in-depth interview provides answers to the fourth sub-research question if the framework practically addresses the challenges of IoT-driven DPP.

3.2 Research Methodology

This section describes how the study was structured and conducted, building on the foundation of DSR framework introduced earlier. The research methodology outlines the key phases of the research as well as the data sources used in the process.

3.2.1 Literature Review

An extensive review of academic and technical literature was conducted to build the knowledge base on IoT architectures, reference models, circular economy applications, DPP, and EV operational context. The review was guided by the principles of systematic qualitative research (Boell & Cecez-Kecmanovic, 2015). The regulatory landscape was the main focus, specifically on the EU Battery Regulation 2023/1542 (European Commission, 2023) and related European Commission documents. This ensured that the artifact would align with concrete policy mandates for DPPs in EV battery value chains. This step also examined how these regulatory and architectural efforts were being reflected in active European pilot projects, with notable projects being CIRPASS (European Commission, 2023) and Battery Pass (Battery Pass Consortium, 2023). These projects were analyzed to understand how technical capabilities and DPP were being integrated in real-world contexts, through different scenarios and user stories. Another round of literature review focused on the current IoT architectures and reference models. The analysis aimed to identify key architectural principles that could inspire the artifact design presented in Chapter 4. Insights from this round were used both to identify best practices and to highlight remaining technological and governance gaps. In addition, a gap analysis was conducted to assess how IoT common design pitfalls can be addressed for the specific requirements of DPP.

Together, these combined activities contributed to building the knowledge base of the study and informed both the content and structure of the framework. This phase was essential in ensuring that the framework design would reflect not only academic understanding but also ongoing regulatory trends and industry needs, thereby strengthening both the Rigor and Relevance cycles of the DSR process (Gregor & Hevner, 2013; Hevner et al., 2004; Boell & Cecez-Kecmanovic, 2015).

3.2.2 Framework Design

The initial version of the evaluation framework was developed using the build-and-evaluate logic of the DSR methodology (Hevner et al., 2004). The process began by identifying dynamic data requirements for DPP in EV batteries, primarily from the literature knowledge base for EU Battery Regulation and DIN DKE SPEC 99100. These data attributes were then mapped to the corresponding IoT architecture layers—perception, middleware, and application—to clarify which technical functions correspond to which data points.

For the framework design, literature from established industrial reference architectures was used to provide guidance on lifecycle integration, technical layering, system and stakeholder perspectives. Additionally, limitations of current IoT systems were also highlighted through a gap analysis (Mineraud et al., 2016) as considerations for IoT-based DPP system design. Through CIRPASS initiatives, DPP system architecture and user stories were then used to construct an EV operational context—illustrating how data is generated, processed, and transmitted across lifecycle stages. In addition, stakeholder-specific requirements were systematically embedded in the artifact development process. For instance, OEMs require continuous performance diagnostics and end-of-life tracking to support warranty claims and predictive maintenance; recyclers prioritize dynamic data to determine proper recycling processes, while policymakers focus on lifecycle and regulatory compliance. These perspectives were used to map stakeholder roles to functional system expectations, which in turn guided the definition of the evaluation dimensions in the design phase. From this combined knowledge base, a set of evaluation dimensions was derived. Together, they formed the core criteria, or in other words, the required system functionalities for assessing the DPP readiness of IoT-based architectures.

The framework was structured around two tools: an evaluation matrix to compare architecture profiles and a trade-off table to reveal interdependencies between dimensions. In addition, to test the framework, representative system profiles were drawn from existing academic literature. These profiles, which simulate different IoT-based BMS, were selected based on their relevance, diversity in technical configuration. Due to limited access to proprietary industrial architectures, academic profiles were the only option for testing the framework.

3.2.3 Validation Interview

Semi-structured interview was chosen as the primary data collection method due to its suitability for capturing in-depth, contextualized insights from professionals in a technically complex domain. Given the novelty of DPP regulations and the diversity of implementation practices, interviews allowed for the exploration of tacit knowledge and nuanced perspectives that would not be accessible through surveys or secondary sources (Brinkmann, 2014). Furthermore, conducting these interviews aligns with the relevance cycle of DSR, as they directly engage stakeholders to validate the practical applicability of the artifact in its intended operational environment (Hevner et al., 2004).

For the interview participants, a purposive sampling strategy was employed (Etikan, 2016). This non-probability sampling method is widely used in exploratory and design-oriented research where the goal is to obtain rich, relevant insights from individuals with specialized knowledge rather than a general population (Palinkas et al., 2015). Given the focus on IoT as the enabling technology, it was essential to include participants with strong technical expertise in areas like sensor networks, edge computing, data buffering, latency management, and communication protocols. In addition, experts in EV battery systems, particularly within the automotive industry, were needed to validate the relevance of using IoT for battery-related applications. A third important area of expertise was regulatory knowledge and standardization. Experts familiar with policy—such as the Battery Pass Data Attribute List and CIRPASS architecture—ensured that the framework would be aligned with evolving compliance requirements. Finally, since the framework is ultimately intended for use by EV manufacturers (OEMs), input from solution providers was also incorporated to reflect both the needs of problem owners and the perspectives of those delivering technical solutions.

The process of searching for interviewees involved multiple steps. First, an initial pool of potential participants was assembled through a combination of personal networks, academic referrals, industrial contacts, and targeted outreach via professional platforms such as LinkedIn. Several candidates were suggested through academic channels, particularly from experts already involved in EU-funded projects related to the circular economy, traceability, and battery systems. Others were identified based on their professional involvement in industrial IoT deployment or their advisory roles in regulatory contexts. Participation was confirmed through personal invitations, and care was taken to ensure that the final group represented a balanced mix of perspectives rather than a single stakeholder view. This approach ensures that feedback on the conceptual framework was grounded in practical domain expertise and aligned with current industry efforts and regulatory developments.

3.2.4 Exploratory Interviews

The validation process contains two steps: (i) exploratory interview and (ii) in-depth interview. The main aim of this exploratory round was to test and refine the interview protocol itself and to identify any structural or conceptual issues in the presentation of the evaluation framework. This early feedback loop served as a soft validation stage to uncover unclear terms, overlooked assumptions, or misaligned technical framing before scaling the data collection process. This can be about obvious ambiguities that might be raised during the interview flow but are oblivious to the conducting researcher, or how the framing of evaluation dimensions or architectural logic could be improved. Two exploratory interviews were conducted in this step. Table 1 summarizes the participants' profiles, including their working organization and knowledge domains.

ID	Organization	Knowledge domain
1.1	Mobility Engineering company	Fault diagnostics, System degradation, Event logging system, Diagnostic system manager
1.2	Electrical, Software engineering, Solution company	IoT Physical Device, High accuracy measurement solutions, Data analytics services

Table 1: Overview of exploratory participant profiles

3.2.5 Refining the Interview Protocol

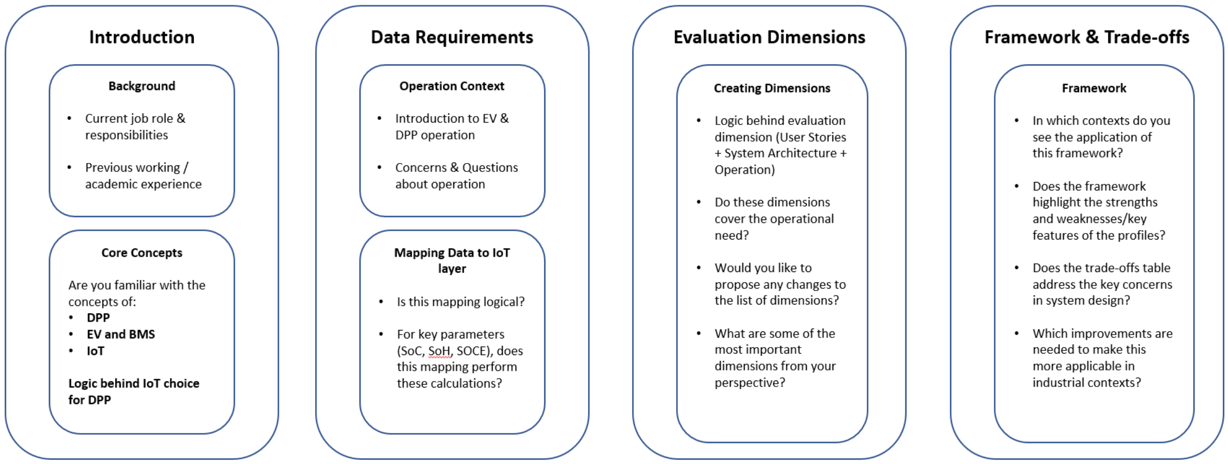


Figure 6: Overview of interview protocol

One key takeaway from the exploratory interviews was the need to clarify several technical terms and definitions. Terms like “Battery Status” or “Temperature Sensing Accuracy” were initially presented with the assumption that their meanings were universally understood. However, experts recommended rewording or expanding these terms to avoid misunderstandings across different stakeholder groups. Another area for improvement was the overall flow of the framework’s explanation. While experts supported the general logic of starting from DPP data points and mapping backward to IoT layers, they noted that some transitions—such as the shift from user stories to system capabilities—needed clearer explanation to avoid confusion, particularly for audiences unfamiliar with DPP implementation. These suggestions were incorporated in the revised materials through improved visuals, clearer section headings, and a more detailed glossary. Figure 6 presents an overview of the interview protocol; a more detailed interview protocol can be found in Appendix C.

3.2.6 In-depth Interviews

Following the exploratory stage, a second round of in-depth expert interviews was conducted to assess the applicability of the framework in various expert contexts. These discussions focused on whether the framework adequately addressed the operational challenges of IoT-driven DPPs, and how well it captures the necessary linkages between IoT components and evolving DPP data requirements. The insights from this phase contributed to the final iteration of the artifact (Gregor & Hevner, 2013). Table 2 provides an overview of the interviewees’ background and domain of knowledge.

ID	Organization	Knowledge domain
2.1	Electrical, Software engineering, Solution company	Advanced IoT and Enterprise Solutions.
2.2	Electrical, Software engineering, Solution company	IoT Hardware Solution, Cloud computing, Digital data collections.
2.3	Electrical, Software engineering, Solution company	Industrial distributed control system and automation project.
2.4	EV OEM	Technical expert on battery safety and battery passports.
2.5	Applied Scientific Research organization	Expert on BMS and SoH data.

2.6	Applied Scientific Research organization	Technical expert in accessing the battery passport via a node data sharing environment.
2.7	Applied Scientific Research organization	Battery researcher, focuses on the optimal use of batteries, battery modelling, estimation, control algorithms, compliance.
2.8	University researcher	Physical layer security, Vehicle-Vehicle communication, Relaying communication.
2.9	University researcher	Battery, Fault Detections, SoH researcher.

Table 2: Overview of in-depth participant profiles

3.2.7 Data Analysis

Hevner et al. (2004) emphasized that rigor in the design cycle should be ensured through appropriate data collection and analysis techniques, and this principle guided the present study. All expert interviews—both exploratory and in-depth—were conducted with consent. Due to privacy concerns, particularly among participants in managerial roles, recordings were not permitted. Instead, interviews were transcribed manually into anonymized summaries to eliminate redundancies, filler expressions, and off-topic content while preserving core insights. The focus of analysis was on conceptual interpretations rather than exact phrasing or non-verbal cues. Interview summaries were stored securely and can be provided upon request. To strengthen research credibility, several qualitative validation strategies were employed. These included triangulation across literature, regulatory documents, and expert interviews, as well as iterative refinement of the interview protocol following the exploratory phase. Although full recordings were unavailable, detailed summaries were used to maintain data integrity and reduce bias. These practices align with established approaches for ensuring trustworthiness in qualitative research (Nowell et al., 2017).

Data analysis was conducted using computer-assisted qualitative data analysis software, specifically ATLAS.ti, to systematically derive patterns and insights from the interview data. Following Corbin and Strauss (1990), the analysis proceeded through several iterative steps. First, all interview summaries were uploaded into ATLAS.ti, and relevant segments were marked using the quotation tool, accompanied by descriptive labels to support retrieval and cross-referencing. Second, open coding was applied to generate initial codes based on emergent insights. Third, the code list was refined by merging overlapping codes and clustering related concepts into broader categories. Finally, the network view tool in ATLAS.ti was used to explore relationships among codes and categories, helping to identify thematic connections and dependencies. The resulting themes reflect key opportunities and challenges in implementing IoT-driven DPP for EV batteries.

4. Evaluation Framework Design

This chapter presents the design process for the evaluation framework, the main artifact of this study. Chapter 4.1 covers the legally required dynamic datapoints, followed by the mapping between data and the responsible IoT layers. Based on this foundation, Chapter 4.2 translates the regulatory and technical requirements into concrete evaluation dimensions. And lastly, Chapter 4.3 presents the core components of the evaluation framework: the evaluation matrix and the trade-offs table.

4.1 Analysis: Data and Requirements for DPP

To begin the framework development, this section identifies the core technical and regulatory requirements for dynamic data in EV battery DPPs. It establishes which data attributes are mandated and how they relate to IoT system functions, forming the foundation for subsequent steps and hence answering the first sub-research question.

4.1.1 Overview of DPP Data Requirements

The development of the evaluation framework begins with identifying the data requirements for the DPP, with a particular emphasis on dynamic operational data relevant to the lifecycle of EV batteries. This step creates a foundation for the framework by establishing what types of information are essential for DPP compliance and where such data resides within the IoT, BMS architecture. This foundation not only informs the technical criteria for system evaluation but also sets the stage for structuring data around functional layers and responsibilities. In the context of EV batteries, dynamic data refers to information that varies over time, capturing operational conditions, environmental stresses, and usage behaviors. Examples include the SoC, charging/discharging cycles, accident records, and overcharge/deep discharge events. These parameters are vital for ensuring traceability, durability assessments, and end-of-life decision-making across multiple actors in the battery value chain, such as manufacturers and recyclers (CIRPASS, 2024a). In contrast, static attributes, such as manufacturer ID, production date, or chemical composition, do not fluctuate and are therefore excluded from the scope of this framework.

Required Attribute	Category	Sub-Category	Mandatory
Temperature information	Performance and durability	Temperature conditions	Mandatory
Remaining capacity	Performance and durability	Capacity, energy, and voltage	Voluntary
Remaining usable battery energy	Performance and durability	Capacity, energy, and voltage	Voluntary
State of Charge (SoC)	Performance and durability	Capacity, energy, and voltage	Mandatory
Number of full charging/discharging cycles	Performance and durability	Battery lifetime	Mandatory
Number of deep discharge events	Performance and durability	Negative events	Voluntary
Number of overcharge events	Performance and durability	Negative events	Voluntary
SOCE (state of certified energy)	Performance and durability	Capacity, energy, and voltage	Mandatory
Remaining power capability	Performance and durability	Power capability	Voluntary
Information on accidents	Performance and durability	Negative events	Mandatory
Battery status	Identifier/product	Product data	Mandatory

Table 3: Summary of required dynamic data attributes (DIN DKE SPEC 99100)

The structure and categorization of dynamic attributes were taken from the DIN DKE SPEC 99100 standard, developed by the Battery Pass consortium. This standard outlines the formal data attribute list for the DPP, including both static and dynamic parameters relevant across the battery lifecycle. It provides detailed guidance on attribute granularity, reporting obligations, and classification of data as either mandatory or voluntary. For example, it specifies whether the data is mandatory or voluntary and outlines the level of granularity—typically at the battery system or module level—at which the information should be captured. The document is particularly relevant to this framework because it offers a reference point for determining which dynamic data attributes are technically and regulatorily significant for DPP compliance. Table 3 outlines the key dynamic attributes required for the DPP in the EV battery case. The Category column groups each attribute by its function, primarily focusing on Performance and Durability for operational metrics, and Identifier/Product for traceability data, as defined in Section 6 of the DIN DKE SPEC 99100. The Sub-Category further refines this grouping into technical clusters such as Temperature Conditions, Negative Events, Capacity, Energy, and Voltage, helping align data points with their measurement context. The Mandatory column indicates whether the attribute is required by regulation; this depends on both battery type and use-case relevance. Mandatory attributes, like SoC and Charging Cycles, are essential for compliance and traceability, while voluntary ones, such as Remaining Capacity, provide added diagnostic value but are not strictly required.

Thermal, Lifecycle, and Safety Considerations

Among the most critical indicators for safety and operational longevity is Temperature Information, mandated as a dynamic attribute under “Temperature Conditions.” Batteries exposed to temperatures beyond their recommended range may undergo thermal degradation, which can severely reduce capacity or cause hazardous failure (Ma et al., 2018). Therefore, temperature extremes—especially time spent in high or low charging conditions—must be recorded and monitored as outlined in Clause 6.7.7 of the DIN DKE SPEC. The regulation emphasizes this important metric by requiring not only temperature range thresholds but also actual exposure durations, particularly during charging. In terms of degradation tracking, the Number of Full Charging/Discharging Cycles is a mandatory dynamic parameter that represents cumulative stress on battery chemistry, directly affecting lifespan. Closely associated are the Number of Deep Discharge Events and Number of Overcharge Events, both of which, although voluntary, serve as event indicators. According to the specification (Clause 6.7.8), such events are pivotal for diagnosing misuse or abnormal wear and are especially valuable for predictive maintenance or second-life qualification assessments.

Battery Performance and Energy Parameters

A cluster of data attributes—SoC, Remaining Capacity, Remaining Usable Battery Energy, and SOCE — provides a real-time view of battery condition, central to performance and durability forecasting. The SoC is a mandatory metric defined as the available energy expressed as a percentage of the rated capacity, adapting to the degradation state of the battery (i.e., usable energy capacity). Similarly, SOCE expresses usable energy as a percentage of the certified usable capacity, providing a normalized view of health particularly relevant to EV applications. These indicators are dynamic, changing during use, and crucial for evaluating range, performance, and residual battery value. Complementary to SoC and SOCE, Remaining Capacity and Remaining Usable Battery Energy offer more granular insights into energy deliverability. Though Remaining Capacity is mandatory for certain battery types (e.g., LMT and stationary battery energy storage system), it is recommended for others and aligns with the EU Battery Regulation’s view of SoH as a multi-parameter indicator.

4.1.2 Classification of Dynamic Data Attributes for DPPs

To translate the identified dynamic data attributes into system requirements, a structured mapping to the IoT architecture layers is essential. This mapping ensures that the DPP framework aligns not only with data collection mandates but also with the technical capabilities of BMS. Accordingly, each data point from the DIN DKE 99100 specification is categorized into one of four principal IoT layers—perception, middleware, network, and application—based on the nature of its origin, processing needs, and intended function within the system. Table 4 illustrates how each data point is mapped to a specific IoT layer and BMS module.

Required Attribute	IoT Layer	BMS Module
Temperature information	Perception	CMU
Remaining capacity	Middleware	MMU
Remaining usable battery energy	Middleware	MMU
State of Charge (SoC)	Middleware	MMU
Number of full charging/discharging cycles	Middleware	MMU
Number of deep discharge events	Middleware	MMU
Number of overcharge events	Middleware	MMU
SOCE (state of certified energy)	Middleware	MMU
Remaining power capability	Middleware	PMU
Information on accidents	Application	PMU
Battery status	Application	None

Table 4: Mapping of Required DPP Data Attributes and IoT Layers

The Perception layer is the physical sensing tier responsible for acquiring raw signals from the environment. According to IoT architecture models, the perception layer is essential for gathering real-time environmental stimuli before higher-level interpretation takes place (Shafique et al., 2020). Therefore, temperature information is situated at this layer because it originates directly from thermal sensors embedded in the Cell Monitoring Unit (CMU). Accurate temperature data is critical for battery safety and performance management, particularly during charging cycles or under extreme conditions.

The Middleware layer serves as the core processing stage within the IoT stack, responsible for aggregating sensor data, executing embedded logic, and generating interpretable metrics. This layer hosts the majority of the dynamic attributes due to their derived or computed nature, often involving multi-sensor inputs and temporal analytics. Attributes such as SoC, Remaining Capacity, Remaining Usable Battery Energy, SOCE, and Remaining Power Capability are all calculated values rather than direct measurements. These are processed primarily by the Module Monitoring Unit (MMU) or the Power Management Unit (PMU) for power-specific indicators. For example, SoC is computed through voltage integration algorithms that account for usage patterns, aging factors, and environmental conditions—activities well-aligned with middleware functionality (Colaković & Hadžialić, 2018). Similarly, event-based indicators such as the number of charging/discharging cycles, deep discharge events, and overcharge events are also aggregated by the MMU over time, emphasizing the middleware layer's role in lifecycle diagnostics. The ability of middleware to support context-aware processing and QoS management makes it the critical intermediary layer in smart battery systems (Uviase & Kotonya, 2018)

At the top of the architecture stack lies the Application layer, which is responsible for interfacing with external systems, regulatory platforms, or user interfaces. Attributes such as Information on Accidents and Battery Status are assigned here due to their high-level reporting function and integration with cloud-based or enterprise-level software. These data points often involve event synthesis or manual classification, rather than automatic derivation from sensor input.

Information on Accidents, for example, is typically logged via the Power Management Unit (PMU) upon detecting anomalies such as impact shock, thermal runaway, or system fault conditions. Once compiled, such records are transmitted through the application layer for DPP traceability, compliance logging, or post-incident diagnostics. Meanwhile, Battery Status—which reflects lifecycle stages such as “in use,” “retired,” or “repurposed”—requires no direct BMS computation and is typically updated through external system logic or manual input, justifying its position outside of specific BMS modules.

4.1.3 Mapping Data Attributes to IoT Layers

Required Attribute	Category	Sub-Category	Mandatory	IoT Layer	BMS Module
Temperature information	Performance and durability	Temperature conditions	Mandatory	Perception	CMU
Remaining capacity	Performance and durability	Capacity, energy, and voltage	Voluntary	Middleware	MMU
Remaining usable battery energy	Performance and durability	Capacity, energy, and voltage	Voluntary	Middleware	MMU
State of Charge (SoC)	Performance and durability	Capacity, energy, and voltage	Mandatory	Middleware	MMU
Number of full charging/discharging cycles	Performance and durability	Battery lifetime	Mandatory	Middleware	MMU
Number of deep discharge events	Performance and durability	Negative events	Voluntary	Middleware	MMU
Number of overcharge events	Performance and durability	Negative events	Voluntary	Middleware	MMU
SOCE (state of certified energy)	Performance and durability	Capacity, energy, and voltage	Mandatory	Middleware	MMU
Remaining power capability	Performance and durability	Power capability	Voluntary	Middleware	PMU
Information on accidents	Performance and durability	Negative events	Mandatory	Application	PMU
Battery status	Identifier/product	Product data	Mandatory	Application	None

Table 5: Full mapping between DPP Dynamic data requirements and corresponding IoT layers

Table 5 presents a consolidated mapping between regulatory data requirements outlined in DIN DKE SPEC 99100 and their corresponding placement within a layered IoT architecture and BMS modules. This mapping acts as a critical intermediary between high-level compliance obligations and practical system implementation. Each row in the table represents a dynamic data attribute relevant to battery performance, durability, or identity, indicating whether the data is mandated or voluntary, and where in the IoT system it is logically handled—from sensing at the perception layer to processing in the middleware, to final reporting at the application layer. This structure provides a transparent mapping for how data flows within a DPP-compatible battery system, enabling analysis of technical capabilities, system readiness, and potential bottlenecks. From this mapping, several insights can be derived as follows:

Attribute Layer Density Insight

A clear pattern emerging from this mapping is that most mandatory DPP attributes are fulfilled through perception- and middleware-layer functions, emphasizing that IoT capabilities are not supplementary but foundational to compliance. This distribution mirrors recent IoT taxonomic research, which identifies middleware as the locus of semantic interoperability, security, safety coordination, and embedded intelligence in complex, multi-device systems (Alkhabbas et al., 2019). Unlike several existing approaches, such as the Global Battery Alliance pilot—which takes a cradle-to-gate[1] perspective with limited operational detail (Global Battery Alliance, 2024)—and the Battery Pass project, which largely aligns with baseline legal requirements (Battery Pass, 2023), the present mapping specifies the direct IoT-layer functions needed to operationalize each data requirement. Similarly, while Berger et al. (2023) provide an information model for DPP data flows, their focus remains on identifying actor-specific data needs, without explicitly connecting them to IoT system architecture. By integrating this regulatory-to-technical mapping, the framework advances beyond current models, offering a more operationally actionable bridge between compliance objectives and engineering design.

Data Ownership

The mapping of DPP-required attributes also reveals a modular structure of responsibility across the BMS hardware. The CMU is assigned to low-level sensor readings (e.g., temperature), while the MMU manages computationally intensive metrics, including SoC and deep discharge events. The PMU oversees attributes that pertain to battery pack-level coordination and incident reporting. Interestingly, some attributes such as battery status are not natively computed by any BMS module but are instead managed via external systems (e.g., cloud platforms), suggesting a multi-stakeholder model for DPP compliance. Flexibility and modularity in battery system design are needed because use conditions may vary (Rothgang et al., 2015). Similarly, the same design principle can also be applied to the IoT choices for DPP implementation.

In summary, the key regulatory data requirements for DPPs in this study focus on dynamic attributes as outlined in the DIN DKE SPEC 99100. These data points were mapped to specific IoT layers and BMS modules based on their origin and processing needs. While specifications such as DIN DKE SPEC 99100 provide comprehensive listings of required attributes, they do not explicitly map these requirements to IoT system layers or functions. This study addresses that omission by offering a structured alignment between regulatory data requirements and the technical architecture needed to fulfil them, thus positioning the framework as meeting both compliance and technical soundness. This answers sub-research question 1 by establishing how these requirements translate into concrete system functions necessary for DPP implementation.

[1] Cradle-to-gate: Environmental assessment from raw material extraction through manufacturing, ending when the product leaves the factory, excluding use and disposal (ISO, 2006).

4.2 Analysis: Evaluation Dimensions

While the previous chapter establishes what data needs to be captured for DPP compliance, this chapter shifts focus toward translating regulatory data requirements into concrete technical evaluation criteria. The goal is to use this set of criteria to assess and compare various IoT architectures on how well they can support the EV battery data lifecycle. This step provides a bridge between regulatory and system levels, and hence answers the second sub-research question.

4.2.1 Reference Architecture for IoT and DPP Use Case

From the literature review, industrial reference works were also included in this section for inspiration to design the framework. Among the most prominent are RAMI 4.0 (Reference Architecture Model for Industrie 4.0) and the Industrial Internet Reference Architecture (IIRA). Each offers a different structuring logic that, while not designed specifically for DPP, contains elements that can be usefully adapted to support their implementation in the EV battery domain.

RAMI 4.0 is structured as a three-dimensional model that maps industrial assets across hierarchical levels (from physical devices to enterprise systems), lifecycle phases (from development to disposal), and IT architecture layers (asset, integration, communication, information, functional, and business) (Schweichhart, 2016). This division aligns well with the granularity necessary for the DPP requirements. Its main purpose is to present a comprehensive model for interoperability, modularization, and standardization among different industrial components and operators (Platform Industrie 4.0., 2018). These objectives are very similar to the use of DPP and the challenges it is facing, but in different contexts. While the RAMI framework focuses specifically on smart manufacturing settings, its emphasis on the data flow across lifecycle stages is crucial and an inspiration for a similar framework related to lifecycle, in this case, the DPP for EV batteries.

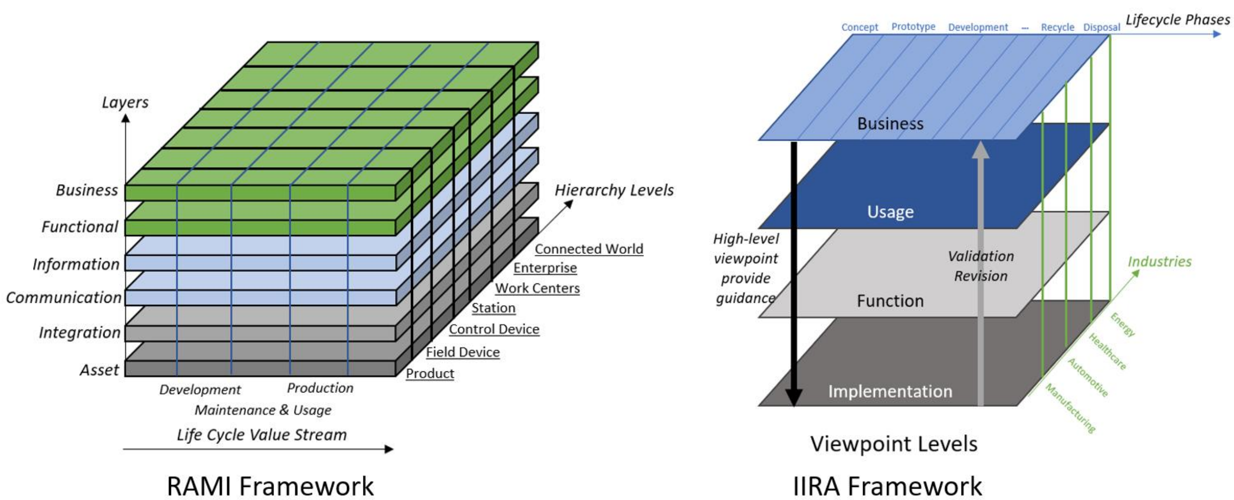


Figure 7: Adopted visual models of the RAMI and IIRA reference frameworks

On the other hand, the IIRA, developed by the Industrial Internet Consortium, offers a more viewpoint-based model, dividing the system into business, usage, functional, and implementation perspectives (Lin et al., 2017). In addition, IIRA is grounded in the ISO/IEC/IEEE 42010 (an international standard for system architecture), making it excel in defining system-wide concerns such as trustworthiness, security, and interoperability (Industrial Internet Consortium, 2022). This feature has made IIRA particularly relevant for understanding cross-stakeholder alignment and architectural patterns in DPP ecosystems. While less lifecycle-focused than RAMI 4.0, IIRA offers valuable guidance for managing complex interactions between technical functions and policy requirements—particularly when designing access control, data privacy, or audit layers in regulated environments like battery passports.

It is important to understand the context in which each of the frameworks performs best. For RAMI 4.0, it provided detailed guidance for manufacturing and production environments through specific standards and industrial practices such as ISA-95 (enterprise and control system standard) and IEC 62890 (lifecycle management standard) (Plattform Industrie 4.0, 2018). In the DPP EV settings, IoT enables real-time monitoring, control, and optimization of assets across the EV's entire lifecycle, from design and commissioning to operation, maintenance, and decommissioning. The goal is to improve efficiency, reduce downtime, and ensure regulatory compliance by creating a digital representation of every physical asset (for EV, it can be battery packs, modules, drive units, telematic systems, etc.). RAMI 4.0 supports this by offering a structured framework that integrates standards like ISA-95 and IEC 62890, providing detailed guidance for mapping functions, data, and lifecycle stages within a manufacturing hierarchy. Its production-specific focus is also one of its main limitations, making it less adaptable to cross-industry applications outside the manufacturing sector. RAMI is best suited for companies operating within the manufacturing and process industries that prioritize compliance with European standards and require a detailed mapping of the product life cycle, asset administration, and hierarchical factory automation (Schweichhart, 2016).

On the other hand, IIRA is well-suited in cases of heterogeneous systems, distributed, and in multiple domains. It is particularly effective for orchestrating complex systems-of-systems and integrating IT and operational technology across diverse sectors (Industrial Internet Consortium, 2022). For example, IIRA has been applied in predictive maintenance scenarios within smart factories, where edge devices attached to machines monitor real-time conditions such as temperature, vibration, or wear. These data are then processed at the platform tier to detect anomalies or forecast failures, while the enterprise tier coordinates maintenance schedules, inventory, and reporting to management systems. In such settings, the four-viewpoint structure helps align the high-level business goals with the technical domains across different stakeholders. In the case of DPP, this is very relevant due to the complex nature of stakeholders in the battery value chain, ranging from central governing bodies, OEMs, consumers, and other second-life processing facilities and supply chain. Nevertheless, its higher level of abstraction can complicate implementation, particularly for any stakeholders that lack mature architectural capabilities. Furthermore, unlike RAMI 4.0, IIRA ‘s limited focus on lifecycle management makes it less applicable for the DPP use case, which is battery-lifecycle-centric.

Adopting either RAMI 4.0 or IIRA alone would provide an incomplete foundation for developing a robust evaluation framework for the potential use of IoT for DPP in EV battery contexts. Each framework has its own preferred contexts and different specific use cases. For example, RAMI application scope is predominantly manufacturing-centric, and it lacks the systemic stakeholder-driven analysis that IIRA provides. On the other hand, while IIRA offers multi-domain interoperability, it is abstract in areas requiring domain-specific modelling—such as the detailed sensor-level data handling and lifecycle mapping crucial for DPP compliance. Therefore, relying exclusively on IIRA might leave gaps in operationalizing specific DPP technical requirements, such as the edge-layer capture of thermal faults or structured logging of lifecycle events. A hybrid approach leverages the layered rigor of RAMI to manage sensor granularity, middleware processing, and asset lifecycle stages, while IIRA contributes the high-level scope needed to incorporate policy compliance, system-of-systems orchestration, and data governance. In effect, combining both frameworks enables a more holistic and technically grounded evaluation of IoT-BMS architectures in line with the evolving standards of the Battery Pass consortium and the functional expectations of the broader EV ecosystem.

4.2.2 Suitability for DPP

Since no framework is suitable for the needs of DPP in EV industry, several components of both RAMI and IIRA are combined and adapted to better suit DPP context. From RAMI 4.0, the "Administration Shell" concept can be incorporated. This shell is defined as a "digital interface or envelope" that encapsulates all digital information and services related to an asset (e.g., a machine, sensor, software module, or product component) (Plattform Industrie 4.0., 2018). The Administration Shell is not simply a monolithic file, component, or database. It is a structured, modular information model that represents several critical functions within an IoT system, such as Digital Identity, Standardized Interoperability, Data Integration, and Lifecycle Monitoring. This aligns with DPP's need to maintain traceable, machine-readable records of battery data across lifecycle events. RAMI's layered stack—from physical assets through communication to information and business layers—can also be used to validate and structure the IoT architecture profiles under evaluation. These architecture profiles can represent full-scale solutions, with variations in devices, functionalities, and architecture that OEMs can consider as options for their own selection.

Meanwhile, from IIRA, the "Functional Viewpoint" fits in well with the setting of DPP in the EV situation. The function viewpoint focuses on defining what the system must do in terms of functionality, answering realistic and operational questions (e.g.: What are the key functions the system must perform? How do these functions relate to each other? Where in the architecture do these functions live?). These questions help technical decision-makers clarify the system roles, avoiding mixing different levels of tasks together. In addition, the functional viewpoint can create a direct link between the required data and the technical function responsible for generating or managing it. This is the most important factor, as the Battery Pass only published the data requirements but did not specify which technical layers would be affected. Without such a mapping, it remains unclear where—within the system architecture—specific data must be captured, processed, or stored, making implementation ambiguous for developers and system integrators. More importantly, how certain changes in design, functions can affect the overall system. The functional viewpoint helps bridge this gap by aligning high-level regulatory or business requirements with concrete architectural components (e.g., edge devices, gateways, cloud services) that are responsible for data generation, transformation, and transmission. In different cases of industries or product lines, this functional viewpoint can help stakeholders map unique requirements with system capabilities. Additionally, IIRA's inclusion of edge-cloud continuum architectures (namely the three-tier pattern) offers reusable models for hybrid processing and coordination, reducing the computing load on central processing. This architectural model structures processing across three layers: edge, platform, and enterprise for distributed data handling and decision-making. Its importance lies in addressing one of the most pressing challenges in IoT today: the computational limitations of edge devices. As sensors and embedded systems become more widespread, especially in resource-constrained environments like electric vehicles or industrial machinery, offloading heavy processing tasks to intermediary or cloud layers becomes essential. The integration of these elements ensures that both the vertical traceability and horizontal integration requirements of the DPP are comprehensively addressed (Industrial Internet Consortium, 2022; Plattform Industrie 4.0, 2018).

From an IoT perspective, the addition of the gap analysis conducted by Mineraud et al. (2016) provides the real-world shortcomings of different IoT platforms as a stark reminder and consideration for any IoT framework design. This analysis offers a foundational overview of the strengths and limitations of existing IoT platforms, evaluating their capacity to meet the needs of diverse stakeholders across technical, functional, and business dimensions. By systematically assessing key features such as device heterogeneity, data ownership, processing capabilities, developer support, and marketplace integration, the study reveals critical shortcomings that hinder the scalability and interoperability of IoT solutions. This analysis is particularly important for the development of an IoT evaluation framework, as it highlights the criteria necessary for robust platform assessment and underlines the importance of aligning IoT architectures with evolving demands in areas like traceability, user control, and cross-sector collaboration—key requirements for applications such as DPP.

Area	Gap Identified from the paper	Why It Matters for DPP	Suggested resolution
1. Semantic Interoperability	Lack of uniform data models and semantic indexing	DPP requires structured, interoperable data (e.g., JSON-LD) across lifecycle stages and systems	Middleware/application layer supports RDF/JSON-LD;
2. Edge Processing and Buffering	Cloud-only analytics dominate; edge storage missing	DPP data (e.g., SoC logs, accidents) must persist during connectivity loss and enable local pre-processing	The middleware layer supports offline event queues, edge analytics, and sync retry logic
3. Data Ownership & Access Control	Access policies are too simple; lack of local storage or encryption	Lifecycle data needs privacy control; OEMs or users must define visibility rights (e.g., accidents, charging)	Application layer enforces role-based access; supports local pre-encryption
4. Heterogeneous Device Integration	Platforms require proprietary gateways; limited protocol support	EV systems combine CMUs, MMUs, PMUs from multiple vendors; interoperability is critical	Perception layer uses open protocols (e.g., CoAP, MQTT); profiles tested for multi-vendor compatibility
5. Lifecycle Awareness & Adaptability	Platforms are not designed to adapt to lifecycle state changes	DPP requires tracking and updating data across stages (e.g., 2^{nd}-life use, end-of-life recycling)	Functional layer supports dynamic configuration updates and lifecycle-triggered policy changes

Table 6: IoT platform and function gap analysis, adopted from Mineraud et al. (2016)

The gaps identified in Table 6—ranging from poor semantic interoperability, edge processing to insufficient data ownership mechanisms and limited adaptability—highlight systemic weaknesses in current IoT platform implementations that neither RAMI nor IIRA fully address on their own. This gap analysis validates RAMI's need for standardized semantic data layers (e.g., RDF Resource Description Framework or JSON-LD), Administration Shells, and interoperability. For the IIRA framework, it confirms the emphasis on distributed edge/cloud coordination and functional and business-driven data governance.

Although neither framework addresses nor is designed for DPP-specific needs, a combination of RAMI 4.0's asset-lifecycle mapping with IIRA's functional viewpoints offers a complementary perspective, balancing between the technical capabilities and functional needs of different stakeholders. In addition, the CIRPASS project and the gap analysis by Mineraud et al. (2016) serve as a reminder and checklist for identifying any shortcomings in IoT and ensuring that proposed solutions address the operational and regulatory demands of DPP implementation.

4.2.3 From Data Requirements to Evaluation Dimensions

Identifying the required data attributes is not sufficient for selecting the right capabilities of an IoT-enabled system. Regulatory frameworks, such as the Battery Pass initiative, list key attributes for DPPs, but they do not specify how these attributes should be technically implemented or maintained over time. For example, the DIN DKE SPEC 99100 standard specifies that “Temperature information” must be periodically collected with a Celsius measuring unit. However, this standard does not indicate the required fidelity of data, along with the intervals at which the data should be collected. Similarly, for other attributes such as SoC or SOCE, only general recommendations on the measuring units and common international standards to follow were given. This creates a gap between the data requirements and the system technical specifications to be able to capture the data. In other words, this gap is about whether the system architecture is capable of recording these events in real time and during the EV operation (Battery Pass, 2025). Furthermore, DPP compliance involves more than just capturing data—it also demands mechanisms to ensure accuracy, data integrity, interoperability, and availability. Therefore, a more abstracted and structured set of evaluation categories was needed to assess whether different IoT architectures can realistically support these dynamic and multi-faceted requirements over the product’s life cycle.

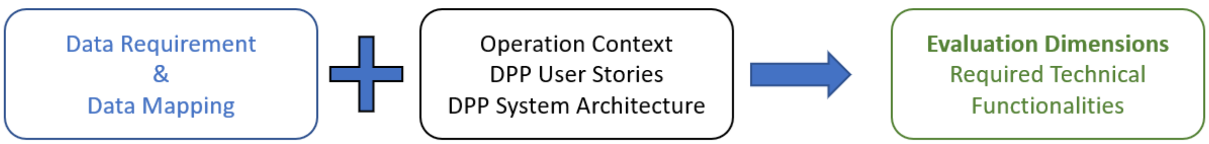


Figure 8: Logic behind the evaluation dimensions

To address this gap, this step introduces the concept of evaluation dimensions—technical capabilities abstracted from the specific data attributes but directly traceable to them, as illustrated in Figure 8. Inspired by the IoT function taxonomy from Dorsemaine et al. (2015), as well as reference frameworks like RAMI 4.0 and IIRA, the evaluation dimensions offer a way to bridge regulatory data points with layered system functions and lifecycle interactions (Schweichhart, 2016; Lin et al., 2017). RAMI 4.0’s lifecycle-layer mapping and IIRA’s multi-viewpoint structuring are particularly influential in defining how sensor-level attributes and stakeholder policies align across perception, network, and application layers.

4.2.4 Justification for the Grouping Method

This framework introduces a series of evaluation dimensions—functional groupings that capture both the nature of the required data and the operational capabilities needed to support it. These dimensions were designed to assess whether a given IoT-BMS architecture can collect, process, store, and transmit the required data with sufficient quality, fidelity, and integrity. The grouping of data attributes into distinct dimensions was based on shared computational, architectural, and regulatory characteristics, such as those described in CIRPASS user stories, DPP reference architecture, and EV operation context as described in Figure 9 (Abdalla, 2024; van Nieuwenhuijze et al., 2025). While data attributes like SoC, temperature logs, or event counts were identified in legislation and standards, these attributes must be connected to a certain technical function responsible for processing such metrics. In this way, the data requirements, along with the EV operation context, were translated into technical functions to inform meaningful decision-making and evaluation in selecting the right IoT architectures. In addition, this grouping provides a layer of abstraction that links heterogeneous data to shared architectural demands, modularity, and traceability across implementation contexts. The grouping was conducted as follows:

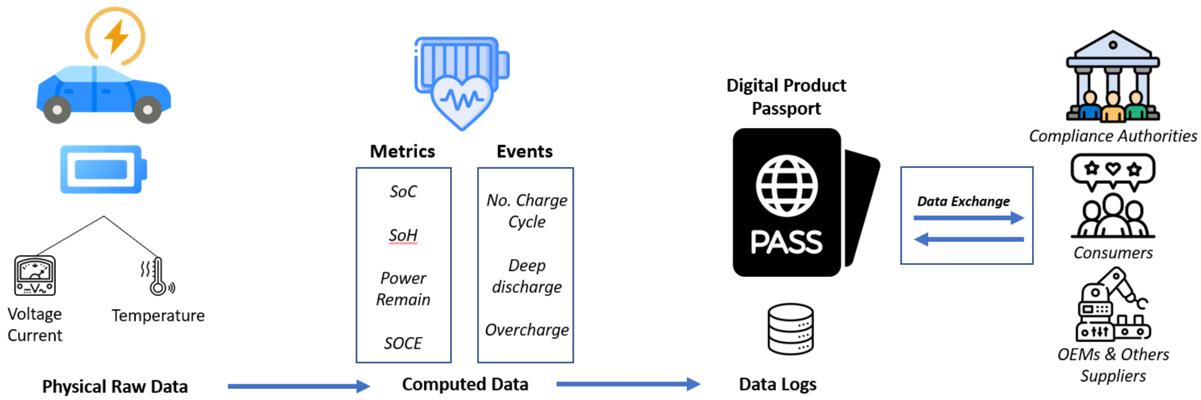


Figure 9: DPP in EV operation context

Voltage and Temperature Sensing Accuracy

This dimension captures a fundamental capability of any IoT-BMS system: the ability to perform reliable, physical measurements, such as voltage, current, and temperature metrics. In the required attributes list, only the "Temperature information" is directly taken from physical measurements. Most of the other metrics are byproducts of these physical measurements and need higher calculation logic based on the raw physical data. Therefore, this evaluation dimension grouped together attributes such as:

- *Temperature information*
- *Remaining capacity*
- *Remaining usable battery energy*
- *Number of full charging/discharging cycles,*
- *Number of deep discharges*
- *Number of overcharges*
- *State of Charge (SoC)*
- *State of Certified Energy (SOCE)*
- *Remaining power capability*.

All of these rely on analog sensing, digital conversion, and signal conditioning to derive accurate values. These attributes are collected primarily at the Perception Layer, using the CMU and voltage/temperature sensors embedded in the battery management system. They are then processed within the Middleware Layer, where SoC and capacity are inferred through algorithms (van Nieuwenhuijze et al., 2025). This grouping reflects that high-fidelity sensing is a prerequisite for many downstream computations and event detections. In the user story "Writing to DPP", the technician's update depends entirely on correct readings captured during inspection, demonstrating how sensing accuracy impacts data integrity at multiple lifecycle stages (Abdalla, 2024).

Real-Time Event Detection

Attributes like the number of full charging/discharging cycles, overcharge events, and deep discharge incidents are grouped under this dimension, as they rely on the system's ability to process data patterns in real time. These attributes are not merely measurements but inferred events, often defined by thresholds or time-series anomalies. Processing these requires embedded logic in the Middleware Layer, often located in MMU or PMU. The grouping is based on their common dependence on edge-level computing for timely event classification. This design is evident in the DPP system architecture, where real-time analytics modules must flag deviations and trigger appropriate notifications or logs (van Nieuwenhuijze et al., 2025). This dimension is also related to the EV operational safety, as many key events must be flagged and analyzed within a specific timeframe for the vehicle control unit to act accordingly, preventing any hazards and keeping the user safe.

Edge Storage Buffering

The third dimension includes all attributes that require robust local data retention during periods of limited or no internet connectivity. This covers nearly all operational data—such as charge/discharge cycles, SoC logs, and event timestamps—since these need to be preserved and synchronized later with central registries or DPP endpoints. The shared architectural requirement here is a local buffering mechanism within the Middleware Layer, which retains data using memory storage. CIRPASS reference architecture recommends the inclusion of local data queues and buffers to support asynchronous uploads (van Nieuwenhuijze et al., 2025). The rationale for this dimension is strongly reflected in the document includes repair user stories describing how repairers write repair actions into the DPP—both with the REO's authorization and independently. The grouping ensures that any architecture lacking this edge storage capability will be clearly identified as non-compliant for environments with intermittent connectivity.

Latency to Cloud

Some DPP data attributes—especially those relevant for enforcement—must be transmitted to central registries or cloud endpoints with minimal delay. The "Latency to Cloud" dimension groups such attributes, including SoC, SOCE, and recent event logs. While this may not be mandatory in all DPP scenarios, use cases such as customs inspections or accident responses depend on low-latency, high-availability transmission. These operations span from the Middleware to the Network Layer. In the section on customs authorities, officials use the EU registry/DPP to verify the product identifiers and declaration information for release into free circulation. A network delay could jeopardize clearance or flag false alarms, highlighting the operational importance of this dimension (Abdalla, 2024).

Data Format Compatibility

This dimension addresses the need for semantic and interoperability across sectors and systems. Attributes such as temperature data, accident information, battery status, and usage cycles must be encoded in formats that external platforms can consume, typically using JSON-LD, or RDF-based structures. This functional requirement spans from the Middleware to Application Layers, and involves schema validation, metadata tagging, and format conversion modules. CIRPASS proposes the use of composable DPP templates and pre-defined ontologies to maintain consistency across heterogeneous datasets (van Nieuwenhuijze et al., 2025). For example, in the user story on NGO access to DPP data (Abdalla et al., 2024), third parties analyze product information for circularity, sustainability, and compliance purposes. In such cases, providing the data in a structured format such as JSON is important because it enables automated processing, integration with analytical tools, and consistent interpretation across diverse datasets, thereby improving the reliability and scalability of circularity assessments. The grouping here reflects a common compliance burden: any attribute that must be exchanged externally must be structured to known standards. Table 7 summarizes the key evaluation dimensions to fulfil the DPP operational requirements. More details on the grouping logic and user stories used to create these dimensions can be found in Appendix D.

Evaluation Dimension	Affected Data Requirements	IoT Layers
1. Voltage/Temperature Sensing Accuracy	- Temperature Information	Perception
	- SoC, - Remaining capacity, Remaining usable energy, Power capability - No. of full charge/discharge cycle, - No. Deep discharge, - No. Overcharge, - SOCE, - Remaining Power Capability	Middleware
2. Real-Time Event Detection (Event & Data Computing)	Only processed data points in the Middleware layers: - No. of deep discharge events /overcharge events/ charging & discharging cycles - SoH, SoC - Remaining Capacity / Usable energy / Power capability	Middleware
3. Edge Storage (for saving data logs)	All required data points	Middleware
4. Latency to Cloud (for digital data transfer)	All required data points	Network
5. Data Format Compatibility (for interoperability)	All required data points	Middleware Application

Table 7: Summary of Evaluation Dimensions and affected attributes

In addition, the following dimensions were also included in the analysis to form a full operational picture of DPP. However, to prevent overcomplexity for the framework in the initial state, these dimensions were considered to be optional and would be validated later with expert interviews about their importance.

Secure Message Authentication

This dimension assesses whether data transactions—especially DPP updates—can be cryptographically authenticated. This is critical for EV systems, where updates to lifecycle data (e.g., after battery servicing, or replacement) must be validated to prevent tampering or fraud. Attributes affected include any that are mutable (e.g., accident logs, diagnostics, SoC status) and are frequently updated during EV operation or maintenance. Therefore, this requires a digital signature or token-based verification mechanism at the Application Layer. CIRPASS proposes using authentication mechanisms via HTTP (Hypertext Transfer Protocol) headers and digital seals during update interactions, particularly from Responsible Economic Operators (REOs) and service providers (van Nieuwenhuijze et al., 2025). This dimension is directly supported by user stories where data is written to the DPP during post-market service or reuse by third parties (Abdalla, 2024). For example, in the story "Writing into the DPP with the original REO's authorization," secure authentication is required to validate the write permission. The grouping of attributes here reflects their common vulnerability to falsification and need for data origin traceability—especially when product safety and legal responsibility are at stake.

Lifecycle Update

The DPP system must support updatable and resolvable identifiers to reflect the evolving state of the product over its lifecycle. This includes attributes such as ownership status, condition post-refurbishment, or geographic deployment. In the EV context, such updates are frequent, especially for battery reuse, leasing, or after-market modifications. The dimension groups all attributes that are subject to change after the initial issuance of the DPP and must be reflected via updates. According to the CIRPASS system architecture, this is handled via lifecycle endpoints that support redirection and mutability (Jousse, 2024; van Nieuwenhuijze et al., 2025). Data platforms must allow authenticated updates and maintain a history of versioned snapshots. This capability is illustrated in the user story “Transferring the responsibility for a product,” where EV battery modules are handed over to a second-use facility. The ability to update metadata dynamically ensures that DPP remains a live representation of the product’s current status.

Stakeholder-Specific Access Controls

The DPP system must regulate who can read or write what data, depending on their role, such as manufacturers, recyclers, consumers, customs officials, or service centers. Attributes affected include sensitive or competitive data (e.g., SoC algorithms, precise thermal history), as well as public-facing attributes like recycling instructions. As described in multiple CIRPASS user stories, especially “Reading with default or restricted access,” where the public and authorised actors have different views of the DPP (Abdalla, 2024). Technically, the architecture recommends the implementation of Access Control Lists and Decentralised Identifiers to grant or restrict access dynamically. The access rules are enforced at the Application Layer, informed by the stakeholder’s role and authorization token. In practice, architectures that lack this capability cannot be deployed across multi-stakeholder value chains without risking data leakage or non-compliance.

In summary, the evaluation dimensions defined in this framework directly address the current gaps in the IoT platform, as summarized in the gap analysis Table 6, adopted from the work of Mineraud et al. (2016). The Data Format Compatibility dimension specifically responds to the gap in Semantic Interoperability by requiring platforms to adopt structured, interoperable formats (such as RDF/JSON-LD). This dimension will become necessary when DPP data are exchanged across systems and lifecycle stages. The Edge Storage Buffering dimension targets the Edge Processing and Buffering gap, enabling local storage of key dynamic data (e.g., SoC, fault events), and ensuring that data persists during connectivity loss — a critical requirement for DPP traceability. The Data Ownership & Access Control gap is addressed through the Stakeholder-Specific Access Controls dimension on the application layer. Finally, the Lifecycle Awareness & Adaptability gap is supported by the Lifecycle Update, which ensures dynamic system updates throughout the product lifecycle (Mineraud et al., 2016). In this way, the evaluation dimensions were created not only with the DPP requirements in mind but also with the common pitfalls of other IoT platforms. Hence, answering the sub-research question 2 on the evaluation criteria for IoT in DPP implementation.

4.3 Evaluation Framework: Evaluation Matrix & Trade-off Table

This chapter answers the third sub-research question by outlining the main content of the evaluation framework, built upon the work of previous chapters. In this framework, the evaluation matrix is introduced, along with the trade-offs table as a parallel component. The structure of the framework is explained accordingly. In addition, the chapter also provides examples of the framework application to showcase its usage and the main content to be used for expert validation later.

4.3.1 Structure of the Framework

The purpose of this evaluation framework is to offer a structured method for assessing the DPP-readiness of different IoT functionalities in the EV domain. Building upon the evaluation dimensions introduced in the previous chapter, this framework utilizes those dimensions into a comparative matrix that helps decision-makers and experts to benchmark their options and architectural profiles. Its central aim is to translate the abstract, compliance-driven requirements of DPP into a tangible decision-support tool that can guide architectural selections and system design decisions. Despite the ambitious scope of the DPP concept, particularly in the battery domain, stakeholders still face substantial fragmentation in system design practices, regulatory interpretations, and architectural choices (Berger et al., 2023). This heterogeneity results largely from the absence of an industry-wide architectural guideline that can balance technical performance, regulatory obligations, and cross-stakeholder interoperability (CIRPASS, 2024a; CIRPASS, 2024b).

Evaluation Dimension	**IoT Layer**	**Profile 1:**	**Profile 2:**	**Profile 3:**	**Profile 4:**
Voltage / Temperature Sensing Accuracy	Perception, Middleware				
Real-Time Event Detection	Middleware				
Edge Storage	Middleware				
Latency to Cloud	Network				
Data Format Compatibility	Perception Middleware, Application				

Table 8: Evaluation Matrix

Table 8 illustrates the structure of the evaluation matrix. The matrix here seeks to mitigate these issues by defining evaluation dimensions that are both technically grounded and context specific. These dimensions—such as voltage/temperature sensing accuracy, real-time event detection, offline buffering, cloud latency, and data format compatibility—are not arbitrary metrics. Instead, they arise from the operational demands recorded in CIRPASS user stories and reference architecture documents. The framework maps these evaluation dimensions to different IoT architectural layers to enable a granular comparison of candidate BMS configurations. Each dimension is grounded in DPP-specific data attribute requirements. This structured evaluation becomes particularly relevant in light of the documented lack of interoperability, semantic alignment, and cohesive guidance in existing DPP-system implementations. As noted in the CIRPASS standardization roadmap, many components—such as API specifications or lifecycle event logging—remain under-defined, leaving individual actors to create divergent and often incompatible solutions (CIRPASS, 2024b; CIRPASS, 2024c). The framework aims to serve as a reference mechanism that not only addresses this fragmentation but also enhances cross-sector dialogue in shared performance expectations. For instance, recyclers and second-life operators require historical battery performance data and fault logs, while OEMs prioritize real-time status updates and secure identity links for compliance and warranty validation (CIRPASS, 2024a). The framework's main strength lies in its ability to translate these stakeholder needs into actionable evaluation points across IoT layers and compare the options at hand directly.

4.3.2 Trade-off Analysis

Trade-off analysis is a critical factor often overlooked in early-stage architecture planning, leading to blind spots in system design before prototypes or pilot deployments begin (Orellana et al., 2024). Literature on DPP implementation often addresses individual technical functions in isolation, without systematically exploring the interactions between them. The inclusion of an explicit trade-off table in this framework addresses this shortcoming by illustrating how enhancing one capability can directly influence other parameters. Given that IoT-based BMS are highly complex and dynamic environments, architectural decisions taken in one area—such as improving sensor accuracy—inevitably impose constraints or performance impacts in others (Mulpuri et al., 2025; Su et al., 2014). Industrial and academic literature repeatedly emphasizes this coupling (Su et al., 2014; Industrial Internet Consortium [IIC], 2022). For example, enhancing sensing accuracy increases data volume, which raises communication latency and requires greater buffering capacity at the edge. This relationship is well documented in the IIRA framework, which warns that "optimizing isolated functions rarely leads to optimal system-wide outcomes" (IIC, 2022). By surfacing these dependencies, the trade-offs table helps designers predict and quantify these cascade effects. An analysis was conducted to build the trade-off table.

Voltage/Temperature Sensing Accuracy defines the fidelity and resolution with which systems capture raw physical measurements from EV battery cells. Accurate voltage and temperature readings are foundational for reliable calculation of SoC, SoH, and detection of anomalies such as overcharging or thermal runaway (Madani et al., 2023; Hannan et al., 2017). Higher sensing accuracy improves real-time event detection reliability by reducing false positives/negatives in threshold-based alarms (Erhan et al., 2021). However, it also increases cumulative data volumes for edge buffering, particularly during offline operation (Kreković et al., 2025). This increase in data traffic elevates demands on transmission latency (Fadzil Hassan et al., 2023), edge processing, and storage buffers (Hannan et al., 2017). Moreover, integrating high-fidelity sensing with semantic data models (e.g., RDF/JSON-LD) further increases payload size and latency (Jara et al., 2014). Finally, richer sensor data often motivates the adoption of structured formats to support interoperability across DPP stakeholders (Jara et al., 2014).

Real-time Event Detection refers to the system's ability to process raw data, identify, and respond to significant event metrics—such as overcharging, deep discharges, or thermal excursions—within a short, bounded time window (Madani et al., 2023; Krishna et al., 2024). These detections depend on near-continuous monitoring of voltage, current, and temperature, combined with localized processing or threshold logic to flag abnormal behavior before it leads to system degradation or safety risk (Hannan et al., 2017). In the context of DPP, such events must also be timestamped and stored in a tamper-proof, traceable format for future audits and regulatory compliance. This dimension relies heavily on the fidelity and frequency of voltage and temperature sensing. High-resolution and frequency measurements increase detection granularity and reduce false positives, but they also raise raw data volume, affecting both edge buffering capacity and cloud latency (Madani et al., 2023; Su et al., 2014). Additionally, the structure of the data format plays a role: the use of semantic models such as RDF or JSON-LD can introduce serialization overhead, delaying the transmission or processing of event logs (Jara et al., 2014). Network constraints can further delay the transmission of alerts, particularly in systems that lack local edge response capabilities (Orellana et al., 2024).

Edge Storage Buffering is directly impacted by both real-time event detection and sensing accuracy. Higher sensor fidelity and faster sampling produce more granular data, increasing storage volume per unit time (Madani et al., 2023). Similarly, frequent event detection generates bursts of log entries that must be stored until transmission is feasible (Krishna et al., 2024). Moreover, data format compatibility can further amplify storage requirements: semantic formats such as RDF/JSON-LD often increase the size of each buffered entry compared to flat schemas (Jara et al., 2014). As a result, storage needs can scale non-linearly with function upgrades in sensing, detection, or formatting. Insufficient edge storage may cause data loss during periods of cloud unavailability, undermining real-time detection integrity and DPP traceability. For example, if a thermal event occurs during a temporary disconnection and cannot be buffered, the incident will not be logged into the DPP, jeopardizing compliance. Conversely, well-structured buffering systems can offload the pressure from low-latency network design, allowing temporary disconnection without system failure (Su et al., 2014). For DPP integration, buffering is not only compulsory but also a compliance mechanism. Lifecycle traceability mandates that no critical operational data be lost, even temporarily. However, provisioning sufficient memory for edge storage is challenging due to hardware constraints, especially in compact or cost-sensitive systems (Krishna et al., 2024).

Latency to Cloud refers to the system's connectivity and ability to transmit data to designated cloud servers. In the context of DPP compliance, cloud latency is critical because it affects the system's responsiveness to operational anomalies, timeliness of reporting, and availability of verifiable lifecycle records (Krishna et al., 2024). Cloud latency is impacted by the volume and frequency of sensed and detected events. High-frequency sensing or real-time detection can flood the network with data packets, increasing transmission. Moreover, edge storage buffering behavior affects latency indirectly: systems with large buffer backlogs may introduce batching or retry delays during synchronization. The data format also plays a key role: semantically enriched formats like JSON-LD increase payload size and serialization complexity, both of which extend transmission time and processing load (Jara et al., 2014; Su et al., 2014). DPP systems often rely on cloud-hosted registries for certification, compliance monitoring, and data integrity. However, reducing latency typically requires enhanced network protocols, or increased bandwidth—each of which adds system complexity or cost (Krishna et al., 2024; Su et al., 2014).

Data Format Compatibility refers to the system's ability to structure, encode, and exchange data in standardized formats across heterogeneous platforms. In the DPP context, this means supporting structured, semantic formats (e.g., JSON, JSON-LD, RDF) that allow for consistent interpretation by OEMs, recyclers, auditors, and regulators (Jara et al., 2014; GS1 Europe, 2024). Format compatibility is essential for interoperability, long-term archival, and integration with external systems such as EU regulatory databases. Semantic data formats are inherently more complex. As a result, they increase data volume, impacting latency to cloud, storage buffering, and even event reporting speed (Su et al., 2014). Parsing and serializing semantic data (e.g., converting internal sensor logs into RDF triplets or JSON-LD schema) requires processing overhead, which can strain low-power or memory-constrained devices. The choice of data format can influence how events are logged and interpreted, affecting the accuracy of lifecycle traceability. More structured formats allow richer descriptions of events (e.g., linking causes to effects, applying ontologies), which enhances DPP compliance but slows down transmission and buffering (Krishna et al., 2024). To comply with DPP standards, architectures must support machine-readable formats that are consistent, secure, and forward-compatible. Designers must decide whether to structure data at the edge, gateway, or cloud, balancing fidelity with feasibility and lifecycle cost.

Table 9 presents the trade-off relationships between the evaluation dimensions identified in the framework. The table adopts a lower-triangular structure, where only the cells below the diagonal are populated, ensuring the reader's focus is on unique trade-off without unnecessary repetition. This design avoids redundancy, as trade-offs are bidirectional—if "Dimension A" affects "Dimension B" in one way, the reverse interaction is already implied.

Evaluation Dimension Trade-offs	Voltage/Temperature Sensing Accuracy	Real-Time Event Detection	Edge Storage Buffering	Latency to Cloud	Data Format Compatibility
Voltage/Temperature Sensing Accuracy					
Real-Time Event Detection	Direct input: higher accuracy improves detection reliability, also requires more computing power				
Edge Storage Buffering	More events logged = more storage required	Frequent detection events increase buffer demand and storage stress			
Latency to Cloud	Higher sensor fidelity may increase data size, slightly impacting latency	Slow network could delay event reporting	Prolonged disconnection increases buffering needs		
Data Format Compatibility	More precise data may require a more structured semantic representation	Formatting may delay event logging or require buffering	Semantic formats increase buffer size and edge processing needs	Delay may affect structured data sync time	

Table 9: Trade-off table for the framework evaluation dimensions

Overall, the integration of the evaluation matrix and trade-off table provides a structured bridge between regulatory requirements, system architecture, and operational feasibility. Unlike many previous models that present these aspects in isolation, this framework captures the interdependencies between dimensions and evaluates their maturity within different implementation profiles. This approach enables stakeholders to identify potential conflicts, synergies, and prioritization pathways according to their specific objectives and operational contexts.

4.3.3 Candidate IoT Architecture Profiles

As introduced in Chapter 2.3, four academic IoT-based BMS architectures were selected to serve as candidate profiles for evaluating the applicability of the proposed framework. The selected academic profiles were systematically scanned and analyzed to identify content related to the DPP evaluation dimensions defined in this framework. Particular attention was given to any explicit or implicit references to dimensions such as sensing accuracy, real-time event detection, edge storage, latency, and data format compatibility. Relevant technical details were extracted and filled into the evaluation matrix for that profile. For some profiles, due to the context and different focus of the original study, some information related to the DPP dimensions was absent. Therefore, some inferences were made based on the described system characteristics (e.g., sensor placement, network protocol, data handling methods). Table 10 summarizes how these profiles fit into the evaluation matrix as an application example.

4.3.4 Application of the Framework

Evaluation Dimension	**IoT Layer**	**Profile 1: Centralized Low-cost BMS**	**Profile 2: Decentralized wireless BMS**	**Profile 3: Centralized Wireless BMS with TSCH-Based Slot scheduling**	**Profile 4: Distributed BMS with Hierarchical Cloud Integration**
Voltage / Temperature Sensing Accuracy	Perception, Middleware	No mention of temp sensor. Use of 10-bit A/D converter, 0.125 µs conversion for voltage data	1s sampling; voltage, temp, SOC per module;	500 ms sampling rate; safety window (2.5–4.2 V, −13–60°C);	BMP180 temp sensor with BATT-14CEMULATOR as high precision battery emulator
Real-Time Event Detection	Middleware	Yes: detects deep discharge via GSM email	Yes: periodic SoC / SoH updates via MQTT	Yes: slot frame-aware scheduling to maintain QoS and prevent event loss	Yes: voltage, current, temp, pressure + SoC/SoH/DoD; sampling ~100ms–1s
Edge Storage Buffering	Middleware	No persistent storage, cloud sync only	Partial buffering in node memory	Modules act independently; allow local data use and reuse; support second-life use	Secure embedded logging (SEL). Hierarchical block storage; supports offline buffering
Latency to Cloud	Network	1-minute rate update through GSM/GPRS	Leader election: avg. 5.19 s; data aggregation: avg. 1.17 s; cloud latency not explicitly stated	Designed for 500 ms delivery to root; no explicit cloud latency given	Sensor read ~27 ms; full BMS-cloud ~19.54 s; REST transfer
Data Format Compatibility	Perception Middleware, Application	No explicit structured data format. Only web UI and email	Google Sheets API — no RDF/JSON or standard format	Not mentioned. Raw small data payloads (voltage/temp); format not specified	Proprietary structured log blocks (SNDEF-based); DPP-aligned, not RDF/JSON-LD

Table 10: Evaluation Matrix with architecture profiles

Profile 1 and 2

In the case of profiles 1 and 2, the evaluation matrix reveals several key differences in system capabilities and DPP readiness. Profile 1, with centralized BMS topology, features basic voltage sensors with cloud dashboard and email alerts via GSM (Global System for Mobile Communications)/GPRS (General Packet Radio Service) (SIM808) communication, built on Arduino-based architecture (Wahab et al., 2018). It targets a cost-effective and practical solution with a simpler architecture. However, it may be limited in scalability and depth of diagnostics, particularly when compared to more advanced decentralized systems. On the contrary, Profile 2 by Faika et al. (2018) presents a distributed and autonomous wireless battery management architecture designed to eliminate the single points of failure associated with conventional centralized systems. Its moderate latency, use of MQTT (Message Queuing Telemetry Transport), and cloud integration make it suitable for scalable deployments in electric vehicle fleets or energy storage systems.

Applying the trade-off table further clarifies how these differences affect other system designs. Profile 1 prioritizes the lightweight system described in the table that minimizes latency and complexity. However, its reliance on Wi-Fi connectivity and relatively narrow focus on a single battery pack means that latency to the cloud and event detection are more susceptible to disruption, especially in rural or bandwidth-limited regions. Profile 2 places considerable emphasis on real-time event detection and network resilience, enabled by its dynamic leader election and decentralized coordination. According to the trade-off matrix, this kind of design requires careful handling of edge storage buffering, as frequent detection events must be logged and shared efficiently without overwhelming node memory. Profile 2's data aggregation processes are handled via Google Sheets API, though not semantically structured for DPP needs, potentially increasing buffer and processing demand. In conclusion, Profile 2 is optimized for resilience, coordination, and adaptability, while Profile 1 prioritizes affordability, simplicity, and user-facing functionality, each trading off different dimensions to serve distinct application contexts.

Profile 3 and 4

In another comparison, profile 4 by Bašić (2023) presents a detailed and layered battery monitoring framework using secure gateways and structured log blocks. The proposed system emphasizes fine-grained measurement with sampling frequency between 100ms and 1s, and cloud interaction, which are highly compatible with the DPP requirements. On the other hand, Profile 3, by Le Gall et al. (2022), offers a more scalable architecture optimized for embedded systems with constrained resources. It can be seen that data collection is less fine-grained, with a sampling rate of approximately 500ms. However, this system leverages other lightweight protocols and Time Slotted Channel Hopping (TSCH) to minimize latency and improve robustness across distributed nodes. From the evaluation matrix, the comparison has shown that Profile 4 achieves stronger end-to-end traceability and diagnostic depth, while Profile 3 prioritizes real-time, energy-efficient transmission within a TSCH-based mesh topology.

The trade-offs table, when applied to these two profiles, shows that Profile 4 emphasizes sensing accuracy, which inherently leads to increased data volume and thus places greater demands on cloud latency and real-time event reporting. Hence, it will also have a greater need for edge storage buffering during network disruptions. Furthermore, Profile 4's structured and layered data formats, while aligned with DPP data format compatibility, will require more semantic structure, potentially introducing additional processing delays. On the contrary, Profile 3 demonstrates how a design that prioritizes real-time communication and lower latency must accept trade-offs in terms of data precision and structured format. In conclusion, Profile 3 fits well for systems where immediate response and system simplicity are favored over deep and structured analytics. Profile 4 is better suited for contexts demanding high data fidelity and extensive cloud integration, even at the cost of response time and higher buffering/storage overhead.

5. Validation: Expert Interviews

After designing the framework, this chapter presents the validation through expert interviews. Chapter 5.1 begins with results from the two exploratory interviews. Chapter 5.2 follows with the key insights, analysis of eleven expert interviews, with a summary in Chapter 5.3. The results offer practical insights into the framework's strengths, limitations, and relevance in real-world contexts. The content here directly contributes to answering the fourth sub-research question.

5.1 Insights from Exploratory Interviews

The exploratory interviews with two technical experts from a solution provider and a major system integrator revealed valuable insights that contributed to the refinement of the framework. While their backgrounds differed, both experts engaged with the logic and structure of the framework, offering complementary perspectives on its clarity, usability, and practical alignment with industry conditions. Both experts affirmed the framework's foundational logic—starting from DPP data requirements and tracing them backward to the IoT architecture layers. This reverse-engineering method was recognized as a robust way to assess whether specific IoT configurations could realistically support the monitoring, transmission, and verification of DPP-required data. It also helped surface whether current technical practices and infrastructure aligned with regulatory ambitions.

A central theme in both conversations was the framework's flexibility. Interviewee 1.2 emphasized that OEMs vary widely in their maturity, resourcing, and priorities. As such, applying a uniform set of evaluation dimensions may not be effective. Instead, interviewee 1.2 recommended that the framework allow users to select or prioritize dimensions based on their goals. For instance, a smaller or newer OEM might focus more on integration, while a mature company may invest in robust stakeholder authentication or lifecycle traceability. This adaptability was viewed as essential to ensuring broad relevance and reducing friction in adoption. From a technical perspective, interviewee 1.1 pointed out that dimensions like “Edge Storage” are already standard requirements in many industrial IoT implementations. Building on the same opinion, interviewee 1.2 added that after the list of basic requirements is defined, the next questions will be about the detailed technical specifications of each dimension. For example, “How fine-grained should the data be?” or “What is the appropriate response time?”.

Another shared insight was the importance of translating technical evaluation dimensions into business-relevant impacts. Both experts emphasized that decision-makers—particularly those involved in procurement, compliance, or systems planning—need to understand how each dimension maps to concrete outcomes such as development costs, system complexity, vendor lock-in risks, or long-term serviceability. Adding a clear link between technical performance and strategic or economic outcome would help the framework transition from a technical checklist into a more holistic decision-support tool. Overall, the exploratory interviews underscored the need for a framework that is technically sound, flexible in application, and aligned with business and regulatory requirements. The insights gathered from this exploratory phase informed multiple soft improvements to the framework and played a critical role in refining the subsequent interview protocol for broader expert engagement.

5.2 Insights from In-depth Interviews

5.2.1 IoT & Data Requirement Mapping

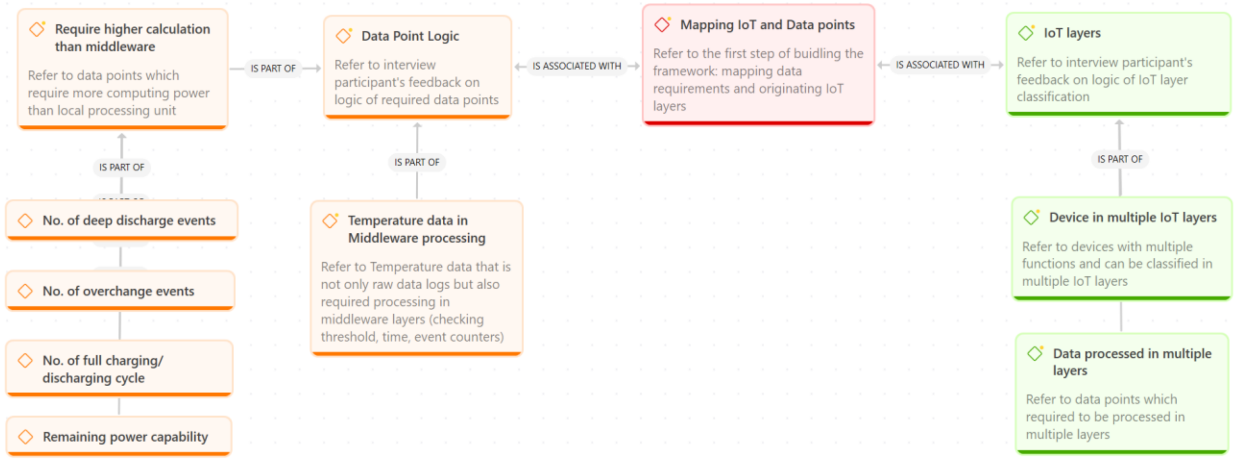


Figure 10: Overview of discussions for IoT and Required Data Mapping

In this section, the analysis of the in-depth interview presents several core themes in the discussion for the framework building steps. Figure 10 illustrates the key discussion themes that generate most comments and arguments from interview participants for the mapping between IoT and Data requirements.

Complexity in Middleware Processing and Computing

A recurring theme across interviews was that certain dynamic data attributes—particularly those requiring complex algorithms, such as deep discharge/overcharge events or remaining power capability—may exceed the computational scope of conventional middleware. While middleware is effective at processing raw operational data into DPP-relevant metrics like SoC, SoH, and lifecycle events, interviewees stressed that some calculations go beyond embedded rule sets. For example, interviewee 2.6 noted that interpreting operational logs into meaningful events, such as the number of full charge/discharge cycles, may require processing at the application layer. Similarly, interviewee 2.4 emphasised that advanced performance metrics are often AI-driven and involve complex inference models, which differ from standard middleware operations.

These perspectives point to the need for more granular distinctions within the framework regarding which technical layer is responsible for specific metrics. Interviewees 2.5 and 2.8 confirmed that middleware responsibilities typically include signal conditioning, event recognition, and threshold-based classification of sensor inputs. However, next-generation SoH models and other AI-based analytics may surpass the capabilities of embedded middleware, warranting a separate architectural category. Thus, while middleware remains central to IoT–DPP architectures, its role should be stratified according to the complexity of data transformation required.

Processed Data and Devices in Multiple IoT Layers

The temperature data also sparked many discussions across multiple interviews. While most experts acknowledged that raw temperature readings originate in the perception layer, several pointed out that recognizing thermal thresholds were crossed or anomaly events occurred—requires additional processing. Interviewee 2.5 suggested a dual categorization: if the temperature data is used purely as a log, it clearly belongs to the perception layer; however, if the system must detect events like thermal overloads or persistent exposure records, then it involves middleware-level computation. Agreed also by interviewee 2.1, who explained that modern IoT hardware often includes minimal embedded computing capabilities at the sensor level, allowing basic processing functions to be handled locally. Together, these perspectives suggest that temperature data may lie in the boundary between perception and middleware layers, challenging any rigid, single-layer classification in the evaluation framework.

A central insight from the interviews is that the boundaries between IoT layers are increasingly fluid, particularly in edge-enabled architectures. Experts emphasized that many data attributes undergo initial processing at the perception layer before being further refined in the middleware or application layer. Interviewees 1.2 and 2.2 both pointed out that field devices such as smart sensors and control modules now routinely incorporate basic computational capabilities, blurring the line between sensing and processing. This was further illustrated by interviewee 2.6, who questioned whether charging cycle data—traditionally considered middleware logic—might actually be finalized at the application layer due to additional aggregation and formatting needs. These perspectives reinforce that IoT systems in EV batteries often rely on hybrid, multi-layer computation chains, which must be reflected in any evaluation framework that maps data responsibility.

In modern IoT ecosystems, devices often serve overlapping roles across multiple architectural layers. Interviewees from solution-provider backgrounds, particularly from interviewee 1.2 and 2.1, noted that IoT modules used in EV battery systems frequently combine sensing, pre-processing, and basic network functions into a single hardware unit. This multifunctionality challenges the traditional four-layer architectural model that assigns strictly siloed roles to each layer. According to these experts, a more flexible approach is needed, where device capabilities are interpreted based on function rather than strict architectural boundaries. Such devices might simultaneously collect temperature readings, calculate thresholds, and format data for upstream transmission—indicating active participation in perception, middleware, and even application-level processes. As a result, the evaluation framework must be adaptable enough to accommodate hybrid-device behavior and modular integration strategies.

5.2.2 Evaluation Dimensions

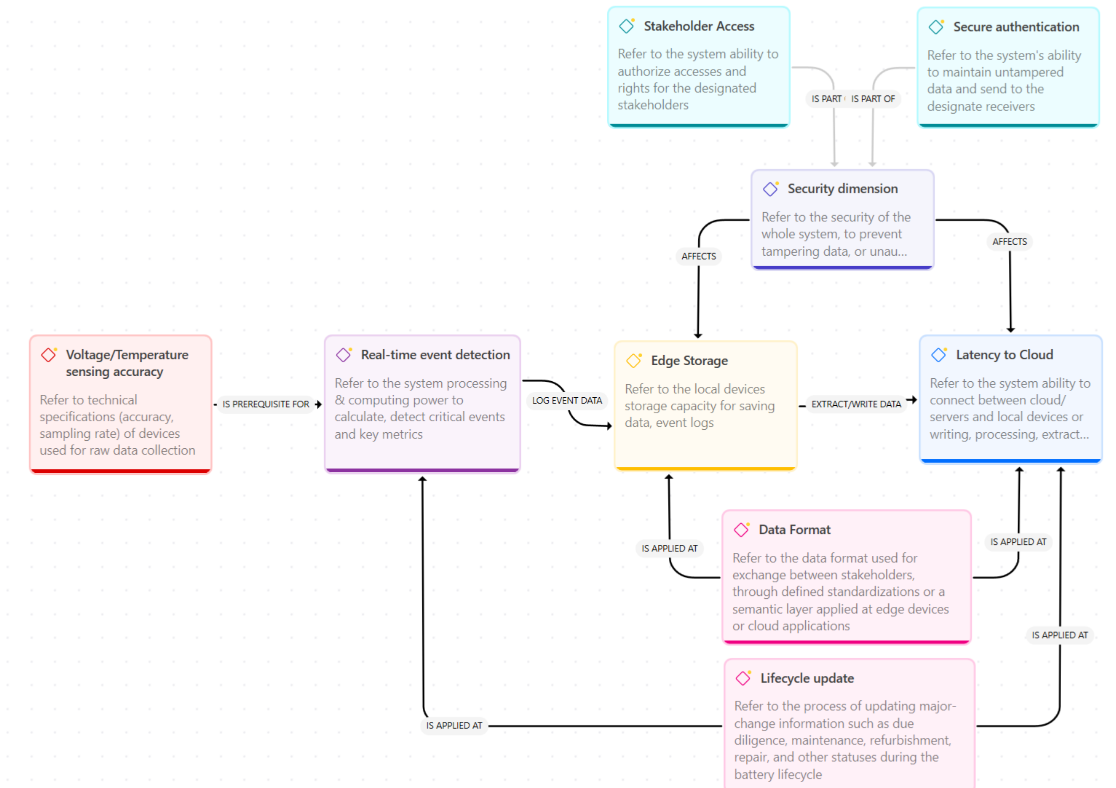


Figure 11: Overview of evaluation dimensions for DPP

Interview results reveal the participant's perspective regarding how evaluation dimensions interact with other, summarized in Figure 11. The following section highlights key opinions for each dimension.

Voltage/Temperature Sensing Accuracy

Sensor accuracy is widely regarded as the foundation of any IoT monitoring system (Teh et al., 2020). Similarly, interviewing experts agreed on the importance of this dimension, and it should refer not only to the presence of sensors but also to their technical specifications, such as resolution and sampling rate. As participant 2.1 noted, "this dimension will be the starting point for other later process steps to depend on". It emphasizes that high-quality sensor is the backbone of downstream computation or fundamentals in any control systems, as interviewee 2.3 remarked. Or in other words, other metrics are the byproducts of sensor-collected data, as shown in Figure 11, as a prerequisite for Real-time event detection. From a safety perspective, interviewee 2.4 added that this dimension is "safety-critical" and cannot be treated as optional or peripheral. Since accurate voltage and temperature readings are foundational for safe operation and warnings in case of extreme events, the sensor's detailed specifications must follow existing and emerging legal regulations regarding safety standards. Existing regulations like GTR 22 and Euro 7 have already prescribed the sensing thresholds, which will serve as a reference range or minimum baseline for selecting specifications. Overall, all interviewees acknowledged the importance and high priority of this dimension. However, to future-proof this dimension, interviewees 2.3 and 2.7 suggested that this should be renamed to "Sensing accuracy" in case of additional types of sensors being added/removed.

Real-Time Event Detection

All the experts agreed that Real-time event detection is indeed one of the core dimensions to be included in the framework, as the data output of this function will be the required data points for the DPP. This dimension can also be called “Edge Processing” since both refer to the system’s capacity to process incoming data streams and compute critical operational metrics. Several participants, from device and solution provider companies, pointed out that the available computing power that can be put on current edge devices is somewhat limited. Therefore, OEMs will have to select only key metrics to be processed locally, while other less critical but more complicated metrics can be processed over cloud servers. Interviewee 2.4, from an EV OEM perspective, confirmed this insight and provided two commonly used criteria to decide the local processing, which are “Battery safety” and “Fault Diagnosis”. The edge-cloud processing problem can also be connected to the data storage problem, which will be combined as “Edge-Cloud continuum” and discussed later in the trade-off section.

Edge Storage

Edge storage function is more than just storing data; it also responds to external data extraction requests, which gives it application-layer characteristics. However, edge storage, while still being a core operational dimension, is not “strategically valuable” and should not be “overemphasized” in the framework. Because this function is legally mandated and most fault logging systems already include it as a standard, making it a baseline feature. In addition, interviewee 2.4 remarked that OEMs should question their real value beyond compliance: “How valuable is offline mode?”. This will help them avoid overengineering unless it offers business value. From a policy perspective, interviewee 2.6 also provided that “More storage does not mean better compliance unless data is structured and utilized well”. From these insights, the importance and priority of edge storage are not as high as previously proposed.

Latency to Cloud

This dimension refers to the system’s ability to connect and transfer data with the external networks or servers. Although considered to be a baseline operation feature for DPP, many experts argued that this dimension should not be a major point of focus, unless it provides additional revenue streams or is safety-related. Interviewee 2.5 clarified how low latency supports stakeholder updates, particularly for DPP use cases (e.g., compliance verification, second-life evaluation). However, the interviewee 2.7 provided in addition that latency is context-specific, and ensuring correct data mapping and compliance is more critical than real-time transmission for DPP purposes. In cases where a live data connection is needed, this dimension will be a valid technical concern. Nevertheless, interviewees 2.1 and 2.2 also added that this dimension depends on external network infrastructure, which OEMs cannot fully control, and transmitting high-fidelity data to the cloud increases bandwidth costs, especially in commercial deployments. Therefore, latency to cloud should be a baseline function for DPP, but with less importance and should be considered as complementary to edge storage.

Data Format Compatibility

Data format is a controversial dimension where most of the expert opinions are divided into three groups. Interviewees 1.1, 1.2, and 2.2 ranked this dimension as “optional” because they viewed format compatibility as customer-driven (depending on different OEMs) and as “belonging to a later stage” after data processing. Interviewees 2.5, 2.6, and 2.8 took a more neutral stance, noting that this dimension is closely tied to system interoperability and required better clarification on implementation strategies (either at the edge devices or cloud processing with semantic layers). Interestingly, interviewee 2.6 commented that OEMs would prefer semantic layers for proprietary reasons, while startups or “new players” prefer already existing standardization for cost-efficiency. But “Industry-wide standardization is difficult and slow, so semantic layers will likely remain common,” as commented by interviewee 2.2. The third group, including interviewees 2.1, 2.3, and 2.4, proposed that this dimension should be one of the highest priorities in a multiple vendors/stakeholders scenario. From a solution provider perspective, industry-wide format standardization can greatly improve interoperability, reduce cost, simplify service delivery, especially analytics, because no semantic conversion is required. From an EV OEM perspective, data format was ranked as second in priority, immediately after lifecycle updates, emphasizing that format compatibility ensures data can be read, interpreted, and verified across the battery lifecycle. If the format is inconsistent, other DPP functions like stakeholder access or second-life assessment could fail systematically.

Security

Security emerged in expert feedback not as a single requirement, but as a combination of two interlinked sub-dimensions: Stakeholder Access and Secure Authentication. Most experts supported combining these into a unified “Security” category. Interviewees (2.5 and 2.6) with DPP legal and regulatory experience commented that “Stakeholder Access is a key feature mentioned in many DPP documents,” and it should thus be core rather than an optional dimension. For solution-provider interviewees 2.1, 2.2, and 2.3, they reported that security is the foremost concern raised by high-level clients, particularly for cloud-based solutions involving sensitive behavioral data. This reinforces the viewpoint that trustworthiness is a precondition for broader adoption between various stakeholders. Notably, participant 2.4 provided a unique and business-oriented perspective by explicitly identifying stakeholder-specific access control as a critical business enabler. This capability allows OEMs and suppliers to segment data visibility across actors. Following the logic of data is the new oil (Schwab et al., 2011), the Stakeholder-access enables new monetization models across the battery’s lifecycle—for example, by granting access to second-life service providers or recyclers under defined conditions. While all the participants did not delve deeply into technical details of security, they clearly linked data governance and selective access to strategic outcomes such as revenue generation and operational efficiency. Collectively, these insights affirm that security is not merely a supportive feature but a foundational requirement for enabling trust, regulatory compliance, and business value realization in the deployment of IoT for DPP purposes.

Lifecycle Update

Among the eight evaluation dimensions examined, lifecycle update consistently emerged as a vital yet initially underemphasized component, with several experts advocating for its elevation to core status. Lifecycle update refers to the system’s ability to modify, log, and transmit updated battery data across its operational lifespan, including during maintenance, repurposing, or recycling. Several experts underscored that DPPs must not be limited to static snapshots of battery data but should support ongoing updates to reflect real-world changes in status, ownership, and condition. Participant 2.4 was the most outspoken in this regard, explicitly ranking lifecycle update as the highest priority, even above data format and sensing accuracy. The ability to document and trace battery modifications over time—such as component replacement, second-life transitions, or regulatory compliance updates—is essential for maintaining the integrity and usability of the DPP. Without it, the DPP risks becoming obsolete the moment the battery leaves the OEM factory. In a similar tone, interviewee 2.3 mentioned that this dimension is highly related to compliance audits and contractual obligations in regulated industries. Solution providers and system integrator participants also strongly supported making lifecycle updates a core dimension, especially in cloud-integrated architectures, where stakeholders can view the battery evolution. For research and optimization purposes, lifecycle updates are not just valuable but necessary for looking back at the history, estimating the accurate SoH, and safety evaluations. While a few experts considered the lifecycle update helpful but not core, placing more emphasis on stakeholder-specific access. Others, including participants 2.6 and 2.8, incorporated it conceptually through the proposed

"Lifecycle Information" function, which combines latency and storage to support continuous data retrieval and updating. Collectively, these insights suggest that lifecycle update is not simply an enhancement, but a functional necessity for ensuring that DPP systems remain relevant, reliable, and compliant throughout the battery's use, reuse, and end-of-life pathways.

Summary of the Evaluation Dimensions

Ranking	Evaluation Dimensions	Purpose
1	Sensing Accuracy	For raw data collection and safety-event processing
2	Real-time Event Detection	
3	Security	For securing data integrity and preventing unauthorized access
4	Lifecycle Update	For updated information across the battery lifecycle
5	Data format compatibility	For interoperability between various systems and stakeholders
6	Latency to cloud	For key events, data logs extraction and transmission
7	Edge storage	

Table 11: Ranking of Evaluation Dimensions based on expert interviews

Table 11 presents the revised evaluation dimensions and their ranking based on expert interviews. Each dimension was refined or re-ranked according to stakeholder insights. Sensing Accuracy (Rank 1) was unanimously emphasized as foundational for both safety and downstream computation. Based on this, the dimension was renamed from "Voltage/Temperature Sensing Accuracy" to "Sensing Accuracy" to allow future expansion beyond temperature and voltage. Real-time Event Detection (Rank 2) was validated as essential for vehicle diagnosis and on-the-fly data processing, a core system function. Together, these two dimensions form the technical core of the system's sensing and local intelligence.

At Rank 3, Security was elevated in priority as strongly advocated by experts, to combine message authentication and stakeholder-specific access control into a single dimension. This reflects a growing concern and its critical role in enabling trust and compliance across stakeholders. Lifecycle Update (Rank 4) was previously underemphasized but was reclassified as a core dimension based on OEM input that ongoing updates are vital for traceability and circular economy goals. Data Format Compatibility (Rank 5) generated divergent views—some experts saw it as optional, while others ranked it highly for interoperability. The dimension was retained with lower priority due to possible mitigation via semantic layers. Latency to Cloud (Rank 6) and Edge Storage (Rank 7) were both deprioritized. Experts highlighted their status as either infrastructure-dependent or already standard across platforms, suggesting limited strategic value. These dimensions remain in the framework but are treated as supportive features rather than decision-critical elements.

This revised ranking reflects the interpretation of expert feedback, distinguishing between foundational sensing and processing capabilities, critical trust-enabling dimensions like security and lifecycle updates, and infrastructure-linked support functions. The ranking also accommodates both technical and operational concerns, enabling a more robust and industry-aligned assessment framework for evaluating the readiness and effectiveness of IoT architectures in EV battery DPP systems.

5.2.3 Evaluation Matrix and Trade-off Table

Evaluation matrix

The expert feedback on the evaluation matrix and architecture profiles expressed a strong support for the framework's structured approach and agreed that the matrix is a useful tool for assessing how various IoT configurations align with the requirements of DPP. Interviewees from industries (2.1 and 2.2), as well as research organizations (2.5 and 2.7) affirmed that the matrix's comparison logic is very similar to the industrial approach when evaluating their systems for other requirements. However, it is recommended by interviewees 2.3, 2.6, and 2.7 that scoring guidelines should be provided to make the framework more intuitive. Rather than rigidly quantitative, this guideline should be made subjective and context-driven to accommodate differences in device maturity, supplier capabilities, and regulatory interpretations.

Regarding the profiles, interviewees 2.4 and 2.6 noted that Profiles 1 and 2 align with existing or near-market implementations—Profile 1 resembling a low-cost, minimum-compliance setup, and Profile 2 offering a scalable architecture for broader stakeholder engagement. In contrast, Profiles 3 and 4 were noted as more experimental or research-oriented, with advanced features like full-cloud analytics or decentralized edge intelligence, but unlikely to be feasible for most OEMs in the near term due to cost, complexity, and integration challenges. Due to these profiles being constructed from literature, experts observed that their technical details were not presented on a common measurement scale, and using a consistent basis would improve comparability. Interviewee 2.4 cautioned against overengineering and stressed that architecture choices should be guided by business value and revenue potential, not just technical details. Therefore, the profiles should be simplified to reach a wider range of audiences rather than just technical experts.

A common theme across feedback was the importance of clarifying the use case scenario for the matrix. Interviewees 1.1 and 2.7 suggested that beyond comparison, the matrix should help stakeholders identify functional gaps and guide system upgrades. They also proposed linking the technical dimension scores to operational or business outcomes, such as second-life readiness or regulatory compliance, which would enhance the framework's strategic decision-support value. For non-technical stakeholders, including business managers or regulatory advisors, interviewees 1.1 and 2.2 recommended developing a simplified visual summary, such as a heatmap or performance radar chart, to make profile strengths and weaknesses more intuitively understandable. Overall, the expert feedback confirmed the practicality and relevance of the evaluation matrix and profile comparison approach, while calling for enhancements in adaptability, interpretability, and business alignment. Experts encouraged future iterations to incorporate flexible scoring guidelines, consider economic trade-offs, and embed user-friendly summaries to ensure the framework is actionable across both technical and executive decision-making levels.

Trade-off Table

Of all the components presented in the proposed evaluation framework, the trade-off table stood out as the most intellectually engaging and discussion-provoking element. While other dimensions prompted agreement or prioritization, the trade-off model elicited critical reflection, nuanced technical observations, and rare experiential knowledge from a diverse range of experts. It became clear throughout the interviews that the concept of trade-offs resonated strongly with practitioners, who routinely navigate these tensions in their daily design, deployment, and regulatory alignment work. Rather than treating each dimension in isolation, the trade-off table engaged with the experts to reflect on how improving one technical function impacts other functions in many ways. As interviewee 2.2 strongly noted, "No system is perfect, and every function comes with a set of constraints." Stakeholders with industrial roles emphasized operational and infrastructure constraints, while research-focused participants prioritized compliance integrity and design completeness. This dual perspective reinforces the trade-off model's role in bridging technical requirements and feasibility, a gap seldom addressed explicitly in state-of-the-art frameworks. More trade-off discussions can be found in Appendix E.

5.3 Summary of Expert Insights

Data Requirement, IoT Mapping, and Evaluation Dimensions

Most interviewees appreciated the framework's breakdown into discrete technical dimensions, such as sensing accuracy, edge storage, data format compatibility, and security. This approach was seen as a helpful abstraction, especially for benchmarking different system configurations or identifying bottlenecks in existing deployments. However, interviewees 2.2 and 2.6 emphasized that these functions are not always cleanly separable in practice, urging for groupings or thematic clusters, such as "Lifecycle Information" (combining edge storage, latency, and event detection), or "Communication Architecture" (encompassing format, latency, and access control). The classification of certain dimensions as "core" versus "optional" prompted strong reactions. For instance, sensing accuracy was almost universally treated as foundational. In contrast, lifecycle update—initially framed as optional—was seen by several experts (interviewee 2.2 and 2.4) as operation-critical, particularly for enabling second-life scenarios and regulatory traceability. As interviewee 2.4 quoted: "Without lifecycle update, DPP is at risk being obsolete the moment the EV leaves the factory". Likewise, security functions (message authentication and stakeholder access) were consistently elevated to core status due to their role in preserving trust, preventing tampering, and enforcing compliance obligations. In addition, stakeholder access was regarded as monetizing dimension (which can provide new revenue streams as data platform subscription). This feedback informed the revision of the framework's ranking to be more relevant with existing contexts from expert's insights.

Trade-offs, Stakeholder Constraints, and Architectural Preference

Rather than debating whether a function was important, many experts focused on how it interacts with others, i.e., the trade-off it introduces. For example, increasing sensing fidelity might improve event detection, but also burdens storage and processing pipelines—especially at the edge. Similarly, allowing dynamic lifecycle updates introduces security risks and stakeholder coordination challenges. These discussions revealed that successful system design is not about maximizing every feature, but about strategically navigating functional tensions within the constraints of infrastructure, cost, and governance models. This emphasis directly validated the central role of the trade-off table within the evaluation framework. Interviewees brought differing assumptions and constraints based on their organizational backgrounds. OEM experts (interviewee 1.1 and 2.7) focused on realistic deployment conditions, including mobility-related latency, existing BMS architectures, and commercial rollout pressures. In contrast, experts from research and academic institutes (interviewee 2.5 and 2.6) emphasized compliance structures, reference architecture integrity, and public-interest value. Solution providers like interviewee 1.2 and 2.2 added insights from the integrator perspective, often highlighting cost-performance trade-offs and the impact of legacy infrastructure. These contrasting positions underscored that no single architecture is universally optimal, and that evaluation must reflect contextual adaptation.

Technical Design and Business Value

Finally, many experts encouraged moving beyond purely technical evaluation to explicitly link architectural decisions to business outcomes. For instance, robust lifecycle update capabilities were seen not just as a compliance feature but also a potential revenue stream, enabling battery resale, predictive maintenance, and aftermarket services. Similarly, the degree of standardization adopted could influence ecosystem compatibility or OEM differentiation strategies. These insights suggest that the evaluation framework—and especially its trade-off analysis—should serve not only as a technical scoring tool, but also as a strategic decision-making instrument for long-term system planning. In addition to providing detailed insights into specific technical trade-offs, experts also reflected on the system-level conditions that shape architectural decisions. These include not only technical constraints, but also external infrastructure dependencies, regulatory boundaries, and value-driven business decisions. Figure 12 summarizes how these contextual forces intersect to determine what trade-offs are encountered and which solutions are feasible.

At the core of the expert feedback was the recognition that system design trade-offs are not isolated technical challenges but are often triggered or constrained by factors beyond the system itself—including evolving legal requirements for data access, market-driven service innovation, and the availability of telecommunications infrastructure. Understanding these interactions is crucial to interpreting how trade-off decisions are made and why certain technical sacrifices are tolerated or prioritized.

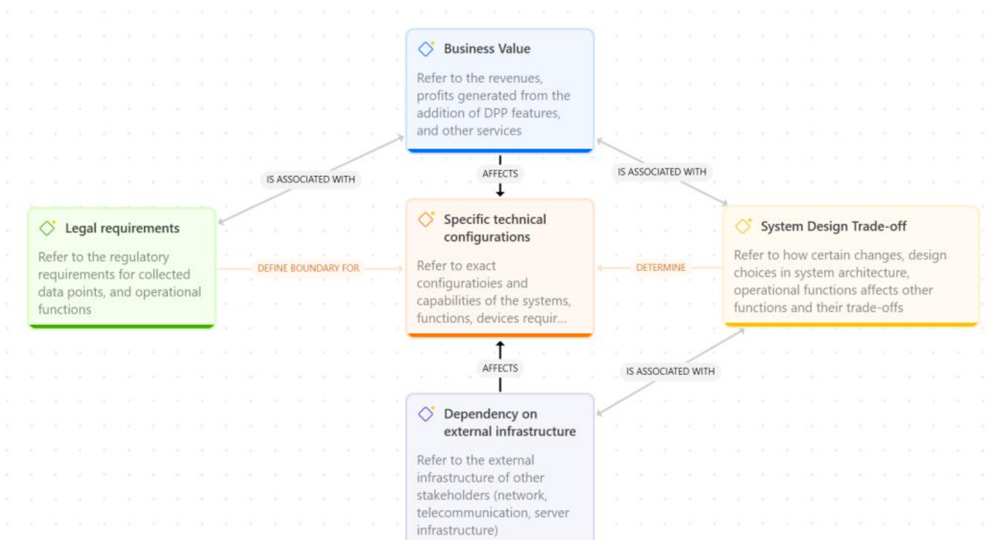


Figure 12: External factors influencing system design

In summary, the expert feedback inspired substantial refinements to the evaluation framework. Several evaluation dimensions were renamed and re-prioritized to better reflect their operational and regulatory significance, reflecting the industry practice. Comments on the evaluation matrix and trade-off table identified specific areas requiring adjustment to preserve their relevance and decision-support value. Overall, the validation process indicates that the framework provides a practical basis for assessing IoT-driven DPP adoption, while also revealing targeted modifications needed to address real-world challenges—thereby contributing to the resolution of sub-question 4.

6. Result - Refined Evaluation Framework

The refinements presented in this chapter are based on the insights gathered during the validation process, ensuring that the framework is both technically robust and operationally relevant. Chapter 6.1 presents the refined evaluation matrix, including a more intuitive legend, while Chapter 6.2 provides a more detailed update of the trade-off table.

6.1 Evaluation Matrix

Evaluation Dimension	IoT Layer	Profile 1	Profile 2	Profile 3	Profile 4
Sensing Accuracy	Perception, Middleware	Medium - Voltage & temp sensors	Medium – Wireless voltage, temp sensing	High – QoS control for sensing accuracy	High – High-quality battery emulator
Real-time Event Detection	Middleware	Low - Manual trigger logic only	Medium – Node-based signal propagation	High – Event-based scheduling & TSCH	Medium – Basic event handling at edge
Security	Perception Middleware, Application	None – No mention of encryption or access control	Low – ZigBee/LoRa, but no security discussed	Medium – Only TSCH mentioned	Medium – Access control mentioned, no protocol detail
Lifecycle Update	Middleware, Application	None – No update mechanism	Low – Decentralized BMS without OTA support	Medium – Central controller manages updates	High – OTA lifecycle & modular updates
Data Format Compatibility	Middleware, Application	Low – Local Format	Medium – CAN-based messaging	Medium – Scheduler structured output	High – Modular, interoperable format support
Latency to Cloud	Network	Low – Only Cloud storage	Medium – Wireless with moderate delay	High – TSCH routing minimize latency	High – Cloud-edge coordination present
Edge Storage Buffering	Middleware	None – No mention of local storage	Low – Real-time transfer only	Medium – Temporary local data management	High – Persistent edge storage defined

Table 12: Refined Evaluation Matrix with dimension importance ranking

The refined evaluation matrix in Table 12 incorporates seven key dimensions that reflect what is technically needed for a DPP system to function. The order of dimensions in the matrix reflects their relative importance as ranked by expert stakeholders during validation, with higher-listed dimensions (at the top) considered more critical; however, this prioritization may shift depending on the specific context, objectives, or priorities of different users such as OEMs, regulators, or solution providers. The four architecture profiles represent alternative implementations drawn from academic literature. During expert interviews, several participants raised concerns about comparing profiles with inconsistent assumptions or unit measures. In response, the matrix adopts a simplified four-point scale—None, Low, Medium, and High, indicating the level of capability or maturity for each dimension, ranging from completely absent (None) to fully developed and robust (High). This legend was refined based on expert feedback recommending a more intuitive and accessible comparison system that avoids rigid quantification. Where applicable, each matrix cell includes a brief technical annotation (e.g., “TSCH”) to clarify the basis for the assigned rating. This pairing of qualitative labels with descriptive technical facts was developed to strike a balance between usability and detail, a point emphasized by interviewees 2.2 and 2.7. Unlike prior frameworks—such as CIRPASS and Battery Pass, which focus on data-attribute requirements rather than scoring—the refined matrix integrates (i) a scoring scale for cross-profile comparison, (ii) flexible prioritization of dimensions according to context, and (iii) concise technical annotations to justify ratings. These enhancements increase transparency for stakeholders, facilitate scenario-based analysis, and bridge the gap between compliance documentation and system-level design choices.

6.2 Trade-off Table

The trade-off table was refined to illustrate how changes in one technical function often introduce constraints in others—a central theme raised across expert interviews. Rather than evaluating these dimensions in isolation, the table highlights interdependencies that system designers have to routinely navigate to balance between multiple criteria such as performance, cost, compliance, and constraints. Experts consistently pointed out that trade-offs are unavoidable and context-dependent; they must make compromises based on what matters most in each use case. Whether the goal is low-cost rollout or full-featured tracking, this structure makes it easier to weigh what is gained and what might be sacrificed. During the interview process, experts strongly validated the trade-off concept and called for its expansion. As a result, the trade-off table was updated to include Security and Lifecycle Update, two dimensions frequently cited as critical yet underrepresented in the earlier version. Interviewees (e.g., 2.2, 2.4, 2.6) highlighted new tensions that arise when these dimensions are introduced; therefore, an analysis on how these dimensions come into play was required.

In the refined trade-off table, Security dimension encompasses the mechanisms designed to safeguard data integrity, confidentiality, and authenticity across all system layers—from sensing and storage to communication and control. In the context of DPP, security ensures that lifecycle data—including faults, usage logs, and repair records—can be trusted and are not vulnerable to manipulation (Lopez et al., 2017; Orellana et al., 2024). Interviewees emphasized that while cryptographic measures are essential for preventing spoofed or tampered data (e.g., falsified fault reports), they also add processing delays and increase data payloads. These issues place pressure on latency to cloud and edge buffering, especially in resource-constrained environments. Balancing cryptographic strength in the EV resource-constrained system remains an open design challenge.

The Lifecycle Update dimension, as defined in expert feedback, refers not just to firmware updates but to structured documentation of key battery events—such as repairs, repurposing, and ownership transfers—across its operational lifespan. It provides the historical backbone for DPP, enabling due diligence, circular economy operations, and regulatory compliance across all stakeholders (GS1 Europe, 2024). The effectiveness of lifecycle updates depends on multiple other architectural features. Sensing accuracy ensures that abnormal conditions triggering maintenance or repurposing (e.g., thermal excursions, capacity loss) are detected with sufficient fidelity. Real-time event detection provides timestamped logs of such events, while security ensures the authenticity and non-repudiation of the logged updates. Moreover, semantic data format compatibility is necessary to encode updates in a way that remains machine-interpretable across OEMs, recyclers, and second-life system operators. Latency to cloud also matters—delayed uploads may compromise auditability or compliance with reporting deadlines. Finally, edge storage buffering becomes critical when lifecycle events occur in offline conditions. Ensuring accurate, trusted capture of lifecycle events across varied environments presents both technical and governance challenges. Experts also noted concerns around privacy, particularly in second-life resale and cross-border data flows.

Table 13 presents the updated trade-off relationships, incorporating both newly added dimensions and refined insights based on interview input. These refinements were made to better represent the decision-making tensions faced by OEMs, solution providers, and other stakeholders. By explicitly surfacing these interdependencies and their potential operational consequences, the table shifts from being a static reference to serving as a tool for active design negotiation. This approach makes visible the systemic implications of optimizing one dimension at the expense of another—an emphasis often absent in earlier DPP frameworks—thereby supporting more informed evaluation of system architectures in line with real-world constraints and strategic priorities.

Evaluation Dimension Trade-offs	Sensing Accuracy	Real-Time Event Detection	Security	Lifecycle Update	Data Format Compatibility	Latency to Cloud
Real-Time Event Detection	Improved sensing enables more reliable event detection but also requires more processing power.					
Security	Ensure data integrity, protecting against spoofed or tampered readings;	Authenticated events ensure trust in alerts and reduce false positives.				
Lifecycle Update	Lifecycle records demand contextual data; encourages finer sensing accuracy	Lifecycle traceability depends on accurate event detection	Lifecycle data integrity requires cryptographic controls			
Data Format Compatibility	Structured data models may demand greater sensor granularity	Structured formats increase complexity and may delay event processing or require preprocessing.	Complex formats increase encryption overhead validation steps, stressing constrained devices.	Lifecycle records in RDF/JSON-LD ensure interoperability but raise payload size and parsing complexity.		
Latency to Cloud	Bandwidth limits may cap sensing frequency or sampling rates to avoid congestion.	Higher latency can delay time-sensitive detection, affecting event resolution and compliance timelines.	Network-induced delays weaken end-to-end security by prolonging exposure windows.	Delayed uploads can cause lifecycle event mismatches or missed compliance windows in DPP systems.	Serialization overhead adds to packet size, increasing latency in data exchange.	
Edge Storage	Insufficient edge buffering forces data drops during high-frequency sensing.	Limited buffer size restricts detection logs, risking event loss during network outages.	Secure buffers must handle encrypted data blocks, increasing storage needs and requiring reliable power states.	Offline lifecycle events must be cached persistently until successful cloud sync, requiring overwrite protection	Complex structured formats increase edge storage consumption and can require memory reallocation.	Increased latency lengthens buffer holding time, demanding more persistent local memory.

Table 13: Refined Trade-off table

7. Discussion

7.1 Research Findings

This study set out to design a framework that enables technical decision-makers—such as OEMs, EV system integrators, and engineers—to assess and compare the suitability of various IoT-based architectures in meeting the traceability and dynamic data requirements from the DPP for EV battery. Despite the legal pressure for mandatory DPP implementation in 2027, many uncertainties regarding required data points, technical specifications, and cross-industries vision remain unsolved (Berger et al., 2023; Uusitalo et al., 2024). The evaluation framework developed here responds to this regulatory context and draws on the work of industrial consortiums and EU-funded initiatives. While initiatives such as CIRPASS have developed extensive user stories to shape the functional requirements of DPP systems, and Battery Pass has published detailed attribute lists and technical guidance, these initiatives generally stop short of specifying operational-level criteria, which this study addresses.

With IoT as an enabling technology, this research translates abstract policy and regulatory requirements into concrete, IoT system-level evaluation dimensions. These dimensions—such as sensing accuracy or real-time event detection—were derived from the Battery Pass data attribute list, and combined with the DPP system architecture, user stories, EV operation contexts proposed by CIRPASS. Through a bottom-up approach, the framework traces the origin of required data points in the IoT infrastructures, enabling analysis of whether a given system can reliably and securely collect, process, and transmit dynamic operational data for DPP compliance. This approach is consistent with prior work emphasizing the need to connect lifecycle data points directly to infrastructure capabilities (Baars et al., 2021) and aligns with the indicator categories described in Berger et al. (2023), which structure DPP information content according to circularity, diagnostics, and product design attributes. While previous initiatives such as CIRPASS and Battery Pass have proposed high-level data models, they often stop short of providing actionable technical evaluation criteria for IoT engineers (Battery Pass, 2023; Berger et al., 2023). By explicitly mapping DPP data requirements to IoT sensing, processing, and transmission functions, the framework complements these previous works with technically actionable guidance for engineering and design decisions.

The expert interview process has revealed that regulatory pressure alone is insufficient to drive implementation. Stakeholders require complementary technical guidelines and standardization pathways to translate policy mandates into implementable designs. OEMs, legal, and policy experts placed greater emphasis on data protection, standardization, and lifecycle updates because of concerns about proprietary information control and regulatory compliance. This finding is consistent with Berger et al. (2023), who noted that OEMs frequently prioritize data security and product traceability in DPP design, often at the expense of broader interoperability. Similarly, Rufino et al. (2024) highlight that regulatory actors and policymakers tend to stress compliance-related data exchange mechanisms, whereas system integrators focus more heavily on technical performance and implementation feasibility. This emphasis on security and lifecycle updates contrasts with CIRPASS, which prioritizes interoperability and semantic data harmonization, and Battery Pass, which, while incorporating security, focuses more heavily on standard data schemas.

Alongside the evaluation matrix, the framework's trade-off table generated some of the most engaged discussions, particularly around the edge–cloud continuum. Deciding this boundary continues to be a big debate among many interviewees, reflecting both technical and economic pressures faced by stakeholders. Interviewees weighed the operational benefits of high edge processing—cited by interviewee 2.6 as essential for safety—against the increased hardware costs and production constraints raised by interviewees 2.1 and 2.2. According to interviewee 2.4: “Calculation happens in both locations, but cloud only makes sense with high complexity algorithms and analytics requiring data from a large number of vehicles”. This mirrors broader discussions in IoT architecture literature, where edge-heavy approaches are shown to reduce latency and improve reliability but often increase hardware costs and complexity (Uusitalo et al., 2022). CIRPASS emphasizes leveraging affordable, mature technologies with built-in interoperability to enable scalable deployment (CIRPASS, 2024b). Although detailed IoT architectural case studies are not publicly documented, the project clearly addresses affordability and deployment feasibility. Le Gall et al. (2022) similarly note that architectures optimized for dynamic data capture and cloud integration may align well with DPP requirements but are often difficult to deploy in cost-sensitive sectors in EV manufacturing. This persisting, unresolved trade-off underscores the value of decision-support tools for evaluating edge–cloud configurations in DPP contexts. This aligns with calls in the literature for context-sensitive architecture evaluation methods that can guide stakeholders through performance–cost trade-offs, rather than prescribing a single ‘optimal’ design (Uusitalo et al., 2022; Le Gall et al., 2022).

Finally, the research also reveals a growing recognition that DPP implementation decisions cannot be evaluated purely on technical grounds. Multiple participants observed that system design must account for service value and business model implications. For example, incorporating high-fidelity sensor data opens potential for predictive maintenance, warranty optimization, and lifecycle services—functions that extend beyond compliance to create commercial opportunities. This perspective is consistent with recent findings in the Battery Pass project, which highlight second-life applications and predictive maintenance services as primary value drivers in the emerging DPP ecosystem. These findings indicate that future iterations of the framework should more explicitly integrate business-case evaluation alongside technical assessment. Positioning IoT architecture evaluation within both compliance and value-creation contexts may therefore accelerate adoption by aligning stakeholder incentives beyond regulatory obligation.

7.2 Limitations

While this study contributes a methodology to support IoT architecture selection for DPP compliance in the EV battery sector, several limitations should be noted. Some reflect common challenges across the industry, while others are specific to this framework. First, the scope excludes static data requirements. Static attributes, which refer to information that does not change over time, such as manufacturer identification, production site, or material composition, are an essential component of the DPP, but were omitted here because the framework focuses on dynamic attributes that align with IoT monitoring capabilities. This exclusion, while consistent with the framework’s intended focus, limits its applicability for full DPP implementation.

Second, security has not been incorporated as a core evaluation dimension in the current version of the framework. Although data security and system resilience are essential for trust in regulated traceability systems (Saeed et al., 2023), this aspect was only briefly addressed in the current analysis. Future iterations of the framework will need to explicitly integrate security-related capabilities, such as data encryption, access controls, and cyber-resilience of BMS components across IoT layers. Third, since the data collection and analysis were performed by a single researcher, its interpretation and results depend on the researcher’s perspectives and knowledge. In addition, the study's validation interviews were conducted with a relatively small sample, consisting of a total of 11 expert participants. Although these stakeholders were selected based on their technical or strategic involvement in DPP-related activities, the sample may not fully capture the diversity of views across the broader battery value chain. Important perspectives from regulatory authorities, battery recycling firms, and legal compliance officers—who are central to the implementation of the ESPR—were missing. Therefore, expanding the interview base through different methods of data collection is advised to improve this study.

Lastly, the framework currently operates as a qualitative decision-support tool and has not yet been validated through live deployment or tested against real-world system architectures. The mapping of Battery Pass attributes to IoT layers and BMS modules is based on expert interpretation and secondary sources, and while technically plausible, it may not fully reflect the complexity and variability of commercial implementations. As such, the framework should be considered an initial prototype requiring further empirical refinement and validation.

7.3 Suggestions for Future Research

Building upon the previous limitations identified in this study, several directions for future research are recommended to enhance the robustness, applicability, and strategic value of the proposed framework. Some of these directions address gaps already highlighted in prior initiatives such as CIRPASS and Battery Pass, while others extend into less-explored territory. First, there is a need to refine the technical granularity of the evaluation dimensions. While the current framework qualitatively identifies attributes such as sensing accuracy or sampling frequency, it does not establish performance thresholds or compliance ranges. For example, identifying minimum viable sampling rates for SoC monitoring or acceptable latencies for event detection could increase the framework's usability for OEMs, auditors, and system integrators. Future work should determine benchmark values for each dimension, drawing on established standards such as GTR 22 (Global Technical Regulation on In-Vehicle Battery Durability for Electrified Vehicles) and Euro 7, as suggested by interviewee 2.4.

Another priority is developing clearer criteria for managing the edge–cloud continuum. Although edge storage and cloud latency were included in this study, further research should explore formal criteria for deciding which DPP-relevant data should be processed at the edge or offloaded to the cloud. Developing a structured methodology to assess these trade-offs would greatly enhance the decision-making process for both technical and business teams. This could take the form of a decision matrix, simulation tool, or rule-based system that aligns architecture design with the specific use-case characteristics per OEM and compliance needs. Such guidance would address a well-documented gap in the literature, where frameworks acknowledge edge–cloud trade-offs but provide limited actions.

Second, the current trade-off table, while useful, should be evolved into a more structured decision-support tool. Multiple experts in this study suggested that the table provides a foundation for understanding technical compromises, but that it could be extended to incorporate business value, service impact, and cost dimensions. Interviewee 2.4 explicitly characterized the table as being "halfway to a risk management framework." To reach a broader range of users, such a tool could include quantitative scoring schemes that help business leaders make high-level decisions, together with technical engineers and architects. This dual-layered approach would ensure relevance across managerial and operational domains. Finally, future studies could investigate the business value of DPP-related data and services. High-resolution, verified operational data enables new models such as predictive maintenance, performance-based warranties, and second-life certification. Investigating how these services could be monetized—either as internal efficiency gains or customer-facing offerings—would provide insight into the broader strategic potential of DPP infrastructures. This would support organizations not only in meeting compliance requirements but also in leveraging DPP systems as enablers of innovation and competitive advantage.

7.4 Contributions

7.4.1 Scientific Contributions

From a scientific perspective, this study advances the understanding of how regulatory traceability requirements—such as those defined under the ESPR—can be operationalized through system-level design frameworks. It introduces a novel evaluation structure that links the abstract goals of DPPs with the concrete capabilities of IoT architectures. The inclusion of core evaluation dimensions fills a gap in existing literature, which tends to focus either on policy-level analysis or isolated technical components, without integrating the two. Moreover, the framework contributes to a growing body of research exploring architecture-centric approaches to sustainability and compliance. It provides a foundation for future work seeking to quantitatively benchmark architectural performance, incorporate risk trade-offs, and align system design with lifecycle-wide data integrity. By integrating qualitative insights from stakeholders directly involved in the DPP ecosystem, this study also highlights the importance of user-informed architectural evaluation in contexts where technical design decisions must meet evolving regulatory demands.

7.4.2 Managerial Contributions

For industrial practitioners, the framework serves as a decision-support tool that can guide early-stage planning and system design for DPP readiness. It provides a structured method for comparing architectural options based on their ability to meet dynamic data requirements, thus enabling informed investment decisions among OEMs, system integrators, and technology providers. The mapping of DPP attributes to IoT layers and BMS modules offers actionable insight into where and how traceability data should be captured and processed within real-world system architectures.

Importantly, the framework can help decision makers (particularly OEMs, system integrators, and solution providers) anticipate and evaluate trade-offs between competing technical priorities—such as latency, accuracy, storage, and interoperability—before system implementation. The envisioned evolution of the trade-off table into a multi-criteria decision-making tool further enhances its strategic value. By incorporating business value, service potential, and cost implications, the framework can support cross-functional decision-making that aligns technical feasibility with organizational goals.

More broadly, this research equips firms in the battery value chain with a foundation for interpreting and responding to future DPP-related mandates. As regulatory frameworks evolve, the insights and structure provided here can help stakeholders move from compliance as a burden toward compliance as an enabler of service innovation, market differentiation, and sustainable product lifecycle management.

8. Conclusion

This chapter provides the conclusion for this study and summarizes the answers to all the research questions proposed in the previous chapters. In addition, a reflection on the research process, as well as the link to the master's study program, will conclude this study.

8.1 Conclusion

This thesis began with a practical and timely challenge arising from new regulatory demands: the EU introduction of DPP for EV batteries, mandated under Regulation (EU) 2023/1542. While the regulation aims to promote sustainability, traceability, and circularity across the battery value chain, the path to implementation—particularly for dynamic, real-time data—remains technically ambiguous. To support early-stage system design under these evolving conditions, this research set out to answer the question:

"How can a suitable evaluation framework be developed to assess the potentials and challenges of IoT-driven Digital Product Passports for EV batteries?"

In response, the study focused on IoT as a key enabling technology. Given the central role of dynamic data—such as SoC, temperature, and SoH—for second-life applications, IoT offers the technical capabilities in existing BMS infrastructure to sense, process, and communicate these data points. However, a major gap remains in how to evaluate whether existing or proposed IoT architectures can effectively support DPP implementation. This thesis addresses that gap by developing a structured evaluation framework tailored to the specific demands of EV batteries and DPP compliance, specifically targeted at EV OEMs and solution providers.

The framework was developed using the DSR methodology inspired by the work of Hevner et al. (2004), combining insights from literature, technical standards (such as DIN DKE SPEC 99100), and industrial frameworks. Regulatory data requirements were first mapped to the specific layers of IoT architecture to identify where data originates, and which technical functions are critical. From this mapping, the core evaluation dimensions were derived, including several functions such as sensing accuracy, security, and lifecycle update. These dimensions became the foundation for the framework design process.

The resulting evaluation framework consists of two key components: an evaluation matrix and a trade-offs table. The matrix allows technical decision-makers—particularly within OEMs—to compare various IoT architecture profiles based on how well they meet operational and regulatory demands for DPPs. The trade-offs table complements this by revealing systemic interdependencies between dimensions, helping users understand how improving one function (e.g., real-time detection) might introduce new constraints elsewhere (e.g., storage capacity or energy efficiency). This approach ensures that the framework not only illustrates the required functionalities but also brings attention to technical considerations in system design. The framework was iteratively refined through expert interviews, which validated its conceptual logic and practical relevance. Feedback from stakeholders across academia, industry, and OEM contributed to a more refined framework that aligns more with real-world implementation and perspectives.

In conclusion, this thesis offers an evaluation framework—rooted in both policy requirements and technical feasibility—that can help bridge the gap between regulation and system architecture. By translating abstract goals into operational criteria, this research contributes to building a technical foundation for assessing the potential and challenges of IoT in DPP for EV batteries.

8.2 Reflection

During the research process, much time was spent understanding the evolving concept of DPP and how it applies specifically to EV batteries. The topic initially appeared to be centered on technical system design, but through further exploration, it became clear that the issue was far more layered, tied closely to regulatory interpretation, data infrastructure readiness, and decision-making within companies.

One of the challenges I encountered was framing the problem in a way that was both technically rigorous and strategically relevant. Because the concept of IoT-enabled DPPs is still emerging, it was difficult to find concrete case studies or implementation outcomes. This forced me to shift from expecting empirical clarity to focusing on conceptual clarity: breaking down regulatory texts, data attribute lists, and architectural assumptions into design dimensions that could structure future evaluations. Although much of the time was dedicated to literature analysis and framework design, I believe this was essential to develop a broader systems perspective and connect the abstract policy objectives with practical technical structures. What stood out to me throughout the research was how many decisions in technical architecture are influenced not only by hardware limitations or performance goals, but by assumptions around data governance, stakeholder priorities, and interoperability. It made me reflect on how difficult it is to align these dimensions in real industrial contexts, where incentives may not always support transparency or open integration. I also found myself repeatedly asking: how can you design something that is not only flexible for different contexts and use cases, but also robust enough for compliance?

Although the thesis is grounded in IT architecture and IoT evaluation, I came to realize that its true value lies in providing structure for dialogue between engineers, policymakers, and sustainability strategists. The design of the framework is not a technical solution, but a tool to help navigate uncertainties and trade-offs. It revealed to me that successful innovation in this space does not rely on perfect data systems or top-down enforcement, but on the ability to align architectures with evolving norms, shared standards, and long-term goals.

Looking back, this research process helped me appreciate the complexity of developing a solution for the purpose of sustainability and improving the condition of life as we know it. It deepened my understanding of how technical design can support—not dictate—system transformation also challenged me to think more holistically about the role of architecture as not only a structure but a mediator between what is technically possible, strategically desirable, and socially acceptable.

8.3 Link to Management of Technology

This thesis aligns with the MoT domain by exploring how emerging technologies—specifically IoT architectures—can support regulatory innovations like DPP. Positioned between technical design and strategic decision-making, the research reflects the multi-actor and system-level thinking central to the master's courses, such as Technology Dynamics (MOT113A), Research Methods (MOT141A), and I&C Architecture (SEN1611), which were instrumental in shaping the approach. In summary, the MoT program enabled a structured and interdisciplinary analysis of the challenges and opportunities surrounding IoT-driven DPP adoption in the EV sector.

Bibliography

Abdalla, A. (2024). *DPP user stories 2.0*. CIRPASS Consortium. https://cirpassproject.eu/wp-content/uploads/2024/04/DPP_User_Stories_V2.0_Final.pdf

Alkhabbas, F., Spalazzese, R., & Davidsson, P. (2019). Characterizing Internet of Things systems through taxonomies: A systematic mapping study. *Internet of Things, 7*, 100084. https://doi.org/10.1016/j.iot.2019.100084

Ahmid, M., Kazar, O., & Barka, E. (2024). Internet of Things overview: Architecture, technologies, application, and challenges. In W. Boulila et al. (Eds.), *Decision making and security risk management for IoT environments* (pp. 1–20). Springer. https://doi.org/10.1007/978-3-031-47590-0_1

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks, 54*(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast-evolving paradigm. *Ad Hoc Networks, 56*, 122–140. https://doi.org/10.1016/j.adhoc.2016.12.004

Baars, J., Domenech, T., Bleischwitz, R., Melin, H. E., & Heidrich, O. (2021). Circular economy strategies for electric vehicle batteries reduce reliance on raw materials. *Nature Sustainability, 4*(1), 71–79. https://doi.org/10.1038/s41893-020-00607-0

Bašić, F. (2023). *Enabling secure and wireless battery management systems* (Doctoral dissertation). Graz University of Technology.

Battery Pass Consortium. (2023). *Battery Pass project reports*. https://www.batterypass.eu

Battery Pass. (2024). *Battery passport value assessment 2024: Technical, economic and regulatory potential of digital product passports for EV batteries*. Battery Pass Consortium.

Berger, K., Baumgartner, R. J., Weinzerl, M., Bachler, J., Preston, K., & Schöggl, J.-P. (2023). Data requirements and availabilities for a digital battery passport: A value chain actor perspective. *Cleaner Production Letters, 4*, 100032. https://doi.org/10.1016/j.clpl.2023.100032

Berger, K., Baumgartner, R. J., & Weinzerl, M. (2023). Factors of digital product passport adoption to enable circular information flows along the battery value chain. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2023.05.087

Bocken, N. M. P., Short, S. W., Rana, P., & Evans, S. (2016). Product design and business model strategies for a circular economy. *Journal of Industrial and Production Engineering, 33*(5), 308–320. https://doi.org/10.1080/21681015.2016.1172124

Boell, S. K., & Cecez-Kecmanovic, D. (2015). On being "systematic" in literature reviews in IS. *Journal of Information Technology, 30*(2), 161–173. https://doi.org/10.1057/jit.2014.26

Brinkmann, S. (2014). *Interview*. In T. Teo (Ed.), Encyclopedia of Critical Psychology. Springer. https://doi.org/10.1007/978-1-4614-5583-7_161

Castelvecchi, D. (2021, August 19). Electric cars: The battery challenge. *Nature, 596*(7872), 336–339. https://doi.org/10.1038/d41586-021-02222-1

Cerruti, D., Filippini, M., & Savelsberg, J. (2024). *Adoption of battery electric vehicles: The role of government incentives and solar PV* (Policy brief). Centre for Energy Policy and Economics (CEPE), ETH Zurich. https://ethz.ch/content/dam/ethz/special-interest/mtec/cepe/.../Impact-Tax_EV-PV_Policy_Brief_Final.pdf

CIRPASS. (2024a). *CIRPASS_D2.2_DPP use cases report v2.0*. https://cirpassproject.eu/project-results/

CIRPASS. (2024b). *CIRPASS standardisation gaps and roadmap v1.2*. https://cirpassproject.eu/project-results/

CIRPASS 2 – User Stories. (2024). *CIRPASS 2 - User Stories 3.0*. CIRPASS-2 Consortium. https://doi.org/10.5281/zenodo.13902463

Corbin, J. M., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology, 13*(1), 3–21. https://doi.org/10.1007/BF00988593

da Silva, E. R., Lohmer, J., Rohla, M., & Angelis, J. (2023). Unleashing the circular economy in the electric vehicle battery supply chain: A case study on data sharing and blockchain potential. *Resources, Conservation & Recycling, 193*, 106969. https://doi.org/10.1016/j.resconrec.2023.106969

Dorsemaine, B., Gaulier, J.-P., Wary, J.-P., Kheir, N., & Urien, P. (2015). Internet of Things: A definition and taxonomy. In *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST)* (pp. 72–77). IEEE. https://doi.org/10.1109/NGMAST.2015.71

DIN DKE. (2023). *DIN DKE SPEC 99100: Digital battery passport data attribute list*. German Commission for Electrical, Electronic & Information Technologies.

Elkhodr, M., Shahrestani, S., & Cheung, H. (2016). The Internet of Things: New interoperability, management and security challenges. *International Journal of Network Security & Its Applications, 8*(2), 85–102. https://www.aircconline.com/ijnsa/V8N2/8216ijnsa06.pdf

Erhan, L., Ndubuaku, M., Di Mauro, M., Song, W., Chen, M., Fortino, G., Bagdasar, O., & Liotta, A. (2021). Smart anomaly detection in sensor systems: A multi-perspective review. *Information Fusion, 67*, 64–79. https://doi.org/10.1016/j.inffus.2020.10.001

Etikan, M., Alkassim, R. S., & Abubakar, S. M. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4. https://doi.org/10.11648/j.ajtas.20160501.11

European Blockchain Observatory and Forum. (2023). *Blockchain applications in the EU: Challenges and opportunities*. https://www.eublockchainforum.eu

European Commission. (2020). *A new circular economy action plan for a cleaner and more competitive Europe*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0098

European Commission. (2023). *Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries*. *Official Journal of the European Union*.

Fadzil Hassan, D. C., Tran, R., Akbar, I., Paputungan, V., & Khan, M. K. (2023). Improving latency in Internet of Things and cloud computing for real-time data transmission: A systematic literature review. *Cluster Computing, 26*, 2657–2680. https://doi.org/10.1007/s10586-021-03279-3

Faika, T., Kim, T., & Khan, M. (2024). An Internet of Things (IoT)-based network for dispersed and decentralized wireless battery management systems. In *Proceedings of the IEEE Conference*, Texas A&M University–Kingsville.

Ganzha, M., Paprzycki, M., Pawłowski, W., Szmeja, P., & Wasielewska, K. (2017). Semantic interoperability in the Internet of Things: An overview from the INTER-IoT perspective. *Journal of Network and Computer Applications, 81*, 111–124. https://doi.org/10.1016/j.jnca.2016.08.007

Garrido-Hidalgo, C., Ramirez, F. J., Olivares, T., & Roda-Sanchez, L. (2020). The adoption of internet of things in a circular supply chain framework for the recovery of WEEE: The case of lithium-ion electric vehicle battery packs. *Waste Management, 103*, 32–44. https://doi.org/10.1016/j.wasman.2019.12.009

Geetha, K., Suprakash, R., & Lim, M. K. (2024). Digitalization in battery manufacturing: A systematic review and future research directions. *Journal of Cleaner Production*. (In press)

Global Battery Alliance. (2024). *Battery Passport 2024 pilots: Progress report*. https://www.globalbattery.org/media/publications/mvp/gba-bp-progressreport-v1rev2sm-002.pdf

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly, 37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

GS1 Europe. (2024). *GS1 standards enabling DPP*. https://gs1.eu/wp-content/uploads/2024/12/GS1-Standards-Enabling-DPP.pdf

Gupta, B. B., & Quamara, M. (2018). An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. *Concurrency and Computation: Practice and Experience, 31*(11), e4946. https://doi.org/10.1002/cpe.4946

Hannan, M. A., Lipu, M. S. H., Hussain, A., & Mohamed, A. (2017). A review of lithium-ion battery state of charge estimation and management system in electric vehicle applications: Challenges and recommendations. *Renewable and Sustainable Energy Reviews, 78*, 834–854. https://doi.org/10.1016/j.rser.2017.05.001

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

Industrial Internet Consortium. (2022). *IIRA overview and guidance*. https://www.iiconsortium.org/IIRA

International Organization for Standardization. (2006). *Environmental management — Life cycle assessment — Principles and framework* (ISO Standard No. 14040:2006).

Jara, A. J., Olivieri, A., Bocchi, Y., Jung, M., Kastner, W., & Skarmeta, A. (2014). Semantic web of things: An analysis of the application semantics for the IoT moving towards the IoT convergence. *International Journal of Web and Grid Services, 10*(2–3), 244–272. https://doi.org/10.1504/IJWGS.2014.060260

Jousse, A. (Ed.). (2024). *D3.4 DPP system roadmap (v2.0)*. CIRPASS Consortium. https://doi.org/10.5281/zenodo.11096973

Krishna, T. N. V., Prabhu Deva Kumar, S. V. S. V., Rao, S. S., & Chang, L. (2024). Powering the future: Advanced battery management systems (BMS) for electric vehicles. *Energies, 17*(14), 3360. https://doi.org/10.3390/en17143360

Kreković, D., Krivić, P., Podnar Žarko, I., Kušek, M., & Le-Phuoc, D. (2025). Reducing communication overhead in the IoT–edge–cloud continuum: A survey on protocols and data reduction strategies. *Internet of Things, 31*, 101553. https://doi.org/10.1016/j.iot.2025.101553

Langley, D. J., Rosca, E., & Angelopoulos, M. (2023). Orchestrating a smart circular economy: Guiding principles for digital product passports. *Journal of Business Research*. https://doi.org/10.1016/j.jbusres.2023.05.xxx

Laska, J. N., & Baraniuk, R. G. (2011). Regime change: Bit depth versus measurement rate in compressive sensing. *arXiv*. https://arxiv.org/abs/1110.3450

Le Gall, G., Montavont, N., & Papadopoulos, G. Z. (2022). IoT network management within the electric vehicle battery management system. *Journal of Signal Processing Systems, 94*, 27–44. https://doi.org/10.1007/s11265-021-01670-2

Li, H., Kaleem, M. B., Liu, Z., Wu, Y., Liu, W., & Huang, Z. (2023). IoB: Internet-of-batteries for electric vehicles – Architectures, opportunities, and challenges. *Green Energy & Intelligent Transportation, 2*(2), 100128. https://doi.org/10.1016/j.geits.2023.100128

Lin, S., Sedigh, S., & Miller, A. (2017). Industrial Internet Reference Architecture (IIRA) version 1.8. *Industrial Internet Consortium*.

Madani, S. S., Ziebert, C., & Marzband, M. (2023). Thermal behavior modeling of lithium-ion batteries: A comprehensive review. *Symmetry, 15*(8), 1597. https://doi.org/10.3390/sym15081597

Ma, S., Jiang, M., Tao, P., & Song, C. (2018). Temperature effect and thermal impact in lithium-ion batteries: A review. *Progress in Natural Science: Materials International, 28*(6), 653–666. https://doi.org/10.1016/j.pnsc.2018.11.002

Mulpuri, S. K., Sah, B., & Kumar, P. (2025). An intelligent battery management system (BMS) with end-edge-cloud connectivity: A perspective. *Sustainable Energy & Fuels*. https://doi.org/10.1039/D4SE01238K

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods*, 16(1), 1–13. https://doi.org/10.1177/1609406917733847

Orellana, C., Cereceda-Balic, F., Solar, M., & Astudillo, H. (2024). Enabling design of secure IoT systems with trade-off-aware architectural tactics. *Sensors, 24*(22), 7314. https://doi.org/10.3390/s24022314

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*, 42(5), 533–544. https://doi.org/10.1007/s10488-013-0528-y

Plattform Industrie 4.0. (2018). *Details of the asset administration shell*. https://www.plattform-i40.de

Rao, A., Gupta, H., Singh, P., Mittal, S., Singh, U., & Vishwakarma, D. K. (2024). Optimizing electric vehicle efficiency with real-time telemetry using machine learning. In *Proceedings of the 2024 10th International Conference on Mechatronics and Robotics Engineering (ICMRE)* (pp. 27–29). IEEE. https://doi.org/10.1109/ICMRE60776.2024.10532195

Rashid, S., & Malik, S. H. (2023). Transition from a linear to a circular economy. In S. A. Bandh, F. A. Malla, & A. T. Hoang (Eds.), *Renewable energy in circular economy* (pp. 1–18). Springer Cham. https://doi.org/10.1007/978-3-031-42220-1_1

Rothgang, S., Baumhöfer, T., van Hoek, H., Lange, T., De Doncker, R. W., & Sauer, D. U. (2015). Modular battery design for reliable, flexible and multi-technology energy storage systems. *Applied Energy, 137*, 931–939. https://doi.org/10.1016/j.apenergy.2014.06.069

Rufino, C. A., Riva Sanseverino, E., & Gallo, P. (2024). Towards a battery digital passport: Reviewing regulations and standards for second-life batteries. *Batteries*. https://doi.org/10.3390/batteries2024xxxx

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666

Savari, G. F., Krishnasamy, V., Sathik, J., Ali, Z. M., & Abdel Aleem, S. H. E. (2020). Internet of Things-based real-time electric vehicle load forecasting and charging station recommendation. *ISA Transactions, 97*, 431–447. https://doi.org/10.1016/j.isatra.2019.08.011

Schwab, K., Marcus, A., Oyola, J. R., Hoffman, W., & Luzi, M. (2011). *Personal data: The emergence of a new asset class*. World Economic Forum. https://www.weforum.org/reports/personal-data-emergence-new-asset-class

Schweichhart, K. (2016). *Reference Architecture Model Industrie 4.0 (RAMI 4.0)*. ZVEI–German Electrical and Electronic Manufacturers' Association.

Singh, M., Dubey, R. K., & Kumar, S. (2022). Vehicle telematics: An Internet of Things and Big Data approach. In A. A. Kumar, A. El-Mougy, & A. K. Sangaiah (Eds.), *Artificial intelligence and machine learning for EDGE computing* (pp. 235–254). Academic Press. https://doi.org/10.1016/B978-0-12-824054-0.00019-8

Su, X., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481–2501. https://doi.org/10.1007/s11276-014-0731-4

Teh, H. Y., Kempa-Liehr, A. W., & Wang, K. I. (2020). Sensor data quality: A systematic review. *Journal of Big Data, 7*, 11. https://doi.org/10.1186/s40537-020-0285-1

Transport & Environment. (2020). *Mission (almost) accomplished: Carmakers' performance towards their 2020 CO_2 targets*. https://www.transportenvironment.org/uploads/files/2020_10_TE_Car_CO2_report_final-1.pdf

Uusitalo, T., Karhu, M., Majaniemi, S., Kivikytö-Reponen, P., Hanski, J., & Vatanen, S. (2024). Digital product passports in circular economy: Case battery passport. In *Proceedings of Circular Economy Conference* (pp. 1–15). Springer. https://doi.org/10.1007/978-981-99-3818-6_13 van Nieuwenhuijze, H., et al. (2025). *D4.1 Reference architecture (v1.0)*. CIRPASS-2 Consortium. https://doi.org/10.5281/zenodo.15388412

Wahab, M. H. A., Anuar, N. I. M., Ambar, R., Baharum, A., Shanta, S., Sulaiman, M. S., Mohd Fauzi, S. S., & Hanafi, H. F. (2018). IoT-based battery monitoring system for electric vehicle. *International Journal of Engineering & Technology, 7*(4.31), 505–510. https://doi.org/10.14419/ijet.v7i4.31.25472

Wang, J., Zhu, K., & Hossain, E. (2021). Green Internet of Vehicles (IoV) in the 6G era: Toward sustainable vehicular communications and networking. *arXiv*. https://arxiv.org/abs/2108.11879

Wautelet, T., & Ayed, A.-C. (2024). Exploring possible digital product passport (DPP) use cases in battery, electronics and textile value chains (v2.0). *CIRPASS Consortium*. https://doi.org/10.5281/zenodo.10974901

Weiss, M., Patel, M. K., Junginger, M., & van Ruijven, B. J. (2023). Modeling the market penetration of battery electric vehicles: A global analysis. *arXiv*. https://arxiv.org/abs/2306.16152

Wenning, R., Papadakos, P., & Bernier, C. (2024). *DPP system architecture (version 1.9)*. CIRPASS Consortium. https://doi.org/10.5281/zenodo.12206138

World Commission on Environment and Development (WCED). (1987). *Our common future*. Oxford University Press.

Appendix A: Literature Review Strategy

Scope and Approach

The literature review aims to construct a comprehensive understanding of IoT architecture, DPP legal and technical requirements in the context of EV and battery. To achieve this, a systematic approach was employed, combining elements of structured keyword-driven searches with selected academic, technical, and industrial sources. This approach allows this study to establish a knowledge foundation for the design of artifacts in the later stage.

The review covers several interrelated knowledge areas: (1) the conceptual and architectural foundations of IoT, including classifications, taxonomies, and reference models; and (2) use cases and integration of IoT technologies within electric mobility ecosystems, particularly in battery lifecycle tracking and smart vehicles. By bridging these domains, the literature review helps solidify the logic of using IoT as a system that can shape the design and operation of DPP in the EV battery domain. Special attention was given to works that represent industrial IoT architectures—such as RAMI 4.0 and IIRA—as these reference frameworks offer structured insights into component roles, interoperability requirements, and implementation patterns per industry. In parallel, application-oriented studies focusing on EVs and digital product passports were reviewed to understand how abstract architectural principles translate into operational value with the support of an AI tool for structure suggestion and image cover generation.

Research methodology

The literature search was conducted across established academic and scientific repositories known for their extensive coverage in engineering, information systems, and technology management. The following databases were used:

Search Platform	Purpose
Scopus	Broad, multidisciplinary search engine for empirical studies, use-case evaluations, and technical frameworks
IEEE Explore	For searching technical papers, standards for IoT infrastructure, communication technologies, and related systems.
SpringerLink	For access to journals and books in applied sciences and engineering
Google Scholar	Complementary sources to view grey and recent academic papers
Other industrial, regulatory organizations, projects, and standards	For up-to-date industrial knowledge, standards, and insights (e.g.: RAMI, IIRA, CIRPASS, Battery Pass)

Table 14: Overview of literature search engines

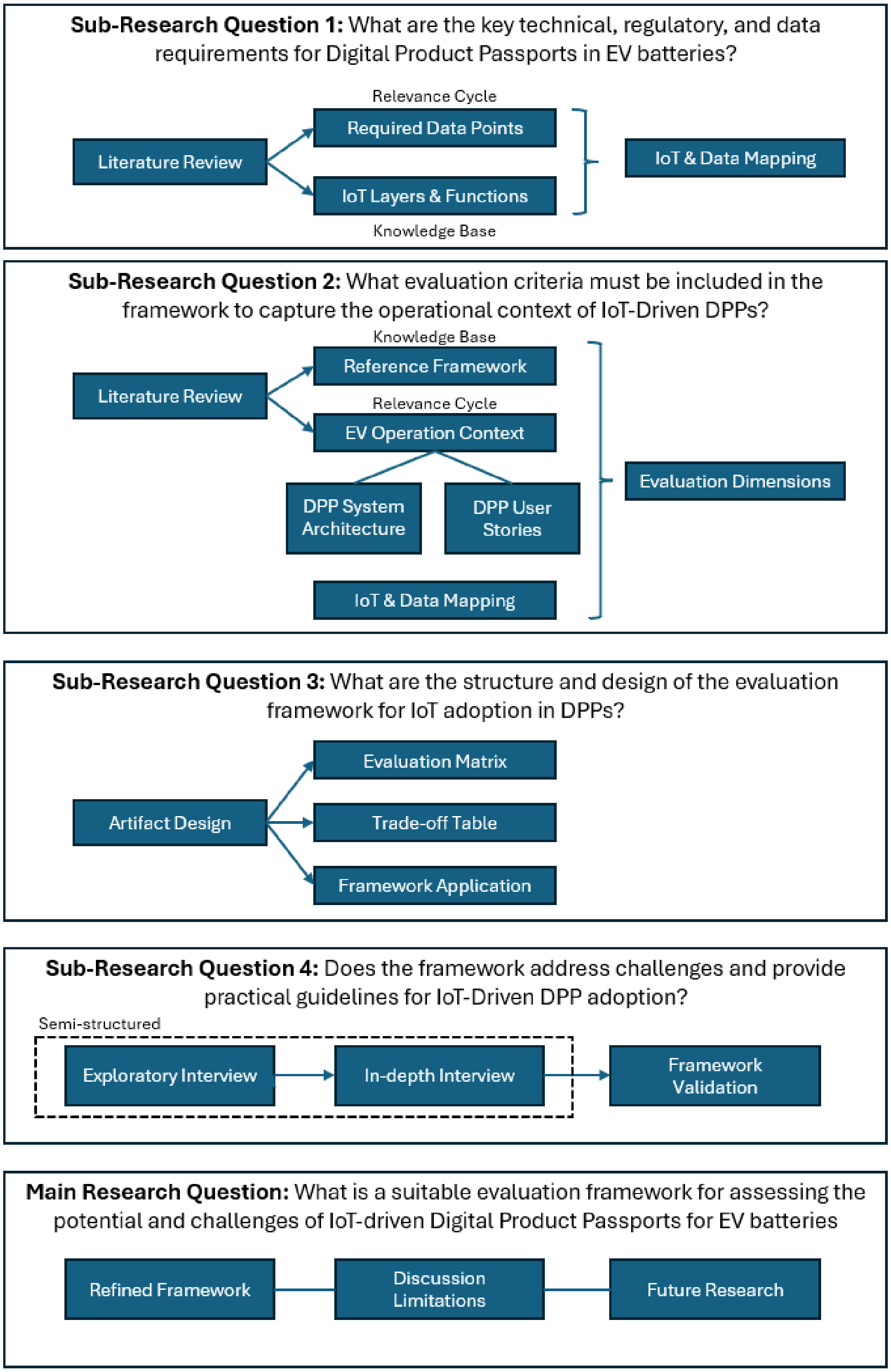
Initial searches were conducted with a general set of domain-specific keywords such as “IoT”, “DPP”, and “EV battery”, but the results yielded too many fragmented articles in various contexts. In the second round of search, Boolean operators (AND, OR) were applied along with more specific key terms such as “architecture”, “taxonomy”, “literature review”, “classification”, and “applications”. This time, the search returned more relevant articles for IoT and EV battery themes but much less for DPP domains. Therefore, more adjustments and specific keywords were included to ensure that the specificity and volume of the results remained manageable and relevant. The table below illustrates the key terms used for narrowing the scope.

Key words	**Example search strings**
System architecture	“IoT” & “System architecture” OR “Literature review”
Reference framework	“IoT” OR “EV” OR “DPP” & “Reference framework”
Reference architecture	“IoT” OR “EV” & “Reference architecture”
Use Case Scenario	“DPP” OR “IOT” & “Use Case Scenario”
Value chain	“EV” OR “Battery” & “Value chain”
Adoption/Application	“DPP” OR “IOT” AND “Adoption”
DPP	“DPP” and “Battery” OR “IoT” OR “Framework”

Table 15: Overview of Keywords and Search strings

Once the search was completed, the first selection process began, starting with English as the preferred language. At this stage, duplicate records retrieved from multiple databases were removed manually to avoid redundancy. Next, publication years were considered as the second selection criterion. Due to the importance of up-to-date information to have relevance, for this study, only literatures from 2015 or later are included. The second phase involved a screening of titles and abstracts to assess preliminary relevance to the research topic. Literature is considered to be relevant if it discusses one of the main themes (IoT, DPP, and EV battery) with any of the keywords shown in the previous table. In total, 12 articles were included for IoT domains, and 6 other documents from consortium projects, industrial standards were added for the reference framework and DPP-related themes.

Appendix B: Research Diagram



Appendix C: Interview Protocols

Introduction

A. Interviewee Background

1. Can you introduce yourself and your background and knowledge domain?
2. What are your responsibilities at your current job role?

B. Core Concepts of this study

1. Are you familiar with the main concepts of this study, including DPP, IoT, and EV/BMS?
2. Do you have any relevant experience with these three domains?
3. Regarding the choice of IoT for DPP in this study, does the logic make sense when applied to the EV batteries case?
4. Do you have any further feedback or questions about the introduced concepts?

C. EV Operational Contexts

During the first phase of the interview, I would like to present to you the DPP in EV operational contexts. In other words, a running example/concept of how IoT, DPP, and EV work together in normal operation conditions. For example, consumers drive their EV to work, and during the process, how the DPP required data is generated, processed, logged, and transferred to stay compliant with regulatory demands, and which IoT layer is responsible for each step in the process.

1. To what extent do you see this EV operational context align with the DPP and IoT functions introduced?
2. What are some considerations, distinction that needs to be clearer from your perspective?

D. Building the framework: Step 1: Mapping Data requirements

The next steps in this study will be built upon this operational context. The following questions will cover the first step of looking into the DPP data requirements, starting with the mapping of required data points and the IoT layers responsible for collecting and processing the data.

1. Do you agree with the logic of this mapping of IoT layers?
2. In your view, which data attributes are most critical for a compliant DPP?
3. Does the calculation of these processed attributes (SoC, SOCE, No. of Charge/Discharge Cycles at the Middleware) match what is normally seen in industrial/academic practices?
4. Are there any considerations or modifications needed for these data points mapping?

E. Building the framework: Step 2: Evaluation Dimensions

After the mapping between the required data points and the responsible IoT layers, the second step begins with translating these data requirements into required system technical functions. From the operational context introduced earlier, the DPP User Stories and System Architecture documents gathered from EU-funded initiatives, the following evaluation dimensions (or so-called required technical functions) are formed as listed in the table. These dimensions include: 1. Voltage/Temperature Sensing accuracy; 2. Real-time event detection; 3. Edge storage buffering; 4. Latency to Cloud; 5. Data format compatibility.

1. Does the logic of combining the operation, user stories, and system architecture to create evaluation dimensions make sense?
2. Does this list of dimensions cover the operational needs of DPP and EV, as explained earlier?
3. What are some of the most important dimensions here from your perspective?
4. From the list of dimensions, would you like to propose any changes to this list? Can you also explain why as well?

F. Building the framework: Step 3: Evaluation Matrix & Trade-off Table

From the list of evaluation dimensions, the evaluation matrix is created with the purpose of comparing available options at hand for EV OEMs' decision-makers. The architecture profiles provided as examples in the evaluation matrix are constructed from academic papers, journals, and dissertations, due to a lack of publicly available industrial data.

1. In which contexts do you see a good application of this framework?
2. Does the evaluation matrix highlight the strengths, weaknesses, and key features of these sample profiles?
3. Can you provide some suggestions for improvement in this evaluation matrix?

Another indispensable component of this framework is the trade-off table, to be used in combination with the evaluation matrix. Acknowledging the fact that these dimensions do not operate separately but rather depend on each other, the trade-off table illustrates this logic by summarizing how technical changes in one dimension can affect the others.

1. To what extent does this table capture the key trade-offs between dimensions as seen in industrial contexts?
2. Can you list out from the table some of the most important and commonly seen trade-offs in real-world system design?
3. How can this framework improve its readability and applicability in industrial contexts?
4. What can be the next potential developments/steps for this framework?

G. Additional questions

These questions will be asked if time allows during the interviews, or they can also be used to trigger more answers from participants in one of the previous sections.

1. Which general improvements are needed to make this more applicable in industrial contexts?
2. Are there any other relevant aspects that we have not considered but can be important to this study?

Appendix D: Creating Evaluation Dimensions

The table below illustrates how the Evaluation Dimensions, in other words, the required technical functions to stay compliant with the DPP concept, are formed from the DPP User Stories, data attributes, IoT Layers, and the logic behind such grouping.

Evaluation Dimension	Affected Attributes	Justification / Grouping Logic	DPP User Story / Operation Scenario	IoT Layer(s)
1.Voltage/Temperature Sensing Accuracy	Temperature, SoC, Remaining capacity, Remaining usable energy, Power capability, No. of full charge/discharge cycle, No. Deep discharge, No. Overcharge, SOCE, Remaining Power Capability	Groups attributes dependent on precise sensor readings and signal processing.	*Post-diagnostics update by REO technician*	Perception, Middleware
2.Real-Time Event Detection	SoC, Remaining capacity, Remaining usable energy, Power capability, No. of full charge/discharge cycle, No. Deep discharge, No. Overcharge, SOCE, Remaining Power Capability	Groups attributes requiring threshold detection and edge processing logic.	*Onboard detection of critical safety events triggering system-level alerts*	Middleware
3.Edge Storage Buffering (Offline Mode)	All operational data points (e.g., SoC history, temperature logs, event records)	Attributes that must persist during offline states, requiring buffering and local memory.	*Writing into the DPP with the original REO's authorization*	Middleware
4.Latency to Cloud	All required/mandatory data points (e.g: SoC, SOCE, Event logs, Temperature)	Attributes that require rapid transmission to enable timely decisions by authorities or services.	*Customs querying battery status at border*	Middleware, Network
5.Data Format Compatibility	All required data points	Attributes needing standardized semantic formats	*NGOs and external platforms querying metrics*	Middleware, Application

		(e.g., JSON-LD) for multi-stakeholder interoperability.		
6.Secure Message Authentication	Diagnostics results, Lifecycle status, SoC updates	Groups sensitive attributes requiring cryptographic signing or trusted origin verification.	*Writing into the DPP with REO authorization*	Perception Middleware Application
7.Lifecycle Update	Ownership, Location, Certification state, Post-refurbishment condition	Attributes whose values evolve over time and need updates at resolvable, versioned URI endpoints.	*Transferring the responsibility for a product*	Application, Network
8.Stakeholder-Specific Access Controls	All sensitive or competitive data (e.g., SoC, thermal logs, product identifiers, UID)	Attributes needing differentiated read/write privileges across actors (e.g., OEMs, recyclers, public authorities).	*Reading with default or restricted access*	Application

Appendix E: Key Trade-offs from Expert Interviews

Trade-off Problem	Description	Expert Insights	System Design Implications
Sensing Accuracy vs. Event Detection & Edge Storage	Improving sensing accuracy through higher-resolution sensors or faster sampling enhances the detection of safety-critical events like thermal runaway or abnormal discharges. However, it substantially increases the volume of data to be stored and processed locally, placing higher demands on edge devices and raising risks of data bottlenecks or system lag.	- Interviewee 1.1 emphasized logging overload if fault codes are too granular. - Interviewee 1.2 highlighted that while detection improves, storage constraints emerge. - Interviewee 2.4 warned that high-resolution sensors add cost and power consumption burdens.	System designers must calibrate sensor fidelity based on available edge resources and prioritize event types most critical to lifecycle management.
Edge Processing vs. Latency to Cloud	Offloading data processing to edge devices enables fast, local decision-making without relying on cloud connectivity, which is ideal for safety-related metrics. However, it requires more powerful processors, higher energy consumption, and complex firmware management, increasing system cost and hardware requirements.	- Interviewee 2.5 and 2.1 endorsed edge analytics for safety functions. - Interviewee 2.4 recommended hybrid strategies, combining edge for immediacy and cloud for lifecycle analytics. - Interviewee 2.7 noted system stability depends on proper allocation of logic.	A hybrid approach is recommended, where safety functions are handled locally and less urgent analytics are deferred to cloud-based systems.
Lifecycle Update vs. Security & Access Control	To enable lifecycle updates, DPPs must allow for data entries to be modified across the battery's use phase. However, this flexibility introduces vulnerabilities such as unauthorized edits, tampering, or version modification unless robust access control, cryptographic verification, and version logging are in place.	- Interviewee 1.1 and 2.5 argued for role-based access protocols. - Interviewee 2.4 called for verifiable update mechanisms tied to stakeholder roles. - Interviewee 2.8 suggested merging authentication and access into a unified security layer for lifecycle robustness.	Lifecycle update mechanisms must be integrated with cryptographic verification and strict, role-based permissioning to ensure data trustworthiness.
Data Format Compatibility vs.	Standardizing data formats supports interoperability between OEMs, recyclers, and regulators. Yet, strict formats may strip away proprietary metadata or granularity, reducing OEM's ability to perform	- Interviewee 2.6 observed that semantic layering is crucial for startups adopting common interfaces.	Architectures may need to support both base-level standard compliance and OEM-specific

Data Richness & Control	advanced analytics or differentiate through enriched data services.	- Interviewee 2.2 explained large OEMs avoid standard formats to retain analytical control.	semantic extensions to satisfy regulatory and strategic needs.
Event Detection vs. System Complexity & Cost	Implementing real-time event detection requires frequent condition monitoring and logic execution, increasing the computational burden on embedded systems. This in turn leads to higher-cost MCUs, extended firmware validation, and more complex software development lifecycles.	- Interviewee 2.2 noted that high-frequency monitoring strains firmware and requires costly processors - Interviewee 1.2 added that validation efforts rise exponentially with processing power. This is particularly relevant in mid-range EVs where BOM cost is tightly managed.	OEMs must align real-time logic capabilities with budget, hardware availability, and product lifecycle timelines, especially for mid-market EVs.
Secure Authentication vs. Usability & Latency	Robust authentication mechanisms (e.g., multi-factor, cryptographic signatures) are essential for secure communication but can increase latency and reduce usability, especially for stakeholders with limited IT capacity, such as small repair shops or informal second-life operators.	- Interviewee 1.1 raised usability concerns for downstream actors like independent garages. - Interviewee 2.8 emphasized context-sensitive security as a way to protect data while maintaining access for varied stakeholders with differing capacities.	Security models should be tiered or context-sensitive, enabling broader participation while preserving essential protection for critical operations.
Standardization vs. Stakeholder-Specific Needs	Industry-wide standards aim to unify data exchange, but they may conflict with legacy OEM systems or internal BMS architectures. Forced alignment can lead to system inefficiencies, loss of customization, or require costly translation layers.	- Interviewee 2.6 highlighted that startups benefit from standards for faster integration, while interviewee 2.2 emphasized OEM’s need to maintain control. Both suggested that flexible or modular standards are needed to resolve this tension.	Standard-setting bodies should promote flexible, modular standards that support translation/adaptation for diverse legacy system architectures.

The four key trade-offs that were most discussed are summarized as follows:

1. **Sensing Accuracy vs. Real-Time Event Detection & Edge Storage**

This trade-off was the most consistently and deeply discussed across interviews, seen as a foundation-level tension in IoT system design. Many experts emphasized that improvements in sensing accuracy—measured by sampling frequency, resolution, and stability—enhance the performance of real-time event detection systems. As interviewee 1.2 noted, "Better input leads to better flags," referring to the way high-frequency voltage or temperature data allows for faster, more sensitive identification of operational anomalies or fault conditions. However, multiple interviewees also raised the compounding downstream effects of increasing data fidelity. Interviewee 2.2 cautioned that higher-resolution data exponentially increases storage requirements, putting pressure on edge storage units that must buffer large volumes of data before upload. Interviewee 1.1 reinforced this view, adding that increased logging not only affects buffer size but also the organization and retrievability of data, especially in systems that group fault or event logs under codes. Similarly, interviewee 2.4 pushed this point further by linking it to hardware-level trade-offs, arguing that sampling accuracy often correlates with higher power draw, increased thermal load, and more expensive sensors—which can become a bottleneck in cost-sensitive EV markets.

2. **Edge – Cloud Continuum**

Another key trade-off highlighted by experts involved the distribution of computation across the architecture. While real-time analytics can be performed locally (edge processing) or remotely (cloud processing), several experts noted that a system's choice between these options reflects deeper design trade-offs between responsiveness, bandwidth, cost, and complexity. Interviewee 2.5 explained that middleware-level logic, such as SoH and SoC estimation, often depends on processing that may either reside on the vehicle or in the cloud, depending on system constraints. Another expert emphasized that investing in local edge intelligence—such as processors embedded in BMS units—can dramatically reduce reliance on low-latency network connections, which may be unstable or unavailable in certain geographies. However, such investment requires higher-capacity, more expensive hardware and introduces firmware maintenance complexity.

Interviewee 2.4 supported this view from an EV OEM perspective, noting that while cloud solutions benefit from scalability and advanced analytics, they are vulnerable to latency bottlenecks, synchronization errors, and data transmission costs. He stressed that edge processing is more practical for safety-critical metrics, such as SoC, which must be updated in real time and are required for battery control, making remote computation impractical. However, for lifecycle-level metrics or fleet-wide learning algorithms, cloud processing is more suitable for providing more complex analytics by through different cross-vehicle datasets. Interviewee 2.7 echoed this layered view, stating that while edge and cloud functions may seem dichotomous, in practice, hybrid architectures are the most realistic, blending immediate processing with periodic cloud uploads, and the trade-off lies in how to allocate computational load effectively across time and function.

3. **Real-Time Event Detection vs. System Cost and Complexity**

Several experts emphasized that while real-time event detection is critical for enabling responsive diagnostics, fault prevention, and safety assurance, it comes with non-trivial cost and system complexity implications. Interviewee 2.2 noted that increasing the sensitivity or frequency of event detection logic inevitably requires more frequent data processing and condition-checking routines, which places added pressure on embedded processors. Interviewee 1.2 similarly remarked that while OEMs desire fine-grained event detection (e.g., thermal spikes, abnormal discharges), they often underestimate the firmware engineering and computing overhead required to support this at scale.

From an implementation standpoint, these demands may necessitate more capable MCUs, larger memory buffers, and custom firmware, each contributing to increased component cost and longer validation cycles. Interviewee 2.4 put a great stress on this concern, warning that real-time systems, if over-engineered, can incur both financial and energy overhead, reducing the efficiency gains they intend to deliver. Therefore, this trade-off becomes most acute when designing for constrained environments or cost-sensitive vehicle segments, where a balance must be struck between system reactivity and overall design feasibility.

4. Standardization vs. Stakeholder-Specific Needs

The interviews also revealed a significant tension between the drive for system-wide standardization—often led by regulatory or industry bodies—and the unique needs and constraints of individual stakeholders, particularly OEMs and suppliers. Interviewee 1.2 and 2.2 both observed that while standardized data formats and architecture layers improve interoperability, many large OEMs prefer to maintain proprietary data structures and internal standards, as part of their broader strategy for product control and service monetization. This introduces a trade-off: adopting common standards may ease compliance and facilitate integration, but it also risks disrupting optimized legacy systems or reducing flexibility in data handling.

Interviewee 2.6 expanded on this by pointing out that smaller, newer market entrants are often more willing to adopt standardized solutions due to lower legacy burden and tighter integration budgets. In contrast, established OEMs may resist top-down standardization, preferring instead to use semantic layers or API-based translation modules to meet external format requirements while preserving internal system autonomy. The trade-off here lies in balancing regulatory alignment and cross-compatibility with local optimization and innovation, a challenge that DPP system designers must confront across the supply chain.

Appendix F: Insights Mappings from Analysis

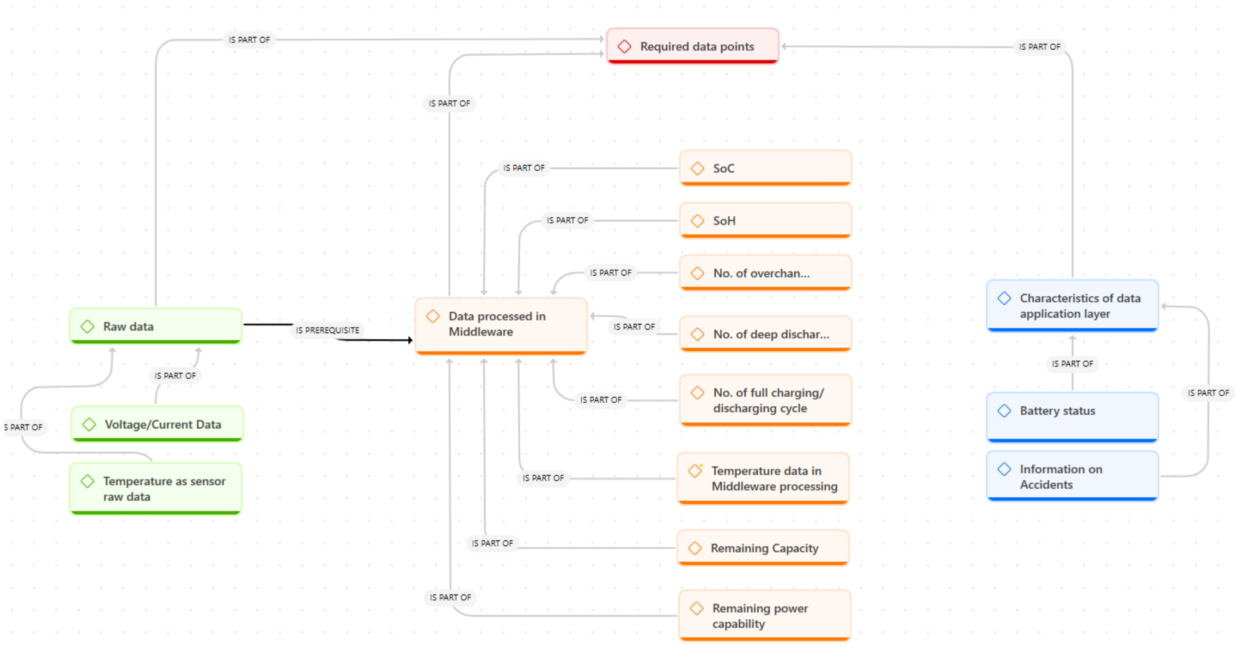


Figure 13: Overview of Required data points

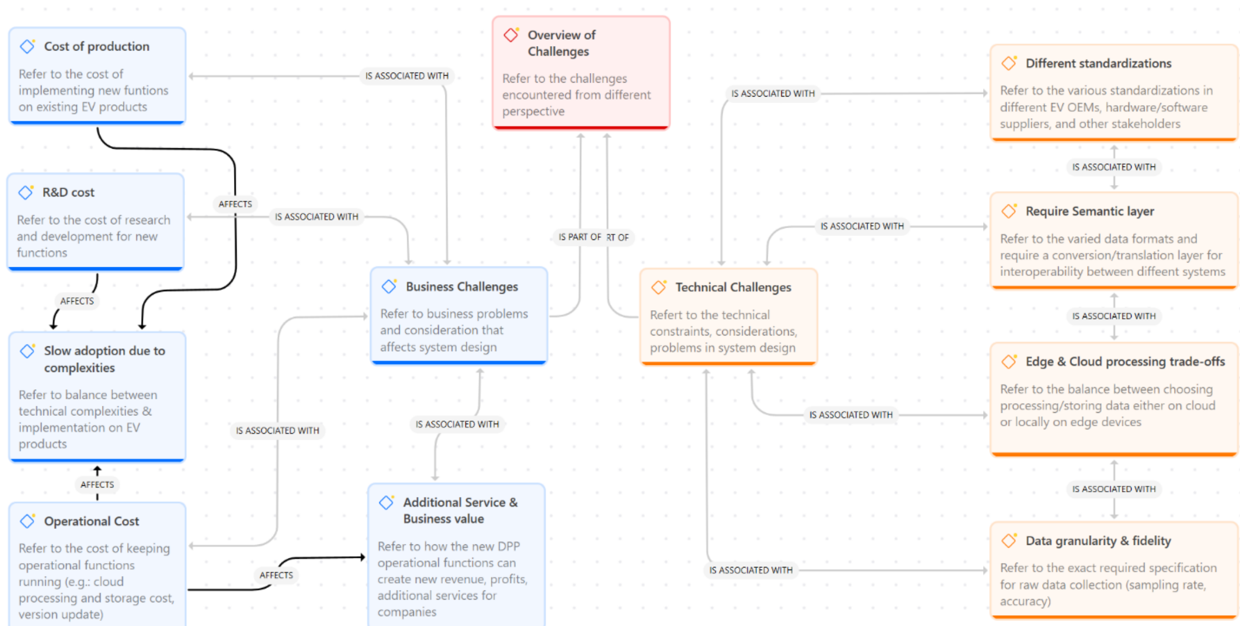


Figure 14: Overview of Challenges from expert interviews

Appendix G: Codebook for Thematic Analysis

Code Group	Codes	Density	Grounded
Business Services & Values & Implications	○ Additional Services / Business Values	2	6
Business Services & Values & Implications	○ Business Challenges	0	5
Business Services & Values & Implications	○ Business functions perspective	1	4
Business Services & Values & Implications	○ Compliance with regulatory requirements	1	1
Business Services & Values & Implications	○ Consumer data access	1	1
Business Services & Values & Implications	○ Cost of Production	1	2
Business Services & Values & Implications	○ Customer demands	2	1
Business Services & Values & Implications	○ Cut operation cost	1	0
Business Services & Values & Implications	○ Low cost	1	0
Business Services & Values & Implications	○ More product transparency from additional data access	1	1
Business Services & Values & Implications	○ Operational Cost	1	2
Business Services & Values & Implications	○ Reduce cost of services	1	1
Business Services & Values & Implications	○ Translate data to functionalities	1	1
Business Services & Values & Implications	○ Translate technical to business needs	4	1
Business Services & Values & Implications	○ Link between technical and business contexts	5	0
Business Services & Values & Implications	○ Control over their systems/products	2	1
Business Services & Values & Implications	○ Data analytics for improving performance	1	2
Business Services & Values & Implications	○ New competitors in the market	1	0
Business Services & Values & Implications	○ Slow adoption due to complexities	2	6
Business Services & Values & Implications	○ Dependency on external infrastructure	2	2
Business Services & Values & Implications	○ Industry-wide standards	2	0
Business Services & Values & Implications	○ R&D cost	2	2

Business Services & Values & Implications	○ Edge-Cloud trade-offs	1	2
Business Services & Values & Implications	○ Reduce complexity for interoperability	1	1
Business Services & Values & Implications	○ High cost	1	0
Business Services & Values & Implications	○ History logs, lifecycle events, usage pattern	2	2
Data & Functional requirements	○ Analyze raw data	1	1
Data & Functional requirements	○ Battery status	5	0
Data & Functional requirements	○ Data origin	3	0
Data & Functional requirements	○ DPP User stories	1	0
Data & Functional requirements	○ Mapping IoT and Data points	7	0
Data & Functional requirements	○ No. of deep discharge events	1	1
Data & Functional requirements	○ No. of overchange events	1	1
Data & Functional requirements	○ Prevent unlogged data	1	1
Data & Functional requirements	○ Raw data	3	3
Data & Functional requirements	○ Remaining Capacity	1	2
Data & Functional requirements	○ Remaining power capability	1	2
Data & Functional requirements	○ Required data points	4	0
Data & Functional requirements	○ SoC	2	1
Data & Functional requirements	○ SoH	2	1
Data & Functional requirements	○ Starting with data requirements	5	0
Data & Functional requirements	○ Subjective mapping	3	0
Framework logic & application	○ Accommodate different usage contexts	1	1
Framework logic & application	○ Benchmark guideline	2	1
Framework logic & application	○ Check for variations in expert opinions	1	1
Framework logic & application	○ Clear content explanation	3	0
Framework logic & application	○ Consolidate framework argument and logic	2	0

Framework logic & application	● Framework applicability	8	7
Framework logic & application	○ Framework flexibility	1	0
Framework logic & application	○ Framework guideline	1	1
Framework logic & application	● Framework improvement	13	7
Framework logic & application	○ Framework logic	5	4
Framework logic & application	○ Framework storyline	4	0
Framework logic & application	○ Improve applicability	4	0
Framework logic & application	○ Improve for better intuitive comprehension	1	1
Framework logic & application	○ Non-experts/Wider audiences	4	0
Framework logic & application	○ Options for decision makers	1	0
Framework logic & application	○ Provide circularity values	1	1
Framework logic & application	○ Quantitative approach for scoring	3	0
Framework logic & application	○ Reduce complexities	1	0
Framework logic & application	○ Require stronger argumentation	1	1
Framework logic & application	○ Scoring guideline	6	1
Framework logic & application	○ Summary with conclusion for each profile	1	1
Framework logic & application	○ Use for comparison of missing functions	4	0
Framework logic & application	○ Various setting	1	2
Industrial/Business/Legal Insights	○ Different standardizations	3	3
Industrial/Business/Legal Insights	○ Legal perspective for core dimensions	3	1
Industrial/Business/Legal Insights	○ Similar structure	3	0
Industrial/Business/Legal Insights	○ Similar to a current industrial trial project	1	0
Industrial/Business/Legal Insights	○ Specifications & Requirements change overtime	1	1
Industrial/Business/Legal Insights	○ Byproduct of raw data	3	1
Industrial/Business/Legal Insights	○ Fault log is not significantly higher with sensor accuracy	1	2

Industrial/Business/Legal Insights	○ Security as major concerns for stakeholders	1	1
IoT Components	○ Application layer	4	0
IoT Components	○ Characteristics of application layer	1	6
IoT Components	○ Handle high logic & calculations	1	2
IoT Components	○ IoT layers	2	0
IoT Components	○ Low relevant for IoT	1	1
IoT Components	○ Middleware	5	0
IoT Components	○ Network module	1	0
IoT Components	○ Perception	2	0
IoT Components	○ Physical device	1	1
Operation considerations & Potential solutions	○ Cloud analytics	1	1
Operation considerations & Potential solutions	○ Cloud-dependent system	4	1
Operation considerations & Potential solutions	○ Computing power	3	2
Operation considerations & Potential solutions	○ Constant update	1	1
Operation considerations & Potential solutions	○ Data analytics	2	7
Operation considerations & Potential solutions	○ Data fidelity	3	0
Operation considerations & Potential solutions	○ Data granularity & fidelity	2	2
Operation considerations & Potential solutions	○ High fidelity	1	0
Operation considerations & Potential solutions	○ High fidelity sensors	2	0
Operation considerations & Potential solutions	○ Overview of challenges	1	2
Operation considerations & Potential solutions	○ Questions for Data format compatibility	2	1
Operation considerations & Potential solutions	○ Required operation dimensions	1	1
Operation considerations & Potential solutions	○ Response rate	1	2
Operation considerations & Potential solutions	○ Semantic layer applied in Middleware	1	3
Operation considerations & Potential solutions	○ Technical challenges	1	5
Operation considerations & Potential solutions	○ Technical specifications	3	0
Operation considerations & Potential solutions	○ Preferred/Required Semantic layers	1	3

Operation considerations & Potential solutions	○ Require higher calculation than middleware	1	0
Operational Dimensions	○ Combine to create Communication	2	1
Operational Dimensions	○ Combined functions	1	0
Operational Dimensions	○ Complementary dimensions	1	2
Operational Dimensions	○ Core dimensions for operation	4	3
Operational Dimensions	○ Create Security dimension	4	3
Operational Dimensions	○ Data Format	10	5
Operational Dimensions	○ Edge calculation	4	2
Operational Dimensions	○ Edge Storage	14	7
Operational Dimensions	○ High priority	6	0
Operational Dimensions	○ Interoperability	1	1
Operational Dimensions	○ Latency to Cloud	15	7
Operational Dimensions	○ Lifecycle information dimension	2	3
Operational Dimensions	○ Live connection not required	2	1
Operational Dimensions	○ Must-have feature	4	0
Operational Dimensions	○ Network latency is not of high importance	2	1
Operational Dimensions	○ Optional dimensions	6	1
Operational Dimensions	○ Physical layer security	1	1
Operational Dimensions	○ Real-time event detection	9	10
Operational Dimensions	○ Secure authentication	8	1
Operational Dimensions	○ Security dimension	9	3
Operational Dimensions	○ Sub-categories of Security	5	3
Operational Dimensions	○ Voltage/Temperature sensing accuracy	7	4
Operational Dimensions	○ Ability to update relevant stakeholders	2	1
Operational Dimensions	○ List of evaluation dimensions	3	0
Operational Dimensions	○ Semantic layer	3	2
Operational Dimensions	○ Stakeholder Access	8	1
Operational Dimensions	○ Support data extract & exchange	4	4
Operational Dimensions	○ Data processed in Middleware	5	10
Operational Dimensions	○ Lifecycle update	3	6
Operational Dimensions	○ Data analytics in middleware	1	2
Operational Dimensions	○ Operational context	5	1
Solution Assessment	○ Advanced options	1	0
Solution Assessment	○ Profile 2 as a more advanced option	1	0
Solution Assessment	○ Similar to industrial approaches	4	0
Solution Assessment	○ Simplify for better comprehension	3	1
Solution Assessment	○ Tailor to different contexts	2	1
System Design & Trade-off	○ Capture key trade-offs between dimensions	3	0
System Design & Trade-off	○ High Complexities	5	0
System Design & Trade-off	○ Overview of standardizations and alternatives	1	0

System Design & Trade-off	○ Select relevant metrics	2	1
System Design & Trade-off	○ Cost of trade-offs	1	1
System Design & Trade-off	○ BMS mapping	2	1
System Design & Trade-off	○ Clear logic for comparison	4	0
System Design & Trade-off	○ Balance between parameters	1	2
System Design & Trade-off	○ Dimension Relationship	2	0
System Design & Trade-off	○ Module management	1	0
System Design & Trade-off	○ Others dimension thresholds will be dependent	1	1
System Design & Trade-off	○ Overloading, prolonged queuing	2	3
System Design & Trade-off	○ System conditions & constraints	2	0
System Design & Trade-off	○ Affect other functions/dimensions	1	0
System Design & Trade-off	○ Profile comparison	6	0
System Design & Trade-off	○ Factor for selecting solution	1	2
System Design & Trade-off Technical insights & discussions	○ Select technical thresholds	1	2
Technical insights & discussions	○ Data processed in multiple layers	7	2
Technical insights & discussions	○ Device in multiple IoT layers	2	1
Technical insights & discussions	○ Fault Logging and Event detecting systems	1	2
Technical insights & discussions	○ Focus on add-on functions	1	0
Technical insights & discussions	○ Group of Fault Codes	2	0
Technical insights & discussions	○ Increase accuracy from multiple perspectives	1	0
Technical insights & discussions	○ Prefer standardization	1	1
Technical insights & discussions	○ Preferred by technical experts	3	0
Technical insights & discussions	○ Temperature as sensor raw data	4	2
Technical insights & discussions	○ Temperature data in Middleware processing	2	2

Technical insights & discussions	○ Validate with other experts	3	1
Technical insights & discussions	○ Variation in technical details	1	5