RISKOPILOT

RISKOPILOT BRIEFING · CRITICAL CONTROLS SERIES

Five gates for safety technology, and the clock that stops them becoming an excuse

A test for technology spending is easy to turn into a reason to do nothing. Five gates for executive committees and boards, and the clock that keeps them honest.

BRUNO HOUNKPATI, CEO AND FORMER VP HSE

NOVEMBER 2026 · 7 MINUTES

Any test for technology spending can be used in two ways. It can stop a company buying a system that changes nothing. It can also give a company a respectable reason to change nothing at all.

The second failure is the quieter one. A committee asks whether the hazard could be designed out, agrees that it could, commissions a study, and three years later the haul road is where it was and so are the people walking beside it.

This article sets out a five-gate test for technology proposals against fatal risks. It then adds the rule most such tests lack.

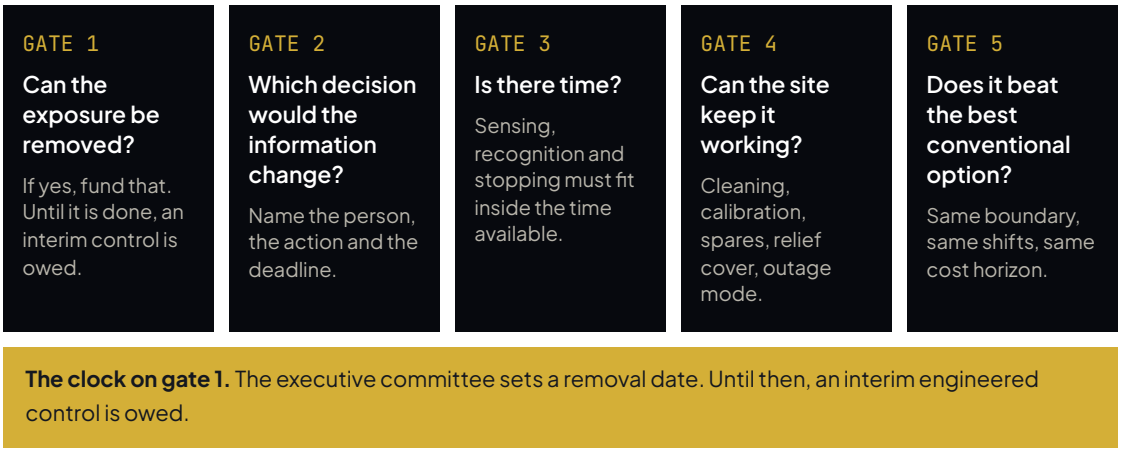
Why test at all

The published evidence does not support buying on trust. A 2023 mapping review of digital safety interventions in construction screened 392 records and kept 24. Most were about developing the technology, and gave low to no evidence of better working conditions or fewer injuries. The Cochrane review of interventions to prevent injuries in construction workers, with a search to April 2017, rated its evidence as very low quality.

So ask every sponsor which of four things has been shown: that the system detects, that someone acts in time, that exposure falls at the same volume of work, or that injuries fall. Most claims stop at the first.

© 2026 Riskopilot · riskopilot.com · contact@riskopilot.com · CC BY-ND 4.0

EXHIBIT



The clock on gate 1. The executive committee sets a removal date. Until then, an interim engineered control is owed.

First, separate two things that are usually sold as one

A system that warns and a system that intervenes are different controls.

A warning depends on a person hearing it, believing it and acting, at the moment of risk. It sits near the bottom of the hierarchy of controls.

A system that slows or stops the machine without the operator is an engineering control. It removes the human reaction from the chain. Regulators have started to treat it that way. South African mining regulations require, where there is a significant risk of collision, that certain machines brake automatically and fail to safe if the operator does not act. A 2015 US rule requires proximity systems on continuous mining machines to stop the machine before it contacts a miner.

The distinction comes first because the gates below treat the two very differently. Sound arguments against warnings are too often used, wrongly, to dismiss intervention.

Gate 1. Can the exposure be removed?

If a layout change, a redesign or a different method takes people out of the hazard, fund that. Segregated routes, ground-level assembly, external cleaning in place of entry, a cold method in place of hot work.

Require: the least-cost credible physical alternative, priced on the same boundary as the technology.

And here is the clock. Removal is often a capital project. So the executive committee sets a date. If the exposure cannot be removed by then, an interim engineered control is owed now, and it stays until the redesign is commissioned. "We are designing it out" is an answer for a quarter. It is not an answer for three years.

© 2026 Riskopilot · riskopilot.com · contact@riskopilot.com · CC BY-ND 4.0

Gate 2. Which decision would the information change?

For every alert there must be one recipient, one expected action and one escalation route, the same on nights, at weekends and for contractors. UK regulator guidance on alarm management says each alarm should have a clear purpose and a defined response.

It fails when the output is a dashboard for managers. That may support learning. It is not a warning and should not be funded as one.

For an intervening system the question changes: which machine function does it command, and who approved that?

Gate 3. Is there time?

Start at the last moment the machine can still reach a safe state and work backwards. With invented numbers, to show the method: 4.0 seconds available, 0.4 to sense and deliver the alarm, 1.3 for the operator to recognise it and act, 2.1 for the machine to stop. The margin is 0.2 seconds. If the measurement uncertainty is larger than that, the evidence cannot support acceptance.

Now take out the 1.3 seconds. That is what intervention does. The same sensor that fails this gate as a warning may pass it as an automatic stop. This is the single best technical argument for intervening systems, and it is an argument from arithmetic that needs no vendor.

It fails when the margin is negative or smaller than its uncertainty.

Gate 4. Can the site keep it working?

A named owner for cleaning, calibration and revalidation. Spares and competent service within reach. A defined mode for loss of power or network, in which the crew can tell a live reading from a stale one.

Intervening systems raise the stakes here. They can brake when they should not, and other equipment can interfere with them. NIOSH has documented a personal dust monitor interfering with proximity detection systems underground. Ask for the failure states, in writing, and test them with nobody in the area.

It fails when nobody on site can restore it, or "normal" and "no signal" look the same.

Gate 5. Does it beat the best conventional option?

Three options, same exposure, same shifts, same cost horizon: the best redesign, the technology, and both together. Cost the whole life, including the labour of investigating nuisance alarms and revalidating after every change.

It fails when the technology matches the conventional option at higher cost, or adds burden without changing decisions.

© 2026 Riskopilot · riskopilot.com · contact@riskopilot.com · CC BY-ND 4.0

The strongest case against this test

"It is biased towards no." Without the clock, it would be. A test that sends every proposal to redesign, with no date, protects the budget and nobody else. The clock is the correction.

"Hierarchy-of-controls purism delays protection people need tonight." Also fair. The hierarchy ranks controls by how little they depend on people. It says nothing about how long each takes to build. An engineered interim control this month can be worth more than an elimination project in year three.

"You ignore the best reason to buy." This is the argument suppliers rarely make. A detection system produces a record of how often people and plant come close. Most sites have never had that denominator. Even where a warning changes no driver's behaviour, the log can show managers where the layout is failing. That is our inference from how such systems record events, and it is a reason to pass a proposal the gates would otherwise stop, provided someone is assigned to read the log and act on it.

Where the boundary is drawn matters more than the sensor

In February 2017 three contractors died and seven were injured when a tank exploded during hot work at a mill in DeRidder, Louisiana. The US Chemical Safety Board found that workers had tested for a flammable atmosphere before starting. They tested outside the tank. The flammable atmosphere was inside.

Every monitoring system inherits the boundary someone drew for it. Before asking whether a sensor works, ask what it is pointed at.

What an executive committee should refuse

- A success measure that counts devices installed.
- A falling alert count with no explanation.
- An injury-reduction percentage from one site.
- Acceptance criteria written after the results.
- A redesign promise with no date and no interim control.

What would change our view

Independent outcome data from sites where intervention has been mandated, with denominators. If that showed exposure or serious injuries falling at comparable work volume, we would move intervention ahead of the pilot stage for those machine types and say so.

Take the last control that failed on one of your sites. Did you lack a timely signal, someone qualified to act, or the authority and money to restore protection? Fund the answer you find, and put a date on it.

© 2026 Riskopilot · riskopilot.com · contact@riskopilot.com · CC BY-ND 4.0

Read the full report. *Time to act: what technology can and cannot add to critical controls* is published by Riskopilot Research on Riskolabs.

Sources

1. Trask, C. and Linderoth, H. (2023). Digital technologies in construction: a systematic mapping review of evidence for improved occupational health and safety. *Journal of Building Engineering* 80, 108082. ScienceDirect.
2. van der Molen, H. et al. (2018). Interventions to prevent injuries in construction workers. *Cochrane Database of Systematic Reviews*, CD006251.pub4. Cochrane Library.
3. Republic of South Africa. Mine Health and Safety Act, 1996: regulations relating to machinery and equipment, regulation 8.10. Government Gazette 38493, 27 February 2015. Automatic-braking sub-regulations in force from 21 December 2022.
4. US Mine Safety and Health Administration (2015). Final rule on proximity detection systems for continuous mining machines. 80 FR 2188.
5. UK Health and Safety Executive. Alarm management.
6. NIOSH researchers. Paper on interference between a personal dust monitor and proximity detection systems.
7. US Chemical Safety and Hazard Investigation Board (2018). Packaging Corporation of America hot work explosion. Report 2017-03-I-LA.

The five gates and the clock are a Riskopilot proposal. The time budget uses invented values. Acceptance criteria for actual work are set by the site's technical authority under local law.

Published under CC BY-ND 4.0. Share unchanged, with attribution. General information, not engineering or legal advice.