THE SAFETY TECHNOLOGY OF RAILWAY SIGNALLING: ITS MOST DISTINCTIVE FEATURES AND ITS WIDER APPLICATION

Yuji Hirao, Nagaoka University of Technology, Japan
Masayuki Matsumoto, East Japan Railway Company, Japan

SUMMARY

This paper discusses the formulation of railway signalling safety technologies and the integration of fail-safety and quantitative analyses, extending the railway signalling safety concept into the industrial field.

In the context of the risk-based safety management approach, safety requirements for railway signalling systems are prescribed in CENELEC/IEC standards. Functional safety nowadays extends to an ever-wider variety of areas, aiming at the application of computers to safety-related systems.

Railway signalling systems based on fail-safe technologies have been built instead of making excessively quantitative safety evaluations. Today, in many fields, higher levels of safety are required, and the prudent approach of railway signalling systems including safety measures against possible failures large and small, is of greater significance.

1 INTRODUCTION

Since microelectronics was introduced to railway signalling, which requires a high level of safety, almost thirty years have passed. Safety is realised by diagnostic functions and safety-fixed outputs on the basis of fail-safe concepts, which have been developed through more than one hundred years of experience in railway operations.

In the context of the risk-based safety management approach, nowadays safety requirements for railway signalling systems are prescribed in CENELEC standards (e.g. EN 50126, 50128 and 50129) as well as IEC standards (e.g. IEC 62278, 62279 and 62425).

In the industrial fields outside railway signalling, the IEC standard of functional safety (IEC 61508) was first introduced in 2000, aiming at the application of computers to safety-related systems, and functional safety nowadays extends to an ever-wider variety of areas, for instance to machinery safety. There is, however, a tendency that the quantitative approach is more emphasized than the qualitative one.

Although the safety levels required vary, the concept of functional safety in the industrial field should be the same as in the case of railway signalling. Fail-safe designs should be regarded as well-tried safety principles and good engineering practices, and recognised as essential to the realization of a high level of safety, particularly in those cases where the safe state of the systems can be defined.

This paper discusses the formulation of railway signalling safety technologies and the integration of fail-safety and quantitative analyses, extending the railway signalling safety concept into the industrial field. This centenary of IRSE is a good opportunity to take a fresh look at the safety technology which has become such a valuable asset at the core of railway signalling.

2 SAFETY TECHNOLOGIES IN RAILWAY SIGNALLING

2.1 The Meaning of Safety Technologies in Railway Signalling and their Categorization

In discussing safety, whether or not a safe state can be defined is an important question. In the case of railways, the stoppage of trains is, in general, the safest when malfunction of relevant systems or any other difficulty happens. This is a specific feature of railway signalling as well as the rationale for fail-safety applications.

Fail-safety can be explained by figure 1. In order to enhance safety, the improvement of the reliability of relevant components is necessary, and this is explained as an ordinary design. If, however, the required level of safety and reliability of the system exceeds a certain degree, a fault-tolerant system approach is necessary. Fault-
tolerant systems, which aim at continuous/non-stop service by means of their redundancy configurations, are widely applied to aircraft or other mission-critical and safety-critical systems. While the fault-tolerant systems are costly, fail-safe systems offer a different aspect. Figure 2 shows a comparison of track relay drive circuits, one of which is by the ordinary design (a) and other by fail-safe design (b). From the viewpoint of functionality, circuit (a) is enough, but circuit (b) includes safety measures, taking into consideration component failure modes and robustness against noise.

![Figure 1: Safety and Reliability](image)

The aim of fail-safe design is to achieve the required safety enhancement at a comparatively low cost, as a trade off system reliability is very often reduced because of the complexity of a fail-safe configuration. It also indicates that reliability is a necessary condition to safety, but not a sufficient condition.

Safety technologies for railway signalling are well described in EN 50129 (IEC 62425), where safety technologies are categorised into three:

- Composite fail-safety
- Reactive fail-safety
- Inherent fail-safety

The basic idea of composite fail-safety is achieved by comparison of at least two items, and any fault is detected by this comparison and negated in a sufficiently short time. Reactive fail-safety is performed by a diagnostic function of a single item, and the fault is negated shortly, which is essentially similar to the case of composite fail-
Inherent fail-safety is realised by the characteristics of a single item of which the failure modes are non-hazardous. These are all for the case of single fault, but multiple faults can be similarly discussed when the independence of each item is guaranteed.

Early railway signalling technologies were developed from the lessons learned from accidents. Because of the difficulties of composite fail-safety and reactive fail-safety in realising comparison and diagnostic functions, as well as negation functions, in a fail-safe manner, inherent fail-safety was the main concern, utilising physical structures or characteristics. Indeed, diagnostic functions were realised by electronic circuits on the basis of specific circuit design, like the ring execution circuit for ATP systems, for example, but this is a rather limited approach.

When microcomputers were introduced in mid 1980s, diagnostic functions became the main force of the CPUs, as composite and reactive functions are realised by CPUs. However, the importance of the inherent fail-safety has not changed because the output must be fixed to a safe state in a fail-safe manner if any malfunction occurs.

### 2.2 Inherent Fail-safety

Before computer-based signalling, inherent fail-safety was the key safety technology. The CPU introduced higher levels of intelligence, characteristically useful for higher diagnostic functions. Although reactive fail-safety functions, ring circuits, for instance, had been introduced before computerized railway signalling, composite and reactive fail-safety came into their own in the case of computerised systems.

It is not necessarily simple to categorise the principles by which inherent fail-safety is realised because the wide range of safety techniques consists of a wide variety of compasses and are all related to each other. The following categorisation, however, explains cause and effect regarding inherent fail-safety.

- Continuously providing energy
- Utilising the asymmetrical nature of component failure modes
- Avoiding potential causes of danger.

#### Continuously providing energy

A typical example of this inherent fail-safety principle is track circuits (Figure 3). In the normal situation, where there is neither a train in the relevant track circuit section nor malfunction of any components, the track relay is continuously provided with electrical energy and the track circuit is clear. When any of the above-mentioned conditions is not met, the electrical energy is not provided and the track circuit is interpreted as being occupied.

Similarly, transformers are used in the relay drive circuit shown in Figure 2 (b). Even if the transistor is stuck at on, the relay is not energised because the transformer cannot pass energy by DC current.

#### Utilising the asymmetrical nature of component failure modes

Relays have been widely used in railway signalling, especially as the main fail-safe components of interlocking systems before the introduction of microcomputers. Japanese signalling relays use, instead of gravity, springs designed appropriately to provide adequate return force as shown in Figure 4. These relays’ fail-safety is realised by the asymmetrical nature of their contact failure modes, namely by non-weldable front contacts.

When the closed front contacts are allocated to the safety-related control, the stoppage of trains can be guaranteed even if malfunction or any dangerous situation occurs. It is reported that the dangerous failure rate of relays is $1.4 \times 10^{-10}$, and the ratio to the safe failure rate is $10^{-2}$ because of the reliability improvement.
Avoiding potential causes of danger

For safety of railway signalling systems, potential causes of danger must be avoided. As shown in Figure 5, in the case of relay control circuits, the possibility of line-cross of cables must be taken into account. The electrical power sources and relays have to be located on different sides, and control contacts have to be inserted into both of the two lines, to prevent the relays being falsely energized.

The above-mentioned fail-safe measures are fairly simple illustrative examples, but there are a wide variety of measures which are actually applied and contribute to railway signalling systems in service. It is very important, facing the generation change of well-experienced engineers, to develop and share a database of these safety measures.

2.3 Fail-safety for Computer-based Systems

As mentioned above, the importance of inherent fail-safety has not changed even for computer-based systems. In applying microcomputers to railway signalling, conventional safety measures based on the asymmetric nature of component failure modes are not available. Instead, however, microcomputers enable high-frequency diagnosis, and this leads to composite fail-safety and reactive fail-safety as well as inherent fail-safety described in 2.1.

The UIC A118 committee contributed greatly to the introduction of microcomputers into railway signalling from the mid-1970s to the mid-1980s. At that time, safety measures were discussed in a qualitative/deterministic way, though the risk-based/quantitative approach was gradually introduced.
Concretely, with regard to hardware safety measures, key hardware safety measures for railway signalling systems are redundant configuration, control of input and output, and error detection and consequent actions. The redundant configuration concept in Japan is the adoption of identical duplicate CPU configuration (identical software) with, mainly, tight comparison at computer-bus level by proprietary fail-safe comparators as shown in Figures 6 and 7. The identical duplicate configuration is also occasionally used with “rough” comparison (i.e. comparison of results). If high system availability is required, a TMR CPU configuration or a stand-by double dual CPU configuration is applied. Input is an important feature for safety processing, and input component error detection and input data check for timing problems are carried out in cooperation with software. Outputs must be fixed to a safe state if any error is detected or any system malfunction happens, and output circuits are designed in a fail-safe manner. A typical measure for this purpose is the provision of alternating current drive to control objects or relays.

In software, system diagnosis which targets hardware and software itself, and fault prevention are main concerns. Hardware items such as CPUs, memories, input and output circuits and other peripheral circuits (transmission coding circuits etc.) are diagnosed by software. The correctness of software implementation, for example, comparison of results gained by different algorithms, detection of infinite loop implementation and of inappropriate address access, and so on, is diagnosed by software and/or hardware. To prevent faults in software, various methods for reliable software, such as restricted interruption, proprietary simple OS and so on, are adopted.
3 NEWLY DEVELOPED RAILWAY SIGNALLING SYSTEMS AND THEIR SAFETY TECHNOLOGIES

In 2002, a new train protection system, DS-ATC (Digital ATC for Shinkansen) was introduced on the Tohoku Shinkansen, aiming at enhancement of functionality, especially at reducing headway. As shown in Figure 8, the DS-ATC ground equipment sends the information on the block section within which the train has to stop, and the onboard equipment generates continuous service braking curves on the basis of the information from the ground as well as an onboard database of track circuits and line profiles. The DS-ATC is an onboard-centered system, and MSK modulated 75-bit information is transmitted from the ground to onboard through track circuits. Digital ATC has also been introduced to the other Shinkansen lines.

Similarly to the Shinkansen, D-ATC (Digital ATC) has been introduced replacing the conventional ATC of the Tokyo metropolitan commuting area, whereby minimum headway has been reduced from 150 sec to 130 sec with a 50-sec stopping time.

![DS-ATC Diagram](image)

Figure 8: DS-ATC (Digital ATC for Shinkansen)

Aiming at the wide range of applicability and the total cost savings, a radio-based train control system, ATACS (Advanced Train Administration and Communications System) was introduced in October 2011. In ATACS, train positions are located not by track circuits but by onboard odometers and checked on the basis of the information from balises, and the train movement authorities are transmitted from radio block centers.

Fully electronic interlocking trackside functional modules, mounted in the signals or wayside interface cases and utilizing optical fibre LAN for data transmission were put into service in 2007 (Figure 9). This system, called Network Signal, is based on the IP-Network technology, and it enables the railway signalling systems to reduce the enormous number of copper cables in the station yard, which greatly contributes to reduce the system contract and replacement work as well as the costs. The optical transmission uses a Passive Optical Network (PON), which is passive in the sense that it needs no electrical power source.

The safety technologies adopted in those newly developed railway signalling systems are characterized as safety-related communication/transmission and network, and safety means the safety of the whole system. Although safety requirements for communication/transmission are prescribed in IEC 62280, key safety measures are realized by CPUs and they are considered to be the extension of the safety technologies discussed in the preceding section.
4 SITUATIONS IN INDUSTRIAL FIELDS AND THEIR SAFETY TECHNOLOGIES

For further understanding of the distinct features of railway signalling safety technologies, a comparison with other industrial fields is useful

4.1 Machinery Safety

Machinery safety is most general in the industrial fields. Although the definition of machinery is prescribed in ISO 12100 (EN 292)\(^{(1)}\), which is the top layer umbrella standard of machinery safety, it may be interpreted as machines which are widely used in factories or plants. A machinery safety system, which is a part of the machine control system, is an assembly of devices designed to protect people from hazards or injuries that could arise from the use of the machine as well as to protect machines against damage due to malfunction.

Similar to the case of railway signalling, the safe state in machinery safety can be clearly defined, i.e. stop. Basic concepts and design methodology for the safety of machinery are given in the standard. Elimination of hazards or risk reduction by protective measures is prescribed and these measures have to be performed in the process shown in Figure 10, of which the upper side measures by the designer are referred to as the three-step method. Here, inherent safety design measures are achieved by avoiding hazards or reducing risks by a suitable choice of design features for the machine and/or for the interaction between the exposed persons and the machine, and these design measures are given as safety principles. More concrete information regarding these safety principles as well as well-tried components are also provided as informative validation tools in ISO 13849-2\(^{(2)}\).

Although the target safety levels are different, the concepts of safety measures in machinery are basically similar to those of railway signalling. Actually, safety principles and well-tried components are related to fail-safe technologies of railway signalling. In addition, categories, which are defined in ISO 13849-1\(^{(3)}\) as the classification of the machinery safety systems in respect of their resistance to faults and their subsequent behaviour in the fault condition, are, in particular in the case of categories 3 or 4, also similar to the fail-safe concept in railway signalling. These categories are achieved by the structural arrangement of the parts, fault detection and/or by their reliability.
4.2 Functional Safety in Machinery Safety

Also in the field of machinery safety, computers have been introduced to enhance functionalities of machines, and the umbrella functional safety standard, IEC 61508, has influenced the safety measures for machines. While the former ISO 13849-1: 1999 stood on the categories, and structural arrangement was the key concept of the safety measures, the new ISO 13849-1:2006 has introduced PLs (performance levels) shown in Figure 11, which consist of some additional quantitative parameters as well as the categories. These quantitative parameters are MTTFd (mean time to dangerous failure), DC (diagnostic coverage) and CCF (common cause failure), and these are almost the same as those of IEC 61508. Indeed the calculation process of these parameters is simpler than in the case of IEC 61508 and the validation tools of ISO 13849-2 is referred, the main concern of relevant engineers at the present time is obtaining probability data of component failure.

Moreover, the merging process of ISO 13849 and IEC 62061 has started this year. IEC 62061(4) is another functional safety standard for machines, and it is clearly influenced by IEC 61508 because the concept of safety by structure as categories is not adopted and only quantitative parameters are available.
Although it depends on target safety levels, fail-safety should be more taken into account in cases where the safe state can be defined, as discussed in 2.1. Not quantitative parameters but structural arrangements for machinery safety correspond to fail-safety in railway signalling.

5 DISCUSSION ON FAIL-SAFETY AND THE QUANTITATIVE APPROACH

By the comparison of the safety approaches of the above-mentioned railway signalling and industrial fields, the distinctive features of railway signalling safety technologies can be discussed.

In the long history of railway signalling, its unique safety technologies have been continuously cultivated. When microelectronics/computers were applied to railway signalling during the 1980s, many detailed, in-depth studies were carried out on the basis of conventional safety technologies, which were rather qualitative/deterministic. Later a risk-based approach was introduced, but basic safety measures for computer-based signalling systems had already been established, and this approach developed to common safety methods, or CSMs.

In Japan there is a feeling that quantitative analysis should be only applied for the purpose of identifying the most critical parts and confirming the consecutive safety approach results. And absolute values should not be regarded as the target by following which the consecutive safety process is decided. Values should be utilised, at a comparatively late phase, to confirm as a result that each consecutive safety process has been appropriate.

On the other hand, especially in the case of machinery safety, computer technologies were, together with a risk-based approach, applied to safety aspects during the 2000s, and this seems to explain the present situation with regard to machinery safety. From the railway signalling point of view, well-tried safety principles and good engineering practices should be applied before quantitative analyses.

6 CONCLUSION

Railway signalling systems based on fail-safe technologies have been built instead of making excessively quantitative safety evaluations. Today, in many fields higher levels of safety are required, and the prudent approach of railway signalling systems including safety measures against possible failures large and small, is of greater significance.

(2) ISO 13849-2:2003, Safety of machinery –Safety-related parts of control systems – Part 2: Validation
(3) ISO 13849-1:2006, Safety of machinery –Safety-related parts of control systems – Part 1: General principles for design