Is there a need to redefine the "safe state" in fail-safe signalling system designs?

Written and edited by Alan Rumsey on behalf of the International Technical Committee of the IRSE

BACKGROUND

As a profession, Signal Engineers can be rightly proud of the significant contributions they have made in maintaining and improving the safety of rail transportation over the past hundred years; an achievement that has required a continuous focus on the details of railway signalling designs, installations and maintenance as signalling technologies have evolved, as new hazard risks have been identified and as unexpected component and equipment failure modes have been uncovered.

This safety record has been achieved, at least in part, through the rigorous application of one of the fundamental principles of a railway signalling, namely that the signal system must be designed to be "fail-safe". This principle has generally been interpreted such that failure of signalling equipment must cause the most restrictive signal indication to be displayed, bringing a train or trains to an immediate stop. In other words, in a railway signalling environment a stationary train is generally regarded as a "safe state". As a consequence, historically many signal systems have effectively only supported two levels of functionality with respect to the safety of train movements:

- Full functionality and a very high level of safety when the signalling system was fully functional, or
- Very limited or no functionality in the event of a signalling equipment failure, with the safety of any subsequent train movements exposed to the risk of human error.

More recently, Signal Engineers have been able to take a more holistic view of rail transportation operations. For example, while bringing a train or trains to a stop may mitigate any immediate hazard of a train collision or derailment, it is recognised that this state may not be free from other hazards.

If we accept the premise that a stopped train is not necessarily always a "safe state" from the perspective of the passenger, nor does a stopped train fulfil its fundamental mission to transport passengers from their origin station to their destination station, then the challenge for the Signal Engineer is not only to achieve a "fail-safe" design, but also a "fail-operational" design, or a design that supports "graceful degradation" that will minimise the probability of a train being brought to an unscheduled and undesirable stop.

With today's more sophisticated and more distributed computer-based, communications-based and information-based technologies, the Signal Engineer now has more tools available to achieve both "fail-safe" and "fail-operational" designs. If one element of a modern signalling system fails, it may now be possible to take advantage of the intelligence and information that remains in other elements of the signalling system to support intermediate levels of signalling functionality that can maintain train operations, even if at a reduced level of performance.

The intent of this article is not to propose specific "fail operational" signalling design solutions, nor to suggests that the signalling system alone should be responsible for mitigating all of the hazards on the railway, but rather to highlight that today a systems engineering and hazard risk-based design process is increasingly being adopted within the signalling profession; a process that expands on the historical definitions of a "safe state" to encompass consideration of all of the hazard risks to which passengers, staff and the general public may be exposed, and that recognises the intimate relationships between system safety and system availability.

FIRST SOME DEFINITIONS

Various definitions can be found in the technical literature and in national and international standards for the terms "fail-safe" and "fail-safe designs". These definitions often reflect the particular perspective of the stakeholders that developed these definitions, but all of these definitions have one thing in common, namely they embody a concept that in the event of a component or equipment failure, the signalling system will enter into, or remain in, a "safe state".

This article therefore does not attempt to redefine or propose a new definition for the term "fail-safe", but rather to expand upon the definition of the "safe state" within the context of a "fail-safe" signalling system design.

Before discussing the definition of the "safe state" we first need a common understanding of terms such as "safety" and "hazards".

"Safety" is defined here as "freedom from unacceptable levels of risk or harm due to faults or failures of equipment, processes and people" which introduces the concept that safety is not absolute, but involves an assessment of risk and a judgement as to whether or not that risk has been mitigated as far as is "reasonably practical" such that the level of risk can be considered acceptable or at least tolerable. The phrase "reasonably practical" itself implies that a risk mitigation measure must not only be possible, but implementable at a cost commensurate with the safety benefits to be gained.

A "hazard" is defined here as "something that can cause adverse effects" and the hazard risk considers both the likelihood that a hazard will actually cause its adverse effects, together with a measure of the severity (i.e. degree of harm) of that effect.

While the definition of Safety is typically not extended to address Security, which deals with harm through malicious intent, the two disciplines become integrated in the design and operation of a railway with consideration of both safety hazard risks as well as security threat risks.

THE CHALLENGE FOR THE SIGNAL ENGINEER

So, in the context of this article, it becomes clear that any discussion on the "safe state" in railway signalling first requires that we consider the following two questions:

- What are the hazards a Signal Engineer should reasonably be expected to be aware of, and contribute to mitigating?
- For those hazards, has the hazard risk been reduced to acceptable (i.e. reasonably practical) levels, without introducing new hazards or imposing undue constraints in mission success, and with consideration of the capabilities and suitability of currently available signalling technologies to eliminate or minimise the risk?

In considering these questions, we also have to recognise that within a rail and transit environment, new hazards may be identified over time, hazard probabilities (and hence hazard risks) may increase, and signalling technologies are continually evolving. As such, any assessment as to whether or not a particular hazard risk has been reduced to as low as is reasonably practical may also change over time. Indeed, in the event of an incident or accident, any determination as to the "reasonableness" of the signal system design will likely be made based on the expectations at the time of the determination, rather than the expectations that may have been present at the time of the signal system design and implementation.

One of the challenges facing the Signal Engineer is that as signalling systems become more sophisticated, they can become more vulnerable to widespread system outages. This in turn can lead to a desire to install additional "back-up" or "fall-back" systems which can further add to the system complexity with associated negative impacts to system reliability, availability and maintainability. If degraded modes of operation were however designed into the signalling system from the outset, could this additional complexity be avoided?

HAZARDS TO BE MITIGATED

So, what are the hazards a Signal Engineer should be concerned with?

The primary hazards that have been of concern to the Signal Engineer have of course included:

- Train-to-train collisions (rear-end, sideswipe, head-on); a hazard that is addressed through signalling systems that provide for train detection, train separation assurance, rollback protection, parted consist protection, route interlocking protection, and traffic direction reversal interlocks, for example;
- Train-to-structure collisions; a hazard that is addressed through end-of-track protection and restricted route protection systems for example;
- Collisions between trains and road vehicles (or people) at grade crossings; a hazard that is addressed through level crossing warning devices, for example;
- Train derailments; a hazard that is addressed through overspeed protection, route interlocking protection, and (potentially) through broken rail detection.

Other hazards may also need to be considered, depending on the specific application (and the following is not intended to be an exhaustive list):

- Hazards associated with collisions with objects on the track;
- Hazards to work crews and work trains on the track;
- Hazards to people on the right-of-way other than work crews;
- Hazards to passengers associated with train movement with train doors open.

When considering all of the above hazards, the hazard event can only occur if the train is in motion. As such, bringing trains to a stop in a timely manner in the event of a signalling failure does result in an acceptable "safe state" as collision hazards (with other trains, road vehicles, objects or people on the track) and derailment hazards will indeed be mitigated.

However, there are other scenarios where bringing trains to an unscheduled and undesirable stop may create hazards, rather than mitigate hazards, such as (and again, this is not intended to be an exhaustive list):

- Hazards to standing passengers through unexpected and unnecessary application of the train's emergency brakes;
- Hazards to passengers stranded within stationary trains for an extended period of time following a signalling equipment failure (for example, multiple trains stranded within a tunnel environment or a stopped train that blocks tunnel ventilation);
- Hazards to passengers who are subsequently evacuated from, or who self-evacuate without guidance from, stationary trains following a signalling equipment failure;
- Hazards of overcrowding on station platforms when a train fails to arrive as scheduled as a result of a signalling failure.
- Hazards related to the subsequent movement/recovery of trains, following a signalling equipment failure;
- Hazards related to trains being brought to a stop and unable to be re-routed from the vicinity of a tunnel fire, or other wayside hazardous incident.

ACHIEVING A "SAFE STATE"

As this list of hazards is expanded, and depending on the specific signal system application, the assumption that a stationary train is **always** a "safe state" may need to be questioned. Indeed, for the increasing number of applications employing fully automatic (unattended) train operations, where there is no train operator available to take responsibility for train movements following a signalling system failure, addressing this question becomes an essential system design consideration.

What if we were to expand the definition of the safe state to include not only bringing a train to a stop, but "*bringing a train to a stop at a location where passengers would not be exposed to unacceptable levels of risk or harm?*" How does this definition influence how a Signal Engineer implements a "fail-safe" signalling system design?

With such a definition, historical signal system design principles may need to be carefully revisited as we migrate from electro-mechanical systems to information-based systems. For example, once a route has been proven for a train and a movement authority has been received by that train, is it always necessary to stop the train, simply because of a short-term loss

in data communication with the wayside whilst running within the limits of it issued movement authority?

With such an expanded definition of the "safe state", providing signalling equipment redundancy and/or providing for various levels of degraded modes of operation, for example, becomes not only a system availability consideration, but also a system safety consideration to be reflected in the overall safety case for the signal system. This in turn should lead to continued evolution and innovation in railway signalling technologies.

Such a definition may also impact the functionality and flexibility to be supported by the signal system under non-signalling equipment failure scenarios. For example, in the event of a tunnel fire, does the signal system (as integrated with tunnel ventilation systems for example) prevent a non-incident train from coming to a stop at a location where passengers would be exposed to harm, or allow a non-incident train to be rapidly routed away from such a location? More generally, does the signal system include functionality to reduce the likelihood of a train coming to a stop at an unscheduled location where passengers could be exposed to harm?

SUMMARY

It is acknowledged that in addition to achieving "fail-safe" signalling system designs, the operational need to be able to move trains after a signalling equipment failure is not a new consideration for Signal Engineers. What this article has attempted to stimulate, however, is consideration of new approaches to signalling system designs that encourage a wider, passenger-centric view of the railways; new approaches that exploit design alternatives outside of traditional signalling design concepts, and new approaches that are based on a broader assessment of hazard risks. This article is not promoting a radical or revolutionary change in signalling system designs, but rather encouraging continued evolutionary innovation that fully exploits the technologies available to Signal Engineers today; technologies that support ever increasing levels of automatic control of our railways.