Whitepaper | Issue 3

Beyond the Hierarchy:

A Modern Approach to Reliable and Effective Safety Controls

Incident Analytics™

www.incidentanalytics.com.au

In this third whitepaper of the series delving into SIFp events, we explore how most controls heavily rely on human behaviour free from error, which therefore makes them vulnerable to failure. We reveal how organisations can overcome this challenge and build more resilient safety systems.

Table of Contents

Prologue

Whitepaper | Issue 3

Prologue

A deep dive into Serious Injury and Fatality potential (SIFp) incidents, controls and antecedents.

We've completed an unprecedented analysis of more than 10,000 incidents and a deeper dive into 680 high-severity potential incidents. This work is the culmination of several years of collaboration with our clients. Thank you to our clients, partners, and team for your contributions.

The result is a series of whitepapers that unpack data, examine research, reveal insights, and showcase real-world case studies and solutions to improve the effectiveness of critical controls in high-hazard industries.

Our whitepaper series explores:

Our first whitepaper, **A deep dive into SIFp: Understanding the misclassification of serious incidents** explores the underlying factors contributing to the misclassification of serious incidents.

Our second whitepaper **Making Critical Controls Work: Overcoming Barriers to Effective Implementation** extends on these research insights and focuses on Critical Controls.

This whitepaper **Beyond the Hierarchy: A Modern Approach to Reliable and Effective Safety Controls** is a technical supplement and expansion on the previous paper and provides more focus on Incident Analytics' evidence-based approach to understanding the adequacy and reliability of controls.

Introducing SCALE®: Evidence-based methodology and analysis technology

Using our SCALE® technology, we analysed the data from more than 10,000 incidents. Our proven approach takes the guesswork out of incident analysis. By using a structured, repeatable approach, we identify which incidents need deeper investigation. This systematic process has resulted in more effective solutions to prevent serious incidents in high-risk work.

Our comprehensive and repeatable fatality potential decision-tree system determines which incidents merit deep-dive analysis. The subsequent analysis leverages a proprietary controls database that helps inform strategies to improve the effectiveness of controls, including:

- Strengthening critical safety controls
- Addressing human behavior patterns
- Fixing gaps in organisational systems

> SCALE ® analysis technology helps determine which incidents need deep-dive analysis. It is built on a robust methodology that enables organisations to better understand the effectiveness of controls and the operational, and system factors that contribute to the conditions for unplanned events to occur.

Severity	Controls	Antecedents	Learning	Exposure
Assess severity and risk context Is there potential for a serious incident and what was the specific high risk task context?	**Determine ineffective controls** Which critical controls would have stopped an incident from happening?	**Analyse causes** Which human, operational, and organisational system factors helped to set the scene for the incident?	**Make sense of findings and prioritise** Which factors should be prioritised to resolve the issue?	**Develop actions to strengthen controls** Which actions will have the greatest impact on exposure and reduce the potential for a repeat event?

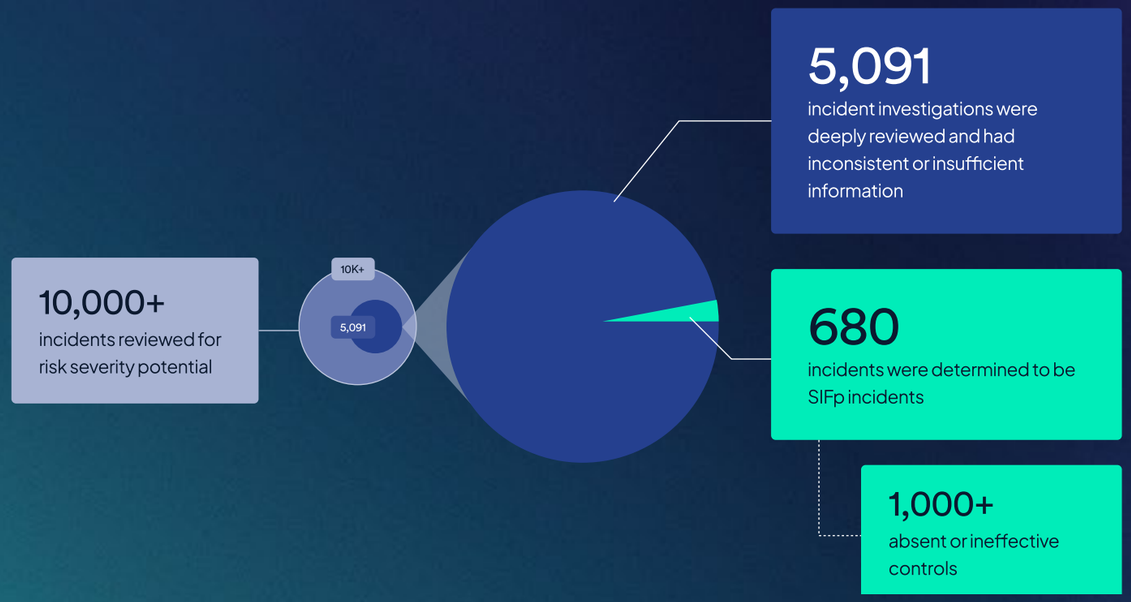
Research study

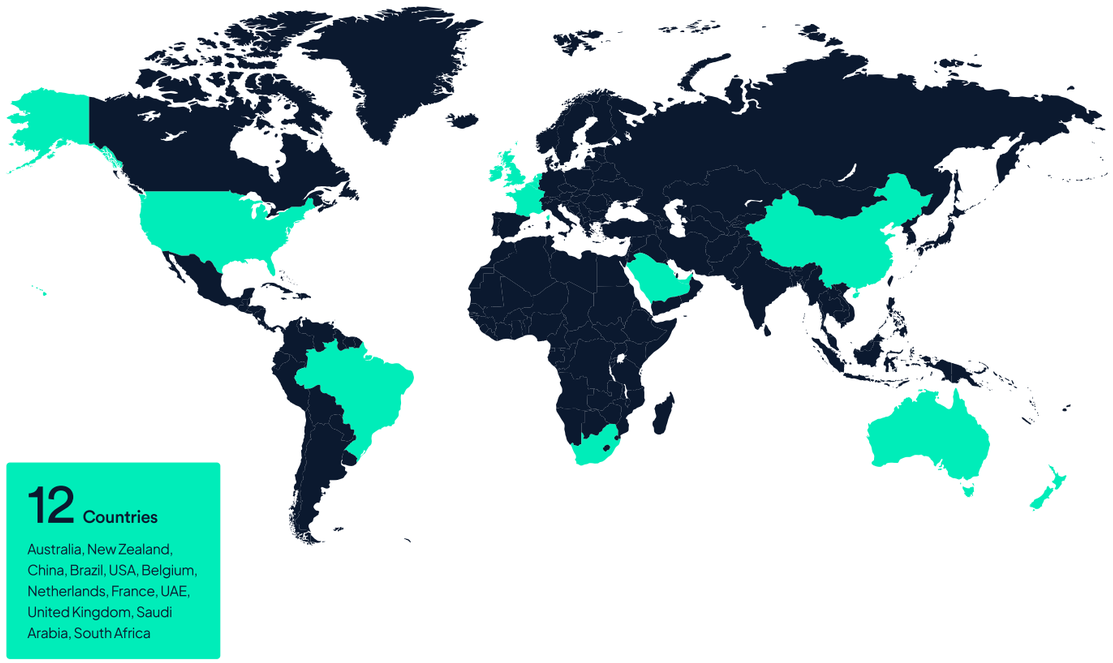
Incident Analytics analysed data from across 12 industry sectors spanning 12 countries and six continents. These industries included mining, road and rail transport, warehousing, utilities, and port operations.

Our research into serious injury and fatality prevention is based on an analysis of data sourced from many real-world operations.

We analysed more than 10,000 incidents and found there is inconsistent taxonomy and insufficient information to inform adequate learning. Where this wasn't an issue, we applied deeper focus (on 5,091 incidents) and of these, 680 had serious injury or fatality potential. These specific incidents were the subject of much deeper review and analysis using SCALE ®.

We identified more than 1,000+ specific controls in high-risk work that were absent or weren't effective in preventing or mitigating SIFp incidents from occurring.





12 Countries

Australia, New Zealand, China, Brazil, USA, Belgium, Netherlands, France, UAE, United Kingdom, Saudi Arabia, South Africa

12 Industry Sectors

- Utilities
- Metals Manufacturing
- Mining
- Engineering
- Food Manufacturing
- Agricultural Services
- Land Management
- Fuel Distribution
- Warehousing
- Rail Operations
- Transportation
- Port Operations

Executive Summary

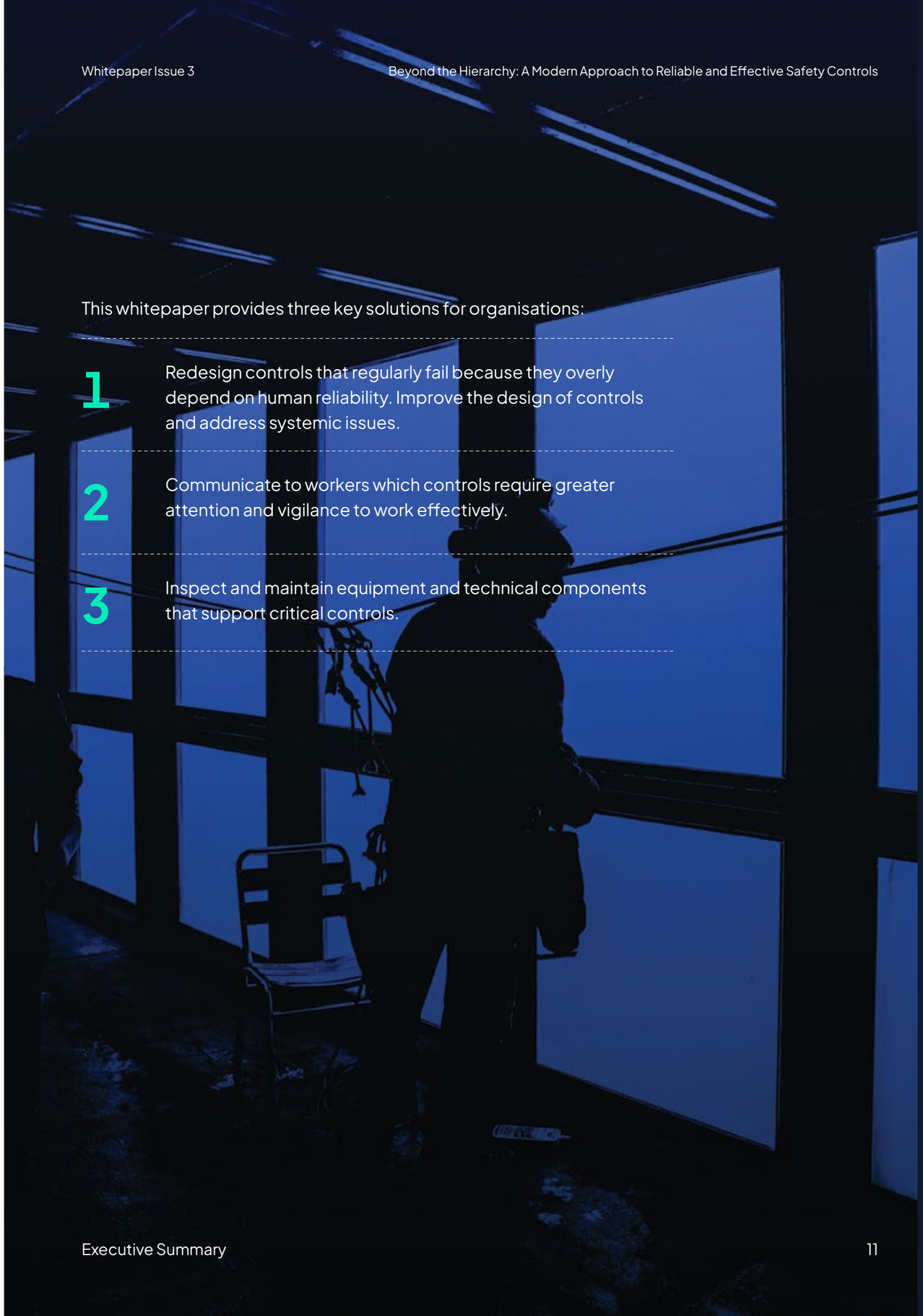
This whitepaper reveals why certain safety controls vary in effectiveness when workers implement them.

Our previous whitepaper discussed why workers often find it difficult to apply critical controls exactly as planned. We highlighted that organisations need to regularly investigate why this happens and how they can address these issues. This whitepaper builds on those insights and illustrates that critical controls are not equal in their ability to manage exposure, even when correctly applied.

Our analysis of over 10,000 incidents found that:

Most controls heavily rely on human behaviour, making them especially vulnerable to human error. Controls that frequently fail should be regularly reviewed to identify opportunities for improvement and reduce dependence on consistent human performance.

> Our research found that 96% of failed critical controls heavily depended on workers staying alert, focused, and making good decisions when faced with both familiar and unforeseen risks.



This whitepaper provides three key solutions for organisations:

1. Redesign controls that regularly fail because they overly depend on human reliability. Improve the design of controls and address systemic issues.
2. Communicate to workers which controls require greater attention and vigilance to work effectively.
3. Inspect and maintain equipment and technical components that support critical controls.

Not all controls are equally capable of reducing serious incidents

Many organisations put significant time and resources into identifying critical risks and making sure the right controls are enabled. However, fewer ask a crucial question: how reliable are those controls once they're in place?

It's important to regularly review the adequacy and reliability of controls, and ask:

- Does the control eliminate or reliably prevent the risk from materialising?
- Will this control still work under pressure, complexity, or real-world constraints?

Not all controls are created equal. Picture a spectrum: on one end, a fixed barrier that physically separates workers from moving machinery. On the other end, a process that depends on a worker remembering every step in a complex isolation procedure. Both are critical controls, but one is clearly more reliable.

This whitepaper introduces ways of thinking about controls that reveal their limitations and offer guidance on how to improve their design. The goal: to make sure controls are not just available, but actually effective in protecting people in high-risk environments.

Special note on control categorisation

Before moving on to concepts about control adequacy and reliability, we note that safety professionals and their organisations may interpret controls and their supporting functions in subtly different ways. For the sake of clarity, this white paper assumes the following:

1. A **Control** is a physical object, human act, or system (object + human) that:
    - Directly prevents or substantially reduces the risk of an unwanted event.
    - Has a performance standard that is specific and can be tested.
    - Is often distinguished as "critical" when its failure would significantly increase the risk of a serious or fatal outcome.
2. **Support Activities** are the processes or tasks that ensure a control measure can exist, function properly, and be sustained (ie. planning, inspections, maintenance, training, supervision, or assurance systems etc).
3. **Verification Activities** include in-field checks that verify a control is implemented, determine a control is effective and functioning as required.

Note: For the purposes of this research, Incident Analytics doesn't make a distinction between controls and critical controls.

1. Control adequacy

Control adequacy refers to how well a particular control limits the chance of harm or failure to a level the organisation considers acceptable.

Some controls provide more protection than others, for example:

- A solid physical barrier under crane work offers far better protection than a few witches' hats marking the area.
- A properly designed and installed scaffold is more effective than using an elevated work platform – and both are more reliable than a ladder.

Control Adequacy

Are the controls appropriately designed to address the specific risks that exist in the workplace?

Does their design match the severity and likelihood of potential exposure to hazards?

What counts as "acceptable risk exposure" varies, depending on factors such as:

- How often workers are exposed to the risk.
- The cost and practicality of different control options.
- The physical work environment.
- The organisation's past experience with serious incidents.

These factors shape how organisations choose and prioritise their safety controls. Understanding adequacy helps make sure those choices are fit for purpose – not just available on paper.

2. Control reliability

Control reliability is about how well a safety control holds up when things don't go to plan – whether that's due to disruptions, unexpected changes, or tough working conditions.

The biggest factor affecting control reliability is how much it depends on people.

Most controls aren't fully automated – they often involve equipment that needs to be used, adjusted, or maintained by workers – even automated systems rely on human support to keep them running properly.

Control Reliability

Can the controls withstand unexpected conditions, ie equipment failure, human error, or environmental changes?

Can operations quickly recover or maintain critical controls during a crisis?

Take the example of a worker using an elevated work platform (EWP), which is generally safer than a ladder:

- An EWP may be the required method, but if the ground is too uneven and scaffolding isn't practical for a one-off job, the worker may need to find another way to complete the task.
- How a worker completes the task may be influenced by time pressure, lack of supervision, unexpected conditions, or faulty equipment.
- When attempting to use the EWP, the worker needs to check for overhead hazards, making sure the EWP is working properly, creating a drop zone, and wearing a harness.

This example highlights just how many factors influence worker decisions and behaviours. It also shows how complex and variable the real-world process of applying controls can be – especially when human judgment plays a big role.

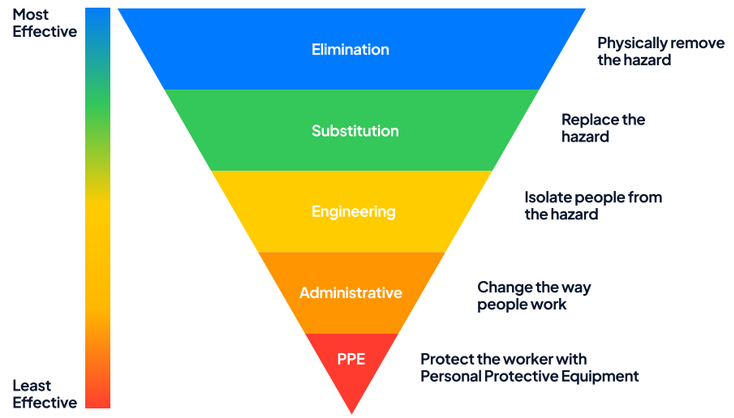
Comparing legacy control assessment methods with SCALE®

Legacy control evaluation

Many organisations use the traditional "Hierarchy of Controls" (HOC) model to evaluate safety actions and control effectiveness. While widely recognised, this model comes with several well-known limitations:

- It's easy to misuse. The categories aren't always clearly defined and can be prone to subjectivity in their assessment.
- There are only five levels. Furthermore, the jump from administrative controls to engineering or elimination is significant in terms of cost, complexity, and effort.
- The model tends to favour engineering solutions over administrative or PPE controls – even though, in some cases, a well-designed PPE solution may be the most practical and effective. For example, leather gators are often the best defence for workers in snake-prone areas.
- The quality and effectiveness of controls can vary greatly – even within a single category. Two controls classified as "administrative" could have vastly different outcomes in real-world use.

Understanding these challenges helps organisations avoid over-relying on the hierarchy alone and encourages a more nuanced evaluation of how well each control actually performs in practice.



SCALE® and the CHA framework: A modern way to assess control effectiveness

To address the limitations of traditional models such as HOC, Incident Analytics developed an evidence-based method called the Control Health Assessment (CHA). This framework extends into the SCALE® analysis process and provides a more accurate way to assess how well controls manage risk in real-world conditions.

The CHA helps organisations:

- Understand how controls actually function – not just how they're meant to be implemented.
- Appreciate the limits of each control's inherent reliability.
- Use a modern control assessment framework that facilitates clearer focus on where the greatest control reliability gains can be made.

The three types of control purpose

Controls may have one of three high-level purposes:

Prevention	Preventing or minimising the risk of a hazard or energy getting out of control. (Prevent existence; Prevent release; Create separation)
Mitigation	Managing a hazard or energy that is out of control. (Mitigate existence; Mitigate release; Provide protection)
Response	Responding to an uncontrolled situation that has become an unwanted event. (Detect event; Responding to, or recovering from an incident.)

The four types of control design

Control design is divided into two main categories: physical (not reliant on human action) and behavioural (reliant on human action).

Physical Controls	Behavioural Controls
Permanent Control *Definition*: Always in place – needs minimal human input aside from maintenance. *Nature*: Passive, built-in, continuously active.	**Technical Control** *Definition*: Requires both equipment and human interaction. *Nature*: Equipment-enabled, but dependent on operator input.
Exposure-Triggered Control *Definition*: Activated automatically when a certain condition is met. *Nature*: Dynamic, automatic response to hazardous exposure.	**Procedural Control** *Definition*: Reliant on people doing the right thing at the right time. *Nature*: Behavioural, entirely human-dependent.

After analysing hundreds of critical controls across high-risk industries, Incident Analytics found that the majority of controls depend on people following procedures perfectly – and even well-intentioned humans make mistakes.

While our research indicates Technical controls tend to be marginally more reliable than pure Procedural controls, they are both reliant on human behaviour, and therefore vulnerable to human slips, lapses or mistakes.

This is why it's essential to strengthen controls when they are found to repeatedly fail, so they don't rely solely on memory, attention, or decision-making under pressure. We can do this by redesigning controls and control systems to be Exposure-triggered, and even more reliable as Permanent controls.

Control Design

Control Purpose		Physical Controls		Behavioural Controls	
		PERMANENT	EXPOSURE TRIGGERED	TECHNICAL	PROCEDURAL
Prevention	Eliminate or minimise **EXISTENCE** of energy/hazard	A1	B1	C1	D1
Prevention	Prevent of minimise **RELEASE** of energy/hazard	A2	B2	C2	D2
Prevention	Create **SEPARATION** from energy/hazard	A3	B3	C3	D3
Mitigation	Provide **PROTECTION** from potential damage	A4	B4	C4	D4
Response	Minimise **IMPACT** of the unwanted event	A5	B5	C5	D5

Below is a simplified version of the CHA framework. We can bring this framework to life with some examples of controls within each of the purpose and design categories:

- **A1** Scaffolding systems with fully enclosed sides (using mesh or panels) to remove risk of fall
- **A2** Pressure release valves that minimise potential build-up of energy
- **A3** A solid wall installed between pedestrians and load-moving equipment areas
- **A4** Fire-resistant coatings or fireproof construction materials to minimise fire damage
- **A5** Shower facilities for workers exposed to hazardous chemicals

- **B1** Safety interlocks that prevent machinery operating if certain conditions aren't met
- **B2** Circuit breakers that automatically cut off electricity if an overload occurs
- **B3** Interlocked guards around moving parts, such as gears, belts, and blades
- **B4** A vehicle airbag that inflates on impact with a moving or stationary object
- **B5** Sprinkler systems that are activated by the presence of smoke or flame

- **C1** Disconnecting electrical equipment from its power source during maintenance or repairs
- **C2** Lockout/Tagout procedures are implemented to prevent workers being exposed to energy
- **C3** Erection of temporary barriers around the drop zone of a suspended load
- **C4** Using an appropriate breathing apparatus when working in dangerous atmospheres
- **C5** Applying a neutralising substance to skin in the event of a hazardous chemical exposure

- **D1** Verifying that energy sources have been isolated by attempting to start the equipment
- **D2** Making sure vehicle is parked with hand brake applied when on sloped ground
- **D3** Maintaining suitable distance from a dangerous line of fire
- **D4** Wearing appropriate gloves to avoid risk of lacerations or burns
- **D5** Follow evacuation routes and procedures in an orderly manner during emergencies

Our research findings

Control design greatly influences SIFp risk.

Our research study of 10,000+ incidents confirms that the way a control is designed – and what it's intended to do – plays a major role in whether it is likely to fail. Certain types of control design are more prone to failure in specific high-risk situations.

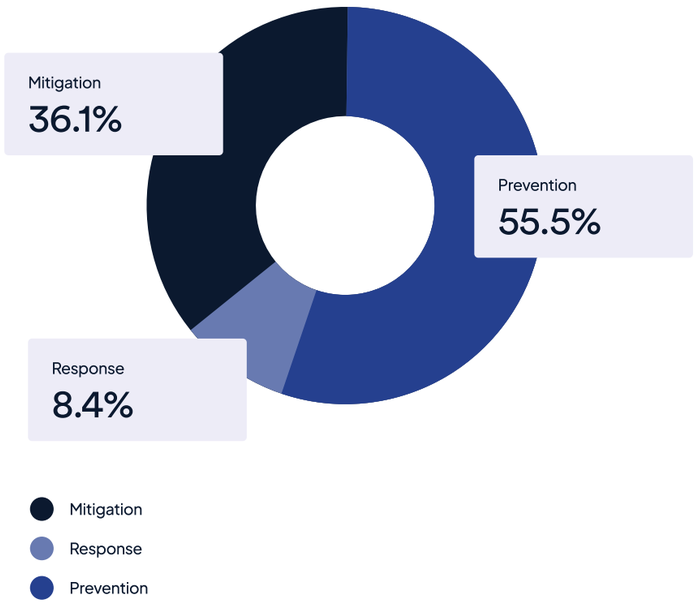
This means organisations must look closely not just at whether controls are in place, but at how they're built and how well they're suited to the risks they're meant to manage. Understanding this link is key to reducing incident potential and improving overall control reliability.

Key finding 1: Control Purpose doesn't strongly predict SIFp incidents

Our analysis of SIFp incidents shows how failed controls were spread based on their intended function.

Interestingly, the figures below align closely with many organisational control registers. We most often see a similar 50/40/10 split for the average volume of controls in each of the three categories of prevention / mitigation / response control purpose. This suggests that the intended purpose of a control – whether it's designed to prevent, mitigate, or respond – isn't a strong predictor of whether it will fail in the real world.

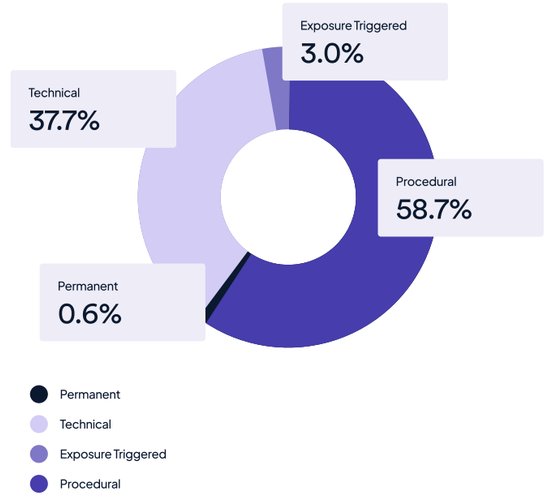
Therefore, control function alone doesn't explain why failures occur. The next section explores another factor that shows a much stronger link to SIFp incidents: control design.



Key finding 2: Control Design strongly correlates with SIFp incidents

Our analysis of controls that failed in serious incidents (SIFp) revealed a clear pattern emerge: control design plays a major role in reliability. These failed controls fall into four categories:

- Only 3.6% of failed controls were physical controls (permanent or exposure-triggered). These were either never implemented or poorly maintained.
- In contrast, a staggering 96% of failed or missing controls were behavioural (technical or procedural)controls. Meaning, workers were expected to take specific actions to make them work.
  - 61% of behavioural controls were procedural, where the worker relied on memory, skill, or awareness to stay safe.
  - 39% were technical, involving equipment that required the worker to use or monitor it correctly.



This data highlights a key vulnerability: controls that rely on human behaviour are far more likely to break down, particularly in complex or high-pressure situations.

> Strengthening these types of controls – or reducing reliance on them – is essential to preventing serious incidents.

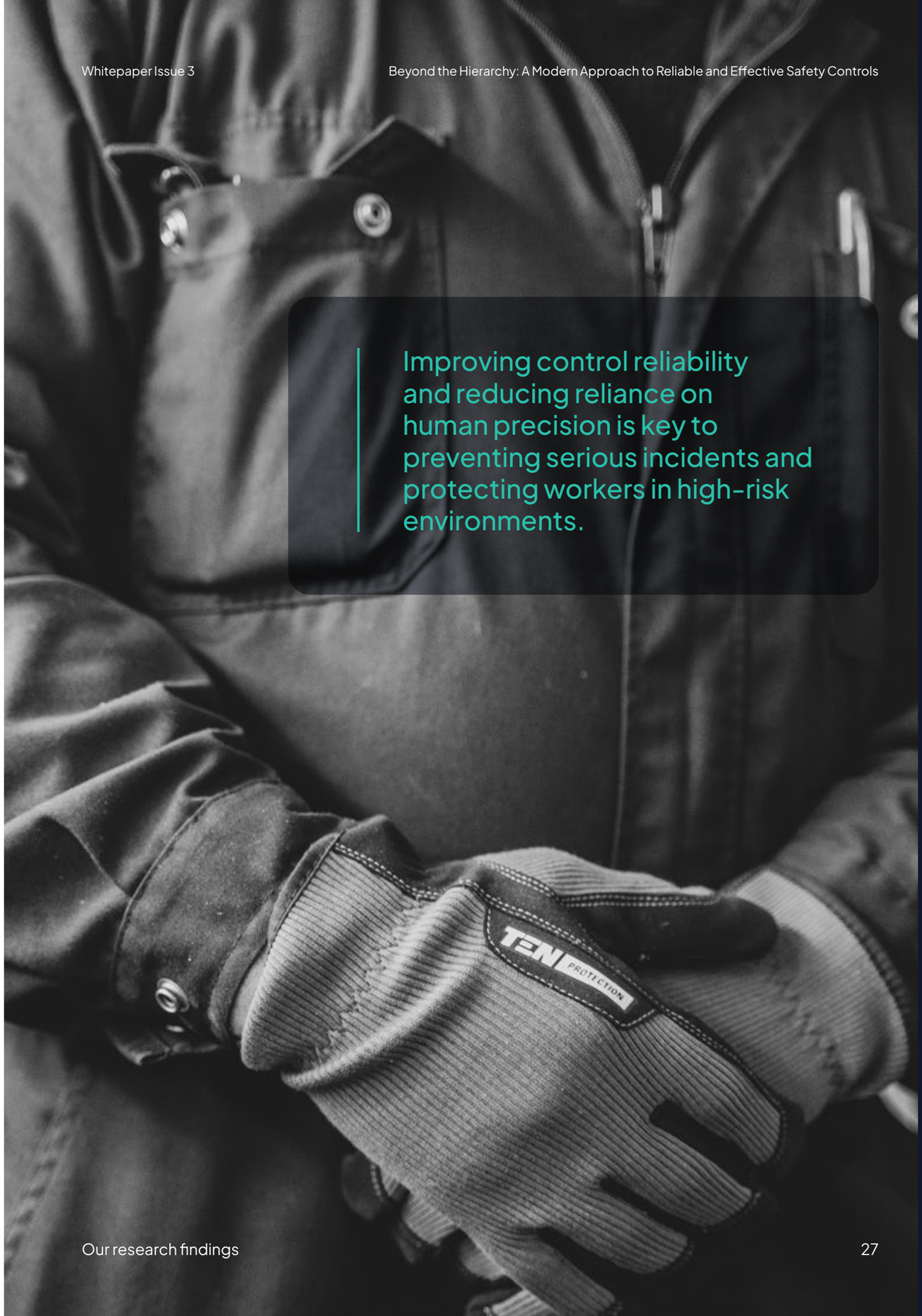
Recommendations for safety leaders

Organisations should focus on improving the design of their controls – implementing more reliable and effective solutions. This is especially important when repeated SIFp events involve procedural controls, which rely heavily on perfect human performance.

Some examples:

Risk	Procedural Controls	Strengthened Physical Controls
Entanglement	*"Do not reach into the machine while operating"*	**Light curtain or presence-sensing device** that halts machine operation if the protected zone is breached.
Vehicle-Pedestrian Interaction	*"Stay within designated pedestrian walkways"*	**Proximity sensors with auto-braking** or **tag-based personnel detection systems** on vehicles that trigger alerts or shutdowns when pedestrians are nearby.
Confined Space Entry	*"Check for hazardous atmosphere before entry"*	**Interlocked entry systems** that only permit access after automatic gas detection confirms safe levels, preventing entry until conditions are verified.
Working at Heights	*"Use fall protection harness and follow permit"*	**Self-closing gates at ladder access points**, or **anchor-point interlock systems** that prevent work platform elevation unless the harness is connected.
Uncontrolled Release of Energy	*"Apply lockout/tagout and verify isolation"*	**Interlock devices that prevent access until energy is fully isolated**, and **smart locks** that detect and record lockout compliance electronically.
Hazardous Substance Exposure	*"Wear PPE and avoid splashes during transfer"*	**Closed-loop transfer systems** or **quick-connect couplings** that eliminate open handling and trigger a shutoff if leakage is detected.

When redesigning a control isn't practical, organisations must take steps to reduce the factors that make implementation inconsistent. That means addressing cognitive demands, operational distractions, or other pressures that influence how workers carry out their tasks.



> Improving control reliability and reducing reliance on human precision is key to preventing serious incidents and protecting workers in high-risk environments.

The influence of purpose and design on implementation of controls

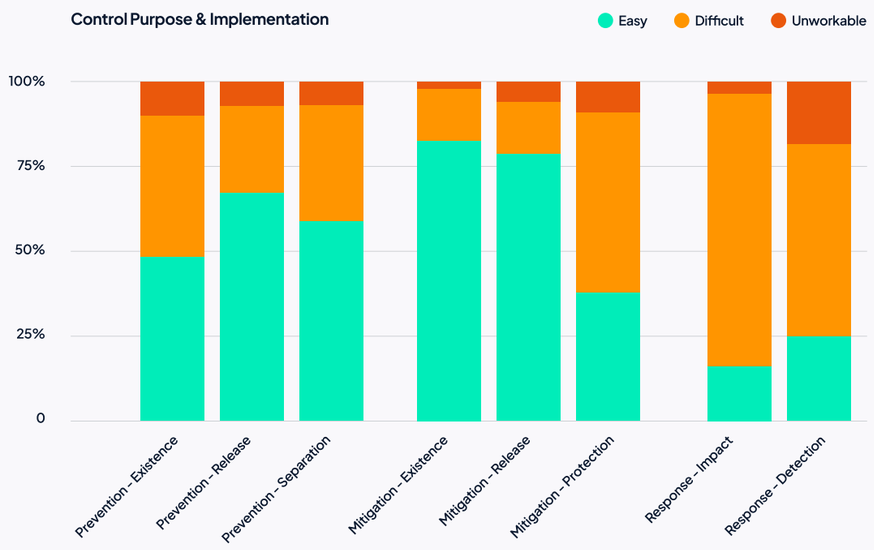
When we analysed how often different types of critical controls were difficult to apply or not workable at all, clear patterns emerged between control purpose and design.

Control purpose and challenges to implementation

> Controls focused on responding to incidents, such as emergency procedures or impact mitigation, were three times more likely to be difficult or unworkable compared to other types.

These response controls are meant to detect and manage the effects of a high-risk exposure once it's already out of control. However, they often fail because:

- Emergency response procedures are not well-known or understood.
- Drills aren't conducted.
- Equipment needed for response is missing or not properly maintained.



> Protection controls – a type of mitigation control – were more than three times as likely to be difficult or unworkable compared to other mitigation controls.

These protection controls are typically used to guard against external hazards such as:

- Extreme temperatures.
- Environmental exposure.
- Risks from remote working.

Their effectiveness depends on:

- Workers understanding how to use them correctly.
- The equipment and procedures being available and easy to access.

To improve reliability, these controls need to be regularly tested and validated – both in terms of physical readiness and worker knowledge. Doing so increases the likelihood they are applied correctly when needed.

Control design and challenges to implementation

Our analysis of control design in SIFp incidents found that permanent and exposure-triggered controls that failed were either not functioning correctly or poorly designed.

Some examples:

- Fire detection equipment not installed in the right place.
- Alarm systems unable to be heard by operators.
- Load movement sensors that failed to work.

This shows the importance of regular inspections and functional testing.

While technical and procedural controls were similar in ease of implementation, when we consider technical controls just in the context of mitigating exposure, they were twice as likely as procedural ones to be difficult or unworkable.

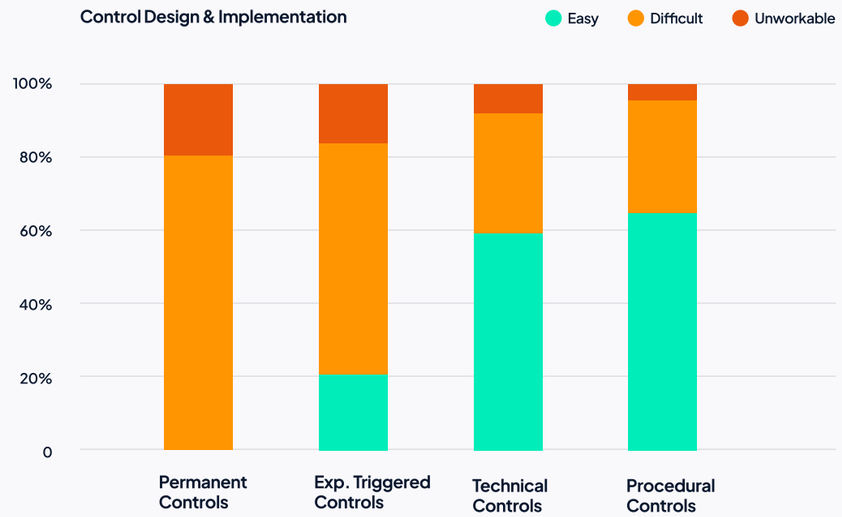
This highlights a critical issue: it's not enough to have the right equipment – organisations must also make sure it works reliably and that workers know how to use it correctly.

Some examples:

- Use of technical PPE for working at height.
- Handling high-pressure or electrical equipment.
- Fire protection systems that aren't automated.
- Scaffold design and setup.
- Load movement and restraint.
- Vehicle-related protection systems.

These controls rely on two things:

1. Workers having the right skills and training to use the equipment.
2. The equipment itself being in proper working condition.



These findings point to a need for better assurance systems that check both worker readiness and control functionality – especially in high-risk environments.

> Improving implementation effectiveness of technical controls means making sure both of these elements are in place. Competency assurance and regular equipment checks are critical to reducing control failure in these high-risk situations.

Understanding that different risks are vulnerable to particular types of control

Each type of risk tends to rely on specific types of controls – and some of those control types are more likely to fail than others.

Falling object risks

Falling object incidents rely almost exclusively on behavioural controls aimed at:

- Preventing the release of energy (61%)
- Creating separation between people and hazards (28%)

These controls are split fairly evenly between procedural and technical types. However, few mitigation controls are used, and those that exist often lack strong performance standards. For example, drop-zone barricading requirements may be vague or inconsistently applied. The most common failures occur in scaffold construction and securing loose objects.

Working at height risks

Working at height incidents show a more even distribution between controls that:

- Prevent the release of energy (55%)
- Mitigate its impact (43%)

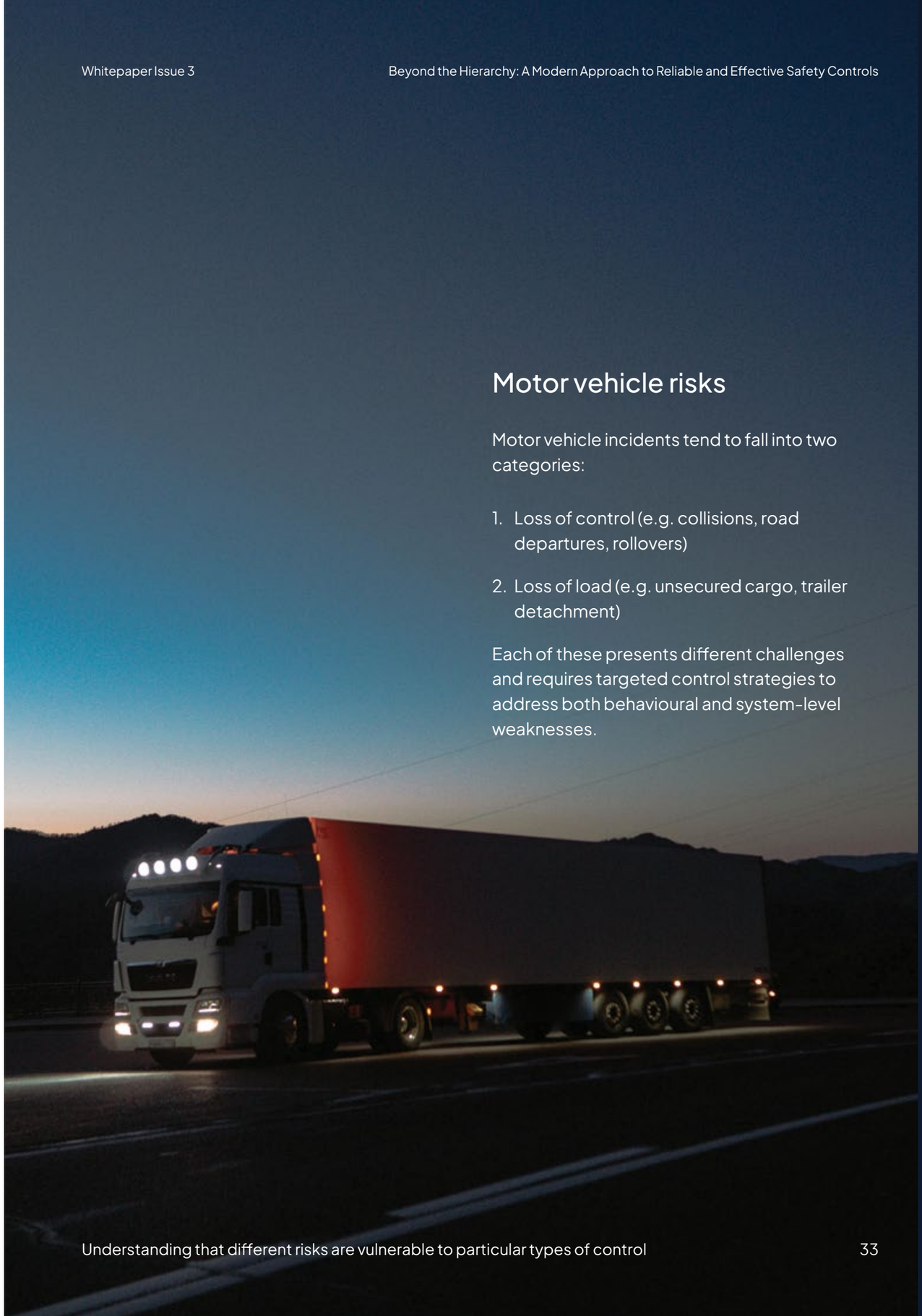
In these cases, almost all controls are behavioural, with most being procedural. Failures commonly involve motorised platforms and fall restraint devices. This makes control verification and supervision essential for managing risks at height.

Motor vehicle risks

Motor vehicle incidents tend to fall into two categories:

1. Loss of control (e.g. collisions, road departures, rollovers)
2. Loss of load (e.g. unsecured cargo, trailer detachment)

Each of these presents different challenges and requires targeted control strategies to address both behavioural and system-level weaknesses.



Loss of control

In motor vehicle incidents involving loss of control, certain types of controls consistently show higher failure rates:

- 46% of the controls are designed to mitigate uncontrolled energy, and nearly all of these are procedural. These failures often stem from slips, lapses in focus, or poor judgement by the driver. Improving driver competence in unexpected emergencies and installing proven automated driver aids are two options for reducing reliance on these fragile behavioural controls.
- 26% of the controls aim to prevent the release of energy. These are split between procedural and technical designs:

- Procedural failures often involve missed vehicle inspections, poor parking practices, and non-compliance with journey management plans.
- Technical failures are usually related to vehicle selection or inadequate maintenance.

> To reduce loss-of-control incidents, organisations must strengthen both behavioural safeguards and system-level controls that support safe driving practices.

Loss of load

In vehicle-related loss of load events, most failed controls fall into two categories:

1. 74% are designed to prevent the release of energy (e.g. securing cargo or ensuring trailer connections).
2. 22% are designed to detect problems as they arise (e.g. through monitoring systems).

Failures are split evenly between human error and mechanical issues.

> Since many mechanical issues should be caught during pre-use checks, one of the most effective improvements is introducing prompts and reminders to make sure inspections are done before vehicle movement.

Exposure-triggered control risks

While exposure-tiggered control failures are much less frequent overall, the three high-risk areas that they happen most are:

1. Unsecured vehicle loads.
2. Fire, explosion, and hot work.
3. Hazardous substance exposure.

In these situations, control systems (such as detectors or alarms) often fail because they:

- Fall out of calibration.
- Don’t trigger properly.
- Lack integration with interlocks or other automatic responses.

The solution? Regular testing and inspection to make sure these detection systems are working exactly as intended – before they’re needed in an emergency.

Key recommendations for safety leaders

Analyse high risk tasks for their complexity, and direct control investment where error is most likely.

To strengthen control reliability, safety leaders need to understand how often humans make mistakes – especially in high-risk environments. Research using the Human Error Assessment and Reduction Technique (HEART) shows that different task contexts produce predictable error rates.

Human Error Rates

Task Type, Experience & Competence, Attention

	Task Context	Predictable error rate
1	Totally unfamiliar task, performed at speed with no real idea of consequences	1 in 2
2	Complex task requiring high level of comprehension and skill	1 in 6
3	Fairly simple task performed rapidly or given scant attention	1 in 11
4	Routine, highly practiced, rapid task involving relatively low level of skill	1 in 50
5	Completely familiar, well designed, highly practised, routine task occuring several times per hour, performed to highest possible standards by highly motivated, highly trained and experienced people, totally aware of implications of failure, with time to correct potential error	1 in 2500

In most work settings, category 5 tasks (very low error likelihood) are rare and category 1 tasks (very high error likelihood) are generally avoided.

Most tasks fall into categories 2, 3, or 4, where the risk of human error is very real and must be factored into safety planning. This matters because organisations can use these predictable error rates to:

- Analyse tasks for their relative complexity and skill requirement.
- Assess tasks based on their likelihood of failure.
- Match control investments to the level of risk.

Rather than assuming a ‘one size fits all’ approach, organisations should use this data to make smarter decisions about where and how to strengthen their controls – particularly for tasks most vulnerable to human error.

Conclusion

Improving the reliability of critical controls is essential to reducing serious incidents and protecting workers.

Our analysis of more than 10,000 incidents confirms that most failed controls rely heavily on human behaviour. Whether it's lapses in attention, errors in judgement, or breakdowns in procedural steps, these vulnerabilities are deeply embedded in how many controls are designed and implemented.

We found that 96% of failed controls in SIFp incidents required workers to be continuously alert, competent, and capable of applying the control under real-world conditions – often without adequate system-level support. This high reliance on human precision makes these controls fragile, especially in high-risk or high-pressure situations.

To reduce these risks, organisations must rethink how controls are designed, implemented, and maintained. It's not enough to make sure controls are theoretically in place – they must be effective in practice.

Organisations should strengthen controls that repeatedly fail due to over-reliance on human reliability. They should also clearly identify which controls require greater attention, training, and verification in the field. Additionally, organisations must make sure the tools, systems, and equipment needed to support safe work are in good working order.

By applying these insights and focusing on practical, evidence-based improvements, safety leaders can significantly reduce exposure and build more resilient safety systems.

Control vulnerability self-assessment checklist

Get deeper and more practical learning about control effectiveness from events with potential for serious consequences by examining multiple incidents with similar exposure types that occurred over a six to 12 month timeframe.

Use our checklist to guide your investigation process:

1. Perform

Perform an analysis of your current control architecture to determine extent of human reliability dependence.

2. Focus

Focus on controls that are absent, have failed, or been poorly implemented in incidents with serious potential.

3. Analyse

Analyse the human error component of control failure, looking more deeply into cognitive aspects.

4. Prioritise

Prioritise high frequency control failures for potential re-engineering to reduce human dependence.

5. Assess

Assess the relative ROI of exposure reduction from control redesign and implement those that will make largest difference.

6. Communicate

Ensure remaining procedural controls are highlighted for greater attention and highest frequency field verification.

Incident Analytics™

Uncover hidden risks, improve controls & prevent serious incidents.

We are a risk management research & data analytics company supporting high-hazard industries including mining, utilities, and transport.

Our research and analysis technology gives senior leaders and safety professionals the business intelligence to help improve safety performance.

We hope our work helps to inform your safety strategies in the workplace. To learn more about Incident Analytics go to our website, or get in touch to see what we can do for your business.

P: 1300 955 300
E: info@incidentanalytics.com.au
www.incidentanalytics.com.au

Revision 2 (Aug 2025)