Upstream Compression, Downstream Consequences: A Risk Migration Framework for Engineering Lifecycle Transitions

Jennifer R. Ayres[1], Rosmina A Bustami[2], Jethro H Adam.

UNIMAS Water Centre (UWC), Faculty of Engineering, Universiti Malaysia Sarawak, 94300, Kota Samarahan, Sarawak, Malaysia

ORCID IDs: [1] 0000-0002-4538-6512 | [2] 0000-0002-8438-8932

Abstract

Commissioning is widely recognised as a critical phase for process safety, yet major incidents and early operational failures consistently reveal commissioning-origin vulnerabilities that were invisible at handover. Existing project risk models assume risk declines immediately after startup, obscuring a fundamental reality: many safety-critical failures originate during commissioning but activate later under normal operating conditions. This temporal disconnect leads to systematic misattribution of commissioning-origin vulnerabilities as operational errors or equipment defects, preventing effective organisational learning.

This paper introduces Commissioning Risk Drift (CRD) as a lifecycle framework grounded in established safety science theory. CRD explains how five interdependent mechanisms—commissioning compression, incomplete functional verification, bypass normalisation, knowledge discontinuity at handover, and activation under real loads—create downstream safety vulnerabilities. Operational manifestations include control instability, alarm floods, incompletely validated safety instrumented functions, and eroded safety margins. CRD operates invisibly because rapid demobilisation severs the link between upstream compression decisions and downstream safety consequences, enabling drift toward unsafe states.

Managing CRD requires lifecycle governance that extends beyond traditional project boundaries: aligning project and operational KPIs, protecting functional testing windows, retaining commissioning expertise through early operations, and implementing CRD-aware handover protocols. The framework repositions commissioning from a terminal project milestone to a safety-critical lifecycle transition requiring sustained process safety governance.

Keywords: Commissioning; Process Safety Management; Risk migration; Safety Instrumented Systems; Operational readiness; Lifecycle safety.

1. INTRODUCTION

Commissioning is routinely described as the final technical hurdle before a facility enters stable operation. In practice, it is one of the most compressed, least predictable, and most consequential phases of the engineering lifecycle. Evidence across energy, water, transport, and industrial infrastructure shows that a disproportionate share of early-life instability, equipment under-performance, and reliability problems originate during commissioning, especially when verification activities are constrained or incomplete (Forcada et al, 2016; Hopkins, 2012). Modular construction commissioning studies document persistent quality issues despite controlled factory conditions, suggesting Commissioning Risk Drift (CRD) mechanisms operate across delivery methods. Despite decades of evolution in process safety management—from Hazard and Operability Study (HAZOP) to Risk-Based Process Safety—commissioning remains the least regulated phase of the facility lifecycle, creating a systematic blind spot in Process Safety Management (PSM) frameworks. Scholarly attention overwhelmingly privileges design, project management, and steady-state operations, leaving the transitional phase between construction and operation under-theorised and poorly conceptualised in risk frameworks. This paper treats commissioning as a lifecycle reliability transition in which risk is transformed, displaced, and inherited rather than resolved. These vulnerabilities often surface weeks or months into operation, after handover teams have demobilised and organisational attention has shifted elsewhere.

This paper proposes Commissioning Risk Drift (CRD) as a mechanism that explains this lifecycle behaviour. First, early operational instability is frequently misattributed to operator behaviour, equipment design, or "bedding-in," obscuring the commissioning-origin mechanisms that drive it. Second, without a lifecycle model that acknowledges how commissioning risk migrates over time, organisations continue to rely on project-stage KPIs, demobilisation practices, and risk registers that fail to capture the cumulative handover of latent conditions into operations. The remainder of this paper develops the conceptual model, examines its operational and safety implications, and proposes governance approaches to mitigate CRD through lifecycle alignment. CRD reveals that commissioning compression systematically undermines these PSM assumptions, creating latent conditions that persist despite rigorous operational safety programs. This gap explains why facilities with mature PSM systems still experience elevated early-life failure rates and safety incidents.

2. BACKGROUND AND LITERATURE REVIEW

2.1 Commissioning as an Under-Theorised Lifecycle Phase

Most engineering risk frameworks conceptualise project delivery as a linear sequence culminating in a lifecycle transition from project delivery to operations. The sparse academic evidence available suggests that commissioning demands more complex decision-making and cross-disciplinary coordination than is usually captured in project governance tools (Leveson, 2011; Hopkins, 2012). Biological wastewater treatment commissioning (Tchobanoglous et al., 2014) exemplifies systems that require extended stabilisation periods, which are rarely accommodated in project schedules. While technical debt frameworks address design-development trade-offs (Kleinwaks et al., 2023), they do not address commissioning-to-operations transitions in practice.

In software and systems engineering, the metaphor of "technical debt" has emerged to describe how pragmatic near-term decisions create long-term technical obligations and system degradation (Cunningham, 1992) A recent systematic review (Kleinwaks et al., 2023) examined technical debt across systems engineering, finding that while the concept has gained traction in software domains, it remains underexplored in broader systems engineering contexts, with only 18 relevant studies identified from 354 papers reviewed.

Technical debt typically describes conscious shortcuts taken during design or development to meet schedule or cost constraints, with the expectation that future refactoring or rework will be required (Boehm & Behnamghader, 2018). CRD, by contrast, describes the unintended migration of latent conditions created during commissioning compression, where incomplete verification and knowledge discontinuity allow vulnerabilities to propagate invisibly into operations. Technical debt assumes visibility and intentionality; CRD operates through obscurity and structural handover gaps. Moreover, while the technical debt literature addresses software architecture and code quality, CRD applies specifically to the physical commissioning of process systems, where safety-critical functions, control loops, interlocks, and alarm systems are verified under constrained conditions that do not reflect the whole operational reality.

Research on mechanical and electrical commissioning highlights workload, time compression, and defect management issues. Water and wastewater literature often focuses on process start-up behaviour, especially the instability seen during biological process commissioning (Bafana et al., 2015). Safety-critical commissioning research identifies performance-shaping factors and human reliability considerations (Reason, 1990; Leveson, 2011). While valuable, these studies remain siloed and do not address the temporal migration of commissioning-origin risk into operations.

2.2 Latent Conditions, Drift, and the Foundations of Risk Migration

Reason’s foundational work on latent conditions establishes that organisational decisions made upstream can remain dormant until triggered by normal operational pressures (Reason, 1990). These latent conditions often arise from shortcuts, unclosed defects, temporary overrides, or incomplete testing — all characteristic of compressed commissioning environments.

Rasmussen’s model of drift toward the boundaries of acceptable performance explains how systems slowly accumulate adaptations under production pressure (Rasmussen, 1997). Systems-theoretic approaches to accident causation (Leveson, 2011) similarly emphasise how upstream constraints shape downstream hazards. Dekker similarly argues that safety problems emerge incrementally as minor adjustments gradually shift systems closer to failure (Dekker, 2014) Safety-II perspectives (Hollnagel, 2014) emphasize how system behaviour emerges from complexity rather than component failures, aligning with CRD's focus on interaction between commissioning compression and operational conditions while these concepts are well understood in operations and maintenance contexts, they have not been applied to commissioning — despite commissioning being a textbook environment for drift: high pressure, incomplete information, time constraints, undocumented workarounds, and competing priorities.

Hopkins’ analyses of major industrial disasters reinforce this view by showing how early-phase decisions and unverified assumptions can propagate into catastrophic outcomes downstream, masked by organisational blind spots (Hopkins, 2012). These insights align closely with commissioning practice, where incomplete functional verification or

undocumented logic changes can appear benign at handover but trigger instability when the plant is loaded, or operating conditions shift.

2.3 Limitations of Existing Risk Tools and Governance Practices

Process Safety Management frameworks—including CCPS Risk-Based Process Safety, ISO 45001, API RP 754, and OSHA PSM—acknowledge commissioning as critical, yet provide limited guidance on managing verification compression or knowledge discontinuity at handover. Such assumptions obscure the reality that many operational disruptions originate from upstream commissioning compression. Most project risk registers are event-focused and milestone-based, making them poorly suited to capturing latent, evolving, or migrating risks. They also typically close once practical completion is achieved, severing the organisational link between commissioning decisions and operational consequences.

Performance metrics reinforce this disconnect. Project key performance indicators (KPIs) emphasise schedule, budget, and milestone achievement — not operational stability or lifecycle performance. Process safety leading indicators (functional tests completed, safety system verifications, pre-startup safety reviews) measure activities during commissioning, but cannot capture the quality or completeness of verification under compressed conditions. Similarly, lagging indicators (early-life incidents, near-misses, safety function failures) attribute problems to operations, obscuring their commissioning. Commissioning teams often demobilise rapidly after lifecycle transition from project delivery to operations, removing the people most capable of diagnosing the origin of later failures. At the same time, operational teams inherit undocumented bypasses, incomplete tuning, and unresolved defects without context or historical knowledge. This structural discontinuity makes CRD both invisible and inevitable.

2.3.1 Process Safety Management Framework Gaps

Contemporary PSM frameworks (CCPS, 2007; OSHA, 1992) organise process safety around design, operations, and organisational elements but treat commissioning implicitly rather than explicitly (Broadribb, 2021). The RBPS element "Operational Readiness" requires verification before startup (CCPS, 2007), yet provides limited guidance on managing verification compression when commissioning windows contract due to upstream delays. Similarly, "Process Knowledge Management" assumes knowledge retention but does not address the rapid demobilisation that characterises project-to-operations handover (Hopkins, 2012).

API RP 754 Process Safety Performance Indicators (API, 2016) define Tier 1 (loss of primary containment) and Tier 2 (challenge to safety systems) events. Still, commissioning-origin vulnerabilities often surface as Tier 3 or Tier 4 events—minor deviations, nuisance alarms, control instability—that PSM frameworks do not systematically track. This measurement gap reinforces CRD invisibility: organisations count early-life incidents but do not trace them to commissioning compression

2.4 Summary

Although multiple disciplines have explored aspects of commissioning, none have articulated a lifecycle model explaining how commissioning-origin risks migrate, evolve, and eventually manifest in operations. Adjacent fields have developed related frameworks—most notably, the concept of technical debt in software and systems engineering, which describes how near-

term pragmatic decisions can lead to long-term system degradation (Kleinwaks et al., 2023_ However, technical debt frameworks assume conscious trade-offs made during design and development, with downstream refactoring as the expected remedy. These frameworks do not address the commissioning-to-operations transition, where latent conditions arise not from deliberate shortcuts but from compression, incomplete functional verification, and knowledge discontinuity at handover.

The convergence of latent condition theory (Reason, 1990) drift models (Rasmussen, 1997) and empirical commissioning studies (Forcada et al., 2016; Babar& Arain, 2019) demonstrates a strong foundation for understanding commissioning-origin risk behaviour. This paper builds on these foundations by introducing CRD as a formal mechanism that explains how commissioning compression creates downstream operational instability—a phenomenon distinct from technical debt but equally consequential for system lifecycle performance.

3. DEFINING COMMISSIONING RISK DRIFT (CRD)

CRD describes the systematic migration of risks created during compressed or incomplete commissioning activities into the early operational phase of engineered systems. CRD originates when commissioning teams—often under pressure from delayed construction, fixed commercial dates, or contractual incentives to accelerate practical completion—shorten or bypass verification tasks that require time, stability, or controlled conditions. These constraints affect activities such as functional testing, interlock and permissive checks, alarm rationalisation, loop tuning under load, instrument calibration, and defect closure.

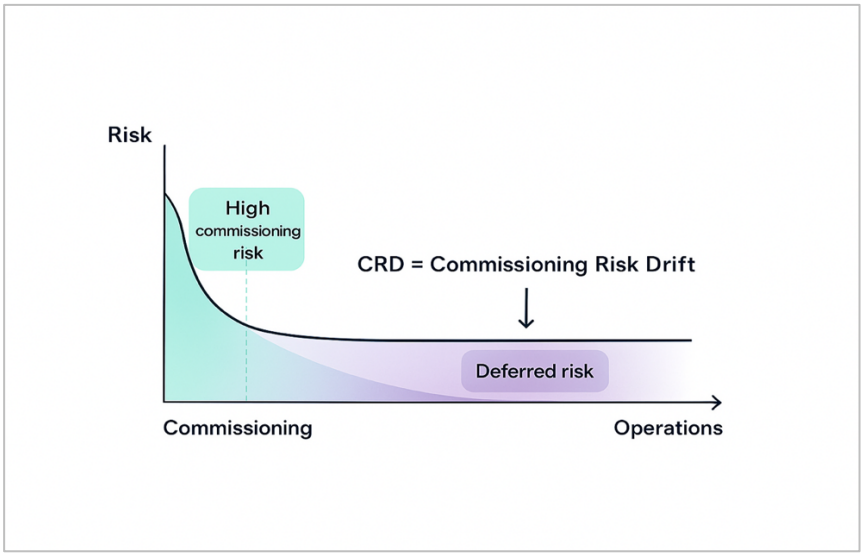

Figure 1. Commissioning Risk Drift (CRD) Lifecycle Curve

In the commissioning context, the drift occurs because unresolved issues are concealed beneath constrained testing conditions, masked by temporary overrides, or normalised as "how the system runs" during the final push to handover.

Structural discontinuities intensify this drift at handover. Commissioning personnel, who hold critical contextual knowledge of what was tested, deferred, and temporarily bypassed,

typically demobilise quickly. Operational teams inherit a system whose vulnerabilities are either undocumented or incompletely understood, leading to downstream failures that appear operational in origin but are, in fact, the delayed consequences of upstream compression.

CRD is therefore best understood as a lifecycle drift mechanism characterised by three interlinked processes:

1. Upstream Compression: Commissioning activities are constrained by schedule, resources, and competing commercial pressures, resulting in incomplete verification.
2. Latent Condition Formation: Workarounds, untested logic, unresolved defects, and temporary bypasses create hidden vulnerabilities embedded within the system.
3. Downstream Activation: Under real operating loads, environmental fluctuations, or optimisation attempts, these vulnerabilities manifest as operational instability, degraded performance, or safety-critical failures.

4. MECHANISMS UNDERPINNING COMMISSIONING RISK DRIFT

CRD arises not from a single failure point but from an interconnected set of mechanisms that shape how risk is created, concealed, displaced, and later activated. These mechanisms are illustrated in Figure 2.

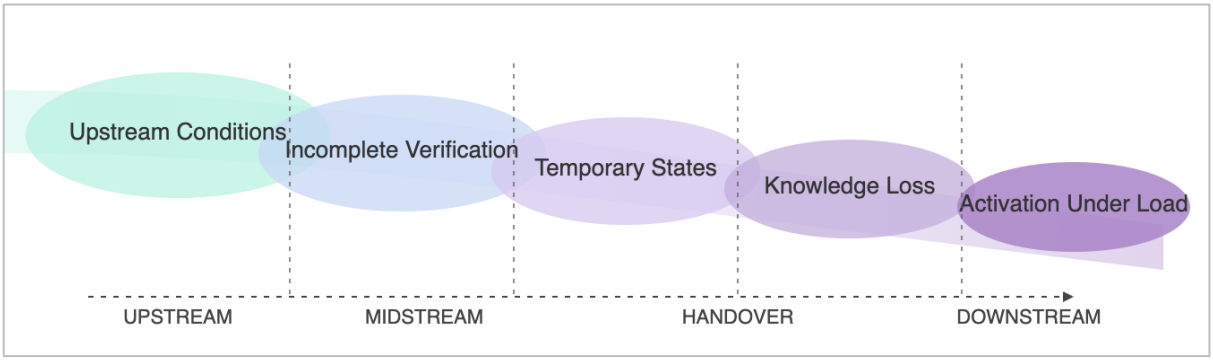

Figure 2. Mechanisms Underpinning Commissioning Risk Drift.

The overlapping phases illustrate how upstream conditions (schedule pressure, resource constraints) drive incomplete verification during commissioning, creating temporary states and undocumented bypasses that persist through handover due to knowledge discontinuity, subsequently activating as operational instability when exposed to real process loads. The progression from left (upstream causes) to right (downstream manifestations) represents the temporal migration of commissioning-origin vulnerabilities into operations.

4.1 Commissioning Compression

Commissioning compression is the primary upstream condition from which CRD emerges. Projects frequently face cascading delays from design, procurement, fabrication, and construction, yet handover dates often remain fixed due to contractual, financial, or political

pressures. As a result, commissioning teams are required to do more with less time, usually while systems are incomplete, unstable, or undergoing parallel modifications. Empirical commissioning studies confirm that such pressure constrains verification activities and forces prioritisation of visible, milestone-driven tasks at the expense of deeper functional testing.

Rasmussen's drift model helps explain this pattern: under production or schedule pressure, systems tend to migrate toward performance boundaries where shortcuts become normalised, and vulnerabilities accumulate gradually rather than through dramatic failure points.

4.2 Incomplete Functional Verification

Incomplete or constrained verification is the mechanism through which compression solidifies into latent conditions. Human factors research (Gokgoz et al., 2024) demonstrates that time pressure increases the likelihood of errors, directly applicable to compressed commissioning environments. Commissioning requires verification across multiple layers: control logic, interlocks, alarms, mechanical integrity, instrumentation accuracy, and system integration. However, these layers are often tested under idealised or non-representative conditions due to limited access windows, temporary dependencies, or unstable construction interfaces (Forcada et al., 2016; Ashrae, 2018)

Reason's latent condition framework applies directly here: omissions created upstream remain dormant until the plant is subjected to the conditions that reveal them—almost always after handover.

Safety Instrumented Function (SIF) validation, required per IEC 61511 (IEC, 2016) to achieve target Safety Integrity Levels (SIL), typically requires proof testing under representative process conditions (Lundteigen & Rausand, 2009). Compressed commissioning often validates SIFs under static or partial-load conditions, creating verification gaps that only become apparent when the SIF is challenged during operations (Lundteigen & Rausand, 2009).

4.3 Normalisation of Temporary Bypasses

Temporary bypasses, overrides, inhibits, or "workarounds" are common in commissioning because systems are rarely complete or stable at first energisation. These are intended to be short-lived tools that enable progress, yet under compressed conditions, they often become normalised. Once embedded, they are difficult to track, easy to forget, and rarely documented adequately. During handover, such temporary states may be unknowingly transferred to operations, where they become embedded modes of functioning.

Dekker notes that normalisation of deviations is one of the most common precursors to operational failure, as organisations gradually shift away from intended design envelopes without recognising the accumulated risk. In process safety terms, temporary bypasses represent controlled degradation of protective layers in Reason's Swiss Cheese Model (Reason, 1990; 1997), yet commissioning pressure normalises these degradations without corresponding risk assessment or Management of Change protocols (CCPS, 2007).

4.4 Knowledge Discontinuity at Handover

Large project schedules put systemic pressure to compress commissioning. Commissioning is knowledge-dense: the teams executing it understand what was tested, what was deferred, what was patched, and what context shaped those decisions (Forcada et al., 2016).

Commissioning personnel typically demobilise within days or weeks of energisation. Operational teams inherit a plant without the embedded understanding of its vulnerabilities, undocumented workarounds, or incomplete verifications. Hopkins highlights that organisational failures often stem not from ignorance but from lost knowledge, in which the people who understood latent vulnerabilities are no longer present when failures occur. Beyond simple communication failures, handover issues reflect deeper organisational memory decay. Recent studies of healthcare facility handovers (Forcada et al., 2022) identify documentation gaps and knowledge discontinuities similar to CRD mechanisms. Organisational memory theory (Walsh & Ungson, 1991) identifies that critical knowledge resides in individuals, and CRD exemplifies how rapid personnel turnover erodes this memory.

Without this continuity, downstream teams interpret failures as operational rather than commissioning-origin issues, reinforcing the invisibility of CRD.

The loss of commissioning knowledge at handover—including undocumented workarounds, temporary configurations, and tacit operational insights—creates significant visibility and learning barriers for operations teams (Ayres et al., 2025). This knowledge discontinuity means that when latent issues surface weeks later, the contextual understanding needed to diagnose and resolve them has already left the organisation

4.5 Activation Under Real Operating Loads

The final mechanism in the CRD chain is activation. Latent conditions created upstream remain harmless until the plant encounters conditions that exceed the limited operating envelope in which commissioning testing occurred. These triggers include:

- Load changes
- Variable feed conditions
- Equipment cycling
- Disturbances and upset conditions
- Environmental or seasonal variability
- Operator optimisation attempts

Only once these real-world factors emerge do the vulnerabilities created during commissioning become visible—often as instability, nuisance alarms, degraded performance, or intermittent equipment faults. These early-life failures are frequently misattributed to operator behaviour or equipment defects, masking their actual commissioning-origin cause.

Safety-critical manifestations include: partial closure of Emergency Shutdown (ESD) valves under full-flow conditions, alarm floods during process upsets that mask genuine safety deviations, interlock failures under actual process dynamics, and pressure relief systems that were never tested at design relief loads.

4.6 Summary of Mechanisms

A predictable chain drives CRD: compression → incomplete verification → bypass normalisation → knowledge discontinuity → activation under load. These mechanisms interact to produce a drift pathway that is largely invisible to conventional project risk tools.

By understanding these mechanisms, organisations can diagnose why commissioning-origin failures persist and why they so often become operational burdens rather than commissioning responsibilities.

5. OPERATIONAL MANIFESTATIONS OF COMMISSIONING RISK DRIFT

This section illustrates how CRD becomes visible only after systems encounter real operational variability. CRD becomes visible only once a system enters real operational conditions. Once these constraints disappear, the latent conditions created upstream begin to surface as inconsistent, intermittent, and seemingly unrelated operational problems. This creates a delayed but predictable rise in instability, alarms, and system misbehaviour, reflecting the activation of commissioning-origin drift.

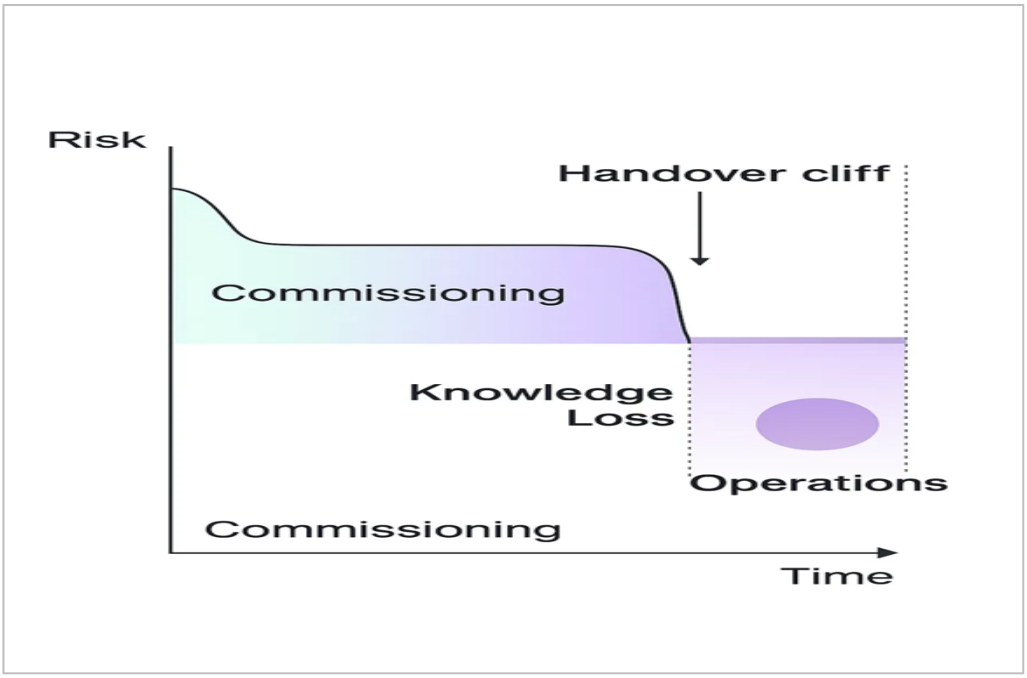

Figure 3. Knowledge Discontinuity and Risk Activation at Handover.

The sharp "handover cliff" in knowledge availability (lower section) represents the rapid demobilisation of commissioning personnel who hold contextual understanding of incomplete verification, temporary states, and deferred defects. The purple circle in operations represents the activation of latent conditions when the system encounters real process loads, disturbances, or optimisation attempts—moments when knowledge discontinuity prevents proper diagnosis and resolution.

5.1 Control Instability and Loop Performance Issues

Distributed water systems present commissioning challenges due to multiple interface points and operational modes (Makropoulos & Butler, 2010). One of the most consistent indicators of CRD is erratic loop behaviour once systems are exposed to real variability. Loops tuned under partial loads or static conditions during commissioning often become unstable when subjected to process fluctuations. Oscillation, overshoot, and sluggish response are common outcomes.

Evidence from real commissioning cases supports this pattern: Bafana et al. (2015) documented instability during the commissioning of an activated sludge process unit, where incomplete tuning and constrained testing windows led to unpredictable process dynamics once biological loading increased. The system appeared stable at handover but exhibited significant oscillations and inconsistent response under real operating conditions—precisely the kind of downstream activation expected under CRD.

Control instability during early operations has direct safety consequences: temperature excursions approaching relief set points, pressure oscillations that challenge containment, level control failures that risk overflow or empty-vessel conditions, and cascade effects in which one unstable loop destabilises dependent control schemes. In safety-critical services (exothermic reactors, high-pressure separators, flammable liquid storage), control instability erodes safety margins that the design assumed would remain intact.

5.2 Nuisance Alarms, Alarm Floods, and Alarm Hygiene Degradation

Alarm floods—defined by EEMUA 191 (EEMUA, 2013) as more than 10 alarms per 10 minutes—overwhelm operator capacity to respond to genuine safety deviations. ISA-18.2 alarm management standards (ISA, 2016) require rationalisation during commissioning, yet compressed schedules often leave alarms in default vendor configurations (Read et al., 2021). The safety consequence: operators become desensitised to alarms, increasing the probability they will miss safety-critical signals (high-high level, low-low pressure, approaching ESD activation) (Bransby & Jenkinson, 1998). Post-incident analyses of major process safety events consistently identify alarm floods as masking critical process deviations, with inadequate commissioning rationalisation identified as a contributing factor (Hollifield & Habibi, 2010).

5.3 Safety Instrumented System Vulnerabilities

CRD has particularly severe consequences for Safety Instrumented Systems (SIS), where incomplete commissioning directly degrades achieved Safety Integrity Levels. IEC 61511 (IEC, 2016) requires proof testing SIFs under conditions representative of actual process demands, yet commissioning compression often limits testing to:

- Logic verification on cold/empty plant: SIFs tested without actual process fluids, temperatures, or pressures

- Partial stroke testing of final elements: ESD valves tested to intermediate positions rather than full closure against design differential pressure

- Sensor calibration without process variability: Transmitters calibrated in lab conditions rather than verified across operating ranges

- Interlock testing without realistic permissives: Safety sequences validated under ideal conditions that do not represent upset scenarios

These verification gaps mean the SIS enters operations with unquantified integrity degradation. The organisation believes it has SIL-2 or SIL-3 protection, but the actual achieved SIL may be significantly lower due to commissioning-origin vulnerabilities. This creates a false sense of security that persists until a process demand reveals the SIF's inability to perform as designed.

The temporal lag between commissioning verification and SIF demand activation makes causation invisible: when a SIF fails to prevent a hazardous event six months into operations, incident investigation attributes the failure to maintenance, operations, or equipment degradation—rarely to incomplete commissioning verification.

5.4 Intermittent or Cascading Equipment Faults

CRD frequently manifests as intermittent equipment faults—trips, stalls, sensor drift, or sporadic shutdowns—that defy straightforward diagnosis. These behaviours often emerge weeks into operation and reflect conditions that commissioning did not adequately test: variations in load, startup transitions, or interactions between subsystems.

This pattern aligns with findings by Hansen and Mikkelsen (2008), who analysed repeated start-up problems in industrial processes and found that many intermittent failures originated from commissioning-stage omissions, such as untested interlocks, incomplete logic validation, or performance tuning carried out under unrealistic constraints.

5.5 Hidden Defects Reappearing as Early-Life Failures

Defects deferred during commissioning often reappear in early operation. Because these defects reflect unresolved commissioning work, operations teams typically lack the contextual knowledge required to identify them. Hopkins (2012) has shown that such minor, unaddressed issues become disproportionately impactful once systems encounter normal dynamic loads and operator adjustments.

5.6 Operational Workarounds Becoming Embedded Practice

Temporary modes used during commissioning can become normalised during operation if they are not removed and reverified. Under CRD, workarounds created for “just getting through startup” often persist unnoticed. Dekker (2014) describes this phenomenon as the normalisation of deviance—small, temporary compromises become accepted operational norms.

5.7 Elevated Maintenance Burden and Spurious Corrective Work

CRD often leads organisations to treat commissioning-origin issues as equipment problems. Assets may be repeatedly recalibrated or repaired without resolving the underlying cause. Hopkins (2012) notes that such early-life maintenance spikes frequently reflect upstream verification gaps rather than genuine failures. Reliability engineering's 'bathtub curve' (Abernethy et al., 2006) attributes early-life failures to manufacturing defects, but CRD suggests many originate in commissioning compression.

Excessive maintenance during early operations degrades process safety in multiple ways: increased personnel exposure (more entry permits, hot work, confined space), more frequent system isolations (increased bypass/inhibit frequency), degraded configuration control (temporary modifications becoming permanent), and maintenance error introduction (reassembly mistakes, calibration drift). CRD therefore creates a compounding safety vulnerability: commissioning-origin defects trigger maintenance interventions that, in turn, introduce new safety risks.

5.8 Early Operational Performance Shortfalls

Empirical studies show commissioning quality directly affects early operational performance (Mills et al., 2006). Yet, the mechanisms remain under-theorised. While reliability theory addresses infant mortality (Rausand & Høyland, 2004), it rarely distinguishes commissioning-origin from manufacturing-origin failures. Plants affected by CRD often struggle to meet performance guarantees or maintain stability during early operation. Rasmussen (1997) shows that performance-shaping factors during system development correlate strongly with downstream process variability, further supporting CRD's lifecycle pattern.

5.9 Summary

The operational manifestations of CRD are diverse but share a common signature: instability, intermittent faults, alarm floods, and elevated maintenance emerging after handover. These symptoms reflect not operational shortcomings, but the delayed activation of vulnerabilities created during commissioning—a pattern observed across multiple sectors (Bafana et al., 2015; Hansen & Mikkelsen, 2008).

6. SAFETY IMPLICATIONS OF COMMISSIONING RISK DRIFT

CRD has significant implications for safety-critical systems.

6.1 Incomplete Validation of Safety Instrumented Functions

Safety Instrumented Functions (SIFs) depend on verification under realistic dynamic conditions. Lundteigen and Rausand (2009) show that SIF allocations and validations are highly vulnerable to commissioning-stage shortcuts, documenting cases where SIFs passed commissioning checks but later failed under live process disturbances. Despite precise validation requirements (e.g., IEC 61511, 2010), commissioning compression often constrains functional testing.

This verification gap has profound implications: LOPA studies that credited SIFs with 100x or 1000x risk reduction (SIL-2 or SIL-3) based on design calculations may have actually achieved only 10x reduction (SIL-1 or below) due to incomplete validation (Lundteigen & Rausand, 2009). Organisations operating with this false precision systematically underestimate process safety risk

6.2 Bypasses and Overrides Creating Hidden Safety Exposure

Temporary bypasses, inhibits, or overrides are essential commissioning tools—but dangerous if undocumented or left in place. Dekker (2014) notes that once deviations become normalised, organisations lose awareness of the reduced safety margin. SIF validation requires representative process conditions (Lundteigen & Rausand, 2009), yet commissioning constraints often limit testing to static states. Under CRD, bypasses created for commissioning convenience usually remain into operations, leaving safety functions compromised without operator knowledge.

Undocumented bypasses disable protective layers that LOPA studies assumed were reliable and independent. When multiple bypasses accumulate—all individually 'temporary' but

collectively persistent—the facility's actual risk profile diverges dramatically from its documented Safety Case or Process Hazard Analysis.

6.3 Alarm Behaviour Masking or Overwhelming Critical Signals

Alarm floods, nuisance alarms, and chattering alarms degrade situational awareness, making it difficult for operators to detect genuine hazards. Read et al. (2021) confirm that poorly configured alarms from commissioning often overwhelm operators during early operations, masking critical signals that require intervention.

6.4 Misattribution of Early Warning Signs

CRD contributes to the misinterpretation of weak signals. Hopkins (2012) repeatedly shows how organisations dismiss or misclassify early indications of system drift, mainly when those signals originate from upstream decisions that have been forgotten or were poorly documented.

6.5 Drift Toward Unsafe States Under Operational Pressure

Rasmussen's (1997) drift model explains how systems tend toward boundaries under production pressure. CRD accelerates this by embedding vulnerabilities *before* operations begin.

6.6 Disappearance of Safety Knowledge at Handover

Accident learning frameworks (Le Coze, 2019) emphasise organisational adaptation, yet commissioning-origin failures are often overlooked as a distinct category. Commissioning teams possess detailed knowledge of incomplete tests, temporary modifications, and known weaknesses. Patterson and Wears (2015) describe this as "risk of organisational memory decay"—a key CRD accelerant.

6.7 Systematic Erosion of Defence-in-Depth

Reason's Swiss Cheese Model (Reason, 1990; 1997) conceptualises accidents as occurring when holes in multiple defensive layers align. CRD creates a distinctive failure mode: commissioning compression systematically introduces holes across multiple layers simultaneously, because commissioning affects instrumentation (detection layer), control systems (prevention layer), alarms (warning layer), interlocks (mitigation layer), and procedures (recovery layer) concurrently. The facility entered operations with pre-existing hole alignment that commissioning was supposed to eliminate. This explains why early-life incidents often appear catastrophic "out of nowhere"—the holes were aligned from day one, waiting only for an initiating event.

This pattern aligns directly with CRD's mechanisms, which embed multi-layer vulnerabilities before operations begin.

6.8 Summary

Hopkins' concept of institutional memory loss (Hopkins, 2012) applies precisely to commissioning handover. The people who understood which alarms were rationalised versus defaulted, which interlocks were tested under representative conditions versus partially validated, which bypasses were temporary versus forgotten—all demobilise within weeks.

This is organisational amnesia by design: project structures ensure knowledge evaporates at the moment it becomes most valuable.

7. Managing CRD Through Lifecycle Governance

Because CRD emerges from structural lifecycle misalignments, its mitigation requires governance interventions rather than technical fixes alone. Digital tools such as BIM (Zou et al., 2017) offer potential for mitigating CRD by enhancing commissioning documentation. The mechanisms underlying CRD indicate that it cannot be mitigated solely through technical fixes. The 'cost of quality' framework (Crosby, 1979) applies to commissioning: adequate verification is cheaper than operational remediation. Because CRD is a lifecycle behaviour emerging from organisational pressures, knowledge discontinuities, and fragmented governance, its management requires structural alignment across project, commissioning, and operational domains. This section outlines governance strategies that address the upstream drivers, midstream vulnerabilities, and downstream manifestations of CRD.

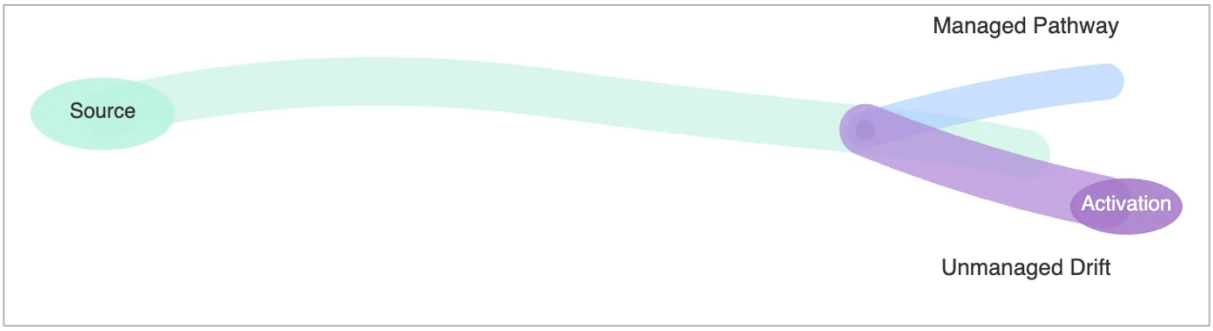

Figure 4. Lifecycle Governance Pathways for Managing Commissioning Risk Drift.

The divergent pathways illustrate how organisational responses to commissioning compression determine downstream outcomes. The Managed Pathway (upper, blue) represents lifecycle-aligned governance—protected testing windows, continuous commissioning presence, CRD-aware handover documentation, and early operations revalidation—resulting in controlled, anticipated activation of residual commissioning issues. The Unmanaged Drift pathway (lower, purple) represents conventional project delivery where commissioning is treated as a finite milestone, teams demobilise immediately after handover, and latent conditions accumulate invisibly before manifesting as operational instability. The branching point (purple intersection) emphasises that CRD is not inevitable but reflects organisational governance choices at the commissioning-operations boundary.

7.1 Aligning Project and Operational KPIs

Aligning commissioning KPIs with operational stability metrics — such as early-life reliability, alarm performance, and fault recurrence — creates incentives for thorough verification rather than superficial milestone delivery. Hopkins (2012) emphasises the critical role of KPI alignment in preventing upstream decisions from undermining downstream safety.

Align with Process Safety Performance Indicators (API, 2016): Track Tier 3/4 events during early operations as commissioning quality indicators. Measure alarm flood frequency, control loop performance, and safety system challenges during the startup period.

7.2 Management of Change Across Project-Operations Boundary

Implement Management of Change protocols that span the project-operations boundary (CCPS, 2007). CRD-aware MOC would require: (1) documentation of all commissioning-phase temporary configurations, (2) explicit closure verification before handover, (3) operational MOC review of any commissioning deferrals, and (4) commissioning personnel participation in early-operations MOC reviews.

7.3 Staged Pre-Startup Safety Review

Extend Pre-Startup Safety Review (PSSR) beyond its traditional single-point-in-time execution (CCPS, 2007; OSHA, 1992). Implement staged PSSR: initial review before energisation, interim review after functional testing under partial loads, final review before unrestricted operations.

7.4 Protecting Functional Testing Windows

Organisations can reduce CRD by contractually safeguarding testing periods. Reason (1990) highlights that complex system tasks require protected cognitive and temporal capacity — without which error likelihood increases.

7.5 Continuous Commissioning Presence Into Early Operations

Despite comprehensive commissioning frameworks in regulated industries (ISPE, 2019) the temporal migration of commissioning-origin risk remains under-conceptualised. Knowledge transfer literature (Argoe & Ingram, 2000) emphasises that tacit knowledge requires sustained interaction, yet commissioning demobilisation occurs within weeks. Retaining key commissioning personnel into the early operational phase ensures that emerging failures can be traced and resolved by those who understand the system's commissioning history. This approach aligns with reliability engineering principles, which emphasise continuity through early-life failure periods (Kaba et al., 2019).

7.6 Treating Bypasses and Overrides as Risk Artefacts

Despite clear standards (ISA, 2016), alarm rationalisation is frequently deferred under commissioning pressure. Instead of treating bypasses as temporary conveniences, organisations should categorise them as explicit risk artefacts requiring:

- formal approval
- documentation
- removal verification
- post-removal functional testing

This avoids the normalisation cycle that Dekker (2014) describes, where minor deviations silently accumulate into system-weakening patterns.

7.7 CRD-Focused Handover Packages

A CRD-aware handover package must capture the commissioning context that traditional documentation omits, including:

- a list of all temporary bypasses and overrides
- unresolved commissioning defects
- deferred verification tasks
- logic changes made during start-up
- known vulnerabilities or "watchpoints"

Hopkins (2012) notes that accidents often result from the loss of organisational memory. A CRD-focused handover is therefore a memory-preservation tool that reduces downstream drift.

7.8 Early Operations Revalidation

Early operations should include revalidation of:

- SIF performance under dynamic conditions
- alarm configuration and nuisance-rate thresholds
- logic sequences under load variability
- loop behaviour and stability
- interlock and permissive chains under representative flows

This acknowledges that commissioning tests performed under constrained conditions may not represent real operating behaviour.

7.9 Summary

By integrating governance around verification, knowledge continuity, and CRD-aware handover, organisations can significantly reduce drift and strengthen system stability. This lifecycle alignment ensures that commissioning-origin vulnerabilities are addressed proactively rather than inherited blindly by operations.

8. DISCUSSION

The recognition of CRD reframes commissioning from a finite technical task to a lifecycle risk-creation phase whose consequences extend far beyond handover. A key contribution of this paper is conceptual: CRD synthesises established safety-science theories — latent condition, organisational drift, normalisation of deviation (Dekker, 2014), and organisational memory loss (Hopkins, 2012) — and applies them to commissioning, a phase that is largely overlooked in academic research.

CRD reveals that current PSM frameworks (CCPS, 2007; OSHA, 1992) contain a structural assumption: they assume commissioning delivers what the design intended. HAZOP identifies hazards; LOPA quantifies risk; SIL studies specify protective functions; commissioning supposedly verifies that these are implemented correctly. CRD demonstrates that this assumption is systematically violated when schedule pressure compresses verification.

This has profound implications for PSM maturity models and PSM auditing (Hopkins, 2012). Organisations can achieve high PSM maturity scores (robust HAZOP processes, documented SIL calculations, trained operators, formal MOC) yet still experience elevated risk if commissioning compression creates verification gaps. PSM frameworks must explicitly incorporate commissioning verification quality—not just completion checklists—as a core PSM element.

Risk-Based Process Safety (CCPS, 2007) requires revision to position "Operational Readiness" not as a single handover gate but as a transitional phase requiring sustained governance.

The mechanisms identified — compression, incomplete verification, bypass normalisation, knowledge discontinuity, and activation under load — provide a coherent explanatory model for patterns practitioners have long recognised but lacked language to articulate. Risk in complex projects (Williams, 2017) often emerges from interactions between subsystems, aligning with CRD's emphasis on commissioning-operations interface.

The governance recommendations extend beyond commissioning departments. CRD highlights that organisations need lifecycle-aligned governance models that integrate commissioning, operations, and maintenance through shared KPIs, protected testing regimes, structured knowledge transfer, and continuity of expertise.

The concept shares intellectual lineage with technical debt theory from software and systems engineering, which similarly explores how near-term pragmatic choices create future system obligations (Cunningham, 1992; Ashrae, 2018). However, CRD addresses a fundamentally different phenomenon occurring at a different lifecycle stage with distinct operational characteristics.

Technical debt typically describes *intentional* trade-offs: developers consciously accept suboptimal code or architecture to meet delivery deadlines, with explicit awareness that future refactoring will be needed. The debt is visible, documented, and exists primarily in software artefacts. By contrast, CRD emerges from *structural conditions* inherent to compressed commissioning environments—time pressure, resource constraints, incomplete plant stability, and competing commercial priorities—rather than from deliberate technical compromises.

Moreover, technical debt assumes a path to remediation through refactoring, whereas CRD-origin vulnerabilities often surface only after commissioning teams have demobilised, making root-cause diagnosis difficult and remediation costly.

These distinctions suggest that while technical debt provides a practical adjacent framework, CRD requires its own theoretical development, governance models, and mitigation strategies tailored to the unique sociotechnical dynamics of commissioning. Future research might explore whether CRD and technical debt can be integrated into a broader "lifecycle risk

accumulation" framework, recognising that different phases generate different forms of inherited vulnerability through various mechanisms.

Future research could examine CRD signatures across industries, measure the prevalence of commissioning-origin failures, and evaluate the effectiveness of CRD-aware governance interventions. Such work would advance the theoretical foundations of commissioning as a distinct socio-technical phase.

8.1. Limitations and Boundary Conditions.

First, CRD is a conceptual framework developed through the synthesis of safety science theory and commissioning practice observation rather than empirical validation through quantitative study. While the mechanisms are grounded in established theories (Reason, 1990; Rasmussen, 2011; Dekker, 2014; Hopkins, 2012) and align with documented commissioning challenges (Babar & Arain, 2019), the framework requires empirical testing through longitudinal case studies, quantitative failure analysis, and cross-sector prevalence studies to establish generalizability and predictive validity.

Second, CRD applicability is strongest in complex, safety-critical process systems where commissioning involves extensive functional verification, safety instrumented function validation, control system integration, and alarm rationalisation under time-constrained conditions. The framework may not apply—or may apply with diminished significance—to simple installations, systems with extended commissioning periods that allow complete verification under representative loads, or contexts where commissioning personnel remain engaged during extended operational ramp-up.

Third, while this paper identifies governance interventions to mitigate CRD, the effectiveness, cost-benefit trade-offs, and implementation challenges of these interventions remain empirically unvalidated.

Finally, CRD focuses on the commissioning-to-operations boundary and does not address broader lifecycle risk accumulation mechanisms during design, procurement, or the long-term operational phase.

Section 8.2 Positioning CRD Relative to Traditional Project Risk Models

Traditional project governance assumes risk declines after commissioning, consistent with the “bathtub curve” model of early-life failure. Commissioning Risk Drift (CRD) identifies a different lifecycle behaviour. During commissioning, compression verification activities are constrained, suppressing early-failure signals rather than eliminating the underlying vulnerability.

Table 1: Divergence between Traditional Governance and CRD Reality

Feature	Traditional Project Governance Model	Commissioning Risk Drift (CRD) Model
Risk Trajectory	**Linear Decay:** Risk decreases as punch-list items are closed.	**Migration:** Risk transforms from "visible defects" to "latent conditions" (Drift).
Verification Logic	**Binary:** "Pass/Fail." If the test passes, the risk is zero.	**Contextual:** "Pass with Context." A pass under compressed conditions creates dormant risk.
Bypass Handling	**Exception:** Bypasses are temporary anomalies to be cleared.	**Normalisation:** Bypasses become the "new normal" operational baseline (Mechanism 2).
Handover State	**Clean Break:** Project ends; Operations begins. Knowledge is transferred via documentation.	**Discontinuity:** Project demobilises; Operations inherits a "black box." Knowledge is lost (Mechanism 3).
Failure Attribution	**Operational Error:** "Why did the operator fail to detect X?"	**Upstream Origin:** "Why was the system commissioned with X latent?"

While traditional models treat verification as a binary pass/fail activity and handover as a clean transition, CRD highlights the role of context, knowledge discontinuity, and bypass normalisation in shaping downstream outcomes. Systems that appear stable at handover may therefore enter operation with embedded vulnerabilities that only become visible once operational variability increases.

CRD does not reject established reliability theory; rather, it defines a boundary condition under which conventional early-life failure assumptions no longer hold. In compressed projects, early operational instability is not stochastic “infant mortality” but the delayed activation of commissioning-origin vulnerabilities. This positions CRD as a foundational concept for future lifecycle safety research.

9. CONCLUSION

Commissioning Risk Drift (CRD) offers a new lens for understanding the lifecycle behaviour of risk in engineered systems. These conditions manifest as instability, alarm floods, intermittent faults, and degraded safety margins — symptoms that are often misdiagnosed because their commissioning origin is invisible.

By defining CRD and mapping its mechanisms, operational signatures, and safety implications, this paper provides a robust conceptual foundation for rethinking commissioning governance. Effective management of CRD requires aligning project and operational incentives, safeguarding verification windows, documenting and removing bypasses, preserving commissioning knowledge through lifecycle transition from project delivery to operations, and revalidating critical functions under real load conditions.

Recognising CRD transforms commissioning from a milestone-driven activity into a lifecycle responsibility. Addressing it strengthens system reliability, reduces early-life failures, and enhances safety performance across complex engineered systems.

REFERENCES

API (American Petroleum Institute). (2016). API RP 754: Process Safety Performance Indicators for the Refining and Petrochemical Industries, Second Edition. Washington, D.C.

Argote, L., & Ingram, P. (2000). Knowledge transfer: A basis for competitive advantage in firms. Organizational Behavior and Human Decision Processes, 82(1), 150-169. https://doi.org/10.1006/obhd.2000.2893

ASHRAE (2018). ASHRAE Guideline 0-2018: The Commissioning Process. American Society of Heating, Refrigerating and Air-Conditioning Engineers, Atlanta, GA.

Ayres, J. R., Bullen, K., May, I., Gamage, S.H.P.W., & Bustami, R. A. (2025). Commissioning as workplace learning: Visibility, identity, and tacit knowledge risks. engrXiv Preprints. https://doi.org/10.31224/5995

Babar, S., & Arain, F. M. (2019). Factors influencing commissioning of MEP systems in Pakistan. Journal of Engineering, Design and Technology, 17(5), 1039–1060. https://doi.org/10.1108/JEDT-11-2018-0318

Bafana, A., Kumar, G., Kashyap, S. M., Kanade, G. S., & Shinde, V. M. (2015). Dynamics of effluent treatment plant during commissioning of activated sludge process unit. Environmental Science and Pollution Research, 22(5), 3538–3546. https://doi.org/10.1007/s11356-014-3576-5

Boehm, B., & Behnamghader, P. (2018). The Incremental Commitment Spiral Model as a systems engineering process improvement. Systems Engineering, 21(1), 65-81. https://doi.org/10.1002/sys.21635

Bransby, M.L., & Jenkinson, J. (1998). The management of alarm systems. HSE Contract Research Report 166/1998. Health and Safety Executive, London.

Broadribb, M.P. (2021). Guidelines for integrating process safety into engineering projects. Process Safety Progress, 40(1), e12179. https://doi.org/10.1002/prs.12179

CCPS (Center for Chemical Process Safety). (2007). Guidelines for Risk Based Process Safety. John Wiley & Sons, Hoboken, NJ.

Cunningham, W. (1992). The WyCash portfolio management system. ACM SIGPLAN OOPS Messenger, 4(2), 29-30. https://doi.org/10.1145/157710.157715

Dekker, S. (2014). The Field Guide to Understanding 'Human Error' (3rd ed.). CRC Press, Boca Raton, FL. https://doi.org/10.1201/9781317031833

EEMUA (2013). EEMUA Publication 191: Alarm Systems - A Guide to Design, Management and Procurement (3rd ed.). Engineering Equipment and Materials Users' Association, London, UK.

Forcada, N., Macarulla, M., Gangolells, M., & Casals, M. (2016). Handover defects: Comparison of construction and post-handover housing defects. Building Research & Information, 44(3), 279-288. https://doi.org/10.1080/09613218.2015.1039284

Forcada, N., Gangolells, M., & Casals, M. (2022). Critical factors affecting handover from construction to operation and maintenance of healthcare facilities. Journal of Building Engineering, 56, 104733. https://doi.org/10.1016/j.jobe.2022.104733

Gökgöz, M., Güvenc, U., Altun, M., & Kahraman, C. (2024). Investigation of failures during commissioning and operation of photovoltaic power plants. Applied Sciences, 14(5), 2083. https://doi.org/10.3390/app14052083

Hollifield, B., & Habibi, E. (2010). The Alarm Management Handbook: A Comprehensive Guide, Second Edition. PAS, Houston, TX.

Hollnagel, E. (2014). Safety-I and Safety-II: The past and future of safety management. CRC Press, Boca Raton, FL. https://doi.org/10.1201/9781315607511

Hopkins, A. (2012). Disastrous Decisions: The Human and Organisational Causes of the Gulf of Mexico Blowout. CCH Australia, Sydney.

IEC (2010). IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector. International Electrotechnical Commission, Geneva, Switzerland.

IEC (International Electrotechnical Commission). (2016). IEC 61511-1:2016 Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements. Geneva, Switzerland.

ISPE (2019). ISPE Baseline Guide Volume 5: Commissioning and Qualification (2nd Edition). International Society for Pharmaceutical Engineering, Tampa, FL.

ISA (International Society of Automation). (2016). ANSI/ISA-18.2-2016: Management of Alarm Systems for the Process Industries. Research Triangle Park, NC.

Kaba, A., Barnes, S., & Dalglish, E. (2019). Commissioning simulations to test new healthcare facilities. Advances in Simulation, 4(1), 13. https://doi.org/10.1186/s41077-019-0107-8

Kleinwaks, H., Batchelor, A., & Bradley, T. H. (2023). Technical debt in systems engineering—A systematic literature review. Systems Engineering, 26(5), 675-687. https://doi.org/10.1002/sys.21681

Le Coze, J. C. (2019). Learning from accidents: adaptations of High Reliability and Safety-II frameworks. Safety Science, 117, 443–454. https://doi.org/10.1016/j.ssci.2019.04.006

Leveson, N. (2011). Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, Cambridge, MA.

Love, P. E. D., Matthews, J., Simpson, I., Hill, A., & Olatunji, O. A. (2014). A benefits realization management building information modeling framework for asset owners. Automation in Construction, 37, 1-10. https://doi.org/10.1016/j.autcon.2013.09.007

Lundteigen, M.A., & Rausand, M. (2009). Architectural constraints in IEC 61511: Do they have the intended effect? Reliability Engineering & System Safety, 94(2), 520-525. https://doi.org/10.1016/j.ress.2008.06.006

OSHA (Occupational Safety and Health Administration). (1992). Process Safety Management of Highly Hazardous Chemicals, 29 CFR 1910.119. U.S. Department of Labor.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Read, G. J. M., Salmon, P. M., Lenné, M. G., & Stanton, N. A. (2021). The state of science: evolving perspectives on "human error." Ergonomics, 64(5), 609–632. https://doi.org/10.1080/00140139.2021.1953615

Reason, J. (1990). Human Error. Cambridge University Press, Cambridge, UK. https://doi.org/10.1017/CBO9781139062367

Reason, J. (1997). Managing the Risks of Organizational Accidents. Ashgate, Aldershot, UK.

Selvik, J. T., Bellamy, L. J., Dahl, R. E., Heggset, J., Hokstad, P., Håbrekke, S., & Sandtorv, H. (2020). Addressing human error when collecting failure cause data in railway incidents. Reliability Engineering & System Safety, 204, 107156. https://doi.org/10.1016/j.ress.2020.107156

Tchobanoglous, G., Stensel, H. D., Tsuchihashi, R., & Burton, F. (2014). Wastewater Engineering: Treatment and Resource Recovery (5th ed.). McGraw-Hill Education, New York, NY.

Walsh, J. P., & Ungson, G. R. (1991). Organizational memory. Academy of Management Review, 16(1), 57-91. https://doi.org/10.2307/258607

Xue, X., Zhang, R., Yang, R., & Dai, J. (2014). Innovation in construction: A critical review and future research. International Journal of Innovation Science, 6(2), 111-126. https://doi.org/10.1260/1757-2223.6.2.111