IRSE
Institution of Railway Signal Engineers

Back to basics: Principles of railway safety engineering

BACK TO BASICS

David Nicholson

This article continues the 'back to basics' series, looking at the principles of safety engineering as applicable to a railway, particularly hazard and risk assessment, identification and analysis techniques. Previous 'back to basic' articles have touched on the safety inherent in each of the systems discussed; this article considers how safety is achieved.

> "If we wish to avoid harm, we should seek to reduce risk"

Definitions

Before we begin, it is necessary to be clear on definitions and what is meant by the different terms used.

- Safety: Freedom from unacceptable risk.
- Risk: The combination of the likelihood of occurrence resulting in harm and the degree of severity of that harm.
- Harm: Physical injury, material damage.
- Severity: A measure of the amount of harm.
- Accident: An unintended event or series of events that results in harm.
- Hazard: A condition that could lead to an accident; a potential source of harm; an accident waiting to happen.
- Cause: Any event, state or other factor which might contribute to the occurrence of a hazard.
- Safety measure: An action reducing the risk of a hazard.

The definition of 'safety' introduces the concept that some risk is acceptable. This might seem surprising at first reading, but there are plenty of people who indulge in activities that others consider too dangerous (e.g. bungee jumping or flying). Others can see the benefits that it brings to them (e.g. thrills or speed of travel).

This raises the question of who determines whether a risk is acceptable or not. Sometimes this is purely personal (whether to bungee jump or fly), but when a service (such as rail travel) impacts on the general public, it is usual for governments to establish legislation with which those providing the service must comply. The legislation is usually aimed at reducing the amount of potential harm to the general public and workers, whether that harm is shock, injury, permanent damage (e.g. loss of a limb or hearing loss) or fatality.

This is not a simple action for governments to achieve as the public they are seeking to protect is not consistent in their perceptions of acceptable levels of risk. There is often a large outcry from the public when a single train accident results in several deaths, but the very many single deaths that occur each day on the roads is felt tolerable. This inconsistency is something that railway, and other, engineers have learnt to live with.

From the definition of 'risk' we can see that if we wish to avoid harm, we should seek to reduce risk. This is achieved either by reducing the likelihood of occurrence of harm, reducing the severity of the harm, or both. Putting it another way, we can reduce risk through two different approaches: the first is to reduce the likelihood of an event happening where the outcome may be harm; the second is to reduce the amount of harm should that event take place.

The definition for a hazard can also be expressed as 'an accident waiting to happen'. No accident has taken place, but there is a dangerous situation where if something else happens, it can lead to an accident. Thus, for any given hazard, all that is needed is a trigger event to start the process which ultimately leads to the accident. An example hazard is a level (or at grade) crossing with no form of protection. The hazard (the accident waiting to happen) occurs when a train is approaching. There has not been any accident, but one could happen if there was a car approaching (the trigger event). An approaching car may now collide with the train resulting in an accident with consequences beyond the railway boundary.

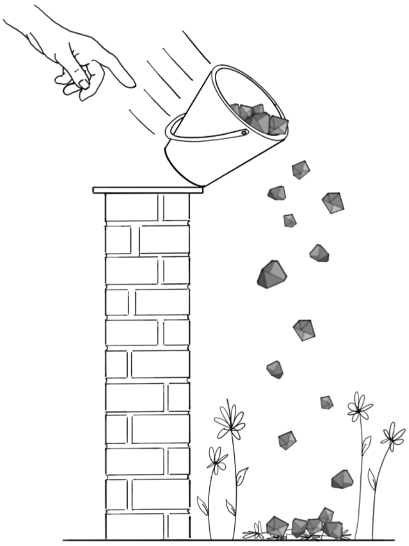


Figure 1 – Hazard to accident.

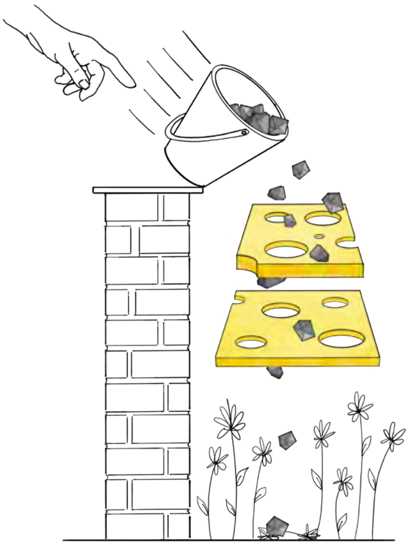


Figure 2 – Hazard to accident – reduced risk.

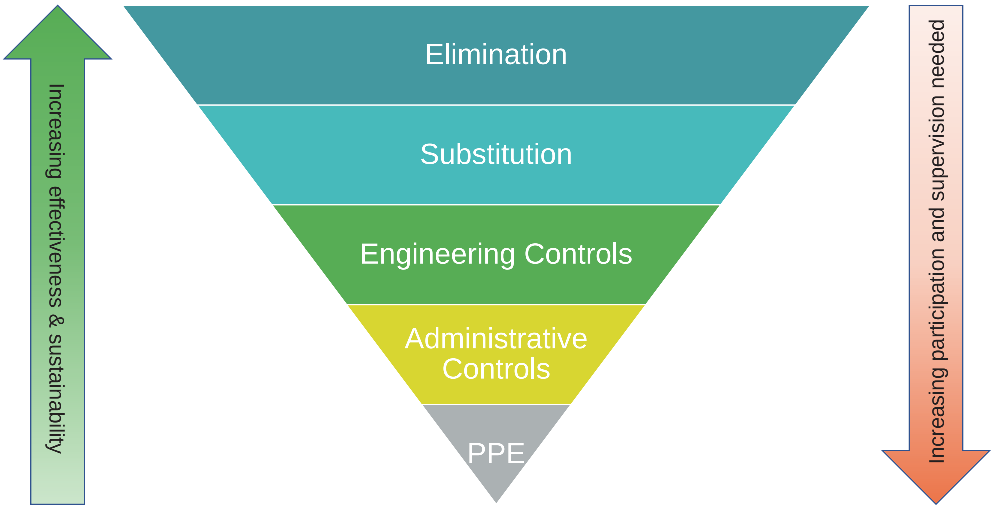

Increasing effectiveness & sustainability
Elimination
Substitution
Engineering Controls
Administrative Controls
PPE
Increasing participation and supervision needed

Figure 3 – Hierarchy of control.

> “Risk reduction measures are sometimes expressed in a hierarchy of control”

This sequence of events is illustrated in Figure 1 where: the level crossing is the wall; the hazard is shown as the bucket of stones on top of the wall; the trigger event is the hand knocking the bucket over; and the accident is the stones falling onto the flowers.

Risk reduction

From the diagram, we can see the accident can be prevented, or limited, quite simply by:

- Removing the hazard: Design the railway without a level crossing.
- Reducing the frequency with which the hazard occurs: Reduce the number of trains that use the crossing.
- Reducing the frequency of the trigger event: Reduce the number of cars that use the crossing, for instance by providing an alternative and more attractive route for car drivers to use).
- Reducing the likelihood of a collision: Design a level crossing system that warns of an approaching train; install barriers and road traffic lights to stop road traffic; provide railway staff to stop traffic; have the train sound its horn on approach; ensure good sight lines.
- Reducing the severity of a collision: Reduce the speed of approaching trains; provide space for a car to divert into at the last minute; design cars to survive the impact of a train. This last point about car design is outside the scope of railway projects but indicates how solutions can lie outside of the expected areas of interest as shown in Figure 2.

Trying to limit the number of falling stones in our illustration in Figures 1 and 2 is not a perfect solution. Any of the examples given above can fail. If the means to limit the falling stones is shown as barriers with holes, it is obvious that some stones still make it through the holes in both layers and crush the flowers underneath. But the impact, or severity, of that accident is (hopefully!) smaller than it might have been if no protection was put in place – fewer flowers are crushed!

Risk reduction measures are sometimes expressed in a hierarchy of control. This is shown in Figure 3.

WACHT tot het rode licht gedoofd is er kan nog een trein komen
WACHT

Substitution may see a level crossing replaced with a bridge, although bridges bring their own set of hazards. *Photo Shutterstock/ Ivonne Wierink.*

The explanation of the different levels is as follows:

- Elimination: design out the hazard (e.g. remove the need for the road to cross the railway).
- Substitution: replace the hazard with something less hazardous. For instance, we could replace the level crossing with a bridge. While in this example this might seem very close to elimination, bridges bring their own set of hazards due to bridge strikes, or vehicles or objects falling onto the railway from the bridge thereby blocking the line).
- Engineering: use work equipment or other measures to help separate people from the hazard. Examples are warnings, alarms, guarding dangerous machinery from human incursion (e.g. for level crossings, provide lights and audible alarms as the train approaches).
- Administrative Controls: Identify and implement procedures necessary to work safely with the hazard. For example, we could provide instructions and training both for train driver and road users on how to use the different types of level crossing.
- Personal Protective Equipment (PPE): This is why motorcyclists wear crash helmets. Or why people erecting scaffolding are tethered. There is no example here for a level crossing. But it is, for example, why many railway administrations require their trackside staff to wear high-visibility clothing. This makes them more visible to the train driver, who can sound the train's horn, thereby giving the trackside staff more time to get clear of the approaching train.

The temptation, because it's both inexpensive and quick to implement, is to rely on the lower levels of risk reduction, namely administrative controls or PPE. People are unreliable at carrying out instructions and obeying alarms, particularly under stressful conditions. Therefore, the reliance on these lower levels of control should only be used where elimination, or substitution or the use of engineering controls cannot be achieved.

"The temptation is to rely on the lower levels of risk reduction"

"Determining the safety benefit over the lifetime of the safety measure is a little harder and, at times, controversial"

Safety benefits and costs

It is expected that the engineering and operations teams will implement good practice and adopt the hierarchy of controls from the outset. Choosing which control in the hierarchy to apply introduces the concept of calculating the costs involved to introduce a safety feature and then comparing that with the safety benefit.

Calculating the costs is relatively straightforward by asking questions such as: How much will it cost to provide this extra design feature? How much do any extra parts or items of equipment cost to purchase? How much more will it cost to operate and maintain the railway with this safety feature implemented?

Determining the safety benefit over the lifetime of the safety measure is a little harder and, at times, controversial, not least because in addition to fatalities, there are so many different types of injury (both physical and mental). Does the age of the individual matter? Or the number of their dependants? Does the number of injuries or fatalities in any one incident make a difference?

A number of countries have adopted a method of converting injuries and fatalities into a common measure. One method is shown below as a Comparable Fatality Score (CFS) (note that other countries and other railway administrations may have different conversion rates):

- 10 major injuries to 1 fatality.
- 100 minor injuries to 1 fatality.
- 1000 negligible injuries to 1 fatality.

Each CFS is converted into a monetary value, a figure that is set independently, usually at a national level, typically with a figure around £1.5m to £2m per comparable fatality. By comparing the risk to life without the safety measure to the risk with the safety measure, a reduction in the CFS can be calculated. This benefit can then be compared to the cost of implementing the safety measure. This allows for a simple Cost-Benefit Analysis (CBA). If the cost of implementation is much higher than the reduction in CFS, then the project does not have to implement the safety measure. In the UK, for example, a project is obliged by law to reduce risk to As Low As Reasonably Practicable (ALARP) and it is this process of comparing project costs with a reduction in CFS that enables the project team to justify its decisions.

"Demonstration of sufficient safety level is a complex and challenging process"

The demonstration of sufficient safety level is a complex and challenging process. Different countries will have different approaches to demonstrate what is acceptable and what is not. Adopting good practice through adherence to standards or qualitative arguments may be sufficient, with a CBA only used in the more complex situations. However, CBA on its own is not sufficient to demonstrate acceptable safety levels. It cannot, for example, be used to claim that adherence to statutory duties is not required, or that intolerable risks are somehow acceptable just because they offer a good CBA. Legislation often weights the decision towards safety, requiring risk reduction measures that may not seem necessary when judged by a CBA alone. And it should be noted that benefits may not be limited to safety. There may, for example, be efficiency or environmental benefits as well.

Defence in depth

How do we design systems that are 'safe'? We consider a process known as 'Defence in depth'. This consists of seven sequential steps as discussed below.

Error avoidance: We work to prevent design errors occurring in the first place by:

- Keeping the design simple. An overly complicated system makes it harder to detect errors in the design of the system. Safety and non-safety elements of the design should be kept separate. Avoid novel design features and the use of subtle techniques that are not clearly understood by others. Don't provide functionality that isn't required in case it is inadvertently activated. This is particularly pertinent for software where complex subroutines and self-modifying code can result in faults in operation.
- Adherence to standards: People have spent a lot of time documenting how things should be done so that those who follow can benefit from their experience. It also ensures that people adopt a common approach to their understanding of functional operation.
- Configuration Management: We need to ensure that people are working from the correct design information, and that the final design drawings are marked correctly so that the installation, test and commissioning engineers can have confidence they are installing, testing and commissioning the correct design.
- Competence: Ensure those designing the system know what they are doing! Competence is defined as the combination of knowledge and experience, which can be grown through training, mentoring, observation and assessment.

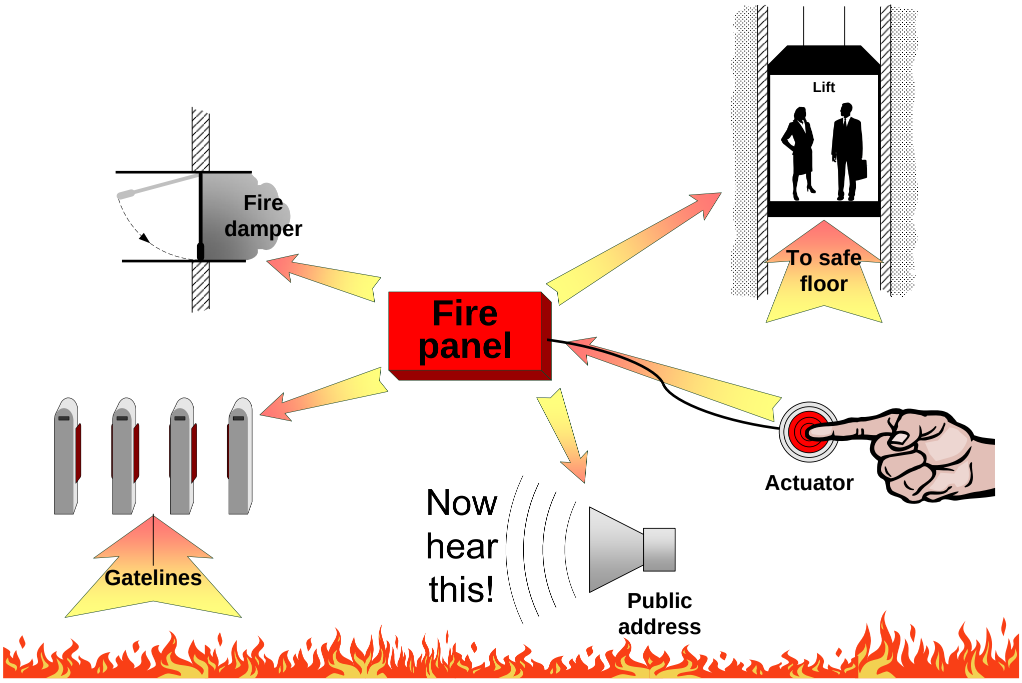
Error detection: If there is an error in the design, we want to find it and remove it before it is installed. This means designing for testability and validation, checking and reviewing designs, performing simulations, doing software code walkthroughs and undertaking development testing.

Fault avoidance: Even where the design is error-free, faults can occur in operational service, and so controls must be applied to minimise the risk. These controls include:

- Design for reliable operation, by ensuring components are not stressed when in service (e.g. too much current through electrical components, or too much load for mechanical elements) and by choosing reliable components.
- Perform proactive maintenance when in service by maintaining at regular intervals or by having systems that alert the maintainer when in need of maintenance.

Personal Protective Equipment is important, but cannot guarantee workers' safety. *Photo Shutterstock/ Ian Stewart.*

Figure 4 – Simplified station fire panel interface diagram



"How are hazards identified before they result in accidents?"

Fault detection: We are dealing with real-life mechanical and electrical systems which will wear and fail. So we want to ensure that faults can be detected and rectified before any life-threatening situation arises. We do this through:

- Specifying appropriate testing and maintenance intervals and thresholds.
- Where there are several similar items, these can be compared to determine where their behaviour diverges.
- Provision of in-service self-diagnostic facilities.
- For software, the use of watchdog timers or plausibility checks on data.

Fault tolerance: Knowing that faults will occur, we can design our systems to tolerate certain levels of faults. Examples include:

- Redundancy: Providing more than one channel for the same information or control flow. A common approach in computer-based systems is to have three computers undertake the same calculation and a voting system checks that at least two of them agree. This is known as a 2-out-of-3 voting system). Note this protects against random hardware failures (one channel may fail) but not against systematic faults where there is a software fault which causes all three channels to produce the same wrong output.
- Diversity: This is similar to redundancy except that the channels use different hardware and/or software to avoid many systematic errors. This can be through design diversity (the 2-out-of-3 voting system uses different microprocessors), functional diversity (e.g. automatic braking, but with a driver on board to act in case the automated system fails), manufacturing diversity (procure the same product but from different suppliers).

Failure handling: We can ensure that we can handle failures well through:

- Using known physical or electrical properties to ensure that should a fault occur, it fails to a known state (e.g. gravity returns a signal arm to the stop position).
- Provision of alarms or other warning indicators.
- Instructions for people to follow in the event that something does go wrong.

Hazard mitigation: Finally, given the system may fail in an unsafe way despite all the above best efforts, we consider implementing other measures to reduce the overall risk such as crash worthiness of vehicles.

Hazard identification and analysis

This is all good theory. But how are hazards identified before they result in accidents? There are three areas we need to consider:

1. The functions the system has to perform.
2. The users of that system and how they are expected to interact with it.
3. Interfaces with other systems.

In order to do this, the system you are analysing needs to be comprehensively defined and understood. Consider the introduction of a station fire panel in an underground station as shown in Figure 4.

The fire panel has one function: upon receipt of an input from the actuator, it sends a control signal via each of its interfaces to external systems, so they can perform their functions.

In this example, there are three groups of people: firstly the one who presses the actuator who may need some instruction or guidance on when to press the actuator and what to expect next; secondly station staff who need training in the

Guideword	Definition
No or not	No part of the intended result is achieved or the intended condition is absent
More (higher)	Quantitative increase
Less (lower)	Quantitative decrease
As well as	Qualitative modification/increase (e.g. additional material)
Part of	Qualitative modification/decrease (e.g. only one of two components in a mixture)
Reverse/opposite	Logical opposite of the design intent (e.g. backflow)
Other than	Complete substitution, something completely different happens (e.g. wrong material)
Early	Relative to clock time
Late	Relative to clock time

Table 1 – Hazard identification guidewords.

Likelihood category	Classification term	Time frame	Midpoint likelihood estimate	Description
5	Frequent	Less than 1 year	1 in 6 months	The event is likely to occur frequently (probably annually).
4	Probable	1 year to 5 years	1 in 5 years	The event is likely to occur often.
3	Occasional	5 years to 10 years	1 in 10 years	The event is likely to occur several times.
2	Remote	10 years to 100 years	1 in 50 years	The event can be expected to occur during the lifecycle.
1	Improbable	100 years or greater	200 years	The event is unlikely but may by exception occur.

Table 2 – Likelihood categorisations.

Severity category	Classification term	CFS equivalence	Description
1	Negligible	0.001	Non-reportable injury
2	Minor	0.01	Minor injury
3	Major	0.1	Major injury or multiple minor injuries
4	Critical	1	Single fatality or multiple major injuries. Equivalent to 1 CFS
5	Catastrophic		Multiple fatalities

Table 3 – Severity categorisations.

"A HazID involves systematically considering each function, user operation and interface"

event of an alarm; thirdly members of the public who are expected to evacuate the station when the alarm is activated. Designers and maintainers are also important for any system but are not considered in this particular scenario.

Five separate interfaces are identified, each of which will have electrical, mechanical, physical and functional properties. These are:

1. The actuator input.
2. The fire damper which closes the damper to restrict the flow of oxygen to a fire.
3. The ticket gates, designed to open to permit the quick and safe exit of passengers.
4. Automated public address system which initiates announcements alerting passengers to the need to evacuate the station.
5. Lifts which must move people to a deemed safe floor.

It is quite usual to hold a Hazard Identification (or HazID) workshop. It is important to get representation from people who are experienced in the system being considered, the environment in which it will operate and how things might go wrong. A HazID involves systematically considering each function, each user operation (or reaction in the case of members of the public) and each interface. The conversation is seeded with guidewords to encourage the meeting to think about how the function, user or interface might not work as intended. An example of potential guidewords and their meanings are shown in Table 1.

The workshop members can consider whether each deviation from intended operation represents a genuine hazard. Once all reasonably foreseeable hazards are identified, the hazards can be analysed to determine their likelihood and severity of outcome. This aids understanding of the risk and enables effort to be focussed on those with the highest risk. This analysis is often done qualitatively, and it is usual to see categorisations of likelihood and severity similar to Tables 2 and 3.

Likelihood		Severity					Risk classification
		1	2	3	4	5	
		Negligible	Minor	Major	Critical	Catastrophic	
5	Frequent	Medium	High	High	High	High	**Intolerable risk:** Activity not permitted. Hazard to be avoided or reduced.
4	Probable	Medium	Medium	High	High	High	
3	Occasional	Low	Medium	Medium	High	High	**Tolerable risk:** Control measures to reduce risk rating to a level which is as low as reasonably practicable (ALARP).
2	Remote	Low	Low	Medium	Medium	High	
1	Improbable	Low	Low	Low	Medium	Medium	**Negligible or low risk:** Control measures to be maintained and reviewed to control residual risk as far as reasonably practicable.

Table 4 – Risk matrix.

This allows a matrix of risk classification to be developed where particular combinations of likelihood and severity can yield a risk that is intolerable, tolerable or negligible. An example is shown in Table 4.

Note that all of the above tables are examples. Different railway authorities may have different categorisations and different acceptable levels of risk. All such categorisations and levels must be justified, and this is typically done in a safety plan. In extreme cases, likelihood and severity may need to be calculated quantitatively; this is much harder to do.

Now the hazards are identified and their risk has been considered, safety measures can be designed to reduce those risks to a more acceptable level. A project may need to bring together a number of representatives to determine if a risk is acceptable based on proposed measures.

"There will always be engineering failures"

Causes vs hazards

A common mistake in this process is to confuse causes of hazards as hazards. This can result in a long list of so-called hazards to manage, increasing the time and cost involved to complete the design. Avoiding this confusion is achieved by being clear about the functions of the system being developed, its users and its interfaces. This usually entails developing a diagram showing all the possible interfaces, making sure this includes the human interactions as well as technical interfaces. In the fire panel example, the function of providing an alert to each of its interfaces could have a hazard of 'No alert to the interfaces'. This could happen because the power supply to the panel was faulty. The failing power supply is a cause of the hazard.

Be alert!

Samuel C Florman was a Civil engineer who started his career in the 1950s. In his book, "The Civilised Engineer" he writes (p149):

> *"There will always be engineering failures. But the worst kinds of failures, the most inexcusable, are those that could readily be prevented if only people stayed alert and took reasonable precautions.*
>
> *"...experience teaches us that society requires a cadre of concerned citizens – engineers foremost among them – to urge proper action and to persist when rebuffed.*
>
> *"Engineers, being human, are also susceptible to the drowsiness that comes in the absence of crisis. Perhaps one characteristic of a professional is the ability and willingness to stay alert while others doze. Engineering responsibility should not require the stimulation that comes in the wake of catastrophe."*

Staying alert requires the engineer to identify, then assess the risks arising from the works being undertaken. As engineers, we need to be alert to how the design will be operated and how the system will be maintained. We must foresee changes in the operating environment that will affect the system's operation and consider how that design will eventually be decommissioned. Risks can arise through many areas. This includes the physical aspects, human behaviours, the processes which govern how tasks are performed, and the ability of people to perform a task when under pressure. Having assessed the risks, the engineer must design the system (consisting of people and processes as well as the products themselves) to mitigate against those risks.

About the author ...

David is the professional head of discipline for Engineering Management in SNC-Lavalin Atkins and works to grow the skills and knowledge of those who provide the technical leadership of projects. Beginning with an understanding of the operational needs, he specifies, designs and changes railways to make them safe, operable and fit for purpose.

As a railway systems engineer with a broad knowledge of rail systems, disciplines and operations, coupled with experience across the whole development lifecycle, David has taken projects from initial concept through design and development through to implementation.

He is currently working in the Engineering Management Office of the East Coast Digital Programme, bringing digital railway techniques to Network Rail's main line from London to Edinburgh.