Novel Mathematical Directions for Unifying Safety Integrity Levels

Safety integrity level unification across IEC 61508 (SIL), ISO 26262 (ASIL), DO-178C (DAL), and other standards remains mathematically underdeveloped despite decades of industrial use. This research identifies **several largely unexplored categorical and algebraic frameworks** that directly address the core challenges of "lossy mappings" and "dimensional heterogeneity" between standards. The most promising directions combine **institution theory** for heterogeneous specification interoperability, **quantale-enriched categories** for formalizing cross-standard distance, **sheaf theory** for compositional local-to-global reasoning, and **resource theories** for safety budget tracking. Critically, while these mathematical tools have been successfully applied in analogous domains—particularly ontology alignment and healthcare terminology unification—their application to functional safety standards represents significant unexplored territory.

Galois connections offer precise semantics for "lossy but useful" translations

The fundamental problem of cross-standard mapping—that semantic equivalence is impossible yet structural correspondence exists—finds natural expression through **Galois connections**. A Galois connection between posets $(A, \leq)$ and $(B, \leq)$ consists of monotone functions $F: A \to B$ and $G: B \to A$ satisfying $F(a) \leq b \iff a \leq G(b)$. This structure captures exactly the "best approximation" property needed for safety level translation: F gives the tightest upper bound in B for any element of A, while G provides the tightest lower bound in A for any element of B.

The composites $G \circ F$ and $F \circ G$ form **closure and kernel operators** respectively, with the key property that $G \circ F(a) \geq a$ (inflationary). This means the round-trip translation from SIL to ASIL and back always results in an element at least as stringent as the original—precisely the conservative behavior required for safety certification. When $F \circ G$ equals the identity (a **Galois insertion**), the abstract domain captures exactly some aspects of the concrete domain without loss, providing a formal characterization of when cross-standard translation is lossless.

Research in ontology alignment has directly applied Galois connections to analyze mappings between upper ontologies (DOLCE, GFO, SUMO). A 2013 study on "Compatible and Incompatible Ontology Mappings" demonstrated that when mappings between ontologies fail to form a Galois connection, this failure **precisely identifies semantic incompatibilities**. This methodology could be immediately adapted to detect and characterize incompatibilities in SIL $\leftrightarrow$ ASIL $\leftrightarrow$ DAL correspondences. Adjoint functors generalize this to categories, where the "free-forgetful" adjunction paradigm—with the forgetful functor R losing structure and left adjoint F freely generating the best compatible structure—models how cross-standard translations attempt to reconstruct lost information "to the best of their ability." Bartosz Milewski's Programmi…

Institution theory provides the foundation for heterogeneous specification interoperability

Goguen's institution theory offers the most mature framework for integrating heterogeneous logical systems, making it exceptionally relevant to safety standard unification. (nLab) An institution I = (Sign, Sen, Mod, ⊨) consists of a category of signatures, functors for sentences and models, and a satisfaction relation satisfying the crucial **satisfaction condition**: truth is invariant under change of notation. Each safety standard can be formalized as an institution with its own signatures (hazard classifications, integrity levels, verification requirements), sentence structures (safety requirements), and models (compliant systems).

Institution comorphisms $\mu: I \to I'$ provide the mechanism for cross-standard translation, consisting of signature translation Φ, sentence translation α, and model reduct β. The fundamental property—that comorphisms preserve semantic consequence—ensures that safety properties proven in one standard transfer correctly to another. This addresses a critical gap where current cross-standard mappings lack formal semantic guarantees.

The **Grothendieck construction** enables "flattening" a diagram of institutions into a single unified institution. Given institutions for IEC 61508, ISO 26262, DO-178C, ECSS, and IEC 62304 connected by comorphisms, the Grothendieck institution provides a single framework where each standard retains its native formalism while cross-standard proofs become possible through the unified structure. Mossakowski's 2002 work established that Grothendieck institutions based on comorphisms provide a sound foundation for heterogeneous specification. (Semantic Scholar)

The **DOL (Distributed Ontology, Modeling and Specification Language)** OMG standard, developed by Mossakowski, Kutz, and Codescu, provides practical infrastructure for this approach. DOL supports "as-is" integration of specifications from different logics, modular composition through extension and union operations, and formal alignment mappings between heterogeneous ontologies. The **Heterogeneous Tool Set (Hets)** implements this framework, supporting 25+ logics connected by comorphisms, with development graphs enabling structured heterogeneous proofs. No existing work applies this infrastructure to safety standards—a significant opportunity for extending DOL with safety-specific constructs including PFD calculations and HARA parameters.

Quantales and tropical semirings capture the algebraic structure of risk composition

Quantales—closed monoidal suplattices with an associative tensor product distributing over joins—provide exactly the right level of abstraction for safety level composition. The **Lawvere quantale** $([0,\infty], \geq, +, 0) \cong ([0,1], \leq, \times, 1)$ is fundamental for metric spaces and probability reasoning. (University of Portsmouth) Its "ultra" variant $([0,\infty], \geq, \max, 0)$ directly models safety level composition where max/min operations dominate. The **Łukasiewicz quantale** with truncated addition ($u \oplus v = \min\{u+v, 1\}$) suits bounded probability aggregation.

The connection to failure probability is precise: Risk Reduction Factor (RRF) relates logarithmically to SIL, so in the log domain, SIL addition becomes RRF multiplication—**exactly tropical/max-plus structure**. A 2004

paper on "Reliability Calculus Using Max-Plus Algebra" demonstrated direct application to finding system structure functions, tracking lowest achievable system reliability, and determining component reliability combinations ensuring system reliability bounds. ScienceDirect However, no work connects quantale theory specifically to safety integrity level frameworks.

Enriched categories over quantales (Lawvere metric spaces) offer a principled framework for measuring "distance" between cross-standard safety levels. In a quantale-enriched category, hom-objects take values in the quantale, satisfying $d(x,z) \leq d(x,y) + d(y,z)$ (triangle inequality) and $d(x,x) = 0$. Cross-standard distance $d(SIL_x, ASIL_y)$ would measure "translation loss," with positive values indicating information loss, zero indicating exact equivalence, and ∞ indicating no valid mapping. The triangle inequality ensures transitivity: translating SIL → ASIL → DAL loses at most as much as the sum of direct translations.

Lax functors preserve structure only up to non-invertible morphisms, with $F(g \circ f) \leftarrow F(g) \circ F(f)$ (comparison morphism, not isomorphism). This precisely models "lossy" cross-standard translation where composing safety measures in Standard A, translating individually to Standard B, may differ from translating the composite. Recent work cautions that lax functors are "ill-behaved" in bicategory terms—rigorous foundations require **double categories** or careful treatment of lax-oplax pairs.

Sheaf theory addresses local-to-global safety composition

Sheaves provide a canonical framework for the principle "local consistency implies global consistency"—precisely the challenge of SIL decomposition where subsystem requirements must compose to system-level safety. Research has identified two senses of compositionality in sheaves: the **vertical sense** where presheaves preserve spatial relations as algebraic relations, and the **horizontal sense** where data attached to open sets glues together to construct data on larger sets. Royal Society Open Science

Cellular sheaves have been successfully applied to distributed multi-agent coordination (Hanks et al., arXiv 2025), representing local constraint systems for data on networks. Sheaf Laplacians translate local constraints into operators for distributed algorithms. Jakobhansen A 2025 paper on "Task Sheaves for Distributed Computing" demonstrated that non-trivial sections correspond to valid solutions, while **obstructions to global sections represent system limitations making tasks unsolvable**— ResearchGate directly relevant to identifying when safety decomposition is fundamentally impossible.

The application to safety is direct: model system architecture as a base space (poset of subsystem containment), safety requirements as stalks, SIL decomposition rules as restriction maps, valid system-level safety as global sections, and **sheaf cohomology as obstruction detection** for decomposition failures. Hansen's work establishes that sheaf cohomology measures "distance" between separated presheaves and their sheafifications—quantifying the degree of compositional failure. ResearchGate A meta-theorem for sheaf-based decision problems states that problems formulated as sheaves can be solved in linear time on compositionally-constructed inputs, arXiv suggesting efficient algorithms for verifying safety decomposition validity.

Topos theory extends this to heterogeneous logical systems. Different safety standards embody different "logics": IEC 61508 uses probabilistic and categorical reasoning, ISO 26262 uses risk-based HARA parameters,

DO-178C uses deterministic failure condition classification. Each standard's reasoning framework can be modeled as a topos with its own internal logic, with safety level lattices internalized within the topos structure. **Geometric morphisms** between topoi preserve geometric theories (roughly first-order with existential and disjunctive axioms) but may not preserve all higher-order properties— (nLab)precisely characterizing what safety properties transfer versus what is lost. Caramello's "bridge" methodology using **classifying topoi** provides a principled approach to relating standards through their shared semantic foundation.

Contract-based design reveals gaps requiring lattice-theoretic extensions

Westman and Nyberg's foundational work on "Extending Contract Theory with Safety Integrity Levels" (IEEE HASE 2015) established that contract structures—directed acyclic graphs organizing contracts over an architecture—can formalize SIL inheritance and decomposition. Their key formal definition captures the "take maximum" rule: **$SIL\_R = max(SIL\_R_1, ..., SIL\_R_n)$** for requirements a contract must fulfill. The CPS Specifier tool demonstrated practical applicability at Scania.

However, significant gaps remain. Current frameworks lack **quantitative semantics**: SILs are treated as discrete labels without probability-theoretic underpinning or formal connection to PFD requirements. **Decomposition formalization is incomplete**: while inheritance patterns are captured, IEC 61508's specific arithmetic rules (SIL 3 → SIL 2 + SIL 2 requiring independence proof) and common cause failure analysis remain external to contract semantics. Most critically, **no cross-standard unification exists**—different standards have different decomposition semantics not captured by any unified framework.

Benveniste et al.'s 2018 monograph established that contracts form a **lattice structure** (Inria) with conjunction $C_1 \sqcap C_2$ (weaker assumptions, stronger guarantees) and a dominance relation. This lattice-theoretic foundation aligns with safety level orderings but doesn't address conditional operations. The fundamental gap is that **standard decomposition rules are not pure lattice operations**—they require additional verification of independence and CCF analysis. This suggests the need for **conditional lattices** where operations are defined only on certified subsets, or **product lattices** L = L_functional × L_systematic × L_probabilistic capturing multiple aspects with morphisms between standard-specific structures.

Recent advances include the Pacti tool (2023-2024) supporting compositional analysis with "hypercontracts," stochastic contracts (Nuzzo et al.) using bounded StSTL for probabilistic requirements, and compositional barrier certificate methods. The railway domain has seen substantial progress with OCRA-based temporal logic verification enabling decomposition of large networks. Yet the specific open problems—unified SIL/ASIL/DAL lattice structure, conditional composition operators, quantitative contract lattices, and compositional independence verification—remain unaddressed.

Analogous domains demonstrate successful mathematical unification approaches

The **Ontology Alignment Evaluation Initiative (OAEI)** provides the most mature benchmark for heterogeneous schema mapping. Key mathematical insights include distinguishing matching (probabilistic

similarity) from mapping (logical axioms), using confidence-weighted assertions rather than binary equivalences, and supporting multiple relationship types (equivalence, subsumption, disjointness, part-of). Wikipedia Category-theoretic formalization by Zimmermann et al. (2006) defined **V-alignments** as pairs of morphisms with common domain, with categorical operations for ontology merging, alignment composition, and intersection. Inria

NIST's OLIR Program for security framework mapping (NISTIR 8278A) demonstrates formal methodology transferable to safety standards: relationship types (subset, intersects, equal, superset, not related), rationale categories (syntactic, semantic, functional), bidirectional mappings, and Derived Relationship Mappings for computational gap analysis. Critical insight: mappings document that control domains have different structures and objectives, with many-to-many relationships requiring expert validation.

The **ICD-11/SNOMED CT harmonization** represents the most ambitious terminology unification, using a common ontology (subset of SNOMED CT concepts) as shared semantic foundation, ResearchGate axiom-based alignment in OWL, and hybrid semantic matching combining lexical and ontological methods. When multiple methods agreed on mappings, **93% accuracy was achieved**— NCBI a critical finding for safety standard unification suggesting that multi-method consensus dramatically improves reliability.

Common patterns emerge across all domains: **intermediate reference ontologies** provide semantic grounding for alignment (like BFO in ontology alignment); hybrid approaches combining lexical, structural, and semantic methods outperform single techniques; bidirectional mappings reveal asymmetries (translating "A to B" differs from "B to A"); and no domain has achieved full formal unification of heterogeneous standards—**dimensional heterogeneity remains theoretically unsolved**. Successful strategies include modular architecture allowing local extensions while maintaining global coherence, version-controlled mappings with lifecycle management, and confidence-weighted rather than binary assertions.

Resource theories and coalgebra offer novel compositional semantics

Resource theories from quantum information (Coecke, Fritz, Spekkens 2016) formalize situations where certain resources cannot be freely created—exactly the constraint facing safety margin allocation. The core structure consists of a symmetric monoidal category P of processes and a wide subcategory P_free of "free" processes, with resource conversions as morphisms using free processes to transform costly resources. wordpress The key **monotonicity property**—if $A_1 \geq B_1$ and $A_2 \geq B_2$, then $A_1 \otimes A_2 \geq B_1 \otimes B_2$—ensures compositional reasoning. dagstuhl

A novel **Safety Resource Theory** would model failure probability allocations as resources "consumed" through composition, with safety margins as costly resources that cannot be freely created. Objects would be system components with associated failure probability budgets; morphisms would be safety-preserving compositions; free processes would be compositions that don't increase hazard exposure. Monotone properties track failure probability (non-increasing under safe composition), diagnostic coverage, and proof obligation complexity. Marsden and Zwart's "Quantitative Foundations for Resource Theories" (CSL 2018) provides categorical

foundations for cost-annotated conversions and enriched categories with quantitative hom-objects—directly applicable infrastructure. (dagstuhl)

Coalgebraic methods offer behavioral semantics where integrity levels emerge as equivalence classes. Rutten's Universal Coalgebra (2000) establishes that behavioral equivalence—two states are equivalent iff mapped to the same point in the final coalgebra—captures "observationally indistinguishable" systems. For safety, systems at the same SIL would form a behavioral equivalence class based on observable failure modes, hazard propagation behavior, and diagnostic response patterns. The **final coalgebra** would serve as a universal safety behavior space, with cross-standard mapping becoming functors between coalgebras preserving behavioral equivalence.

String diagrams provide visualization for safety composition, with wires carrying failure probability bounds typed by integrity level, boxes representing components with input/output failure specifications, and diagram equations expressing SIL-preserving architectural transformations. Series composition (failure rates add), parallel redundancy (failure rates multiply), and voting (2oo3) become graphical rewrite rules. No existing work applies this framework to safety—a significant gap given that safety systems are fundamentally compositional.

Concrete recommendations for extending the research program

The most promising immediate directions focus on **institution-theoretic unification**: formalizing each safety standard as an institution with explicit signatures, sentences, and models; constructing trial comorphisms between pairs (particularly SIL ↔ ASIL); analyzing Galois connection properties of existing informal mappings; and prototyping in DOL/Hets to leverage existing infrastructure. The DOL/Hets ecosystem provides ready tools that could be extended with safety-specific constructs.

Quantale-theoretic foundations require formal definition of a "Safety Quantale" capturing risk reduction composition rules from IEC 61508, with proof that the tensor product satisfies quantale axioms. Implementation of tropical semiring methods for fault tree analysis would extend existing max-plus reliability calculus to multi-standard environments. Enriched category frameworks for cross-standard distance formalization would provide the rigorous metric structure currently lacking.

Sheaf-theoretic safety architecture models should be developed with base spaces as subsystem containment posets, restriction maps encoding decomposition rules, and cohomology computations on realistic system architectures to identify composition obstructions. Cellular sheaf algorithms could be implemented for automated safety case composition and verification, leveraging recent distributed systems work.

Resource-theoretic safety budgets require adapting quantum resource theory infrastructure to safety contexts, with formal characterization of "free" versus "costly" safety operations and compositional tracking of failure probability allocations through system architecture.

Key researchers to engage include **Till Mossakowski** (Otto-von-Guericke University Magdeburg) on DOL and Hets, (Ease-crc) **Razvan Diaconescu** (Romanian Academy) on institution theory foundations, **David Spivak** (MIT) on applied category theory and sheaves, (Wikipedia) and the Benveniste/Nuzzo groups on contract theory

extensions. The mathematical machinery exists and has been proven in analogous domains—the gap is specifically its application to functional safety standard unification.

Conclusion

This research identifies a significant opportunity at the intersection of advanced categorical/algebraic structures and functional safety engineering. The "lossy mapping" problem finds precise formalization through **Galois connections** (best approximation) and **lax functors** (non-exact preservation). The "dimensional heterogeneity" problem is addressed by **institution theory** (heterogeneous logic integration), **quantale-enriched categories** (distance metrics over non-standard value domains), and **geometric morphisms** between standard-specific topoi (characterizing what properties transfer). The compositional nature of safety decomposition aligns with **sheaf-theoretic local-to-global principles**, **resource theories** for budget tracking, and **coalgebraic behavioral equivalence**.

What makes these directions particularly promising is their proven success in analogous domains—ontology alignment achieved 93% accuracy through multi-method consensus using category-theoretic foundations; healthcare terminology unification successfully employed common ontologies and hybrid semantic matching; security framework mapping developed formal relationship taxonomies with computational derivation. These techniques are directly transferable to safety standard unification, yet the specific application remains essentially unexplored. The research program thus has both solid theoretical foundations from category theory and practical validation from analogous engineering domains—requiring primarily the bridging work to adapt these tools to the specific requirements and constraints of functional safety certification.