



Safety by Design Under Strain: A Case Study in System Convergence

Vol 3; edition 3; September 2026

Author: Chris Clarke

Email: Chris.Clarke@powerco.co.nz

ORCID: <https://orcid.org/0009-0002-5308-3842>

DOI <https://doi.org/10.26686/nzjhsp.v3i3.11139>

Abstract

Safety by Design (SbD) is increasingly embedded in high-risk industries to promote alignment with the hierarchy of controls by eliminating or minimising risk through engineering and system design rather than reliance on administrative or personal protective equipment controls (Safe Work Australia, nd).

In practice, however, applying SbD is not straightforward. Complexity emerges where engineering, organisational systems, human factors, contractor delivery models, commercial pressures, and regulatory frameworks intersect within dynamic operating environments.

This paper presents an abstract case study based on a significant network event within a New Zealand electricity distribution context involving excavation works, repeated asset interactions, and eventual exposure to a live high-voltage asset. The event resulted in unplanned network disruption and elevated risk to both workers and the public, requiring rapid decision-making across multiple organisational boundaries, including local authority-led contracting environments where no direct commercial relationship existed with the asset owner.

Using a qualitative, reflective approach, this study examines how SbD principles were applied, adapted, or constrained in practice. The concept of System Convergence Strain is introduced to describe how overlapping duties, fragmented contracting chains, and competing priorities create ambiguity and shift risk control away from engineered systems toward frontline judgement under uncertainty. The findings challenge the assumption that safety can be effectively managed within organisational boundaries and instead position safety as an emergent property of interacting systems.

1. Introduction

Safety by Design (SbD) is central to modern risk management, focusing on eliminating hazards and reducing exposure through engineering and system-level controls (Safe Work Australia, 2014, nd; WoKanse & Fruen, 2022; WorkSafe NZ, 2018).

Within the New Zealand electricity distribution sector, regulatory instruments such as NZECP 34 define Minimum Approach Distances (MADs) to reduce the risk of contact with live electrical infrastructure (WorkSafe NZ, 2001).

Section 34 of the New Zealand Health and Safety at Work Act (2015) reinforces this by establishing shared responsibilities between PCBUs, requiring consultation, cooperation, and coordination across organisational boundaries (WorkSafe NZ, 2017).

However, these responsibilities are difficult to operationalise in environments where asset owners, Local Authorities, and contractors operate within separate safety, quality, environmental, and commercial systems, often without direct contractual alignment.

This paper explores these dynamics through an abstract case study and introduces the concept of System Convergence Strain to explain how safety risks increase when engineering, organisational, and human systems interact under real-world conditions.

2. Literature Review

2.1 Safety by Design and Engineering Intent

SbD is grounded in the hierarchy of controls (Worksafe NZ, 2020), prioritising elimination and engineering controls as the most effective means of reducing exposure (Safe Work Australia, nd). Within electricity distribution, this is reflected through design standards, physical separation, insulation systems, and MADs defined under NZECP 34 (WorkSafe NZ, 2001). However, SbD assumes hazards can be identified and controlled during design phases (Galvin & Donnelly, 2022). This assumption is not always valid.

Infrastructure environments are inherently variable, requiring ongoing adaptation beyond original design intent (Gibb et al., 2015). This aligns with the distinction between “work as imagined” and “work as done” (Hollnagel, 2014), where real-world conditions diverge from design assumptions.

Engineering controls are therefore only effective when the broader system supports their consistent application. While standards such as ISO45001 (2018) promote integrated safety systems, integration frequently degrades when systems cross organisational boundaries.

2.2 Human Factors and Work-as-Done

Traditional safety models emphasise compliance; however, contemporary human factors research recognises that safety emerges from system performance rather than procedural adherence alone (Dekker, 2015). In high-risk environments such as excavation near live assets, conditions are dynamic, requiring real-time adaptation (Hollnagel, 2014).

Human and Organisational Performance (HOP) principles recognise that human error is a normal aspect of work and that systems must be designed to support safe performance (Safety Stratus, nd). Decision-making is further influenced by cognitive bias, particularly under time pressure and uncertainty (MacLean, 2022).

Under conditions of system strain, human judgement becomes both a critical control and a potential point of variability. This reflects the paradox identified by Reason (2000).

As organisational complexity increases and multiple systems interact, workers and supervisors are increasingly required to interpret incomplete information, reconcile competing priorities and therefore adapt established processes to the realities of work.

These adaptations frequently enable work to be completed safely and successfully, demonstrating the resilience of people operating within complex systems.

However, where organisational systems are poorly aligned, ambiguous, or operating under convergence strain, the same adaptive capacity can also expose latent weaknesses at the interfaces between those systems.

Human judgement therefore does not create system convergence strain; instead it becomes the mechanism through which existing organisational vulnerabilities are either successfully managed or inadvertently revealed.

2.3 Leadership and Safety Culture

Leadership significantly influences how safety is prioritised and enacted.

Transformational leadership enhances engagement (Bass & Riggio, 2006), while authentic leadership fosters trust (Avolio & Gardner, 2005). Psychological safety enables individuals to raise concerns without fear of negative consequences (Edmondson, 2019) and servant leadership emphasises responsibility for the wellbeing of others (Greenleaf, 2002). Safety culture is shaped not only by formal systems but by shared values and behaviours (Reason, 1998), reinforcing that safety outcomes are socially mediated as well as technically defined.

2.4 Regulatory Frameworks and System Complexity

HSWA establishes overlapping duties but provides limited operational guidance for managing risk in complex, multi-party environments (WorkSafe NZ, 2017). Complex adaptive systems theory suggests outcomes emerge from interactions rather than linear cause-and-effect relationships (Project Management Institute, 2022). When systems are not aligned, even well-designed controls can lose

effectiveness (Ezerins et al., 2022). This reinforces that safety is not determined by design or compliance alone, but by how effectively systems integrate across organisational boundaries.

3. Methodology

A qualitative, reflective case study approach was used, based on direct observation and involvement in a significant network event involving excavation and infrastructure interaction. Data sources included field observations, incident patterns, and stakeholder interactions.

The analysis was further refined through formal peer review by experienced practitioners within the electricity distribution sector, providing critical challenge and strengthening system level interpretations.

4. Findings

4.1 Excavation Risk

Excavation represented the most persistent and immediate hazard within the event. Despite the presence of established controls, such as service location plans and subsurface detection technologies, repeated asset strikes occurred, indicating a systemic failure in control effectiveness rather than isolated operational error. Key contributing factors included the build design itself, incomplete or inaccurate service information, over-reliance on detection technology, inconsistent excavation practices and time and productivity pressures influencing on site decision-making.

These conditions collectively reduced the reliability of controls that, whilst present in principle, were not consistently executed in practice. In addition to workforce exposure, open trenches created direct and uncontrolled risk to the public, particularly in high-foot traffic environments.

This extended the risk profile beyond the worksite to include vulnerable populations and unplanned interactions with the hazard. Guidance identifies excavation as a high-risk activity requiring robust planning, ground stability management, and controlled work practices (WorkSafe NZ, 2016).

However, the findings suggest a disconnect between prescribed controls and operational delivery, where implementation was variable and often degraded under pressure. This aligns with Reason (1998) concept of latent system weaknesses, where adverse outcomes emerge not from a single failure, but from the alignment of multiple system breakdowns.

In this case, excavation risk was not unmanaged due to absence of controls, but rather due to their inconsistent application within a strained system context

4.2 MAD Encroachment

Minimum Approach Distances (MADs), as defined under NZECP 34 (WorkSafe NZ, 2001), function as a critical engineering control designed to prevent contact with live electrical infrastructure.

However, repeated encroachments were observed, driven by spatial constraints in an urban environment, proximity of machinery to assets and operational pressure to maintain progress. Over time, these conditions contributed to the normalisation of deviation, where operating outside prescribed limits became increasingly accepted as part of routine work practice.

The eventual contact with live infrastructure illustrates a systemic control failure characterised by four conditions where the:

- hazard was not fully understood
- control was not clearly defined
- control was not understood
- control was not maintained

This pattern reflects a broader system issue rather than individual non-compliance.

Clarke (2026) identifies similar dynamics within rail environments, where exposure risk persists despite the presence of well-established controls, due to gaps in implementation and system alignment. The findings reinforce a critical insight: when organisational systems fail to make compliant work reasonably practicable, human judgement becomes the adaptive control that enables work to continue.

In this context, MADs transitioned from an administrative control to variable boundary managed through real-time on-site decision-making by non-electrically competent personnel, increasing reliance on human performance under constrained conditions focused on the task itself, not the hazard

4.3 Asset Condition and Hidden Risk

Asset status, degradation, including cable delamination and insulation failure, can introduce significant uncertainty into the electricity operating environment.

This was not the case or evident in this event. Design assumptions regarding asset status and integrity are therefore not always valid in practice, increasing the likelihood of unexpected control failure during excavation and handling activities.

This reflects a known limitation of Safety by Design (SbD), which often assumes static asset status including condition. It does not fully account for ageing infrastructure and time dependent degradation (Gibb et al., 2015; ISO45001, 2018).

However, a more critical issue than degradation itself was the lack of visibility and shared understanding of asset condition and how it functions across interacting parties.

In this case, the excavation contractor was not directly engaged by the asset owner and was not undertaking network-specific work. As a result, key knowledge about asset behaviour and associated hazards was not effectively transferred, and risk decisions were made without system-level understanding.

This created a fundamental disconnect in that workers did not perceive themselves as working within an electrical environment, yet they were directly exposed to electrical hazards. This gap in hazard recognition extended beyond underground cables to include overhead high and low voltage lines, ground-mounted transformers and associated earthing systems.

This limited understanding extended further into fault current pathways and earthing loop behaviour which influenced on site safety control decisions. In one instance, open trench excavation exposed an earthing circuit associated with a 200kva ground-mounted transformer.

Temporary metal fencing was installed to manage public fall risk. While appropriate for one hazard, this control unintentionally introduced a secondary electrical exposure pathway:

- during a network fault, the earthing system could elevate local ground potential
- the conductive fencing could become energised
- this inadvertent energised exposure zone extended significantly beyond the immediate work area (up to ~150 metres).

This represents a classic risk trade-off under incomplete system visibility, where a locally rational control inadvertently amplifies another hazard. Consistent with (Dekker, 2015), such outcomes are not the result of negligence but of decisions made without full system awareness.

The issue therefore extends beyond worker competence to system design and information flow. Where asset owners are not directly engaged, critical knowledge about infrastructure behaviour under fault conditions is not consistently shared with those exposed to the hazard.

Clarke (2026) similarly emphasises that exposure persists when engineering knowledge is not distributed across all actors interacting with the system. This reinforces a key principle: Exposure risk is defined not by task intent alone, but by proximity to hazard.

Accordingly, Safety by Design assumptions do not hold reliably in fragmented, multi-party environments. Electrical infrastructure safety must therefore be treated as a shared system responsibility.

This requires cross-sector understanding of electrical hazards, explicit communication of asset behaviour under fault conditions and design approaches that account for non-specialist interaction with critical infrastructure.

Without this, degraded assets and incomplete system knowledge will continue to create hidden exposure pathways that remain outside traditional SbD controls.

4.4 Commercial Pressure

A persistent tension existed between public safety protection, restoration urgency and commercial performance expectations. These competing drivers influenced decision-making, often resulting in reduced safety margins, temporary controls or accelerated work execution under constrained conditions. This aligns with (Lingard, 2015), who identified productivity pressure as a recurring source of tension in construction and infrastructure environments where safety and commercial imperatives intersect.

In practice, safety outcomes were significantly influenced within an on and off-site leadership context and organisational culture including the management of the lead contractor. Where physical safety was presented through the commercial chain, risk was more likely to be escalated and addressed appropriately. Where the commercial chain was absent, risk acceptance increased and deviations from ideal control conditions became more likely (Edmondson, 2019).

This demonstrates that safety is not solely a technical outcome, but a socially mediated process shaped by leadership, culture, commercial influence and decision-making dynamics. In effect, safety performance emerged as a negotiated balance between operational and commercial urgency and risk tolerance rather than a fixed engineering condition.

4.5 Contracting Complexity

A key structural complexity arose at the interface between the asset owner, council as principal client, and multiple contractors executing work under fragmented contractual arrangements.

Although all parties held duties under the Health and Safety at Work Act (HSWA), no single party retained full end-to-end control of the operating environment.

This created several systemic challenges – there was:

- no direct contractual relationship between asset owner and lead contractor on site
- limited visibility of contractor capability and execution context
- reliance on asset owner guidance for control decisions without formal transfer of responsibility Council frequently sought direction from the asset owner, effectively requesting operational control input while maintaining contractual separation from execution risk.

This created a legal and operational paradox:

- Providing direction increased the risk of blurred governance and accountability.
- Withholding direction increased reliance on local judgement to manage unresolved operational risk.

Rather than representing a failure of individuals or organisations, this tension emerged from the interaction of governance, contractual and operational systems with competing objectives.

Consistent with complex systems theory, such ambiguity is an inherent feature of multi-party infrastructure environments (Project Management Institute, 2022). As a result, coordination relied heavily on informal mechanisms such as relationships, influence and advisory input rather than structured control pathways. This is not a robust safety control model but a compensatory response to fragmented system design.

4.6 Advisory Without Authority

Within this system, the asset owner functioned primarily in an advisory capacity, providing technical input without formal authority over contractor execution. This created inherent variability in how advice was interpreted, applied, and prioritised across different delivery contexts as well as being unable to be replicated. The absence of enforceable control mechanisms other than refusing Close Approach Consent meant that influence replaced authority as the primary mechanism for risk shaping.

While this enabled flexibility, it also introduced inconsistency in control implementation and increased dependence on interpersonal relationships rather than structured governance. This condition highlights a key limitation in distributed infrastructure systems: technical authority without operational control produces variability in safety outcomes

4.7 System Convergence Strain

System Convergence Strain describes a condition where multiple independently governed systems intersect without alignment, resulting in fragmented control, reduced visibility, and the redistribution of risk management to frontline actors. System Convergence Strain emerged where multiple independently governed safety, quality, environmental and commercial systems intersected without a single coordinating authority.

In these environments, multiple organisations operated within overlapping hazard spaces, no single party had complete system visibility or control and both network and worker safety depended on informal coordination rather than hierarchy or direct control. This reflects a shift away from traditional linear safety management models toward complex adaptive system behaviour, where outcomes are shaped by interactions rather than isolated controls which in turn opens avenues for more critical risk control failures.

In such contexts, traditional Safety by Design approaches and safety management systems become insufficient on their own, as they assume stable system boundaries and clear control ownership. Instead, safety performance is driven by the quality of coordination across system interfaces, not the strength of individual controls

5. Discussion

This case demonstrates that Safety by Design (SbD) is fundamentally constrained when applied within fragmented, multi-party infrastructure systems. While engineering controls such as Minimum Approach Distances (MADs), asset design standards, and physical separation remain essential, their effectiveness depends on how they are interpreted, communicated, and enacted across organisational boundaries – often by non-specialist PCBU's or workers.

Traditional SbD approaches implicitly assume stable operating conditions, where hazards are known, assets behave predictably, and controls are consistently applied. However, this case demonstrates that real-world conditions frequently deviate from these assumptions. As a result, risk control shifts from engineered systems into frontline judgement. This shift occurs under time pressure, incomplete situational awareness and variable leadership, where workers are required to adapt in order to complete the task.

A key driver of this displacement was the interface between the local Authority, lead contractor, and asset owner. Local Authorities, whilst a PCBU in their own right; typically act as the initiator and primary client, while downstream PCBUs operate in reactive roles with limited influence over design intent, asset knowledge, or system-level risk visibility.

While contractual responsibilities may be clearly defined, exposure to hazard is not aligned with contractual position. This results in non-specialist workers and third parties making safety-critical decisions without commensurate authority, system understanding, or access to complete information.

This dynamic is amplified by contracting complexity. Multi-layered delivery models involving consultants, joint ventures, and subcontracting arrangements introduce ambiguity in accountability and dilute shared understanding of roles and responsibilities. The absence of a clear “source of truth” for asset and risk information further degrades system alignment.

Under these conditions, coordination relies heavily on informal mechanisms such as relationships, influence, and advisory input. While functional in stable environments, these mechanisms are inherently variable under pressure and uncertainty.

The concept of System Convergence Strain provides a useful lens for understanding this dynamic. It describes a state where engineering systems, human decision-making, commercial pressures, and regulatory obligations intersect without coherent alignment.

In this state:

- engineering assumptions are challenged by real-world variability
- human adaptation occurs without full system visibility
- commercial and operational pressures influence decision-making
- regulatory expectations remain constant but difficult to operationalise.

Collectively, these conditions shift safety control from designed systems toward human judgement under uncertainty. This challenges a core assumption embedded in much of current safety practice:

that safety can be effectively managed within organisational boundaries. Instead, safety performance is better understood as an emergent property of system interaction.

This has significant implications for Safety by Design and infrastructure governance. It suggests that safety outcomes are less dependent on the strength of individual controls and more dependent on the quality of integration across organisational interfaces.

A critical distinction emerging from this case is that exposure is determined by proximity to hazard, not contractual responsibility. Accordingly, improving safety performance in these environments requires a shift in design and governance thinking toward:

- designing for interaction between organisations, not isolated system components
- embedding hazard understanding across non-specialist roles, not just technical experts
- enabling proportional and informed intervention without creating decision-making inhibition under uncertain accountability conditions
- recognising that exposure is defined by proximity to hazard, not contractual responsibility.

In summary, this case demonstrates that in fragmented infrastructure systems, safety is not a property of individual organisations or controls. It is an emergent outcome of how systems interact, and whether those interactions are visible, understood, and aligned.

6. Conclusion

Safety by design remains critical, but it is not sufficient on its own in complex, multi-party environments. Its effectiveness depends on how controls are understood, applied, and maintained across interacting systems.

System Convergence Strain provides a useful explanatory framework for understanding how safety control is redistributed from engineered systems into frontline judgement when alignment breaks down.

The implication is clear:

Safety is no longer defined by how well we design assets — but by how well those assets remain safe when others interact with them under conditions we do not control.

Acknowledgements

The author acknowledges the technical expertise and operational support provided by Gener Reyes (CIW Project Manager), Lynley Dunn (Delivery Manager), Karen Frew (General Manager – Electricity), and Carl Wallworth (Head of Risk) during the operational event that informed this case study.

The author also acknowledges Sean Heasman and Tomas Haerewa for their constructive review and feedback during manuscript development, and Craig Stewart and Jemma Gerring for their ongoing support.

The author did not use artificial intelligence or generative AI tools in the development, writing, or editing of this manuscript.

This work received no external funding.

References

- Avolio, B. J., & Gardner, W. L. (2005, 2005/06/01/). Authentic leadership development: Getting to the root of positive forms of leadership. *The Leadership Quarterly*, 16(3), 315–338. <https://doi.org/10.1016/j.leaqua.2005.03.001>
- Bass, B. M., & Riggio, R. E. (2006). *Transformation leadership* (2nd ed.) Mahwah, N.J. Psychology Press.
- Clarke, C. (2026). Engineering Controls, TAIC Findings, and Exposure in Rail Work Environments. *NZ Journal of Health and Safety Practice*, 3(1). <https://doi.org/10.26686/nzjhsp.v3i1.10608>
- Dekker, S. (2015). *Safety Differently: Human factors for a new era* (2nd ed.) Boca Raton. CRC Press.
- Edmondson, A. C. (2019). *The fearless organization: creating psychological safety in the workplace for learning, innovation, and growth* Hoboken, New Jersey. Wiley.

- Ezerins, M. E., Ludwig, T. D., O'Neil, T., et al. (2022). Advancing safety analytics: A diagnostic framework for assessing system readiness within occupational safety and health. *Safety Science*, 146. <https://doi.org/10.1016/j.ssci.2021.105569>
- Galvin, A., & Donnelly, R. (2022). *Improving health and safety outcomes for the construction sector through better design practice* [Report]. Construction Health and Safety New Zealand, Wellington. <https://chasnz.org/>
- Gibb, A., Lingard, H., Behm, M., et al. (2015). Construction accident causality: learning from different countries and differing consequences. <https://doi.org/10.1080/01446193.2014.907498>
- Greenleaf, R. (2002). *Servant leadership: A journey into the nature of legitimate power and greatness* (25th anniversary ed.). Paulist Press.
- (2015). New Zealand <http://www.legislation.govt.nz/>
- Hollnagel, E. (2014). *Safety-I and safety-II: the past and future of safety management* Farnham. Ashgate Publishing Ltd.
- ISO45001: 2018 Occupational health and safety management systems: Requirements with guidance for use, International Standards Organization, Geneva.
- Lingard, H. (2015). Health and safety in construction.
- MacLean, C. L. (2022). Cognitive bias in workplace investigation: Problems, perspectives and proposed solutions. *Applied ergonomics*, 105. <https://doi.org/10.1016/j.apergo.2022.103860>
- Project Management Institute. (2022). *Complex adaptive systems*. Author. <https://www.pmi.org/disciplined-agile/organizations/cas>
- Reason, J. (1998). Achieving a safe culture: Theory and practice. *Work & Stress*, 12(3), 293–306. <https://doi.org/10.1080/02678379808256868>
- Safe Work Australia. (2014). *Guide for safe design of plant* [Guide]. Author, Canberra. <https://www.safeworkaustralia.gov.au/>
- Safe Work Australia. (nd). *Safe design*. Author. <https://www.safeworkaustralia.gov.au/safety-topic/managing-health-and-safety/safe-design>
- Safety Stratus. (nd). *HOP principles*. Author. <https://www.safetystatus.com/>
- WoKanse, L., & Fruen, L. (2022). Work design. In *Core Body of Knowledge for the Generalist OHS Professional*. Australian Institute of Health and Safety. <https://www.ohsbok.org.au/>
- WorkSafe NZ (2001), New Zealand Electrical Code of Practice for Electrical Safe Distances NZECP 34. Ministry of Consumer Affairs, Wellington. <https://worksafe.govt.nz/>
- WorkSafe NZ. (2016). *Excavation Safety* [Good Practice Guide]. Author, Wellington. <https://www.worksafe.govt.nz/>
- WorkSafe NZ. (2017). *Health and Safety at Work Act 2015*. Author. <https://www.worksafe.govt.nz/laws-and-regulations/acts/hswa/>
- WorkSafe NZ. (2018). *Health and Safety by Design: an introduction* Good Practice Guide. Author. <https://www.worksafe.govt.nz/>