

Designing Error-Resilient Human-in-the-Loop Interfaces for Battery Passport Compliance

Dogan Efe, Elena Andrushchenko, Muhammad Muneeb Riaz, and Roland Jochem

Technical University of Berlin, Chair of Quality Science, Pascalstr. 8-9, 10587 Berlin, Germany

ABSTRACT

The implementation of the Digital Product Passport (DPP) mandated by the EU Battery Regulation (EU 2023/1542) requires the precise recording and continuous updating of technical and lifecycle data for batteries. While large manufacturers typically rely on automated machine-to-machine (M2M) interfaces, small and medium-sized enterprises (SMEs), including both producers placing batteries on the market and downstream actors involved in activities such as repair, repurposing, and dismantling, are more likely to depend on manual data entry to maintain passport records. These environments, characterized by heterogeneous processes, and varying levels of digital literacy, the risk of human error is substantial and directly affects regulatory compliance and operational safety. This paper investigates how data quality can be ensured in manual Human-in-the-Loop processes within the DPP ecosystem. Building on established taxonomies of human error that differentiate between execution slips and knowledge-based mistakes, it applies a multi-layered validation framework for DPP user interfaces. The framework introduces design principles for error-resilient data entry that extend beyond basic syntactic checks to include semantic plausibility controls, for example, cross-validating mass, chemistry, and application type as well as context-aware constraints tailored to specific lifecycle stages.

Keywords: Digital product passport (DPP), Human error, Data entry, SME, Validation, Cognitive load, Interface design, Regulatory compliance

INTRODUCTION

The Digital Product Passport (DPP) is emerging as a central instrument of European product sustainability policy. Its cross-sectoral foundation lies in the Ecodesign for Sustainable Products Regulation (ESPR), which introduces the DPP as a digital information carrier intended to improve transparency, circularity, and legal compliance across product value chains (European Parliament, Council of the European Union 2024). Within this broader regulatory architecture, batteries constitute one of the first product groups for which passport obligations have been concretized through the EU Battery Regulation 2023/1542. The EU Battery Regulation requires the continuous recording and updating of extensive product- and lifecycle-related information across the battery's operational life, including composition data,

carbon footprint information, performance parameters, and end-of-life-relevant attributes (European Parliament, Council of the European Union 2025).

At the European standardization level, CEN-CENELEC Joint Technical Committee 24 (JTC 24) develops the standards required for the implementation of the DPP. Within the JTC 24 standard drafts, spanning DIN EN 18216 to 18246, key specifications address the system-level prerequisites for digital exchange and trust. These include, data exchange protocols, application programming interfaces (API) for passport lifecycle management and data authentication and integrity mechanisms. Collectively, these drafts provide important building blocks for automated Machine-to-Machine (M2M) communication and for the structured creation, retrieval, and updating of DPP content across interoperable systems.

However, the downstream reality of the battery value chain extends well beyond automated enterprise integration. Large companies possess the resources required to develop systems that may connect the DPP ecosystem to Enterprise Resource Planning (ERP) systems and other digital infrastructures via APIs. By contrast, later lifecycle stages such as maintenance, repair, repurposing, and remanufacturing are frequently performed by Small and Medium-sized Enterprises (SMEs) operating in heterogeneous and only partially digitalized environments. In these contexts, records within the Digital Battery Passport (DBP), as the battery-specific implementation of the DPP, may often be updated through manual user input rather than automated data exchange, they do not offer practical solutions for implementing the DPP ecosystem in SMEs, where limited digital infrastructure often requires manually supported workflows and easy-to-use interfaces for data entry and updating.

This gap is highly relevant for the practical success of the DBP. In this context, errors in manual data entry have consequences beyond administrative inconvenience. They can lead to non-compliance, weaken trust in the digital passport data, and create risks for downstream actors relying on correct technical and safety information. This paper therefore addresses the problem of data integrity in manual Human-in-the-Loop DPP workflows. It proceeds from the premise that human error in complex industrial interaction is inevitable but can be systematically reduced through validation logic and workflow structuring.

REGULATORY AND TECHNICAL CONTEXT OF THE DIGITAL PRODUCT PASSPORT

EU Regulation 2023/1542 frames the DBP as a decentralised information system that relies on data contributions from multiple actors involved over the battery lifecycle (Jensen et al., 2023). Data access is structured according to user category, with some information made available to the public, some limited to notified bodies and market surveillance authorities, and some reserved for parties demonstrating a legitimate interest, such as dismantlers, repairers, remanufacturers, and recyclers (European Parliament and Council of the EU, 2025). This multi-audience requirement is significant from an interaction design perspective: the system must support credible use across highly heterogeneous user populations, not merely technical integrations.

The information density required is substantial, current standardization efforts define more than 90 attributes covering material composition, carbon footprint, performance and durability metrics, supply chain due diligence records, and end-of-life data (DIN DKE, 2025). Table 1 summarises the principal regulatory domains and their associated data requirements.

Table 1: Regulatory data domains, requirements, and stakeholder relevance.

| Regulatory Domain | Key Data Requirements | Stakeholder Relevance |
|----------------------------|--|-------------------------------------|
| General Information | Model, type, batch, Product ID, manufacturing date and place | Consumers, authorities, OEMs |
| Material Composition | Chemical composition, recycled content, hazardous substances | Recyclers, manufacturers |
| Carbon Footprint | Lifecycle stage carbon footprints | Regulators, eco-conscious buyers |
| Performance / Durability | Rated capacity, voltage, state of health (SoH) | Repair shops, second-life operators |
| Supply Chain Due Diligence | Responsible sourcing verification for critical raw materials | NGOs, regulators, investors |
| End-of-Life | Instructions for removal, disassembly, and recycling processes | Recyclers, professional dismantlers |

In the underlying data model, however, these data points are represented as hierarchically nested JSON objects. For example, the general information domain may include a *manufacturerInformation* object, which itself contains an *addressOfManufacturer* sub-object with fields such as *country*, *postalCode*, and *streetAddress*. Each element further carries metadata including an *elementId*, a *dictionaryReference URI*, a *valueDataType*, and, where applicable, unit codes expressed in UN/CEFACT format (e.g., KGM for kilograms). To ensure interoperability, semantic dictionaries such as ECLASS are used, while compliance is established by checking the data against a published JSON schema (Jansen et al., 2023).

TAXONOMY OF ERRORS IN BATTERY DATA MANAGEMENT

SMEs active in downstream battery lifecycle stages typically lack dedicated compliance personnel, integrated IT infrastructure, or formal data governance processes. Passport updates are therefore performed by workshop technicians whose primary competence is technical rather than administrative, operating under precursors to error: time pressure, noise, interruptions, and low familiarity with regulatory terminology (CIRPASS Consortium, 2024). This matters because DPP compliance is binary. A single missing mandatory field, incorrectly selected enumerated value, or format violation may be sufficient to invalidate a record entirely. Eurostat (2024) reports that only about one in five EU enterprises employ IT specialists, a share that decreases significantly with company size and the OECD (2021) identifies organisational capacity, not unwillingness, as the principal barrier to SME participation in digital compliance ecosystems. A passport infrastructure designed around API endpoints and schema-validated JSON documents presupposes precisely the

capabilities most downstream lifecycle actors do not have (Sagala & Óri, 2024).

To design effective validation mechanisms, it is first necessary to understand how errors arise in manual data entry. In Human Reliability Analysis (HRA), errors are not treated as purely random events, but as systematic failures resulting from the interaction between cognitive processes and environmental conditions. Drawing on established taxonomies in cognitive ergonomics, errors in the context of the DBP can be divided into two primary categories: slips and mistakes.

Slips: Failures of Execution

Slips occur when the user forms the correct intention but executes it incorrectly, reflecting failures of attention, perception, or motor execution rather than understanding. In battery passport maintenance, they may manifest as transposition errors (entering 98% instead of 89% for State of Health), unit errors (intending to document a battery weight of 500 kg but entering the value into a field expecting tons, thereby recording 500 tons instead of 500 kg), and omission errors (skipping a mandatory field due to interruption). These errors are compounded by performance shaping factors characteristic of SME workshop environments: time pressure, noise, fatigue, and physical constraints such as operating a touchscreen while wearing protective gloves (Boring et al., 2007; Klages et al., 2025). Because the operator's internal understanding is correct, slips typically go unnoticed unless the system provides immediate feedback or input constraints.

Mistakes: Failures of Knowledge or Judgment

Mistakes occur when the user forms the wrong intention but executes it correctly. Unlike slips, they are not caused by faulty execution, but by incorrect understanding, misapplied rules, or insufficient knowledge. As a result, the entered data may appear formally correct while still being factually wrong. In the DPP context, mistakes are particularly relevant because many fields depend on precise technical and regulatory definitions. One example is a classification error during battery repurposing. When updating the battery status, an operator may select *remanufactured* instead of *repurposed* if the distinction is not clearly explained in the interface. The selected value may be entered correctly from a technical point of view, but still represent the wrong legal classification. Another example is semantic misinterpretation. An operator may confuse rated capacity with nominal capacity and enter a plausible value such as 100 kWh in the wrong field. In this case, the syntax is correct and the value appears reasonable, but the content is still semantically incorrect.

Mistakes are particularly critical because they usually pass basic syntactic validation. Detecting them requires semantic plausibility checks, contextual explanations, or decision support mechanisms that help users interpret fields correctly before submitting data.

Systemic Process Errors

A third category, not always foregrounded in human error taxonomies focused on individual performance, concerns errors introduced by the submission process itself rather than by individual actors (Leveson, 2011). These systemic errors manifest when the same violation appears across multiple passports submitted in a batch or time window. Examples include a persistent mapping error in an export script, an incorrectly parameterised template, or a flawed transformation in an API integration layer. Because they affect multiple records simultaneously, systemic process errors carry the highest potential severity.

METHODOLOGY: A MULTI-LAYER VALIDATION FRAMEWORK

Reducing human error in manual DPP creation processes cannot rely on post-hoc data cleaning. Once faulty DPP have been submitted, the resulting compliance, traceability, and safety issues may already have propagated across the value chain. A preventive approach is therefore required in which validation logic is integrated directly into the human-computer interface. To address execution slips, knowledge-based mistakes, and systemic process errors this paper proposes a multi-layer validation framework for DPP validator interfaces.

Instead of treating validation as a single technical check, it organizes verification into three successive layers of increasing sophistication. Each layer targets a different class of error before the data are committed to the DPP ecosystem, such as a central registry or Economic Operator DPP infrastructure. The three layers are: (1) syntactic and format validation, (2) semantic and logical validation, and (3) physical and contextual plausibility validation.

Syntactic and Format Validation

The first layer addresses slips, particularly typing, transcription, and transposition errors. Its purpose is to ensure that all user inputs conform to the formal schema requirements defined for the respective data fields.

A first mechanism is type enforcement. Input fields should be strictly typed so that only permissible value types can be entered. For example, a numeric field for the “weight of battery“ should reject alphabetical characters immediately, thereby preventing basic typing errors at the point of entry.

A second mechanism is pattern matching for structured identifiers. Fields such as Product ID or Economic Operator ID typically follow defined alphanumeric patterns, for example ISO/IEC 9834-8 UUID structures or GS1-based identifier formats. These patterns can be checked in real time using regular expressions. If an operator omits a digit or inserts a hyphen in the wrong place, the system can provide immediate feedback before the input is accepted.

A third mechanism is unit standardization. This is particularly important for preventing unit-related slips such as confusing kilograms and tons.

Instead of allowing free-text entries such as “500 kg,” the interface should fix the unit in advance and require the user to enter only the scalar value. In this way, the risk of documenting a battery weight in the wrong unit is substantially reduced.

Semantic and Logical Validation

Syntactic correctness alone is not sufficient. A value may be entered in the correct format and still be logically wrong. The second validation layer therefore addresses mistakes by checking whether the entered information is internally consistent and semantically coherent within the dataset.

One important mechanism is temporal logic validation. Battery lifecycle data follow a chronological structure, and the interface should enforce this order. For example, an attempt to enter a second life date that predates the first life production date should trigger a blocking error. Although both dates may be syntactically valid, their relationship is logically impossible.

A second mechanism is hierarchical consistency validation. Battery data are often structured across multiple levels, such as cell, module, and pack. Validation must therefore check whether higher-level values are consistent with the properties of their constituent elements. For example, the total weight of a battery pack cannot be lower than the sum of the weights of its individual modules. Similarly, the declared rated capacity of the pack should correspond mathematically to the configuration of series- and parallel-connected cells. If these relationships do not hold, the discrepancy points either to a data entry error or to a misunderstanding of the battery architecture.

This layer therefore extends validation beyond field-level correctness. It evaluates whether multiple data points fit together in a logically consistent representation of the asset.

Physical and Contextual Plausibility Validation

The third layer addresses the most complex class of mistakes: entries that are formally correct and logically structured, but implausible when assessed against physical reality or the operational context. This layer is especially important because such errors are unlikely to be detected by standard compliance-oriented forms.

One mechanism is physics-based plausibility checking. User input can produce values that satisfy formatting rules while remaining physically impossible. For example, a user may accidentally enter an extra zero, resulting in a calculated specific energy density of 3,000 Wh/kg. Although the number is syntactically valid, it lies outside the physically plausible range for current lithium-ion battery systems. The system can therefore calculate derived values and compare them against known heuristic boundaries. If an input implies an energy density outside a plausible range, for example 50-300 Wh/kg, the interface should trigger a plausibility warning.

A second mechanism is category-based contextual validation. The EU Battery Regulation distinguishes between battery categories such as Light Means of Transportation (LMT) and industrial batteries. These categories are associated with different technical and regulatory profiles. If a user selects

the category LMT, for example for an e-scooter battery, but enters a weight of 800 kg, the system should flag this as a contextual mismatch. The value may be numerically valid, but it is inconsistent with the selected product category. Such checks help prevent classification errors in which operators unintentionally assign the wrong regulatory profile to an asset.

This validation thus complements the previous validation stages by connecting interface logic to battery-domain knowledge. It does not merely test whether data are correctly formatted or internally consistent, but whether they plausibly describe a real battery in a specific lifecycle context.

Summary of the Framework

By combining syntactic, logical, and plausibility-based validation, the framework acts as a multi-stage filter for manual DPP updates. It reduces execution slips, detects data inconsistencies, and identifies domain-specific errors in their physical and regulatory context. When applied across multiple DPP records, it can also reveal recurring error patterns that indicate systematic issues affecting more than one passport, thereby helping to protect the validity and reliability of DPP data.

JSON SCHEMA VALIDATOR FOR BATTERY PASSPORT PAYLOADS

Background: Schema Complexity in the Battery Passport

The Battery Passport JSON schema is structurally complex, consisting of modular sub-schemas, nested objects, multi-level arrays, and conditional dependencies between fields (BatteryPass Consortium, 2023, 2024).

For this reason, manual inspection of Battery Passport payloads is inherently unreliable. Errors may remain hidden in deeply nested elements or only become apparent when dependencies between multiple fields are taken into account. A validator that resolves the nested schema logic and highlights the exact path of each violation can therefore reduce the cognitive effort required for review and increase the likelihood that non-obvious inconsistencies are detected before submission.

Prototype Validator: Design and Features

A prototype JSON Schema Validator has been developed to implement key elements of the framework. The tool provides a dual-pane interface: an editable JSON view on the left, which allows in-place correction of the submitted payload, and a parsed and syntax-highlighted view on the right, in which lines containing violations are visually shaded. Detected issues are listed in a separate panel with severity labels, JSON path references, and plain-language explanations of the violated constraint (see Figure 1).

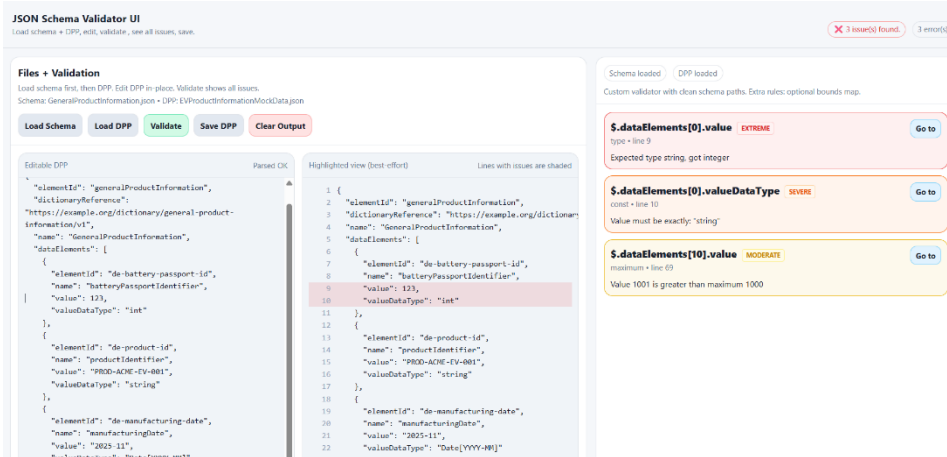


Figure 1: JSON schema validator.

The practical value of the validator lies not only in detecting invalid data entries, but in making complex schema violations interpretable for users by linking each issue to its JSON path, violated constraint, severity level, and source line. This design principle reflects the recognition that validation is not useful unless its findings are actionable. The features of the prototype are summarised in Table 2.

Table 2: Feature summary of the prototype JSON schema validator.

| Feature | Function | Benefit |
|-------------------------------|---|---|
| Editable JSON view | Allows in-place correction of submitted data | Immediate manual fix before resubmission |
| Parsed & highlighted view | Renders JSON with syntax highlighting; shades erroneous lines | Rapid localisation of structural issues |
| Line-based error localisation | Associates each violation with the source line number | Precise navigation in large, nested payloads |
| Severity labelling | Classifies issues as Extreme, Severe, or Moderate | Prioritisation of corrective actions |
| JSON path reference | Reports exact path (e.g., \$.dataElements[0].value) | Unambiguous identification of the offending field |
| Constraint explanation | States which rule was violated and why | Supports learning and avoidance of recurrence |
| Save & re-validate | Allows corrected payload to be saved and validated again | Iterative correction workflow before final submission |

Severity Classification

A central design decision in the prototype validator is the use of a four-level severity classification for detected issues. This classification distinguishes between errors that primarily affect data quality and those that compromise

the legal, technical, or semantic validity of the passport record. The four levels and their definitions are summarised in Table 3.

Table 3: Severity classification model for DPP validation issues.

| Severity Level | Definition | DPP Example | Required Action |
|---------------------------|---|--|---|
| Extreme / Critical | Record is legally or technically invalid; registration or update fails | Mandatory identifier absent; required nested object structurally invalid; key field wrong type | Immediate correction required; submission blocked |
| Severe | Record exists but contains serious rule violation that threatens validity | Field value violates strict schema constraint; conditional dependency unmet | Correction required before submission |
| Moderate | Data quality reduced; entire passport not necessarily invalid | Implausible value for voluntary data | Review and correction recommended |
| Minor / Warning | Stylistic or low-risk quality issue | Non-critical formatting deviation | Correction preferable; submission may proceed |

Extreme/Critical findings cause the submission to be blocked, as they render the record unusable for registration or update. For example, the prototype reports an EXTREME error when an integer is submitted for the battery passport identifier field although the schema requires a string. Severe findings require correction before resubmission, while Moderate findings mainly reduce data quality and may not necessarily prevent submission, depending on the applicable governance rules (see Figure 1).

DISCUSSION

The transition from static documentation to dynamic DPPs significantly increases the importance of data quality throughout the battery value chain. In practice, the reliability of the ecosystem depends not only on standardized exchange formats and automated interfaces, but also on the accuracy of manually entered data in lifecycle contexts where human operators remain involved. This is particularly relevant for SMEs, where activities such as repair, repurposing, remanufacturing, and dismantling often require direct interaction with passport records. Against this background, the validation framework has implications both for regulatory reliability and for the operational feasibility of DPP maintenance.

Conventional compliance processes often rely on ex-post auditing, in which submitted records are checked for errors only after data entry has already taken place. In a digital and distributed ecosystem, this approach is inefficient and creates avoidable risks for economic operators. The validator proposed in this paper shifts the focus from ex-post correction to ex-ante prevention by embedding validation mechanisms directly into the user interface.

This can be understood as a form of compliance by design. If syntax and logic are checked directly at the point of entry, the system makes it substantially more difficult to generate structurally invalid or logically inconsistent passport records. For SMEs in particular, this reduces the risk of incorrect submissions caused by typographical errors, omissions, or misunderstandings and lowers the administrative effort associated with rejected submissions and correction. In practical terms, the interface functions as a digital guideline: if the system permits submission, the record has at least passed the basic requirements of structural and logical validity.

For SMEs in particular, this reduces the risk of incorrect submissions caused by typographical errors, omissions, or misunderstandings and lowers the administrative effort associated with rejected submissions and correction. For this reason, Human-in-the-Loop validation should not be understood as a substitute for external verification, physical inspection, or trusted third-party certification. For SMEs in particular, this reduces the risk of incorrect submissions caused by typographical errors, omissions, or misunderstandings and lowers the administrative effort associated with rejected submissions and correction

CONCLUSION

The introduction of the Digital Product Passport under the EU Battery Regulation represents an important step toward greater transparency, traceability, and circularity in the battery sector. At the same time, the reliability of this infrastructure depends directly on the quality of the underlying data. As argued in this paper, manual data entry in downstream lifecycle stages introduces a significant source of vulnerability, particularly in SME environments where updates are often not performed through fully automated system integration.

To address this problem, the paper proposed a Human-in-the-Loop validation framework for manual DPP processes. Building on the distinction between slips and mistakes, the framework combines three layers of validation: syntactic and format checks, semantic and logical consistency checks, and physical and contextual plausibility checks. Together, these measures aim to reduce both execution errors and knowledge-based errors at the point of entry and show whether systemic process errors are present. Error-resilient interfaces are a necessary component of trustworthy passport infrastructures. If manual update processes are supported by appropriate validation logic and interaction design, the Digital Product Passport can function more reliably as a regulatory record and as a practical data basis for circular value chains.

REFERENCES

- BatteryPass Consortium (2023). Battery Pass Content Guidance. Version 3.0. Retrieved from <https://thebatteryass.eu>
- Battery Pass Consortium. (2024). Conformity assessment for battery passport data. <https://thebatteryass.eu>

- Boring, R. L., Griffith, C. D., & Joe, J. C. (2007). The Measure of Human Error: Direct and Indirect Performance Shaping Factors. OSTI OAI (U.S. Department of Energy Office of Scientific and Technical Information). <https://www.osti.gov/biblio/915533>
- CIRPASS Consortium (2024). A Study on DPP Costs and Benefits for SMEs, v1.0. EU Digital Europe Programme. <https://cirpassproject.eu/wp-content/uploads/2024/02/CIRPASS-A-study-on-DPP-costs-and-benefits-for-SMEs-v1.0-1.pdf>
- DIN DKE SPEC 99100:2025-02. (2025). Anforderungen an Datenattribute des Batteriepasses.
- European Parliament, & Council of the European Union. (2023). Regulation (EU) 2023/1542 of the European Parliament and of the Council of 12 July 2023 concerning batteries and waste batteries, amending Directive 2008/98/EC and Regulation (EU) 2019/1020 and repealing Directive 2006/66/EC (Text with EEA relevance). <http://data.europa.eu/eli/reg/2023/1542/oj>
- European Parliament, & Council of the European Union. (2025). Regulation (EU) 2024/1781 of the European Parliament and of the Council of 13 June 2024 establishing a framework for the setting of ecodesign requirements for sustainable products, amending Directive (EU) 2020/1828 and Regulation (EU) 2023/1542 and repealing Directive 2009/125/EC (Text with EEA relevance). <http://data.europa.eu/eli/reg/2024/1781/oj>
- Eurostat. (2024). ICT specialists – Statistics on hard-to-fill vacancies in enterprises. European Commission. <https://ec.europa.eu/eurostat>
- Jensen, S. F., Kristensen, J. H., Adamsen, S., Christensen, A., & Wæhrens, B. V. (2023). Digital product passports for a circular economy: Data needs for product life cycle decision-making. *Sustainable Production and Consumption*, 37, 242–255. <https://doi.org/10.1016/j.spc.2023.02.021>
- Klages, B., Metzner, A. B., & Zaeh, M. F. (2025). A methodology for the prioritization of factors influencing human errors in manual assembly lines. *Production Engineering*. <https://doi.org/10.1007/s11740-025-01370-x>
- Leveson, N. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.
- OECD. (2021). *The digital transformation of SMEs*. OECD Publishing. <https://doi.org/10.1787/bdb9256a-en>
- Sagala, G. H., & Őri, D. (2024). Toward SMEs digital transformation success: A systematic literature review. *Information Systems and e-Business Management*, 22(4), 667–719. <https://doi.org/10.1007/s10257-024-00682-2>