High availability: definition, influencing factors and solutions

Martin Rosenberger / Franz Pointner

The aim of using highly available components and systems in the rail sector is to ensure that operation is as smooth as possible. In the field of signalling, the challenge lies in finding a solution that provides the highest levels of satisfaction in terms of being both cost effective and fail-safe. While previously, cost-intensive redundant designs were seen as the only option, more recent developments have created alternative approaches that seek to reconcile the conflicting priorities of cost-effectiveness and availability. In addition to these options, a range of basic conditions that form the foundation for the availability of a signalling system must always be taken into consideration.

1 Definition of availability

In EN 50126, availability is defined as follows: "The ability of a product to be in a state to perform a required function under given conditions at a given instant of time or given time interval assuming that the required external resources are provided." [1] Given the wide range of specialist departments where availability constitutes a requirement for products and systems, this general formulation is used as the basis for a more specific interpretation below.

The degree of availability of a signalling system thus quantifies the probability that this system, in the event of an error or defect occurring, will not fail, but instead can continue to be used without direct human intervention. Accordingly, high availability refers to the ability of the system to ensure unrestricted operation in spite of the failure of a component.

1.1 Quantification of availability

The degree of availability is therefore based both on the duration of the time frame in which the system functions without errors and on the shortness of the time required to rectify faults that occur. The formula set out in EN 50617-2 draws together the vital points under two variables and thereby seeks to make availability quantifiable [2]:

$$A_R = 100\% \frac{MTBF}{(MTBF + MTTR)}$$

Here, MTTR stands for "Mean Time To Repair" – i. e. for the period of time required to rectify an error that has occurred. Depending on the system configuration and gravity of the defect, this may range from a few seconds, for example the time taken to carry out a reset by pressing a button, to significantly longer periods of time, such as those required to replace components.

MTBF means "Mean Time Between Failures" – i. e. the average time period between two errors occurring. It is generally calculated on the basis of the component failure rates. Consequently, it is assumed that loss of availability is caused only by component failures.

In practice, however, further possible causes of faults must be taken into account in addition to this value. From a signalling perspective, such external error sources may be based both on the given technical infrastructure and on other, incalculable influences. These cannot be taken into consideration when calculating availability.

From this, it is apparent that numerous other factors exist that may have a significant impact on both the MTBF and the MTTR, and therefore on the availability of the system. Furthermore, reference is also made to the "required external resources" in the definition cited in the introduction, pursuant to EN 50126.

Figure 1: Busy lines require highly-available systems.

2 Factors with an influence on availability

According to the definition, the highly-available functionality of signalling systems can therefore only be guaranteed if the whole environment offers the best possible preconditions. The influencing factors can be located in three areas:

- the infrastructure and technology as a whole,
- all rolling stock in operation and
- the signalling systems themselves.

2.1 Technical frame conditions

Various measures can make a vital contribution towards optimising these areas, and accordingly towards increasing the availability of a system.

Track

A track that is not maintained to an adequate standard can lead to huge mechanical loads on the wheel sensors mounted on the track. This results in a shortened service life for the sensors.

By means of correct execution of maintenance, such as tamping work carried out in line with the regulations, the MTBF can generally be increased.

Rolling stock

Flat spots on the wheels increase the mechanical loads on the trackside signalling components. Metal components that hang down, or devices that are operated in frequency ranges that are not permitted, can also cause faults. Ongoing maintenance and observation of specifications in the development, construction and operation of rolling stock can therefore have a positive influence on the MTBF.

Preventative maintenance

A vital contribution towards optimisation in the areas of infrastructure, rolling stock and signalling can be made by comprehensive diagnostic options,, and accordingly towards increasing the availability of a system [3]. If trend analyses are evaluated and regular service diagnoses are used to schedule maintenance work, then system failures can also be cut by means of preventative measures. The MTTR is significantly reduced or is no longer relevant for the availability aspect, as appropriate work can be scheduled for times when the system is not operational.

Professional cooperation

The configuration of signalling systems requires expert knowledge, know-how and detailed insight into the operational processes and applicable regulations, so as to ensure that the relevant safety requirements can be met. Even at the planning and specification stage, the diverse configuration options and associated requirements must be discussed in depth and verified by the operator and both the interlocking and component manufacturer.

Placement of components

Under certain circumstances, components that are installed in cubicles may be exposed to extreme climatic conditions, meaning that the MTBF is significantly reduced. Climate-control facilities can remedy the situation here.

Cabling

Corroded clamping units, incorrect wire assignment with star-quad cables and the use of cables stranded as pairs or as individual wires may be the causes of faults. The use of high-quality cabling systems that are and in mint condition therefore contributes significantly to increasing availability. What is more, modern axle counters offer the option of implementing Ethernet-based communication elements [4].

Figure 2: Conditions rendered more difficult by inadequate track maintenance.

Documentation

Documentation that contains errors or is difficult to understand contributes to errors being made in installation, operation, maintenance or repair, which in turn can be the cause of faults. Clearly-documented processes and specifications can make an important contribution towards avoiding errors and to rapid fault resolution.

Commissioning via Plug & Play

Laborious installation work makes the commissioning and replacement of components more difficult. The easier the system is to handle, the faster a new or replacement component can take up its role, thereby reducing the MTTR.

Trained personnel

Last but not least, inadequate training in the area of personnel increases the risk of errors arising during the installation, operation, maintenance and repair of signalling systems. These errors may form the basis for subsequent faults. Qualitative training sessions enable the personnel to carry out their work with as few errors as possible. In addition, the causes of faults that occur can be identi-

Figure 3: Preventative maintenance using modern diagnostic tools.

fied more quickly and appropriate repair work can be driven forward quickly.

Of course, the observation of set maintenance cycles and compliance with specifications in the areas of infrastructure, rolling stock and signalling also plays a fundamental role.

For example, in the TSI (Technical Specifications for Interoperability), the European Railway Agency sets out guidelines that serve to standardise specifications of this type. The aim is to ensure that different projects are developed in line with specific guidelines, so as to guarantee problem-free interoperability at a later date.

The parameters described in ERA/ERTMS/033281, "Interfaces between Control-Command and Signalling Trackside and other Subsystems", therefore constitute vital building blocks when it comes to technical harmonisation of the areas mentioned above and thereby to creating an infrastructure in which signalling systems can function at a highly available level [5].

Figure 4: Lightning strikes can cause faults.

Figure 5: Floods leave long-term damage.

2.2 External factors that cannot be influenced

The common point among all of the factors mentioned up to now is that they can be influenced. Product development in line with specifications, regular maintenance, precise documentation or high-quality training are at the discretion of the manufacturer, system integrator and operator.

Away from these influences and the statistical component failure rates that have already been mentioned, however, environmental factors also arise and may be responsible for the occurrence of faults. For example, here ÖVE EN 60721-3-3/A2 mentions environmental influences such as air temperature, air humidity, the speed of temperature changes, solar radiation, condensation, wind-blown precipitation and many more [6]. Depending on the product specification and requirements, signalling and infrastructure components that can withstand the extent of these influences in an appropriate manner must be developed and manufactured.

In practice, it has become clear that, in addition to these influences that must be taken into consideration in the product specification, less predictable causes of faults also occur frequently. These include, for example, electromagnetic pulses caused by lightning strike or double traction, but also the impacts of flooding or vandalism.

3 Redundancy

In general, the desired increase in availability is achieved through the implementation of redundancy strategies. The number of options available in this regard varies depending on the requirements, and these options in turn are bound up with a range of cost structures.

As a matter of principle, a distinction can be made between partial duplication of specific components and the fully redundant design of the complete system. The latter, in particular, is of course linked to significant additional costs.

3.1 Complete redundancy

Under certain circumstances, redundancy may be vital, especially in the safety-relevant area of signalling. This applies for example to particularly sensitive track sections, such as tunnel systems or bridge sections that are difficult to access, where even the individual failure of one component can lead to significant operational delays.

The highest level of system availability that is called for here can ultimately only

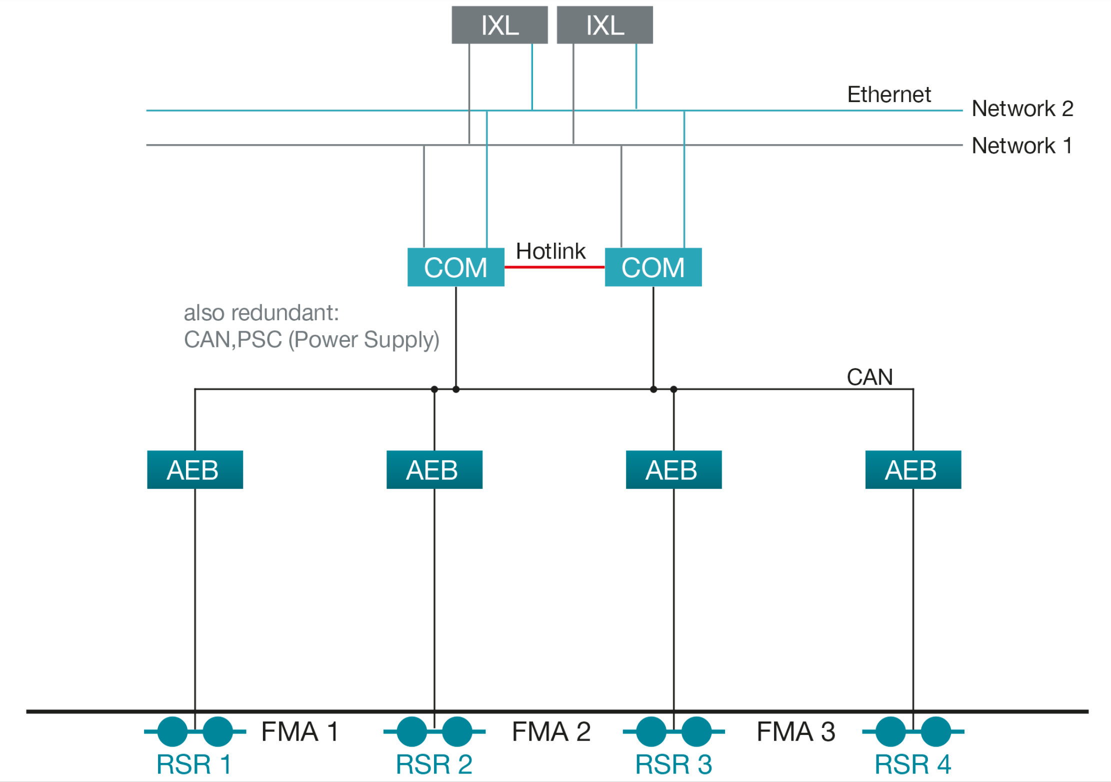

Figure 6: Redundancy at critical points in the indoor equipment

be realised through a complete duplication of all components. However, even in these areas, the implementation of functions to increase the fault tolerance of the system can result in a further optimisation of availability.

3.2 Partial redundancy

The aim of partial duplication is to achieve increased availability at comparatively low additional costs and hardly any additional effort. Two approaches are taken to achieve this:

- duplication at critical points (“single points of failure”),
- duplication of components at particular risk (e. g. outdoor equipment).

Duplication at critical points

In principle, all signalling systems contain components where failure would have serious effects on operations. For example, this concerns modules to provide the power supply or the communication of axle counter and interlocking. In order to avoid failures of the complete system in the event of a fault in one of these components, a redundant design is usually chosen at such “single points of failure”.

Duplication of components at particular risk

As explained in section 2.2, the use of axle counters and wheel detection systems in the signalling field has demonstrated for decades that most faults with an impact on system availability have their origins in the outdoor equipment.

If the concept of partial redundancy is pursued, it follows that the outdoor equipment components that are at particular risk of being affected by these factors must be duplicated to increase availability. However, given the wide range of different types of interference, a permanent increase in availability is not guaranteed even then. In addition, especially a redundant design of the outdoor equipment is frequently associated with considerable additional costs.

In such areas, in particular, considerations of various options to increase availability with the greatest possible cost-effectiveness can prove profitable, as in this respect alternative approaches to increase fault tolerance also offer opportunities to achieve the desired effect.

4 Intelligent fault tolerance

Intelligent, fault-tolerant functions can ensure smooth operation even in the event of a fault. Under certain circumstances, the duplication of individual components – or of the complete system – is not even necessary to achieve higher availability.

By raising the inherent system fault tolerance , the system is able to activate intelligent functions and thereby maintain operations in the event of a fault – particularly if caused by external influences. In many cases, this allows to achieve the required increase in availability.

By complying with the prescribed design specification and consistently taking the safety guidelines into account, a negative impact on the safety level by the use of fault-tolerant functions can be ruled out.

In the following section, two innovative functions that Frauscher can provide with the new generation of the Frauscher Advanced Counter, the FAdC R2, are used as practical examples [7]. With the aid of these functions, the availability of the complete system can be further increased in a cost-effective manner, even in extreme situations. Two different approaches are taken to achieve this.

4.1 Suppression of faults

The Counting Head Control principle (CHC) is used to fundamentally avoid error messages caused by inevitable influences. If the adjacent track sections are clear, the counting head is switched to a stand-by mode. In this idle state, a freely configurable number of undesirable instances of damping can be suppressed. This means that no fault or occupied indication is generated by a short-term influence; no reset is required. Approaching vehicles deactivate the stand-by mode, meaning that they are detected and the

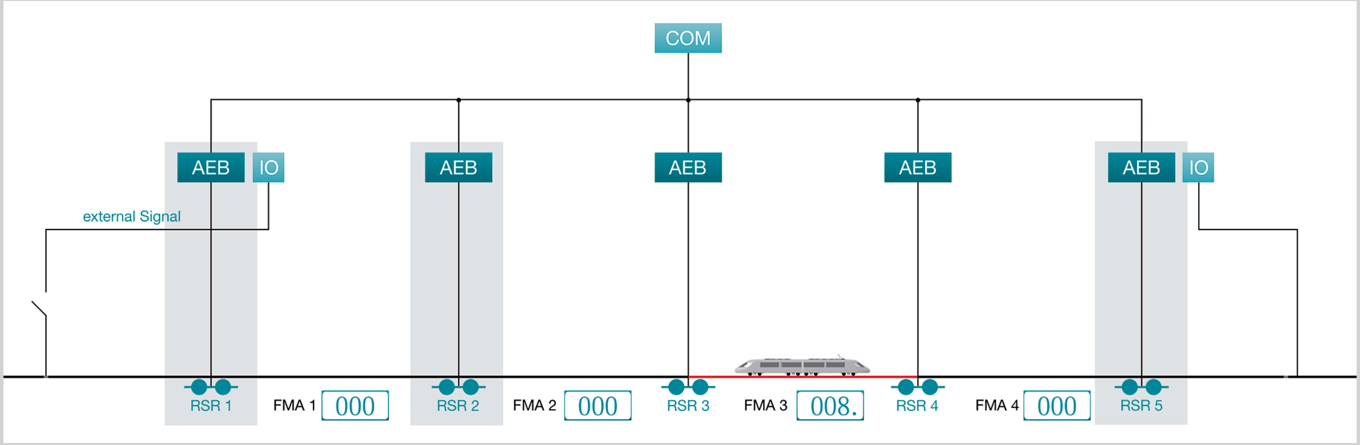

Figure 7: CHC: Active counting heads at traversed sections.

occupied status output is issued in a fail-safe manner. When used correctly, the patented functionality satisfies the safety requirements according to SIL4. Possible triggers for such interference include:

- damping by tools,
- people on the track,
- trolleys
- and other similar triggers.

4.2 Automated fault correction process

The Intelligent Supervisor Track Section process (STS) corrects inevitable external interference in a fully automated manner. By observing the general reset conditions, it is thus possible to further optimise availability without any negative effect on safety.

Every two track sections are overlaid by a supervisor section. Consequently, it is possible for a faulty track section to be reset automatically, without manual intervention, if the corresponding supervisor section is clear. Similarly, a faulty supervisor section is reset if the two corresponding track sections are clear.

As a matter of principle, a distinction is made between two variants when it comes to the depth of integration into the complete system:

Without integration in the interlocking

By means of automatic correction of short-term errors caused by external influences, the duration of the faults – and therefore the MTTR – is reduced, as is the number of reset procedures that have to be carried out by the traffic controller. It will not need the supervisor sections to be integrated into the interlocking. Examples of typical, short-term interference:

- lightning strikes,

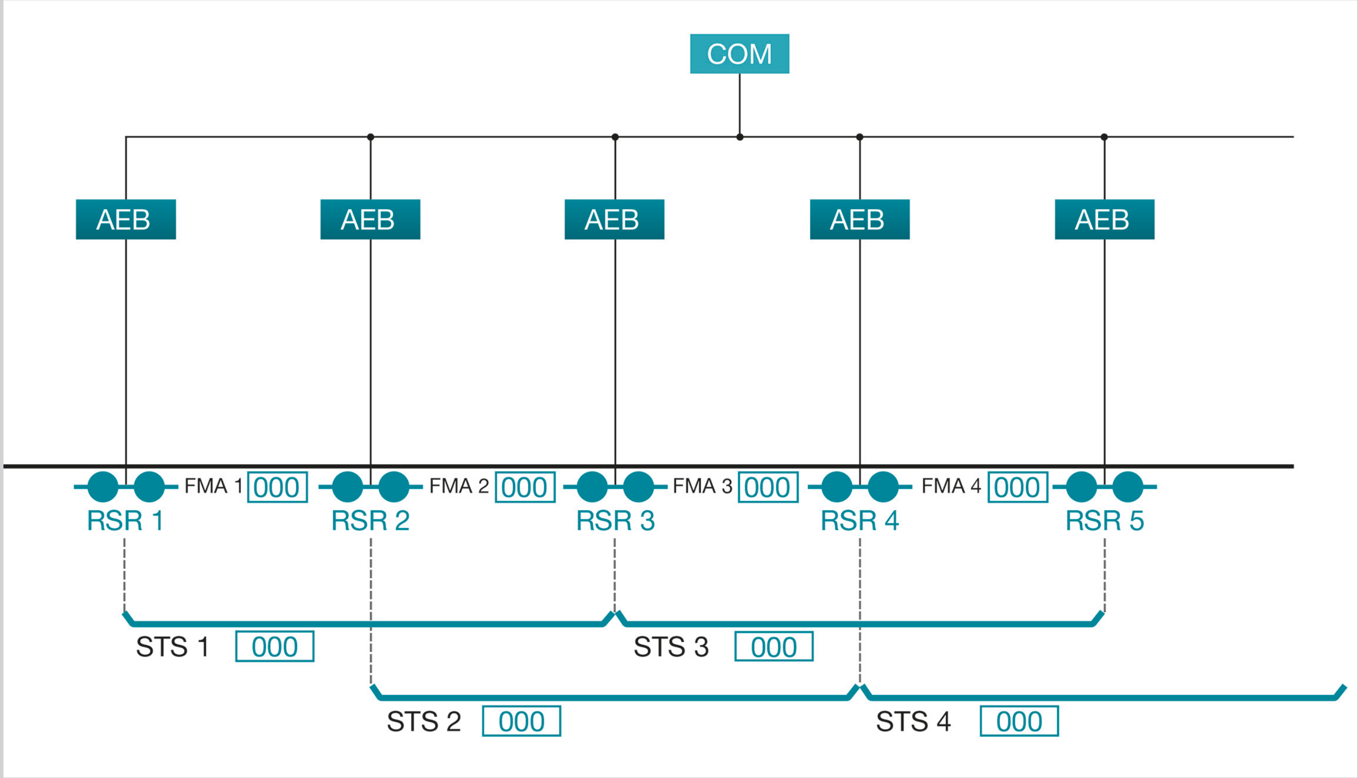

Figure 8: STS: Supervisor sections overlay the existing track sections

- installation of sensors close to the neutral section between two substations,
- impact on the cabling system.

With integration in the interlocking

Particularly on busy or high-speed lines, and in the afore mentioned track areas that are difficult to access, alongside interference caused by factors outside the system, even the failure of individual components can lead to ongoing faults with huge impacts on the timetable.

By integrating the supervisor sections in modern, high-performance interlockings, even permanent errors can be tolerated until such time as the cause can be rectified without any effect on operation. Instead of the two faulty track sections, the associated supervisor section is automatically processed for train detection within the interlocking. Rectification of the cause of the error or replacement of a component can therefore be carried out during maintenance windows, with no time pressure. Examples of typical, longer-term interference:

- component errors and
- cable faults.

5 Outlook and summary

The degree of availability of signalling systems results from the optimal interplay of infrastructure, rolling stock and signalling technology. Intelligent functions incorporated in modern axle counting systems can contribute to the increase of availability and therefore constitute an important step in overcoming the challenges that signalling systems face due to the conflicting priorities of cost-effectiveness and high availability.

LITERATURE

[1] EN 50126, 1999: Bahnanwendungen. Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) [Railway applications, specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)]

[2] prEN 50617-2, 2013: Railways applications – Basic parameters of train detection systems – Part 2: Axle counters

[3] Grundnig, G.; Raschhofer, S.: Increased availability thanks to the FDS Diagnostic System. SIGNAL + DRAHT, 2/2010

[4] Lugschitz, S.; Pucher, C.: New applications through axle counter communications over open networks. SIGNAL + DRAHT, 10/2014

[5] ERA/ERTMS/033281, 2014: Interfaces between Control-Command and Signalling Trackside and other Subsystems

[6] ÖVE EN 60721-3-3/A2, 1997: Klassifizierung von Umweltbedingungen Teil 3: Klassen von Umwelteinflußgrößen und deren Grenzwerte – Hauptabschnitt 3: Ortsfester Einsatz, wettergeschützt (IEC 721-3-3/A2: 1996) [Classification of environmental conditions, Part 3: Classification of groups of environmental parameters and their severities – Section 3: Stationary use, weatherprotected (IEC 721-3- 3/A2: 1996)]

[7] Pucher, C.; Rosenberger, M.: The axle counting system FAdC provides benefits for interlocking integrators and operators. SIGNAL + DRAHT, 4/2012

The authors

Martin Rosenberger M.Sc.
Product Management Director
Frauscher Sensortechnik GmbH
Address: Gewerbestraße 1,
A-4774 St. Marienkirchen
E-Mail:
martin.rosenberger@frauscher.com

Franz Pointner
RAMS Management Director
Frauscher Sensortechnik GmbH
Address: Gewerbestraße 1,
A-4774 St. Marienkirchen
E-Mail: franz.pointner@frauscher.com

ZUSAMMENFASSUNG

Hochverfügbarkeit: Definition, Einflussfaktoren und Lösungen

Ziel des Einsatzes hochverfügbarer Komponenten und Systeme im Eisenbahnbereich ist die Sicherstellung eines möglichst reibungslosen Betriebes. Die Herausforderung im Signaltechnikbereich liegt dabei vor allem darin, sowohl eine finanziell als auch sicherheitstechnisch maximal zufriedenstellende Lösung zu finden. Galten bisher häufig kostenintensive redundante Ausführungen als unumgänglich, haben neuere Entwicklungen alternative Ansätze im Spannungsfeld zwischen Wirtschaftlichkeit und Verfügbarkeit hervorgebracht. Neben diesen Optionen gilt es stets auch eine Reihe von Rahmenbedingungen zu beachten, welche die Grundlage für die Verfügbarkeit eines Signaltechniksystems bilden. Der Grad der Verfügbarkeit signaltechnischer Anlagen resultiert aus dem optimalen Zusammenspiel von Infrastruktur, Schienenfahrzeugen und Signaltechnik. Intelligente Funktionen moderner Achszählsysteme können zur Steigerung der Verfügbarkeit beitragen und damit einen wichtigen Schritt in der Bewältigung der Herausforderungen für signaltechnische Systeme im Spannungsfeld von Wirtschaftlichkeit und Hochverfügbarkeit darstellen.

Buchen Sie schon heute Ihre Anzeige für die **nächste Ausgabe!**

Die Termine für Signal + Draht Nr. 7+8/15:
Anzeigenschluss: **17.7.15**
Druckunterlagen: **24.7.15**
Erscheinungstermin: **13.8.15**

Ihr kurzer Draht zum Anzeigenteam:
Silke Härtel | 040-237 14 227 | silke.haertel@dvvmedia.com
Silvia Sander | 040-237 14 171 | silvia.sander@dvvmedia.com

DVV Media Group
www.eurailpress.de/sd
Eurailpress