Verification of lattice-theoretic safety integrity level formalization

The proposed cross-standard mapping of safety integrity levels contains **significant inaccuracies** alongside some verified claims. While individual standards do form total orders internally, the claimed cross-standard equivalences are problematic, and no official lattice-theoretic unification exists in academic literature or industry practice.

IEC 61508 probability thresholds are accurately stated

The document's claimed PFH (Probability of Dangerous Failure per Hour) ranges for continuous/high-demand mode are **verified correct** per IEC 61508-1 Tables 2 and 3:

SIL	Claimed PFH	Verified PFH	Status
SIL 1	10^{-5} to 10^{-6}	$\geq 10^{-6}$ to $<10^{-5}$	✓ Correct
SIL 2	10^{-6} to 10^{-7}	$\geq 10^{-7}$ to $<10^{-6}$	✓ Correct
SIL 3	10^{-7} to 10^{-8}	$\geq 10^{-8}$ to $<10^{-7}$	✓ Correct
SIL 4	10^{-8} to 10^{-9}	$\geq 10^{-9}$ to $<10^{-8}$	✓ Correct

IEC 61508 also defines a low-demand mode using **PFDavg** (Probability of Failure on Demand), with correspondingly different threshold values. Emerson The risk graph method in IEC 61508-5 Annex D Emerson includes outcomes below SIL 1: Emerson "a" (no special safety requirements) and "-" (risk already tolerable). Wikipedia Each SIL level represents exactly one order of magnitude improvement in reliability—a mathematically elegant structure that supports the total ordering claim.

ISO 26262 uses hybrid qualitative-quantitative assessment

ISO 26262 **does not define explicit probability targets for ASIL determination**—a critical departure from IEC 61508's approach. ASIL levels are assigned qualitatively through Hazard Analysis and Risk Assessment (HARA) combining three parameters: Severity (S0-S3), Exposure (E0-E4), and Controllability (C0-C3). Wikipedia However, once ASIL is assigned, hardware components must meet quantitative **PMHF (Probabilistic Metric for Hardware Failure)** targets:

- **ASIL A**: No quantitative PMHF requirement (qualitative process only)
- **ASIL B**: PMHF $<10^{-7}$/hour, SPFM ≥90%, LFM ≥60%
- **ASIL C**: PMHF $<10^{-7}$/hour, SPFM ≥97%, LFM ≥80%
- **ASIL D**: PMHF $<10^{-8}$/hour, SPFM ≥99%, LFM ≥90%

QM (Quality Management) is verified as the "no safety requirements" level—applied when risk assessment yields negligible hazard classifications. Critically, ASIL B and C share the same PMHF threshold (<10^{-7}/hour) but differ in architectural metrics, demonstrating that ISO 26262's integrity classification cannot be reduced to simple probability thresholds.

DO-178C is fundamentally qualitative with probability targets inherited from related standards

DO-178C itself **defines no quantitative probability thresholds**—it prescribes design assurance through process rigor (number of objectives, verification activities, independence requirements). The probability targets cited in cross-standard mappings actually come from **AC 25.1309-1** (FAA Advisory Circular) and **SAE ARP4761** (Safety Assessment Process):

DAL	Failure Condition	Probability Target (AC 25.1309)	DO-178C Objectives
A	Catastrophic	≤10^{-9} per flight hour	71 (33 independent)
B	Hazardous	≤10^{-7} per flight hour	69 (21 independent)
C	Major	≤10^{-5} per flight hour	62 (8 independent)
D	Minor	>10^{-5} (Probable)	26 (5 independent)
E	No Safety Effect	None	0

DAL E is confirmed as the "no safety effect" level—explicitly stated as being "outside the purview of DO-178C." The rationale for DO-178C's qualitative approach is significant: software failures result from **design errors (systematic failures)**, not random hardware failures, and there is no statistically valid method to calculate probability of software design errors.

ECSS and IEC 62304 use severity-based classification without probability thresholds

ECSS (European Space) defines four software criticality categories (A, B, C, D) where A is highest criticality—opposite to IEC 62304's ordering. LDRA ECSS-Q-ST-40C explicitly states that **probabilistic assessment of software failures is NOT to be used as a criterion for software criticality category assignment**. ecss Classification is based purely on consequence severity of function failure and availability of compensating provisions. ecss

IEC 62304 uses three classes (A, B, C) where C is highest risk. Johner-institute The 2015 amendment introduced risk acceptability considerations beyond pure severity, but **no quantitative probability thresholds are specified**. Aligned AG Class determination follows: Class A (no harm possible), Class B (non-serious injury possible with unacceptable risk), Class C (death/serious injury possible with unacceptable risk). Johner-institute

Cross-standard equivalences are fundamentally problematic

The document's claimed mappings contain significant errors when examined against actual quantitative targets:

Claim	Analysis	Verdict
SIL 3 ≈ ASIL D ≈ DAL A (~10^{-8} to 10^{-9})	ASIL D requires <10^{-8}/hr (within SIL 4 range); DAL A requires <10^{-9}/hr (also SIL 4 range)	**Incorrect**
SIL 4 ≈ ASIL D ≈ DAL A (highest)	All represent highest integrity; quantitatively SIL 4 (≥10^{-9} to <10^{-8}), ASIL D (<10^{-8}), DAL A (<10^{-9})	**More accurate**
SIL 1 ≈ ASIL A ≈ DAL D	ASIL A has no quantitative target; academic research suggests ASIL A is "below SIL 1"	**Disputed**
SIL 2 ≈ ASIL B ≈ DAL C	ASIL B requires <10^{-7}/hr (SIL 3 range); DAL C requires <10^{-5}/hr (SIL 1 range)	**Incorrect**

Wikipedia explicitly confirms: "ISO 26262 does not provide normative nor informative mapping of ASIL to SIL; while the two standards have similar processes for hazard assessment, ASIL and SIL are computed from different perspectives." Taylor & Francis Online Wikipedia Furthermore, "DAL A and ASIL D represent the highest levels of risk addressed by the respective standards, but they do not address the same level of hazard. While ASIL D encompasses at most the hazards of a loaded passenger van, DAL A includes the greater hazards of large aircraft loaded with fuel and passengers." Wikipedia +2

An IEC Technical Report (TR 61508-6-1) on cross-standard recognition is reportedly in development for 2025, which may provide the first official harmonization guidance. Taylor & Francis Online

Structural claims require significant qualification

Total order within standards: VERIFIED. Each standard's integrity levels form a strict linear ordering—SIL 1 < SIL 2 < SIL 3 < SIL 4; QM < ASIL A < ASIL B < ASIL C < ASIL D; DAL E < DAL D < DAL C < DAL B < DAL A (note reversed alphabetical direction). This supports the mathematical claim that individual standards can be modeled as totally ordered sets.

"Join = max" composition principle: PARTIALLY TRUE but oversimplified. When a component serves multiple requirements with different integrity levels, it inherits the highest level—this supports "max." However, both IEC 61508 and ISO 26262 allow achieving higher system integrity from lower-rated components through **decomposition/synthesis rules**:

- IEC 61508 allows SIL synthesis: SIL 1 + SIL 1 → SIL 2 (with redundancy and independence)
- ISO 26262 allows ASIL decomposition: ASIL D → B(D) + B(D), or C(D) + A(D) Infineon Developer Community
- These rules require "sufficient independence" and freedom from common-cause failures Spyrosoft
- Homogeneous redundancy alone is NOT sufficient for level reduction

This violates a simple lattice "join" operation—the composition rules are combinatorial and conditional, not pure algebraic operations.

Universal risk equation: NOT VERIFIED. The claimed equation R = P_hazard × P_exposure × P_unavoidable × Severity_weight is not used universally:

- **IEC 61508**: Uses a risk graph with four parameters (Consequence, Frequency, Possibility of avoiding, Probability of occurrence) combined via graphical decision tree, not multiplication Emerson ResearchGate
- **ISO 26262**: Uses qualitative S×E×C lookup table, not arithmetic combination
- **DO-178C/ARP4761**: Uses severity classification with probability targets per flight hour; inverse relationship (higher severity → lower allowable probability)

Academic literature on lattice-theoretic formalization is sparse

Extensive searching found **no published papers specifically proposing lattice-theoretic formalization** of safety integrity levels. The closest mathematical frameworks are:

Contract Theory Extensions (Westman & Nyberg, 2015): Introduces a "contract structure" graph to capture SIL inheritance and decomposition using assume/guarantee pairs. This provides formal definitions for SIL assignment in accordance with IEC 61508 and ISO 26262, but uses graph structures and refinement orderings rather than explicit lattice algebra.

Contracts for System Design (Benveniste et al., 2012-2018): Develops a mathematical meta-theory with refinement ordering and parallel composition operators. While providing partial order structure, this work focuses on contract composition rather than safety level algebra.

ARRL Proposal (Verhulst et al., SAFECOMP 2013): Argues that Safety Integrity Levels are insufficient for compositional safety engineering, proposing "Assured Reliability and Resilience Level" as an alternative criterion better suited to system composition.

The practical "take the maximum SIL" composition rule used in industry **lacks rigorous mathematical foundation in published literature**. No category-theoretic, pure order-theoretic, or algebraic unification across standards has been formally published. This represents a genuine research gap.

Key limitations that break proposed isomorphism

Several domain-specific factors make direct cross-standard comparison fundamentally problematic:

- **Methodological incompatibility**: IEC 61508 uses quantitative probability targets; H-ON ISO 26262 uses qualitative risk classification; DO-178C uses process-based design assurance objectives
- **Different demand modes**: IEC 61508 distinguishes low-demand (PFDavg) from high-demand/continuous (PFH); automotive treats systems as continuous; aviation uses per-flight-hour metrics
- **Consequence scale differences**: Aviation DAL A addresses catastrophic aircraft loss with hundreds of potential fatalities; automotive ASIL D addresses at most a loaded passenger van—fundamentally different hazard magnitudes

- **Software treatment**: DO-178C explicitly states design errors cannot be probabilistically quantified; IEC 62304 and ECSS similarly reject probability-based software classification
- **Historical independence**: These standards were developed independently by different domain communities (process industry, automotive, aerospace, space, medical) without design intent for compatibility

The proposed lattice-theoretic unification is an intellectually interesting formalization attempt, but current evidence suggests it oversimplifies essential domain-specific factors that safety engineering communities consider non-negotiable for their respective application contexts.