safety

MDPI

Article

Reviewing Diagnostic Assignments in Hardware Design Failure Mode and Effects Analysis: An Industrial Case Study

Andrea Engert [1,*], Ádám Móré [1,2], Attila Trohák [1] and Rafael Ruben Boros [2,3]

[1] Faculty of Mechanical Engineering and Informatics, Institute of Automation and Info-communication, University of Miskolc, 3515 Miskolc, Hungary; adam.more@uni-miskolc.hu (Á.M.); attila.trohak@uni-miskolc.hu (A.T.)
[2] Institute of Engineering and Agricultural Sciences, University of Nyíregyháza, 4400 Nyíregyháza, Hungary; boros.ruben@nye.hu
[3] Institute of Physics and Electrical Engineering, University of Miskolc, 3515 Miskolc, Hungary
* Correspondence: andrea.engert@student.uni-miskolc.hu

Abstract

Diagnostic assignments in automotive hardware design failure mode and effects analysis (HW-D-FMEA) require evidence linking a defined failure scenario to fault observation and an effective system response. This study presents a schema-based framework for reviewing these assignments in existing industrial documentation. Failure descriptions were refined to specify the affected object, the failure manifestation and relevant conditions, and whether the failure concerned the monitored or monitoring function. Candidate mechanisms were assessed for compatibility, operating conditions, observation paths, dependencies, response sufficiency, timing and supporting document status. The framework was applied to the HW-D-FMEA of an electric power steering control-unit platform in series production. Approximately 76% of refined entries retained their baseline assignment status, while 2% received newly identified assignments and 5% were reassigned. For 17%, a baseline assignment could not be retained for mitigation credit; insufficient substantiation of diagnostic dependencies was the predominant reason. The case study illustrates the need for scenario-specific justification and identifies further documentation, analysis or testing needs. These proportions are documentation-level counts, not failure-rate-weighted coverage or measured effectiveness, and because the classification was performed by a single reviewer, its reproducibility remains to be evaluated.

Keywords: failure mode and effects analysis; diagnostic assignment; functional safety; safety mechanism; dependent failures; electric power steering

Check for updates

Academic Editor: Raphael Grzebieta

Received: 2 November 2026
Revised: 21 November 2026
Accepted: 24 November 2026
Published: 27 November 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Automotive electronic systems use diagnostic mechanisms to identify hardware faults and initiate responses intended to prevent or mitigate their system-level consequences. Where these mechanisms are credited in safety analyses, the relationship between a failure mode, its diagnostic observation and the required response must be supported by a technical rationale. HW-D-FMEA documents failure modes, their effects and associated measures. FMEA for Monitoring and System Response (FMEA-MSR) adds monitoring and the resulting system response during operation [1].

The applicability of an assignment depends on how the fault manifests physically, which signal or state makes it observable and whether the mechanism is active under the operating conditions. Detection may involve direct observation of the affected signal or

physical quantity or indirect observation of a consequence propagated through intermediate elements and functions. The fault may also impair the resources needed for observation or response [2]. Detection alone does not justify mitigation if the required response cannot be completed within the applicable time requirement [3]. These conditions must be backed by evidence, which a general failure description and a high-level monitoring reference may not provide.

For example, a generic supply-voltage fault may be associated with a voltage-monitoring function. The assignment may appear appropriate because the mechanism monitors the supply voltage. However, the assessment can differ depending on which supply domain is affected and whether the measurement, reference and processing resources remain operational under the fault conditions. A shared resource does not automatically invalidate the assignment, but it requires examining whether the fault could compromise the diagnostic path; the same failure-mode name can therefore call for different diagnostic justifications.

The study was prompted by HW-D-FMEA entries that combined different failure manifestations under general descriptions and referred to monitoring groups rather than individual diagnostic mechanisms. Assessing these assignments requires examining safety-mechanism effectiveness and dependent failures, which ISO 26262 addresses [2,3]; model-based safety analysis and fault injection can supply evidence [4,5]. The examined records did not always show how such evidence supported each assignment.

This study presents a schema-based failure-description and diagnostic-assignment review framework and examines the assignment differences and gaps in supporting evidence identified when it is applied to industrial HW-D-FMEA documentation. The framework first structures each failure scenario, then reviews the candidate diagnostic mechanism and the intended system response. Two research questions guide the study:

What information and review criteria are needed to assess the applicability of diagnostic assignments?

What review outcomes result from applying the framework to the examined industrial documentation?

The framework was applied to the HW-D-FMEA of an electric power steering control-unit platform in series production, using the safety-mechanism assessment records available at the time of the review. Review decisions were compared with the baseline assignments and summarised descriptively. The main contributions of this study are:

A failure-description schema, with three core dimensions and element-type-specific checklists, that separates scenarios with different diagnostic requirements.

A review procedure that links structured failure descriptions, observation paths, applicability criteria and evidence to assignment decisions.

An industrial case study on a production platform, reporting the review outcomes and reasons for withholding mitigation credit.

2. Background and Related Work

Existing approaches support different parts of a diagnostic-assignment rationale. FMEA structures failure relationships and associated measures. Model-based and system-theoretic analyses address behaviour, operating conditions and control relationships. Fault injection examines system responses to selected faults.

2.1. Hardware FMEA and Diagnostic Assignments

Design FMEA documents the relationships between functions, failure causes, failure modes, failure effects and associated measures. The AIAG & VDA FMEA Handbook provides harmonised seven-step guidance for conducting these analyses. It emphasises

technically precise failure descriptions, consideration of interfaces and operating conditions and critical review of information reused from earlier analyses. These principles apply to the HW-D-FMEA examined here: descriptions must distinguish cases in which diagnostic applicability or the required response differs [1].

Development-stage detection must be distinguished from operational monitoring. Design FMEA assesses potential design weaknesses, assuming that manufacture and assembly conform to the design intent. Its Detection controls are verification and validation activities intended to detect the analysed failure causes or modes before release for production, whereas FMEA-MSR considers fault detection and the subsequent system response during operation. A hardware-in-the-loop (HIL) test may act as a development-stage Detection control, while the operational diagnostic function examined by that test is a Monitoring control. FMEA-MSR also explicitly considers failure scenarios, operating conditions and the combined effectiveness of monitoring and response [1].

ISO 26262 supplies the functional-safety context. Part 3 addresses operating scenarios and the detection, fault-control, state-transition and timing strategies of the functional safety concept [6]. Part 5 addresses hardware safety requirements and the justification of safety-mechanism effectiveness, while Part 9 addresses dependent failures and safety-oriented analyses [2,3].

Together, these sources treat each diagnostic assignment as a technical claim. Depending on the mechanism and application, it can be justified by architectural analysis, behavioural models, dependency assessments or test results.

2.2. Existing Failure-Analysis and Diagnostic-Assessment Approaches

The reviewed approaches differ in how they represent failures and operating conditions and in the output they produce.

2.2.1. Failure Representation and Quantitative Assessment

Avižienis et al. distinguish a fault, the erroneous system state associated with it and a failure in the delivered service [7]. This distinction helps explain why a diagnostic mechanism may observe a propagated consequence rather than the originating fault. In quantitative assessment, the representation must also support classification and aggregation of the failure contributions. Inada et al., for example, evaluate analogue drift faults using parameter ranges classified by safety and detection limits, then combine the classifications with failure-mode distributions and failure-rate data [8]. Their reported coverage is a model-based, failure-rate-weighted result obtained under specified parameter ranges and distribution assumptions [8].

2.2.2. Model-Based Safety Analysis and Automated FMEA

Papadopoulos and McDermid's HiP-HOPS integrates functional failure analysis, interface-focused FMEA (IF-FMEA) and automated fault-tree synthesis on a hierarchical system model [9]. IF-FMEA represents output failures as logical combinations of internal malfunctions and input deviations, explicitly considering detection, mitigation, transformation and propagation across component interfaces. Their automotive brake-by-wire case study illustrates how a temporary input omission can result in a persistent stuck output in a peak-detection and removal algorithm [9].

Joshi et al. propose linking nominal system behaviour with explicit fault models. Their wheel-braking example uses formal verification to identify counterexamples involving detection and switchover delays and the consequences of earlier faults [10]. Bozzano et al. analyse mode transitions in a redundant power-steering Electronic Control Unit (ECU) model. Their minimal transition cut sets explain transitions through combinations of faults

and recovery events, excluding events required to reach the source mode. They also account for delayed effects of earlier events [4].

Both analyses depend on their system and fault models [4,10]. Bozzano et al.'s transition cut sets identify event combinations rather than complete ordered execution sequences [4]. Joshi et al. express detection and switchover delays in discrete model steps rather than measured implementation response times [10].

Lee et al. combine Simulink-based design, saboteur-based fault injection and rule-based severity classification to generate FMEA reports for an electronic fuel injection model [11]. Their case study shows that failure effects and severity can vary with the operating mode and the magnitude of the injected signal deviation. In the demonstrated implementation, occurrence and detection ratings remain expert-defined rather than automatically derived [11].

2.2.3. System-Theoretic Analysis and Documentation

Leveson's STAMP (Systems-Theoretic Accident Model and Processes) approach treats safety as enforcement of constraints on system behaviour, while STPA (System-Theoretic Process Analysis) examines unsafe control actions and the circumstances that can produce them. Feedback quality, the controller's process model, operating context and action timing are central considerations [12]. The distinction between issuing a command and confirming its physical effect is especially relevant to diagnostic response assessment. Leveson also describes intent specifications, which integrate safety-analysis results, assumptions, design rationale, requirements and validation information into a traceable system specification. This is a close precedent for organising engineering justification, although its scope is broader than reviewing individual assignments in an existing HW-D-FMEA [12].

2.2.4. Fault Injection and HIL-Based Assessment

Sini et al. present an emulation-based environment whose demonstrated implementation injects permanent faults affecting the programme counter. Their campaign-based classification distinguishes detected faults whose outputs match a fault-free run ("Safe detected") from detections for which mitigation effectiveness is not assessed ("Detected") [13]. Abboush et al. inject faults into sensor and actuator-control signals in a real-time HIL environment comprising a controller prototype and a simulated plant. Their gasoline-engine case study compares system-output traces under fault-free and injected-fault conditions, rather than reporting quantified diagnostic coverage or validating the timing of a complete safety response [5]. The two studies operate at different abstraction levels and provide evidence about different fault representations.

2.2.5. Ontology-Based Integration of Design and FMEA Knowledge

Younus et al. [14] integrate system design models and FMEA through the Function–Behaviour–Structure–Failure Mode (FBSFM) ontology. Their automotive headlamp case study shows how structured retrieval can expose missing failure information and links across system levels. The study focuses on knowledge representation and traceability rather than criteria for crediting individual operational diagnostic assignments.

2.2.6. Dependent-Failure Analysis

Prashanth Reddy and Leburu propose a matrix-based dependent-failure analysis (DFA) that relates hardware sub-blocks to potential influencing elements, including shared power and clock resources [15]. The analyst examines relevant intersections and records the dependency rationale or possible safety mechanisms. Their illustrative system-on-chip

example considers interference through shared buses between safety-related and other peripheral functions [15].

2.2.7. Complementarity of the Approaches and Implications for Assignment Review

Each approach addresses a different aspect: failure propagation, diagnostic performance or dependency relationships. A signal-level injection may reproduce an observable deviation without reproducing every dependency of its physical cause, and a formal model may explain an operating-state transition without establishing the execution time of the implemented response.

An assignment review must therefore connect each result to the failure manifestation, conditions and claim it addresses. Table 1 summarises the comparison and the role of the proposed framework.

Table 1. Comparison of existing approaches and the role of the proposed framework.

Approach and Source	Representation and Analysis Focus	Output or Demonstrated Evidence	Relevance to the Present Framework
FMEA and FMEA-MSR, AIAG & VDA (2019) [1]	Functions, failure relationships, operating scenarios, monitoring and response	Structured evaluations and documented measures	Establish the starting documentation and monitoring–response assessment context
Analogue drift assessment, Inada et al. (2015) [8]	Parameterised deviations, safety and detection limits and failure distributions	Simulation-based classifications and quantitative results under specified assumptions	Illustrates the dependence of coverage information on the selected failure representation
Hierarchical safety analysis, Papadopoulos and McDermid (1999) [9]	Hierarchical system model and interface failure logic, including detection, mitigation and propagation	Component IF-FMEAs and automatically synthesised fault trees	Links component deviations and reactions to system-level failures
Model-based safety analysis, Joshi et al. (2005) [10]	Nominal behaviour extended with fault models	Formal verification results and counterexamples	Supports examination of state history and detection or switchover behaviour
Mode-transition analysis, Bozzano et al. (2020) [4]	States, faults and recovery events	Model-derived minimal transition cut sets	Supports reasoning about operating modes and delayed fault effects
Automated FMEA, Lee et al. (2022) [11]	Parameterised signal faults and operating modes in a Simulink model	Generated FMEA reports with simulated failure effects and rule-based severity classifications	Supports explicit treatment of fault parameters and operating conditions; detection ratings remain expert-defined
STAMP/STPA and intent specifications, Leveson (2011) [12]	Control relationships, feedback, safety constraints and design rationale	Unsafe-control-action analyses and traceable specification structures	Provide precedents for observation–response reasoning and documentation of justification
Emulation-based fault injection, Sini et al. (2022) [13]	Selected programme-counter fault models	Campaign-dependent detection and outcome classifications	Supports checking the relationship between a specified injected fault and detection
Ontology-based design–FMEA integration, Younus et al. (2025) [14]	Design and failure knowledge linked across system levels	Machine-readable repository and structured querying in an automotive case study	Supports traceability and identification of missing failure information; the present framework reviews the support for operational diagnostic assignments

Table 1. *Cont.*

Approach and Source	Representation and Analysis Focus	Output or Demonstrated Evidence	Relevance to the Present Framework
HIL-based signal injection, Abboush et al. (2022) [5]	Signal faults with defined locations and timing in operating scenarios	Observed system-output behaviour in the implemented HIL environment	Supports scenario-specific assessment of system responses to injected signal faults
Matrix-based DFA, Prashanth Reddy and Leburu (2020) [15]	Hardware sub-blocks and potential influencing elements, including shared resources	A dependency matrix supporting engineering assessment and documentation of rationale	Supports identifying dependencies relevant to diagnostic-path applicability
Proposed assignment-review framework	Existing HW-D-FMEA entries and supporting mechanism information organised by refined scenario	Documented assignment decisions, rationale and identified technical or document-status limitations	Provides a defined procedure for reviewing individual assignments without replacing the underlying analyses

2.3. Concepts Required by the Proposed Framework

Failure-mode name and defined failure scenario. A general label such as "inadequate power supply" may combine deviations affecting different objects, operating phases or diagnostic paths. For this study, a defined scenario specifies the affected object, manifestation and applicability conditions, consistent with the Handbook's emphasis on precise descriptions [1].

The following concepts are linked by a scenario-specific justification chain from the failure manifestation, through diagnostic observation and the information needed for a decision to the required system response. Operating conditions, dependencies and timing constrain this chain. Document approval is assessed separately from technical support.

2.3.1. Monitored Function and Monitoring Function

A mechanism's ability to detect faults in another function does not establish detection of its own failures. FMEA-MSR assumes that monitoring operates as designed. Failures of the diagnostic function require separate consideration. An applicable self-test, supervisory mechanism or redundant arrangement may provide support, but its dependencies must also be assessed. The review must establish adequate diagnostic operation under the specified fault conditions and compliance with any applicable independence requirements [1–3].

2.3.2. Direct and Indirect Observation Paths

These are operational terms in the present framework. A direct path observes the affected signal or state at the same or a functionally equivalent point. An indirect path observes a physical or functional consequence through intermediate elements or functions. Neither is sufficient alone: the fault may compromise a direct observation and an indirect one needs justification of propagation, enabling conditions and delays. ISO 26262-5 provides related examples of actuator-level and system-level monitoring, but does not prescribe this particular classification [3].

2.3.3. Detection, Decision Sufficiency and Mitigation

Detecting a discrepancy does not necessarily identify the faulty element or the redundant channel that can be trusted; what is needed depends on the intended response. A discrepancy indication may suffice to initiate shutdown, whereas continued operation on a redundant channel requires evidence supporting the channel-selection decision. A command likewise does not show that the physical transition was completed and where

timing matters, the whole interval from fault occurrence to completed response must be checked against the requirement [3,12].

2.3.4. Diagnostic Coverage and Monitoring Rating

Diagnostic coverage (DC) concerns failure-rate contributions detected or controlled within the scope and assumptions of a safety-mechanism assessment. The FMEA-MSR Monitoring (M) rating evaluates the combined effectiveness of monitoring and system response against the Handbook's rating criteria. DC information may inform the M rating when its assessment scope and assumptions apply to the defined scenario. It does not replace justification of the diagnostic information required for the decision or of the response's effectiveness and timing [1,3].

2.3.5. Technical Applicability and Mitigation Credit

Technical applicability and document approval status are assessed separately. Mitigation credit means that a diagnostic assignment is accepted as a mitigation measure in the FMEA based on its technical support and the required document approval status. A monitoring group is a local documentation reference that groups individual mechanisms, rather than a standardised safety mechanism. Applicability is assessed at individual-mechanism level for each failure scenario.

Figure 1 links the failure scenario, diagnostic observation, decision information and required response, together with the analyses that feed them, the conditions that constrain them and the separate document-approval condition.

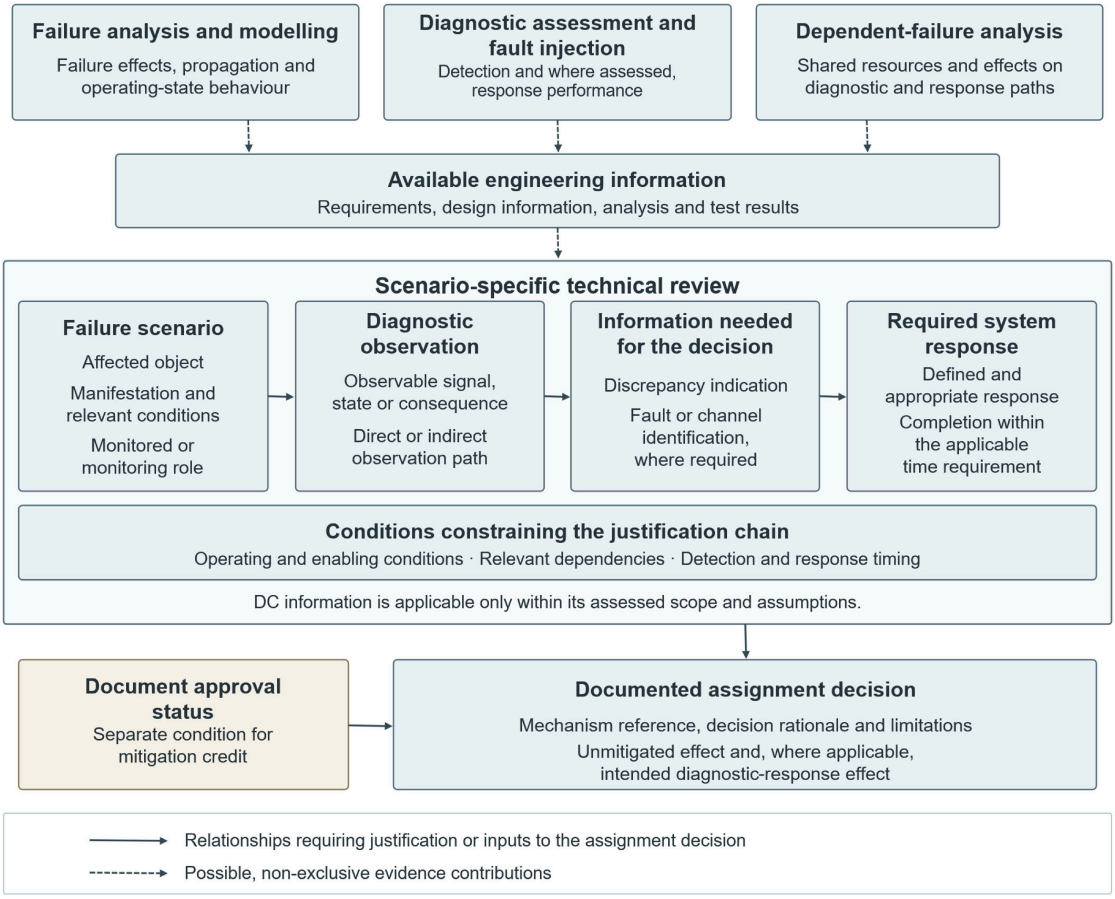

Figure 1. Conceptual relationships and complementary information sources in diagnostic-assignment review.

2.4. Positioning of the Proposed Framework

FMEA-MSR already requires assessment of monitoring and system response for defined failure scenarios [1], while ISO 26262 addresses safety-mechanism effectiveness and dependent failures [2,3]. The proposed framework combines a three-dimensional failure-description schema and element-type-specific checklists with a documented procedure for applying these principles to individual diagnostic assignments in existing HW-D-FMEA documentation. General failure descriptions are refined where diagnostic requirements differ, and monitoring-group references are resolved to specific mechanisms. Applicability is assessed for each refined scenario, including diagnostic-path dependencies and completion of the required response within the applicable time requirement. The decision on mitigation credit distinguishes technical support from document approval status. Intent specifications provide a broader precedent for documenting the supporting rationale [12].

The framework does not introduce a new failure-propagation model, automated FMEA generator or DFA method. It reviews whether the available engineering information, including analysis or test results, supports an individual diagnostic assignment under the refined scenario's conditions and identifies where further substantiation is needed.

3. Materials and Methods

3.1. Study Design and Industrial Context

This industrial case study used the failure-description schema to review documented relationships between ECU failure scenarios, diagnostic mechanisms and system responses under the applicable operating conditions. The revised entries were then compared with their baseline counterparts and classified into C1–C4 (Section 3.5).

The object of the study was the HW-D-FMEA of an electric power steering control-unit platform in series production. The analysis was performed at platform level and covered a common, reusable architecture and the modules within the review scope. The control unit regulates the electric motor that provides steering assistance using sensor inputs and vehicle communication data. The FMEA scope included the control unit's electronics, software functions supporting hardware operation, mechanical design and electrical and mechanical interfaces to the motor and sensors. Within this scope, the study focused on the control unit's hardware modules.

A.E. structured the failure descriptions using the schema and refined them with the responsible module designers. Technical diagnostic-assignment decisions were made by the responsible module engineers using the available safety-mechanism assessment records and engineering judgement. As FMEA moderator, A.E. supported the assessment through structured questions and methodological guidance, documented the revisions and classified the review outcomes. As a contributor to the baseline HW-D-FMEA and the platform's hardware FMEA owner, this author had access to the records and knowledge of the platform's development context.

The review was initiated as an authorised lessons-learned follow-up led by A.E. after completion of the initial platform-development programme, rather than as part of an active development project. No independent second classifier was assigned for the outcome analysis.

3.2. Data Sources and Units of Analysis

The baseline HW-D-FMEA provided the functions, failure-mode descriptions, failure-effect relationships and diagnostic assignments before the review. Where a diagnostic assignment was present, it referenced a monitoring group rather than an individual mechanism. Each group contained several mechanisms with individual identifiers in the safety-mechanism assessment records. The revised HW-D-FMEA documented the descriptions

and diagnostic assignments resulting from the review. The safety-mechanism assessment records provided information on individual safety mechanisms, including their assumed DC and rationale, applicability conditions, requirement links and dependencies. Document approval status was considered when deciding whether a diagnostic assignment could be credited in the revised HW-D-FMEA.

The HW-D-FMEA was initiated at the first milestone of the platform-development life-cycle and developed alongside the platform before entry into series production. After initial development, it continued to be maintained through lessons learned, updates from linked engineering documents and customer requirements fed back from subsequent projects. The baseline was the version available immediately before the 2026 review, which was conducted during series production. The review assessed the baseline diagnostic assignments using the safety-mechanism assessment records current at that time; historical versions of these records were not separately compared.

The review covered the functions and failure-mode entries of the hardware modules. For descriptive analysis, the entries were organised into five functional groups: power supply and energy management, motor control and power electronics, communication interfaces, sensor interfaces and safety and diagnostic functions. Each failure-mode entry was classified according to the primary system function of the affected module.

The functional groups describe the inventory without identifying individual modules. The refined failure-mode entry was the unit of technical assessment and reporting (Sections 3.3–3.5).

3.3. Failure-Description Schema

The schema structures failure-mode descriptions so that scenarios with different diagnostic requirements are separated (Section 2.3). It comprises three information dimensions and six element-type-specific schemas and supplements the existing FMEA process; the structured descriptions are the input to the diagnostic assessment.

3.3.1. Core Information Dimensions

The first dimension identifies the object affected by the failure. Depending on the level of analysis, this may be a signal, component, functional unit, channel or interface. The identification must be specific enough to link the failure mode to a diagnostic mechanism. For example, an undervoltage description must name the affected supply line or functional supply domain rather than refer to power supply conditions in general. Implementation details are reproduced only to the extent needed to distinguish objects with different diagnostic paths.

The second dimension describes how the affected object deviates from its intended behaviour. Distinctions include values above or below a specified limit, missing signals, corrupted data, semantically incorrect but structurally valid data, delayed responses and unstable outputs. These manifestations differ diagnostically: for example, a communication integrity check may detect a corrupted frame but not an incorrect value in a valid frame.

Within this dimension, the operating phase or activation condition is recorded when it affects diagnostic applicability. Relevant phases include start-up, normal operation, standby and periodic self-test. A mechanism active only at start-up cannot automatically be credited for failures arising during subsequent operation. Conversely, a mechanism that relies on a change from a previous fault-free value may not detect a fault already present at start-up.

Dynamic characteristics (fault duration, signal-jump magnitude, drift, oscillation, rise time, delay) are likewise recorded where they influence detectability, diagnostic activation and detection time or the feasibility of completing the system response within the applicable

time requirement. The schema does not prescribe thresholds, which depend on technology and requirements.

The third dimension states whether the failure concerns the monitored function or the diagnostic mechanism itself (Section 2.3.1). If a monitor fails to report an existing fault, the monitor is the object of analysis: the assignment then requires an additional means of checking it, such as a supervisory mechanism or self-test, together with an examination of that means' dependencies. False-negative and false-positive failures are distinguished because their consequences depend on the direction of the error, the affected functions, the system response and the availability of other channels or mechanisms.

3.3.2. Element-Type-Specific Schemas

The three dimensions are supplemented by six element-type-specific schemas (Table 2), which serve as review checklists of failure categories. Not every category applies to every element, and a listed failure does not imply that a diagnostic mechanism exists; for passive protection or filtering, risk reduction may rely on design robustness instead of runtime detection.

Table 2. Element-type-specific failure-description schemas.

Schema	Element Type	Typical Function	Failure Categories to Be Considered
A	Analogue sensors and signal-generating elements	Measurement of physical quantities and signal generation	Missing signal, signal above or below limits, plausible but incorrect signal, drift, sudden signal jump, stuck signal
B	Signal-conversion and signal-processing elements	Conversion, processing and validity indication	Missing output, conversion deviation, incorrect validity indication, data-format or protocol corruption, delayed output
C	Printed circuit boards and passive elements	Signal transmission, filtering and protection	Open circuit, short circuit, reduced electrostatic-discharge protection, reduced electromagnetic-interference filtering
D	Power-supply elements	Voltage generation, energy supply and current limiting	Overvoltage, undervoltage, missing output voltage, delayed voltage rise, oscillating output, failure to activate current limiting
E	Communication interfaces	Data transmission, protocol handling and timing	Missing message, structurally corrupted data, structurally valid but semantically incorrect data, delayed message
F	Software monitoring functions	Fault detection, plausibility checking and self-diagnostics	False-negative and false-positive behaviour, distinguished between start-up and operation

3.3.3. Failure-Mode Refinement and Diagnostic Observation Paths

In the industrial application, the existing failure descriptions were structured according to the three dimensions. Compound descriptions were subdivided where they combined failure manifestations, operating conditions, diagnostic mechanisms or system responses that required separate assessment.

For each refined scenario, the observation path was classified as direct or indirect using the definitions in Section 2.3.2. The review recorded the intermediate elements, enabling conditions, dependencies and delays of the path.

3.4. Diagnostic-Assignment Review Procedure

The procedure checks whether a diagnostic assignment can be credited as mitigation for a failure scenario (Figure 2). It uses the structured failure descriptions and safety-mechanism assessment records. The review starts from a baseline failure-mode entry and any existing diagnostic assignment; the applicable A–F schema structures the failure scenario according to Section 3.3 and each scenario produced by refinement is assessed separately.

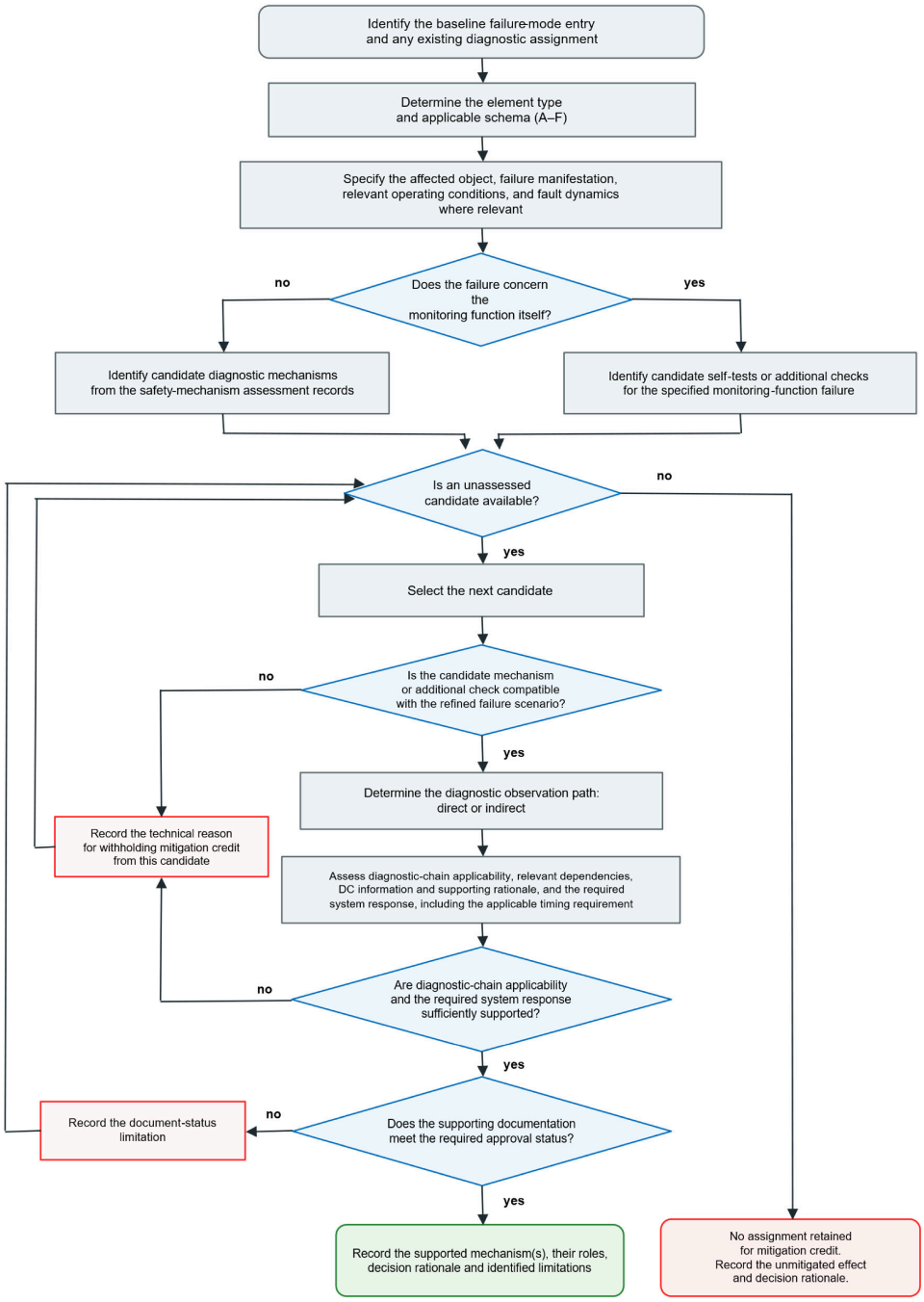

Figure 2. Diagnostic-assignment review procedure applied to each refined failure scenario. Technical support and document approval status are assessed separately before deciding whether to credit a diagnostic assignment as mitigation. Where complementary mechanisms are included in an assignment, each is assessed through the same candidate-review steps.

3.4.1. Identifying Candidate Diagnostic Mechanisms

Candidate diagnostic mechanisms are identified from the safety-mechanism assessment records. Where the baseline HW-D-FMEA contains a monitoring-group reference, the individual mechanisms in that group are examined for potential applicability to the refined failure scenario. Application of other mechanisms from other groups to the refined scenario is also considered and the same records are used for entries without a baseline assignment. Each candidate is referenced by its safety-mechanism identifier and description and examined individually according to Section 3.4.2.

Where mechanisms had complementary roles, the applicable mechanisms were recorded together and their individual contributions to the diagnostic chain were identified. Their joint use was not assumed to provide complete coverage, and individual DC values were not combined without a technical rationale.

3.4.2. Assessing Technical Applicability and MSR Implications

Each candidate assignment is examined using the criteria in Table 3. The assessment links the failure manifestation to the diagnostic observation, the conditions under which detection is possible and the required system response.

Table 3. Criteria for assessing the technical applicability of a diagnostic assignment.

Criterion	Review Question
Physical and functional relationship	Does the mechanism observe the affected signal, component, interface or an identifiable consequence of the failure?
Failure-type compatibility	Is the detection principle compatible with the failure manifestation?
Operating applicability	Is the mechanism active and are its enabling conditions satisfied in the operating phase?
Observation path	Is detection direct or indirect and is the path from the failure to the diagnostic observation sufficiently described?
Relevant dependencies	Could the specified fault impair both the monitored function and the diagnostic path?
System response	Is the response defined and appropriate for the system-level effect and does the diagnostic information support the decision required to initiate it?
Temporal applicability	Does the evidence cover detection and completion of the response within the time requirement?

For indirect observation, the assessment checks whether the intermediate physical or functional relationships support the connection between the failure and its observable consequence. For each scenario, it also examines whether the fault could compromise diagnostic observation or response through shared supplies, references, processing paths or communication interfaces. For failures of the monitor itself, the additional check required by Section 3.3.1 is assessed against the same criteria, including its dependencies. False-negative and false-positive failures are assessed separately.

For scenarios with a timing requirement, the assessment covers the complete interval from fault occurrence to completion of the required system response, including observation, processing, communication and actuation delays. The information is compared with the timing requirement, including the fault-tolerant time interval (FTTI) where one is defined. The review also checks whether the mechanism's DC information and rationale apply to the refined failure scenario, given its failure type, operating conditions, observation path and dependencies. The Monitoring rating (M) is then checked against the FMEA-MSR rating criteria (Section 2.3.4) and each proposed rating requires its own justification.

Technical support was considered sufficient when the responsible module engineer could justify the candidate's applicability and limitations against the relevant criteria in Table 3. This judgement required the failure manifestation and applicability conditions to be specified in sufficient detail in both the refined FMEA description and the individual mechanism description and rationale.

Where a material question remained unresolved, the responsible test engineers were consulted to clarify the available evidence. If uncertainty persisted, additional testing was requested. If the required substantiation could not be obtained during the review, mitigation credit was withheld from that candidate and alternatives were considered. An unresolved evidence gap was recorded as insufficient support, not as demonstrated technical incompatibility.

3.4.3. Recording the Decision and Updating the FMEA

Each review concludes with an assignment decision and rationale. For retained or revised assignments, the FMEA records the mechanism reference, observation-path type and limitations, together with parallel effect chains for the unmitigated effect and the effect associated with the intended diagnostic response.

The effect associated with the intended diagnostic response may be used for MSR severity only when the M = 1 criteria are substantiated [1]. Otherwise, MSR severity is based on the unmitigated effect.

3.5. Outcome Categories and Classification Rules

Each refined entry was classified by comparing the baseline and revised assignment status and, where applicable, the monitoring-group references. The four mutually exclusive categories, C1–C4, are defined in Table 4. For supported assignments, monitoring-group references were used to distinguish C1 from C3. C1 is subdivided into C1a and C1b for reporting.

Table 4. Outcome categories for the comparison of baseline and revised diagnostic assignments.

Code	Outcome Category	Definition
C1	Baseline assignment status retained	The review confirmed the baseline assignment status. The category comprises C1a and C1b.
C1a	Baseline diagnostic assignment retained	A supported diagnostic assignment was retained within the originally referenced monitoring group. The mechanism reference or applicability description could be refined without changing that group.
C1b	Baseline non-assignment confirmed	The review confirmed the baseline decision not to assign a diagnostic mechanism to the refined failure scenario.

Table 4. *Cont.*

Code	Outcome Category	Definition
C2	Diagnostic assignment newly identified	No diagnostic assignment had been documented for the failure mode in the baseline HW-D-FMEA, but an applicable assignment was identified and incorporated during the review using the available safety-mechanism assessment information.
C3	Diagnostic assignment revised	Diagnostic assignments were present in both versions, but the review selected a mechanism from a different monitoring group because the records better supported its relationship to the failure scenario.
C4	No assignment retained for mitigation credit	A diagnostic assignment present in the baseline HW-D-FMEA was not retained because mitigation credit could not be justified from the available technical information or document approval status. No diagnostic mechanism was assigned to the corresponding refined entry in the revised HW-D-FMEA, and no diagnostic-response mitigation path was linked to that entry. The assessment was based on the unmitigated system-level effect.

Classification Rules and Primary Reasons

Each refined entry was compared with the baseline assignment of its parent entry. Entries derived from the same parent could receive different outcomes. C1–C4 were treated as nominal categories.

For assignments classified as C4, the reason breakdown distinguished three technical categories and one document-status category (Table 5). R1–R4 were defined from the recorded reasons when the results were summarised.

Table 5. Reasons reported for assignments not retained for mitigation credit.

Code	Reason	Interpretation
R1	Relevant diagnostic dependencies insufficiently substantiated	The available information did not establish that the diagnostic path would remain capable of performing its intended function under the specified fault conditions.
R2	Signal correctness or redundant-channel status insufficiently substantiated	The available information did not support the claimed ability to establish signal correctness or the relevant state of a redundant channel.
R3	Time-critical state-change detection insufficiently substantiated	The documented detection capability was not sufficiently supported for the relevant time-critical transition.
R4	Diagnostic documentation not approved	The diagnostic documentation had not reached the approval status required for credit in the revised HW-D-FMEA.

For each C4 decision, the rationale recorded whether the limitation concerned missing technical support, information contradicting applicability or document approval status.

Each entry was counted once under its primary reason (R1–R4). Where several limitations applied, the reviewer selected the primary reason using engineering judgement.

3.6. Data Analysis and Traceability

3.6.1. Descriptive Analysis

Baseline and revised assignment statuses were compared descriptively: overall outcome distribution, functional-group differences and primary reasons for withholding mitigation credit. Each refined entry counted once, irrespective of severity, occurrence or DC (no failure-rate weighting). No inferential tests were performed.

3.6.2. Calculation Bases and Rounding

Let N denote the total number of refined failure-mode entries evaluated in the review and n_c the number assigned to outcome category c. The overall proportion for each category is:

$$p_c = 100\frac{n_c}{N} \tag{1}$$

For the C1 subdivision,

The percentages for C1a and C1b use the complete refined inventory as their denominator.

$$n_{\mathrm{C1}} = n_{\mathrm{C1a}} + n_{\mathrm{C1b}} \tag{2}$$

Under the classification rules in Section 3.5, the aggregate proportion of changed review outcomes comprises categories C2–C4:

$$p_{\mathrm{changed}} = 100\frac{n_{\mathrm{C2}} + n_{\mathrm{C3}} + n_{\mathrm{C4}}}{N} \tag{3}$$

This quantity was calculated from the counts and not as the sum of independently rounded category percentages.

Two reporting bases were used for the functional-group analysis. Let n_g denote the number of refined failure-mode entries in functional group g and $n_{c,g}$ the number belonging to both group g and outcome category c. The contribution of a group–outcome combination to the complete reviewed inventory is

$$p_{c,g}^{\mathrm{total}} = 100\frac{n_{c,g}}{N} \tag{4}$$

and its proportion within the functional group is

$$p_{c,g}^{\mathrm{within}} = 100\frac{n_{c,g}}{n_g} \tag{5}$$

The first measure shows how much a group–outcome combination contributes to the complete dataset and the second describes the outcome distribution within the group.

Reason percentages used the number of refined entries classified as C4 as the denominator. Each entry contributed once under its primary reason (Section Classification Rules and Primary Reasons).

Published percentages were rounded independently to whole percentage points. Displayed sums may differ from 100% and rounded marginal values may differ from the sums of rounded table cells. A displayed value of 0% denotes fewer than 0.5% of the entries in the respective base and does not exclude individual occurrences.

3.6.3. Quality Assurance and Documentation Traceability

Individual safety-mechanism references were recorded in the revised HW-D-FMEA wherever an applicable assignment could be established. The revisions were maintained in APIS IQ-RM PRO (Version 8.0-0080) using the parallel effect-chain representation of Section 3.4.3.

4. Results

4.1. Overview of the Reviewed Dataset

The reviewed inventory contained functions and refined failure-mode entries, with both counts of the order of hundreds. The data sources and review timing are described in Section 3.2.

The inventory was organised into five functional groups. Table 6 presents their shares of the refined failure-mode inventory. Power supply and energy management accounted for the largest share, approximately 44%.

Table 6. Functional distribution of the refined failure-mode inventory.

Functional Group	Share of Failure-Mode Entries
Power supply and energy management	44%
Motor control and power electronics	20%
Communication interfaces	12%
Sensor interfaces	14%
Safety and diagnostic functions	11%

4.2. Overall Review Outcomes

Approximately 76% of refined entries were classified as C1. Supported baseline assignments were retained for 55% of all entries (C1a), while the baseline decision not to assign a diagnostic mechanism was confirmed for 21% (C1b). Categories C2–C4 accounted for 24%, with C4 as the largest category. The reasons for withholding credit are presented in Section 4.4. C1 denotes retention of assignment (presence or absence) and for supported assignments, the monitoring group. It does not imply that the failure description or individual mechanism reference remained unchanged. Because the baseline entries referenced groups rather than uniquely identified mechanisms, this comparison does not yield a complete mechanism-level change count. The review outcomes can be seen in Table 7.

Table 7. Overall review outcomes for the refined failure-mode inventory.

Code	Review Outcome	Share of Reviewed Entries
C1	Baseline assignment status retained	76%
C1a	Baseline diagnostic assignment retained	55%
C1b	Baseline non-assignment confirmed	21%
C2	Diagnostic assignment newly identified	2%
C3	Diagnostic assignment revised	5%
C4	No assignment retained for mitigation credit	17%

Note: Percentages refer to the complete refined inventory. C1a and C1b are subcategories of C1; C2–C4 together account for 24%. Definitions: Table 4.

4.3. Results by Functional Group

Tables 8 and 9 give the outcomes by functional group on two bases: within each group (Table 8) and as a share of the whole inventory (Table 9).

Table 8. Within-group distribution of review outcomes.

Functional Group	C1	C2	C3	C4
Power supply and energy management	63%	1%	11%	25%
Motor control and power electronics	95%	0%	0%	5%
Communication interfaces	92%	8%	0%	0%
Sensor interfaces	84%	5%	0%	12%
Safety and diagnostic functions	68%	0%	0%	32%

Note: C1–C4 percentages use the number of refined failure-mode entries within the respective group as their denominator. Outcome codes are defined in Table 4.

Table 9. Contributions of functional groups to the overall review-outcome distribution.

Functional Group	C1	C2	C3	C4
Power supply and energy management	27%	1%	5%	11%
Motor control and power electronics	19%	0%	0%	1%
Communication interfaces	11%	1%	0%	0%
Sensor interfaces	12%	1%	0%	2%
Safety and diagnostic functions	7%	0%	0%	4%

Note: Every percentage in Table 9 uses the complete refined failure-mode inventory as its denominator.

Baseline assignment status was most frequently retained in motor control and power electronics and in communication interfaces. Newly identified assignments (C2) were most frequent within communication interfaces, whereas reassignments (C3) were concentrated in power supply and energy management.

For C4 the two bases rank the groups differently: safety and diagnostic functions have the highest within-group proportion (32% vs. 25% for power supply and energy management), but the larger power-supply group contributes more C4 entries to the whole inventory (11% vs. 4%).

4.4. Observed Reasons for Withholding Mitigation Credit

Table 10 gives the primary reasons for C4 decisions. R1 (diagnostic-path operation insufficiently supported) was predominant, followed by R4 (documentation not yet approved).

Table 10. Primary reasons for withholding mitigation credit from diagnostic assignments classified as C4.

Code	Reason	Share Within C4
R1	Relevant diagnostic dependencies insufficiently substantiated	64%
R2	Signal correctness or redundant-channel status insufficiently substantiated	9%
R3	Time-critical state-change detection insufficiently substantiated	6%
R4	Diagnostic documentation not approved	21%

Note: Percentages refer to C4 entries. Each entry contributes once under its primary reason (Section Classification Rules and Primary Reasons). Reason codes are defined in Table 5.

R1 (power supply and energy management): rationales concerned shared circuitry, references or measurement and processing paths.
R2 (sensor interfaces): signal presence and structural validity alone did not establish correctness and redundant-signal comparison alone did not identify which channel could be relied upon.
R3 (motor control and power electronics): time-critical activation or deactivation; confirmation of command issuance did not establish detection of the physical transition within the relevant time window.
R4 (safety and diagnostic functions): the supporting records of one module were not yet approved for use in the revised HW-D-FMEA.

Section 4.5.2 illustrates an R1 decision; Section 5.1 relates the limitations to the cases and the safety lifecycle.

4.5. Illustrative Review Cases

Three anonymised cases from the platform review illustrate the assessment of diagnostic assignments.

4.5.1. Separating Communication Failure Manifestations

The baseline entry described a general internal communication failure and referenced a communication-monitoring group. Applying schema E separated missing messages from errors in received messages because these manifestations required different diagnostic observations.

Timeout monitoring checked whether an expected message arrived within the specified time window. A cyclic redundancy check (CRC) assessed message integrity, and a frame-counter check assessed sequence consistency. The CRC and counter checks depended on received messages and did not support the assignment for complete communication loss. They did not establish the semantic correctness of structurally valid data.

The mechanism specifications documented the combined use of these checks. The revised entries linked each manifestation to its relevant mechanism while retaining the original monitoring-group reference (C1a).

4.5.2. Assessing Diagnostic Dependencies in Voltage Measurement

The baseline entry described a short circuit in a voltage-measurement module and referenced a voltage-monitoring group. The candidate mechanisms compared voltage measurements. The failure description did not require subdivision.

Their coverage rationale relied on measurement independence, but none of the examined candidates was independent of the affected measurement function. The available documentation did not establish that the diagnostics would remain capable of detecting the specified short circuit despite this dependency.

No sufficiently supported alternative assignment was identified. The baseline assignment was therefore not retained for mitigation credit. The refined entry was classified as C4 with R1 as its primary reason. The assessment used the unmitigated system-level effect.

4.5.3. Separating a Failure Entry by Operating Phase

The baseline entry described a supply-related fault that could cause a measurement function to provide incorrect data and referenced a monitoring group. It did not distinguish between a fault already present at start-up and one arising during operation. Applying schema B separated these scenarios while retaining the same physical fault cause and distinguishing the affected measurement-processing function from its diagnostic checks. The operating-phase limitation of the baseline mechanism had not been explicit in its supporting description.

During operation, a change-sensitive check could use earlier measurement values to identify an abrupt deviation, including one that remained within the static validity range. This rationale could not be transferred to a fault already present at start-up because no preceding fault-free measurement was available. Remaining within the static range did not establish measurement correctness. The start-up assignment therefore combined cross-channel comparison of measurement-derived quantities with channel-specific checks, subject to diagnostic preconditions and persistence requirements. These checks did not depend on observing an initial transition from a fault-free value. They observed the fault through its effects on measurement data rather than directly measuring the affected supply condition.

The supporting safety-mechanism assessment records were reviewed for each check's activation conditions, observed quantities, persistence requirements and relationship to the intended response. The intended response was to use an available alternative measurement channel. The assessment therefore considered whether the diagnostic information supported the channel-selection decision. The operational entry retained the baseline monitoring group with clarified applicability conditions (C1a). A separate start-up entry received an accepted assignment from a different monitoring group (C3). Each entry recorded the applicable individual mechanism references and a phase-specific rationale. Neither assignment was inferred from the common failure description or monitoring-group reference.

5. Discussion

5.1. Principal Findings and Their Meaning

For most refined entries, the review confirmed either the baseline diagnostic assignment or the decision not to assign a mechanism. About one in six entries (C4) could not be credited as mitigation on the available evidence and document status; about four-fifths of

these (R1–R3) were withheld for insufficient technical substantiation and the rest (R4) for document approval status.

The cases illustrate why an assignment must be linked to the failure manifestation and the conditions covered by its supporting information. In Section 4.5.1, separating message absence from errors in received messages linked each scenario to the relevant diagnostic check while retaining the original monitoring group (C1a). In Section 4.5.2, the voltage-comparison rationale did not establish diagnostic operation under the specified short circuit in the presence of the measurement dependencies. Mitigation credit was therefore withheld (C4/R1). In Section 4.5.3, separating start-up and operation prevented evidence for one operating phase from being applied automatically to the other. The R2 and R3 findings further distinguish fault indication from evidence supporting signal correctness, channel selection or detection of a physical transition within the required time window.

Across the safety lifecycle, requirements development specifies the intended response and timing constraints. Design information and safety analyses provide a basis for assessing observation paths and dependencies. Integration and verification can provide evidence of detection and response performance [2,3,6]. The present lessons-learned review revisited the applicability of the available records to individual FMEA assignments during series production, identifying where the scenario–observation–response relationship remained insufficiently supported.

5.2. Limitations and Threats to Validity

The study examined a single steering control-unit platform covering a reusable architecture and five functional groups. No independent replication on other platforms was performed. The transferability of these findings to other architectures, organisations or vehicle-specific implementations remains untested. Functional-group differences may reflect inventory composition and documentation practices as well as differences in diagnostic support.

The statistics use refined failure-mode entries. A baseline entry divided into several scenarios contributes several counts, so the resulting proportions depend on the subdivision applied. Alternative refinement of the same baseline inventory could produce different distributions. The reported proportions therefore describe the refined scenario inventory, not the fraction of original baseline entries whose assignments changed.

Technical assignment decisions involved the responsible module engineers. Outcome classification and primary-reason selection were performed by A.E. Prior involvement in the baseline HW-D-FMEA and responsibility for the platform documentation provided system knowledge but also carried risks of interpretation and confirmation bias. Engineering judgement influenced the assessment of technical support and the selection of a primary reason where several limitations applied. The module engineers' participation in technical decisions did not constitute an independent second classification of the review outcomes. Validating the framework with independent reviewers is planned as part of future research (Section 5.4).

The review combined the baseline HW-D-FMEA with safety-mechanism assessment records available at the time of the review, including updated diagnostic information. Newly identified assignments may therefore reflect additional information or improved traceability as well as the structured review. The study does not isolate the framework's contribution from documentation updates or normal engineering review; a comparison using identical, fixed records is proposed in Section 5.4.

The industrial publication authorisation permits reporting of rounded percentages but not exact counts, including the baseline and refined inventory sizes, the number of subdivided entries and category counts. The underlying documents and detailed review

records also remain confidential. These restrictions limit independent recalculation of the reported percentages and external verification of individual decisions.

No new DC or response-time measurements were introduced. The results concern the justification of mitigation credit, not measured diagnostic effectiveness or demonstrated improvements in system safety. Insufficient evidence for an assignment does not establish that the implemented diagnostic mechanism is ineffective. Physical effectiveness requires verification under the specified fault conditions. The classifications were applied retrospectively; a prespecified protocol is proposed in Section 5.4.

5.3. Strengths and Practical Implications

The review covered every failure-mode entry within the defined scope and all five functional groups.

Different limitations call for different follow-up:

missing applicability information: additional documentation or analysis;
information contradicting applicability: reassignment or a technical change;
dependency concerns: examining whether the fault can impair the observation and response path;
document approval issues: resolution within the engineering documentation process.

The review outputs can support the selection of assignments that need further documentation, dependent-failure analysis, timing assessment or fault-injection testing. An independent safety assessment could examine whether the recorded evidence justifies selected assignments, while independent reclassification would assess the consistency of the reported outcomes. Fault-injection or HIL tests would instead examine detection and completion of the intended response under the specified fault conditions and timing requirement. For a selected scenario, the affected interface, fault onset, observable consequence and required response can inform the injection point and acceptance criteria of a subsequent HIL or fault-injection (FI) test. A new diagnostic mechanism is not required for every scenario without mitigation credit: the unmitigated effect remains the basis for deciding whether further measures are necessary.

Beyond electric power steering, the framework could support diagnostic-assignment reviews in other automotive electronic systems, such as braking controllers and battery-management systems. These systems also involve sensor interfaces, power supplies, communication paths and diagnostic functions whose applicability depends on the defined failure scenario. Adaptation would require system-specific failure categories, operating conditions, dependency information and response requirements. Future applications to these systems could help assess the framework's usability, transferability and reproducibility across different automotive architectures.

5.4. Future Evaluation

An independent second-reviewer assessment should use identical engineering records and a review protocol fixed in advance, including the C1–C4 definitions and rules for selecting primary reasons. Reviewers should record their initial decisions independently and agreement should be assessed before disagreements are resolved. Disagreements can identify ambiguous criteria and decisions that depend on system knowledge not explicit in the documentation.

To distinguish the framework's contribution from that of updated diagnostic information, existing practice and the proposed framework should be compared using the same fixed FMEA and safety-mechanism assessment records. The design should account for reviewer expertise and prior exposure and distinguish substantive assignment changes from documentation refinement.

Application to additional platforms should examine the usability and transferability of the schema and review criteria. Cross-platform comparisons using a common protocol must still account for differences in inventory composition, the level of failure-mode subdivision and the maturity of the supporting records.

6. Conclusions

This study presented a schema-based framework for reviewing diagnostic assignments in hardware design FMEA by linking failure-scenario descriptions, diagnostic observation paths, system responses and supporting engineering evidence. In the documentation review, approximately 17% of refined failure-mode entries had a previously documented diagnostic assignment that could not be retained for mitigation credit on the available technical information and document approval status.

The case study suggests that applicability should be assessed for a defined failure scenario, not inferred from a general monitoring reference. It also shows where further evidence is needed (Section 5.3).

The next step is an independent second-reviewer assessment (Section 5.4).

Author Contributions: Conceptualization, A.E. and Á.M.; methodology, A.E.; software, A.E.; validation, A.E.; formal analysis, A.E.; investigation, A.E., R.R.B. and A.T.; resources, A.E. and Á.M.; data curation, A.E.; writing—original draft preparation, R.R.B.; writing—review and editing, R.R.B. and A.T.; visualisation, A.E. and R.R.B.; supervision, Á.M. and A.T.; project administration, Á.M. and A.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: During the preparation of this manuscript, the authors used ChatGPT (OpenAI; GPT 6.1) to refine the scientific English wording and style of the manuscript following translation. The authors have reviewed and edited the outputs and take full responsibility for the content of this publication.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AIAG	Automotive Industry Action Group
CRC	Cyclic redundancy check
DC	Diagnostic coverage
DFA	Dependent failure analysis
ECU	Electronic Control Unit
FBSFM	Function–Behaviour–Structure–Failure Mode
FI	Fault injection
FMEA	Failure mode and effects analysis
FMEA-MSR	FMEA for Monitoring and System Response
FTTI	Fault-tolerant time interval
HIL	Hardware-in-the-loop
HiP-HOPS	Hierarchically Performed Hazard Origin and Propagation Studies
HW-D-FMEA	Hardware design failure mode and effects analysis
IF-FMEA	Interface-focused failure mode and effects analysis

ISO	International Organization for Standardization
M	Monitoring (rating)
MSR	Monitoring and System Response
STAMP	Systems-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
VDA	Verband der Automobilindustrie (German Association of the Automotive Industry)

References

1. Automotive Industry Action Group; Verband der Automobilindustrie. *Failure Mode and Effects Analysis—FMEA Handbook*, 1st ed.; Automotive Industry Action Group: Southfield, MI, USA, 2019.
2. *ISO 26262-9:2018*; Road Vehicles—Functional Safety—Part 9: Automotive Safety Integrity Level (ASIL)-Oriented and Safety-Oriented Analyses. International Organization for Standardization: Geneva, Switzerland, 2018.
3. *ISO 26262-5:2018*; Road Vehicles—Functional Safety—Part 5: Product Development at the Hardware Level. International Organization for Standardization: Geneva, Switzerland, 2018.
4. Bozzano, M.; Munk, P.; Schweizer, M.; Tonetta, S.; Vozárová, V. Model-Based Safety Analysis of Mode Transitions. In *Computer Safety, Reliability, and Security*; Lecture Notes in Computer Science; Casimiro, A., Ortmeier, F., Bitsch, F., Ferreira, P., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 12234, pp. 99–114.
5. Abboush, M.; Bamal, D.; Knieke, C.; Rausch, A. Hardware-in-the-Loop-Based Real-Time Fault Injection Framework for Dynamic Behavior Analysis of Automotive Software Systems. *Sensors* **2022**, *22*, 1360. [CrossRef] [PubMed]
6. *ISO 26262-3:2018*; Road Vehicles—Functional Safety—Part 3: Concept Phase. International Organization for Standardization: Geneva, Switzerland, 2018.
7. Avižienis, A.; Laprie, J.-C.; Randell, B.; Landwehr, C. Basic Concepts and Taxonomy of Dependable and Secure Computing. *IEEE Trans. Dependable Secur. Comput.* **2004**, *1*, 11–33. [CrossRef]
8. Inada, R.; Hirotsu, T.; Morita, Y.; Hata, T. Diagnostic Coverage Evaluation Method for Analog Circuits to Comply with Functional Safety Standards. In *Proceedings of the SAE Technical Paper 2015-01-0267*; SAE International: Warrendale, PA, USA, 2015.
9. Papadopoulos, Y.; McDermid, J.A. Hierarchically Performed Hazard Origin and Propagation Studies. In *Computer Safety, Reliability and Security*; Lecture Notes in Computer Science; Felici, M., Kanoun, K., Eds.; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1698, pp. 139–152.
10. Joshi, A.; Miller, S.P.; Whalen, M.; Heimdahl, M.P.E. A Proposal for Model-Based Safety Analysis. In *Proceedings of the 24th Digital Avionics Systems Conference*; IEEE: Washington, DC, USA, 2005; Volume 2, pp. 8.C.2-1–8.C.2-13.
11. Lee, D.; Lee, D.; Na, J. Automatic Failure Modes and Effects Analysis of an Electronic Fuel Injection Model. *Appl. Sci.* **2022**, *12*, 6144. [CrossRef]
12. Leveson, N. *Engineering a Safer World: Systems Thinking Applied to Safety*; Engineering Systems; MIT Press: Cambridge, MA, USA, 2011.
13. Sini, J.; Violante, M.; Tronci, F. A Novel ISO 26262-Compliant Test Bench to Assess the Diagnostic Coverage of Software Hardening Techniques against Digital Components Random Hardware Failures. *Electronics* **2022**, *11*, 901. [CrossRef]
14. Younus, H.; Campean, F.; Kabir, S.; Bonnaud, P.; Delaux, D.; Yildirim, U. An Ontological Framework for the Integration of System Design and FMEA. *AIEDAM* **2025**, *39*, e31. [CrossRef]
15. Prashanth Reddy, G.; Leburu, R. Matrix Approach to Perform Dependent Failure Analysis in Compliance with Functional Safety Standards. In *Proceedings of the Third International Conference on Computational Intelligence and Informatics*; Advances in Intelligent Systems and Computing; Raju, K.S., Govardhan, A., Rani, B.P., Sridevi, R., Murty, M.R., Eds.; Springer: Singapore, 2020; Volume 1090, pp. 123–131.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.