SYSTEM DESIGN

A human error risk control hierarchy

Andy Brazier explores a different approach to mistakes

A recent LinkedIn post from the CIEHF highlighted a common issue with our profession: "We spend a lot of time trying to design systems that prevent errors but people will always make mistakes. Not because we're careless but because we're human." It went on to say that the best designs focus as much on error recovery as error prevention. It gave some examples and asked for other suggestions, which prompted an interesting discussion and examples ranging from sink overflows and pencil erasers to computer undo functions and roadside rumble strips.

However, it also highlighted a professional challenge – how do human factors practitioners systematically translate these intuitive, everyday resilience mechanisms into rigorous, safety-critical industrial and engineered systems?

Reducing human error risk

Many sectors recognise human error as a significant contributor to accidents. Unfortunately, individuals working in those sectors in positions with the greatest influence over operational safety, such as design engineers, plant managers and operational leaders, don't always recognise how human factors principles can be applied in practice. This can lead to risk controls that are inconsistent with human factors science, inadvertently introducing new failure modes.

As human factors professionals, we frequently encounter a disconnect when collaborating with technical and operational stakeholders:

- **Administrative bias:** When technical professionals encounter human error risks, they frequently default to low-reliability, administrative controls such as adding 'double-checks' or lengthening procedures. These methods often introduce new failure modes, cause behavioural drift or create a false sense of security.
- **Technology trap:** Conversely, engineered solutions are often introduced under the guise of modernisation, yet they inadvertently increase cognitive load and require higher skill levels.
- **Human factors silo:** Sometimes our own discipline can focus too narrowly on behavioural or cognitive interventions, occasionally under-utilising technical solutions to mitigate human risk.

The proliferation of touch screens is one example. They appear to provide a neat solution, reducing the number of buttons and dials required to operate a device and bringing all controls into one place that can adapt to circumstances. For a multifunction device like a mobile phone, they work well. But in many cases, they're difficult to see, require a high level of manual dexterity and slow down operations because the adaptability makes it difficult to predict where different controls will appear each time they're used. Even on the mobile phone, dialling a number is more difficult on a touchscreen than with old fashioned buttons.

Creating a human error risk control hierarchy

The hierarchy of risk control is well regarded in safety. Could something similar help to bridge the gap between human factors and other disciplines, including the engineers, managers and leaders who are most influential in the way risks are controlled?

> **"How do human factors practitioners systematically translate intuitive, everyday resilience mechanisms into rigorous, safety-critical industrial and engineered systems?"**

The hierarchy is in two parts: Error prevention and error mitigation. While controls at the top of each hierarchy should be considered first, all controls have limitations and the greatest risk reduction will be achieved by ensuring several controls from both parts of the hierarchy are used. This is consistent with the multi-layered approach advocated in process safety through Reason's Swiss Cheese model, bowtie diagrams and layers of protection analysis (LOPA).

About the author

Andy Brazier is a freelance consultant with 30 years' experience in high-hazard industries. His engineering background gives him an insight into how risks are managed in practice, by optimising hardware, software and liveware (people) systems and controls.

Error prevention hierarchy

The following controls should be considered for reducing the likelihood of human error:

Error risk control: Prevention	Explanation	Example (transport-related)
Eliminate	Remove the task completely to eradicate the error potential.	If a journey isn't made, there's no potential for an accident.
Substitution	Redesign the task to an inherently simpler and lower-hazard method.	Selecting motorways, which have a better safety record, instead of country roads. Taking the train instead of the car.
Automation	Create a system that performs the action without human involvement.	Fully autonomous vehicle.
Passive sequence restriction	Physical design makes sequence errors impossible.	Trains on tracks cannot deviate from the defined route, unlike cars on a road.
Passive fool-proofing	Design physical/digital interfaces so incorrect orientation/connection is impossible.	Vehicle petrol filler necks are smaller than diesel nozzles at fuel stations.
Active interlocking	System dynamically detects an incorrect action and halts the operation.	Collision avoidance that applies vehicle brakes if too close to an obstacle.
Visual clues	Making the correct actions visibly obvious.	Road signs (directions and situations).
Procedures and training	Defining a task method that minimises human error risk.	Everyone must pass a test before they're allowed to drive on public roads.

None of these controls can be fully effective. Automation may eliminate the opportunity for operator error but increase risks from maintenance errors.

Passive devices have fewer failure modes than active devices but are difficult to design for every eventuality.

Active devices can fail and are usually quite easy to defeat, so can give a false sense of security. Visual clues, procedures and training can't prevent errors happening but are simple and adaptable controls that can be very effective when they're combined with other error risk controls.

Error mitigation hierarchy

The following controls should be considered for mitigating human error:

Error risk control: Mitigation	Explanation	Example (transport-related)
Passive consequence mitigation	Structural/architectural containment of the energy or hazard.	Roadside barriers that prevent a vehicle crossing onto the opposite carriageway.
Action reversal	Allow operators to step backward to a safe state before the consequence takes effect.	Car racetrack run-off areas that provide drivers the opportunity to recover from an error without damage.
Active warnings and prompts	Alerts a human that they need to take action to deal with a problem.	Parking sensors with audible and visible signals when getting too close to other cars.
Second checks	Independent verification and peer checking.	Tasking a passenger to check for traffic when pulling out of a complicated junction.

Again, none of these controls can be fully effective. The technical controls reduce or change the consequence, rather than preventing them entirely, and can introduce other potential hazards. Active warnings are fully reliant on a human to respond. Second checking is easy to add to a procedure, but in practice can be counterproductive because people change their behaviour when their actions are being checked.

Conclusion

For human factors professionals, this hierarchy serves as an actionable framework to guide safety-by-design. By presenting technical professionals and operational leaders with a structured, familiar hierarchical language, we can steer design conversations away from administrative defaults ('retrain the operator') towards more effective system changes that reduce human error risk. This doesn't involve finding a single, flawless control, as every layer has inherent failure modes. The best solution will be achieved by deliberately layering defences. By systematically combining prevention controls, to minimise the likelihood of an error, with robust mitigation controls – to absorb the fall-out when an error occurs – organisations can design systems that are fundamentally tolerant of human error. ■