



Future-proof Safety Technology  
for Rail Transport

# Guideline

 Dipl.-Ing. Sedat Sezgün, Head of Rail Segment, HIMA  
 Thomas Bell, Technology Development Manager Rail, HIMA

Why deployment of commercial off-the-shelf (COTS) controllers for train control and management systems, interlockings and signaling systems is worthwhile. →

## Summary

---

Proprietary safety technology currently prevails in the railway industry. However, the situation is changing, with more and more system integrators, rolling stock manufacturers and railway operators worldwide opting for standardized, commercial off-the-shelf (COTS) systems. This guideline explains why COTS systems are a more cost-effective and sustainable solution for the safety of interlockings, level crossings, signaling systems and rolling stock, considering both the socio-economic context and current standards and technical requirements. This guideline also describes various aspects which users should consider when selecting optimal COTS systems for their own applications.



**Sedat Sezgün**

Having graduated from Darmstadt University of Applied Sciences in 2006 with a degree in Electrical Engineering, Sedat Sezgün subsequently joined HIMA with responsibility for rail customers. He was appointed Head of Rail Segment in 2015.

E-mail: [s.sezguen@hima.com](mailto:s.sezguen@hima.com)

**Thomas Bell**

Technology Development Manager Rail

E-mail: [t.bell@hima.com](mailto:t.bell@hima.com)

# Contents

- 1. The Socio-economic Context ..... 4**
  - 1.1 The global market for safety technology in the railway industry ..... 4
  - 1.2 User groups and their needs ..... 5
  - 1.3 Legislation, standards and regulatory authorities ..... 5
  - 1.4 Technical conditions and constraints ..... 6
- 2. COTS versus Proprietary Safety Technology ..... 8**
  - 2.1 Proprietary versus standardized ..... 9
  - 2.2 Closed versus open ..... 9
  - 2.3 Maintenance ..... 9
  - 2.4 Future viability ..... 9
  - 2.5 Cost effectiveness ..... 10
- 3. COTS Systems Are Not All the Same ..... 11**
  - 3.1 Certification ..... 11
  - 3.2 Scalability ..... 11
  - 3.3 Innovative maintenance concepts ..... 11
  - 3.4 Flexibility ..... 11
  - 3.5 Training needs ..... 12
  - 3.6 Interoperability ..... 13
  - 3.7 Cybersecurity ..... 14
- 4. Conclusion ..... 15**

# 1. The Socio-economic Context

## 1.1 The global market for safety technology in the railway industry

Around the world, urbanization and growing environmental awareness are leading to greater demand for reliable and environmentally friendly means of transport. This is especially true in large urban centers where more and more passengers must be conveyed safely, quickly and conveniently. Expansion of network capacity is essential to accommodate rising passenger volumes. The key to the necessary boost in productivity and efficiency lies in the consistent deployment of modern technologies. However, financial resources for the necessary modernization measures are lacking in many cases and maintenance is not infrequently ignored, often leading to systems operating past the end of their useful life. This massive modernization backlog, in combination with rising cost pressure due to declining budgets, has increased the need for flexible, cost-effective control solutions in the railway industry worldwide.

The Study "Worldwide Rail Market Study – Status Quo and Outlook 2016" by Roland Berger shows that the volume of the global rail market is estimated at approximately EUR 101 billion, with the share of computer-controlled applications at EUR 11.3 billion in 2015. About one third of the latter is attributed to safety-related electronic systems, translating to roughly EUR 3.7 billion.

The share of safety controllers in safety-related electronic systems in the railway industry was about EUR 253 million in 2015, with the market at that time clearly dominated by proprietary technology. However, a worldwide trend toward commercial off-the-shelf (COTS) technologies is clearly visible, so a continuous

redistribution of this statistic can be expected in the coming years. That is also indicated by the results of a company survey conducted as part of the study "Megatrends in the German Rail Market" by the consultancy ASTRAN in August 2016. In that survey, 14 of the 30 surveyed companies said that they intended to deploy standardized industrial components in the form of commercial off-the-shelf (COTS) technologies in the future.

The question of which is preferable – proprietary safety technologies or standardized, commercial off-the-shelf (COTS) solutions – is currently a hot topic in the market. Among the eight global megatrends listed in the above-mentioned ASTRAN study, the surveyed companies rated the trend "custom solutions versus standardized industrial components" as the most urgent and second only to digitization as the most important trend in the industry.

COTS designates series-production controllers which are sold in large numbers as standard components and deployed in a variety of industry sectors. Thanks to the use of standard components, they are significantly less costly than proprietary systems, while at the same time fulfilling all important safety standards of the railway industry. The global market share of COTS controllers in safety-related electronic systems is expected to be about 25 percent by 2020.

A key challenge in the railway industry is the extreme diversity of the global market for safety technology. As a result of historical evolution, many structures consist of an eclectic collection of heterogeneous technologies from many different decades. In addition, each country has its own rail infrastructure and





standards. At international level, there are many different systems for operating regulations, train control, signaling, electrical supply and other aspects. Another crucial factor in any development towards an increase in use of COTS systems/solutions is the incalculable influence of politics, which should not be underestimated due to the role of regulatory authorities and state ownership of many railway companies.

In light of all this, it is clear that from a global perspective the level of requirements for safety-related electronic systems and use of such systems varies greatly from one country or region to the next. A common factor in all markets, independent of the different situations, is that safety technology is expected to provide a suitable level of safety, namely freedom from systematic and random faults. This requirement exists in similar form in many other industries and is already fulfilled by COTS systems. In addition, a great many functions must comply with safety integrity level 4 (SIL 4), the highest defined safety level.

## 1.2 User groups and their needs

The first thing is to distinguish the various user groups. As end users, railway operators are often state-owned companies. Their strategies and ideas are often strongly influenced by political bodies, such as municipal or regional governments. These political dependencies can make technical approval processes very slow and complicated. Railway operators therefore tend to be hesitant in introducing new technology, such as commercial off-the-shelf (COTS). Once they have made the decision, they often opt for supply and service contracts extending over many years. In order to achieve direct deployment by railway operators, safety technology must therefore meet very stringent demands and demonstrate all necessary national and international certifications. Along with safety and certification, railway operators are primarily interested in ease of use, low failure rates and fast spare parts delivery for safety-related electronic systems.

The second user group for safety technology consists of manufacturers of rolling stock. The core competence of these companies is the end-to-end development, production and commissioning of rolling stock. However, in the area of safety-related electronic systems (controllers, sensors and actuators) the level of expertise in other industries – mechanical and plant engineering, chemical, power plants (including nuclear) and automotive – has evolved further. These industries use COTS systems because it is the most cost-effective solution. That comes from the much higher production volume compared to the railway industry or manufacturers of rolling stock, and from the fact that COTS solutions are regarded as the most progressive in those industries. Here the railway industry can undoubtedly learn from other industries. For manufacturers of rolling stock it is especially important that the deployed safety-related electronic systems meet the expectations and requirements of the end customers, meaning the railway operators. Extremely high safety, reliability and long-term availability are just a few

of the key criteria for safety-related electronic systems used in rolling stock. Certification for acceptance by national regulatory authorities is also essential.

The third large user group is system integrators. They use safety-related electronic systems in the development of their own products, for example interlockings and level crossings, which are often deployed worldwide. In such cases, the end customers are not primarily interested in the type of safety-related electronic system in the product, even though this often forms the core of the product. Instead, they see the product as a package solution. If a system integrator wants to develop a completely new interlocking or level crossing product, they must first put significant effort into development and certification. Accordingly, the safety technology they use should preferably already have suitable certification and offer maximum programming flexibility. Furthermore, system integrators expect safety technology to have long-term availability and future viability, so that the products they develop do not become obsolete after just a few years.

## 1.3 Legislation, standards and regulatory authorities

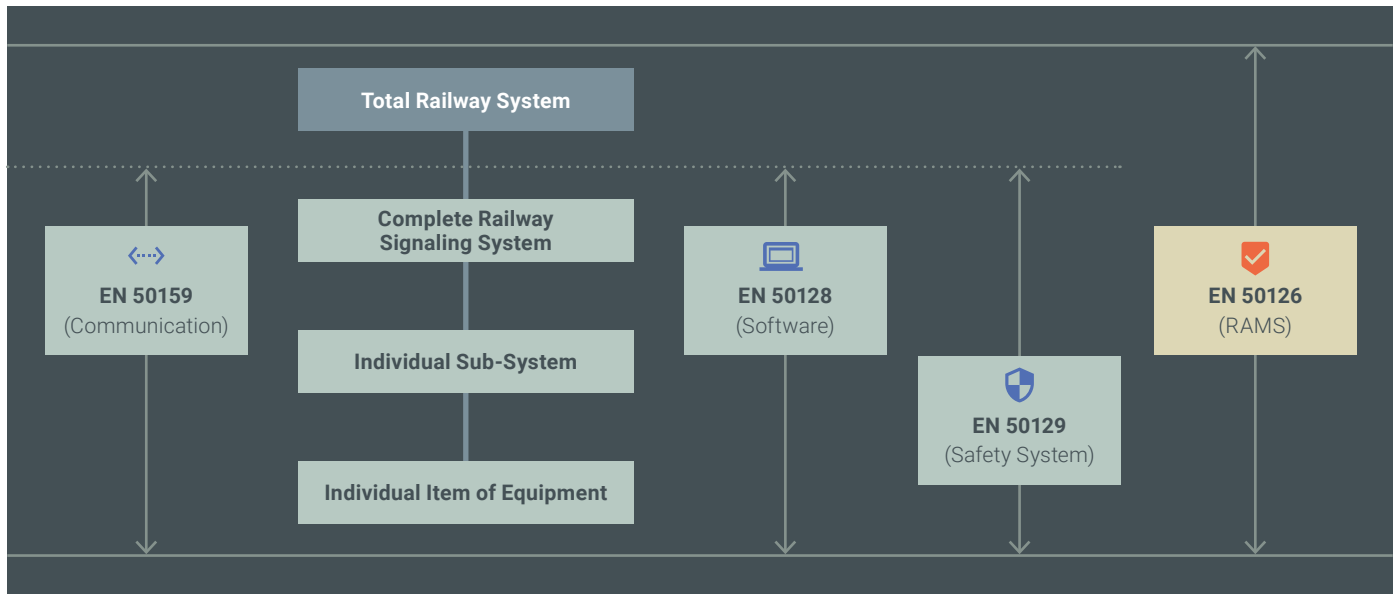
For historical reasons and due to the high importance of safety, the railway industry is greatly influenced by standards and regulatory authorities. General safety standards in Europe, which are governed by the European Committee for Electrotechnical Standardization (CENELEC), are also accepted worldwide. This means that a safety system which is certified compliant with the CENELEC standards can be deployed worldwide in railway applications. In addition to these international standards there are numerous national regulations, which can differ significantly from one country to the next.

The most important CENELEC standards concerning safety-related electronic systems are:

- EN 50126: Specifies basic requirements by defining the terms reliability, availability, maintainability and safety (RAMS)
- EN 50129: Specifies safety-related electronic systems for signaling applications
- EN 50128: Specifies requirements for the software of controllers and protection equipment
- EN 50125-3: Specifies environmental conditions for equipment in railway applications; Part 3 specifically addresses environmental conditions for signaling and telecommunication equipment
- EN 50155: Specifies environmental conditions for electronic equipment used in rolling stock

In addition to these standards, there are numerous statutory regulations at national and regional levels (EU, Asia, Australia, North America, South America, etc.). Nearly all regions have a basic legal requirement that systems and equipment must comply with accepted codes of practice. These statutory requirements are codified and specified by the IEC and ISO

**Figure 1: Scope of CENELEC standards**



in the form of international standards, as well as regulations implemented at EU and national levels, such as Technical Specifications for Interoperability (TSI), CENELEC standards, and EN standards. For example, the European Common Safety Methods (CSM) regulation specifies a failure rate of  $10^{-9}$  for safety controllers.

Finally, there are the national regulatory authorities (also called National Safety Authorities, or NSA), which ensure compliance with all required standards. The approval process for safety-related electronic systems in the railway industry is very complex and can sometimes take several years. Rolling stock in Europe is subject to constant monitoring by the NSAs (EBA, BAV, etc.). Initial approval as well as operation and later modifications to locomotives, multiple-unit trains and so on are subject to strict approval procedures. Among other things, the prerequisites for successful approval of a rail vehicle include a wide variety of formal hardware and software assessments, verification of functional integration, corresponding certificates, and certified components. Documentation according to the latest standards entails considerable effort and expense due to frequent changes to national and international standards. Particularly for rolling stock manufacturers, it is therefore not easy to keep all documents constantly up to date for every deployed component. The presently very extensive and time-consuming procurement and maintenance processes for these verification documents can be significantly reduced with pre-approved and pre-certified COTS components.

## 1.4 Technical conditions and constraints

Modern safety-related electronic systems must comply with a long list of technical requirements. In the course of digitization, which is also making inroads in the railway industry, new

applications are constantly arising and must be supported. Some examples are driverless trains (Automatic Train Operation, or ATO), platform check-in procedures using cameras, door controllers, powertrain monitoring, and pan-European train control management functions. All of these functions can be implemented most economically with an end-to-end COTS train control management system because it supports a variety of I/O modules, various bus systems and high-performance processors.

Another aspect related to the digitization of railway technology is IT security (cybersecurity), because ever more vital control processes are being implemented as cloud-based or Internet-based solutions. Even in the digital age, safety controllers form the basis for critical applications such as level crossings, rolling stock and interlockings. The interplay of safety and security is becoming increasingly important.

A train control management system (TCMS) which controls a complete train with multiple traction, in other words with up to four locomotives forming a traction unit, requires not only SIL 4 compliant implementation for protection against internal systematic and random faults, but also high vehicle availability. Operators strongly dislike and/or are unwilling to accept electronic equipment failures in vehicles costing several million dollars. Extremely high availability is therefore an essential requirement for modern train control management systems. Safety controllers in the railway industry are subject to the same requirements for the probability of failure per hour (PFH) according to the SIL level as those in the process industry, for example (see Figure 2).

To achieve the highest possible availability, and thereby punctuality for railway customers, continuous maintenance of rolling stock is necessary. The rolling stock must be taken to depots

Figure 2: Safety integrity levels according to CENELEC

Tolerable Hazard Rate THR per hour and per function	Safety Integrity Level (SIL)
$10^{-9} \leq \text{THR} < 10^{-8}$	4
$10^{-8} \leq \text{THR} < 10^{-7}$	3
$10^{-7} \leq \text{THR} < 10^{-6}$	2
$10^{-6} \leq \text{THR} < 10^{-5}$	1

for maintenance work. For some maintenance and repair tasks, the control system must be completely shut down in the depot to eliminate the risk of unintentional operation. However, with control systems which are compliant with SIL 3 or SIL 4, have modular and scalable software algorithms and work independently from each other without mutual interference, it is also possible to perform many maintenance tasks without shutting down the control system. This allows many tasks to be performed in parallel, including maintenance of control system hardware and software, which has the overall effect of reducing downtimes. A prerequisite for this is that both the equipment systems and the software tools allow this.

The typical product life cycle in the railway industry imposes very special requirements on safety-related electronic systems. Locomotives and multi-unit trains naturally have very long product lifetimes. These costly assets must remain in service for 30 years or more. A vehicle model or a product family can even have a lifetime of 40 to 50 years. It is therefore inevitable that railway operators have many wishes during the vehicle lifetime which must be implemented by the rolling stock manufacturers. The platform concept also plays a major role with the manufacturers. As a result, up to 20 variants can arise from the originally developed vehicle over the course of time. Therefore, long-term availability and easy, flexible adaptation are important for safety-related electronic systems.



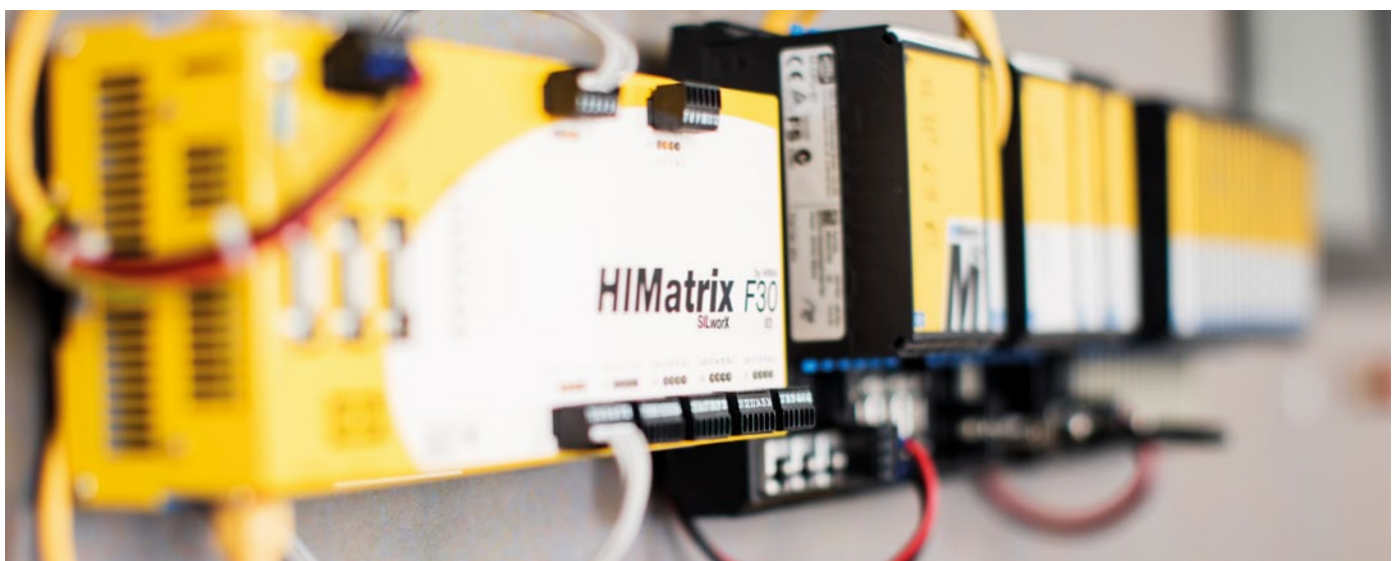


## 2. COTS versus Proprietary Safety Technology

Up to now the railway market has been dominated by proprietary safety solutions. However, the trend is moving toward COTS. There are already applications where the use of COTS is explicitly required – something that was unthinkable a few years ago.

Ten to fifteen years ago there was still considerable resistance to COTS. But around the turn of the present century, rising cost pressure led some railway companies to start considering whether proven COTS safety technology could also be used for rail

transport. To allow safety controllers which already had a proven track record in other vital industries, such as the process industry, to also be deployed in rail transport, COTS manufacturers had to have them tested and certified according to the CENELEC standards. Since the safety requirements of other industries (for example, the process industry) overlap with those of the railway industry, exactly the same hardware and the same operating system could be used for rail transport. It was only necessary to adapt the calculations and documentation, and to migrate the control concept to the CENELEC principles.



Examples of COTS safety controllers which have already proven themselves in numerous vital applications in the process industry and are now being deployed in rail transport: HIMax (top) and HIMatrix (bottom).



The reason for the growing proliferation of COTS solutions can be clearly seen by considering the key criteria which, according to the consensus of expert opinions in the railway industry, should be fulfilled by modern safety solutions and assessing how COTS systems perform in meeting these criteria compared to proprietary systems.

## 2.1 Proprietary versus standardized

Proprietary safety systems are developed solely for a specific function and are produced in small quantities. That makes them more expensive than COTS controllers, and it limits their application flexibility. After original equipment installation, users such as railway operators are forced to procure follow-on systems from the same manufacturer, which is often the control system supplier.

By contrast, COTS systems are standardized systems which are produced in large numbers and have a prior track record in numerous vital applications outside the railway industry. Using standard components gives railway operators flexibility in their choice of suppliers and allows them to select the “best of breed” solution for each application, including safety technology.

## 2.2 Closed versus open

A decisive prerequisite for the digital railway era is networking a wide variety of systems for data exchange. Here as well, COTS safety controllers have an advantage over proprietary solutions because the interfaces of conventional systems are not standardized. That can make it difficult to integrate those solutions into existing heterogeneous automation architectures. Due to proprietary programming, in many cases only the controller manufacturer is able to carry out upgrades, updates and maintenance.

By contrast, COTS controllers have operating systems which are based on globally available standard programming languages compliant with IEC 61131. They also support interfaces for all major communication protocols, including Ethernet, TCP/UDP, RS485, RS422, RS232 and CAN. Standard industrial protocols are used for communication.

## 2.3 Maintenance

Many people come in contact with a safety controller during its long lifetime. They include hardware and software developers, operators and users – train drivers, maintenance staff, assessors, inspectors from approval agencies, and commissioning technicians. Consequently, the system should be as simple and intuitive as possible. The objective is to make it as easy as

possible for all people who deal with vital matters every day to safely and reliably operate and manage very complex machines such as railway vehicles.

Equipment systems, safety architectures and the tools used to develop and maintain these systems should be as simple as possible. In particular, the increasingly important aspect of software engineering should be mastered globally in a uniform manner by as many people as possible. That simplifies handling, maintenance and system extensions.

Furthermore, these very long-used vehicles must be understood by several generations of technicians, engineers and regulatory authorities, in many regions and markets throughout the world. Reducing the complexity of safety systems also reduces the cost of training service employees.

Presently many railway applications are an eclectic collection of proprietary technology, often consisting of several generations of equipment. This lack of standardization and modularity makes maintenance and system extensions very complicated and costly.

Standardization and the widespread use of industry-standard programming languages compliant with IEC 61131 make COTS controllers easier to use and maintain, making operating and life cycle costs significantly lower in comparison to proprietary technology while delivering the same level of safety.

## 2.4 Future viability

Due to the required long-term availability of safety controllers in rail transport, in part made necessary by the long useful life of rolling stock, future viability is a very important evaluation criterion. Accelerating digitization and ever shorter innovation cycles increase the significance of this aspect.

A particular challenge here is to keep the software constantly up to date over a period of 20 to 30 years. However, the hardware must also allow flexible extension and modernization, as much as possible without leading to downtime.

With proprietary technology, the cost of keeping the solutions constantly up to date is relatively high due to the small production volumes. For users there is also a risk that the product may no longer be available for the next application. The standardization and widespread use of COTS systems give users more planning security. That also applies to the availability of spare parts and software updates. With their modular structures and standard communication interfaces, COTS systems are easy to adapt to changing needs that arise many years later.

## 2.5 Cost effectiveness

The share of electronic systems in the railway industry is constantly rising, particularly in distributed applications – for example, based on the European Train Control System (ETCS). This leads to a massive modernization wave. To deal with the conflicting demands of cost pressure and the need for modernization, railway companies are looking for the most cost-effective control solutions.

That is precisely the weak point of the previously predominant proprietary safety technology. The combination of high development costs and low production volumes leads to high costs for the railway companies, and the cost of obsolescence is passed on to the users. In addition, non-standardized proprietary technology makes maintenance more difficult and more costly for both rolling stock and infrastructure. Due to dependency or commitment to a single supplier for extensions, maintenance and servicing, the only stage where competition actually features is at the point of initial equipment procurement.

Many manufacturers of proprietary systems are rooted in the control system world, so conventional safety controllers are often overloaded with a wealth of functions. For example, current electronic interlockings perform many functions that are not relevant to safety, but still cost money. The costs arise

from the fact that these functions are developed and tested in conjunction with the safety functions and must be assessed and certified for freedom of interference with the safety functions. For example, route control functions are also integrated into many interlockings. If you want to include a new route in the process, you have to alter the entire interlocking and in the worst case also have it reapproved, at a correspondingly high cost.

The standard components and high production volumes of COTS controllers naturally result in significantly lower procurement costs. But that is not their only economic advantage. Easier commissioning and maintenance, greater freedom of choice for end customers in selecting suppliers, simpler and more future-proof programming, short delivery times and high availability of spare parts are additional reasons for the significantly lower operating and life cycle costs of COTS systems in comparison to conventional safety technology. As a result, the return on investment (ROI) is distinctly faster.

## 3. COTS Systems Are Not All the Same

---

Now that the advantages of COTS in comparison to proprietary safety technology have been described in detail, it is time to look at the aspects which should be considered when selecting a COTS solution. Although COTS systems are standardized, they differ in terms of details.

### 3.1 Certification

Proprietary technology can unnecessarily complicate the already costly certification and approval processes for rolling stock. For system integrators and manufacturers of rolling stock, it is advisable to employ only COTS systems whose hardware and software are demonstrably compliant with the CENELEC SIL 4 standard. These entire equipment systems are already accepted by the responsible authorities and thereby approved for deployment on all rolling stock as well as all level crossings and interlockings worldwide. A solution of this type significantly reduces the labor expenditure for the user, as certification and approval processes can otherwise take months or even years in some cases. Furthermore, users do not incur any additional costs for subsystems. Last but not least, the risk of project delays – for example due to insufficient compliance with safety requirements or gaps – is minimized. The pre-certified systems allow system integrators to concentrate on the actual application.

### 3.2 Scalability

Rolling stock and railway infrastructure applications usually have a lifetime of several decades. Product families for rolling stock are regularly updated with new versions and/or vehicle generations. For rolling stock manufacturers as well as railway operators and system integrators, flexibility and modularity are therefore decisive criteria for the selection of safety systems. Modifications, changes and extensions can be implemented at much lower cost with COTS systems than with proprietary technology. That is primarily due to the freedom from mutual interference, meaning that when changes and extensions or the addition of new functions, only these individual systems need to be assessed rather than having to retest the entire system.

In this regard it is essential to choose a COTS system in which the hardware and software are optimally harmonized. The software should be based on open programming and industry-standard programming languages. Handling and programming of the controller should be as simple as possible, and should also

be possible during the course of a project without involving the manufacturer. Other key aspects in this connection are backward compatibility of the software and long-term availability of the hardware components. If the selected COTS system has state-of-the-art software tools, it is only ever necessary to test the parts which were actually changed, because freedom from mutual interference is assured by the certified operating system and software programming.

Furthermore, the system architecture should be modular so that the controllers can easily be extended with additional I/O. Ideally, equipment exchange and extensions should even be possible during live operation. This flexibility allows the cost and effort for the development and approval of changes to existing functions to be significantly reduced. In this way, system integrators and rolling stock manufacturers can respond even faster to changing customer wishes on the part of railway operators.

### 3.3 Innovative maintenance concepts

Availability and reduced operating costs are decisive factors for railway operators in order to withstand growing cost pressure and boost profitability. Maintenance plays an important role in this. There are already COTS systems available, such as HIMax, which allow users to develop new concepts for the maintenance and servicing of train control management systems and other subcomponents. They are based on processor modules with up to fourfold redundancy and fully redundant communication and I/O modules. To a certain extent, design support is already present for simultaneous maintenance/exchange concepts during live operation.

As this does not require shutting down the control system for maintenance activities on vital components, such as circuit breakers, brake electronics, power supplies, etc. (as presently required for safety reasons), and maintenance activities on the control system (software updates, exchanging or upgrading modules, etc.) are also possible at the same time, vehicle downtimes can be reduced in the future and vehicles can remain in service longer.

### 3.4 Flexibility

In many cases two control systems are used in railway applications: one for all standard, non-vital functions, and another for functions with SIL greater than 0. Additional architecture



elements, such as redundancy for pneumatic and conventional wiring and channels, are also necessary for SIL 3 and SIL 4. When selecting a COTS controller, it should be ensured that the solution covers the greatest possible range of applications. A HIMax controller, for example, complies with all system requirements from SIL 0 to SIL 4. That significantly simplifies the architecture of the overall train control management system (TCMS). The cost and effort for system changes and extensions is lower due to the smaller number of interfaces. In addition, there is no need for a time-consuming analysis of which functions need to be implemented in which system (SIL 1, 2, 3 or 4). For example, a HIMax controller can simultaneously support standard I/O modules and SIL 4 I/O modules. The simple architecture and transparency lead to greater acceptance and faster understanding by regulatory authorities and expert assessors, reducing the time necessary for approval procedures.

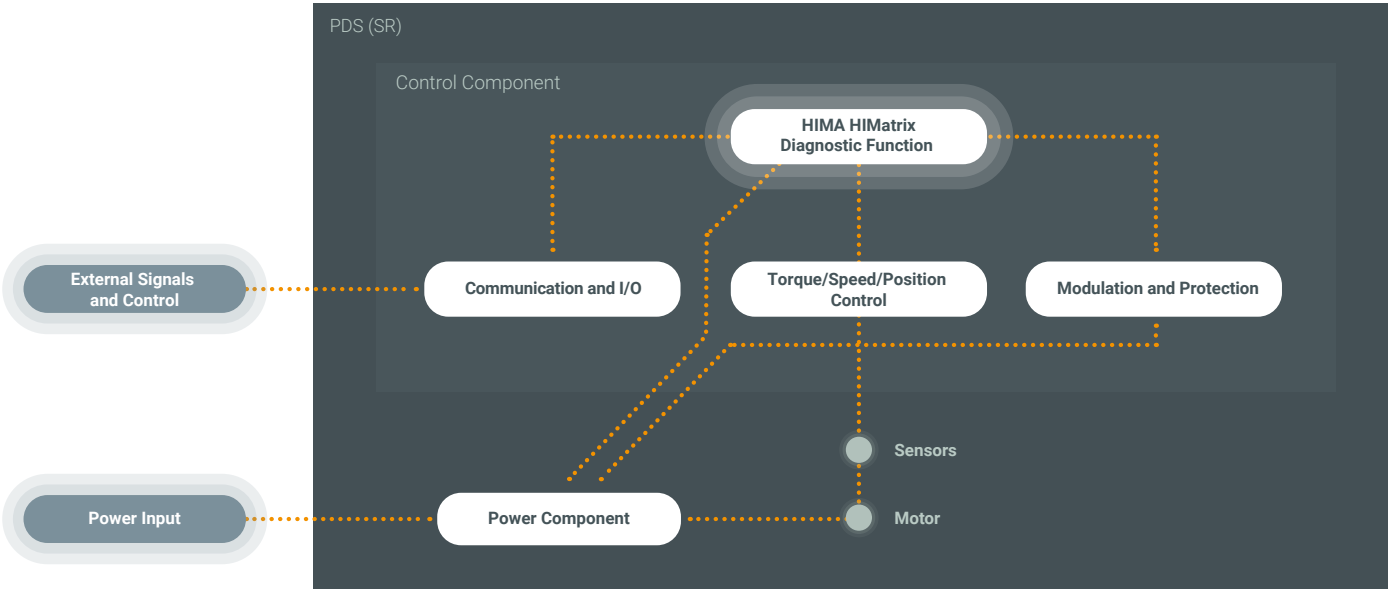
The modular structure and scalable device concept of COTS controllers allow implementation of virtually all rolling stock applications. This includes traction monitoring functions, train control, and standstill, speed and direction monitoring. These COTS systems additionally support plausibility checking, function monitoring and fault detection mechanisms, as well as control functions and logical operations. In some cases they can also handle communication tasks.

### 3.5 Training needs

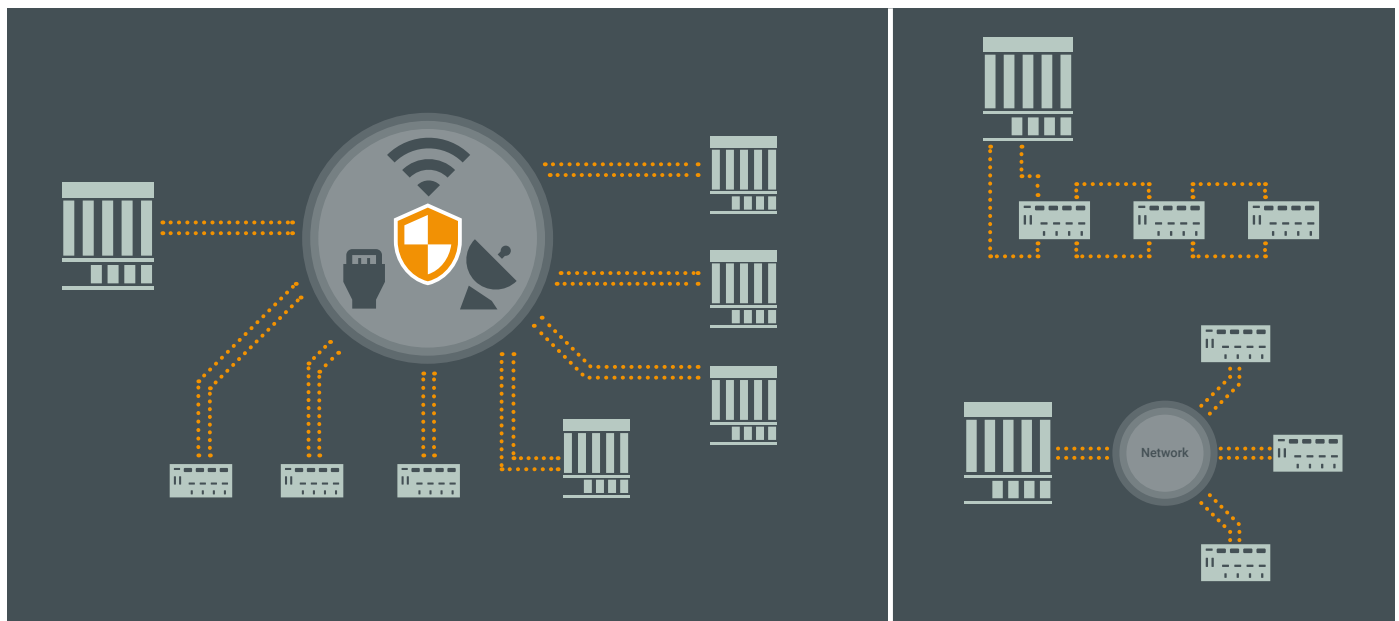
It is important that the COTS software of the chosen solution focuses primarily on useful and essential functions. That eliminates the effort necessary to maintain proprietary train control management systems. This means that the software departments of rolling stock manufacturers are no longer dependent on IT experts whose primary task is to keep the TCMS alive.

Another important factor in the purchasing decision is follow-on costs. With COTS systems based on industry-standard programming languages, such as HIMax, virtually all automation tasks can be implemented using Fupla and/or programming languages generally recommended according to IEC 1131. This enables training needs for service personnel to be minimized worldwide, and makes a larger number of programmers fluent in these programming languages (an estimated 500,000 worldwide) potentially available. Particularly in light of the existing shortage of programmers in many countries, this is a strong selling point with regard to the maintenance and servicing of rolling stock in the global railway industry. With COTS, optimal support for rolling stock with regard to software and launching new vehicles is assured over the entire software life cycle right across the globe.

Figure 3: An example of functional diversity: general architecture of traction monitoring functions in power drive systems



**Figure 4: Comparison of centralized, distributed, redundant and non-redundant system architectures**

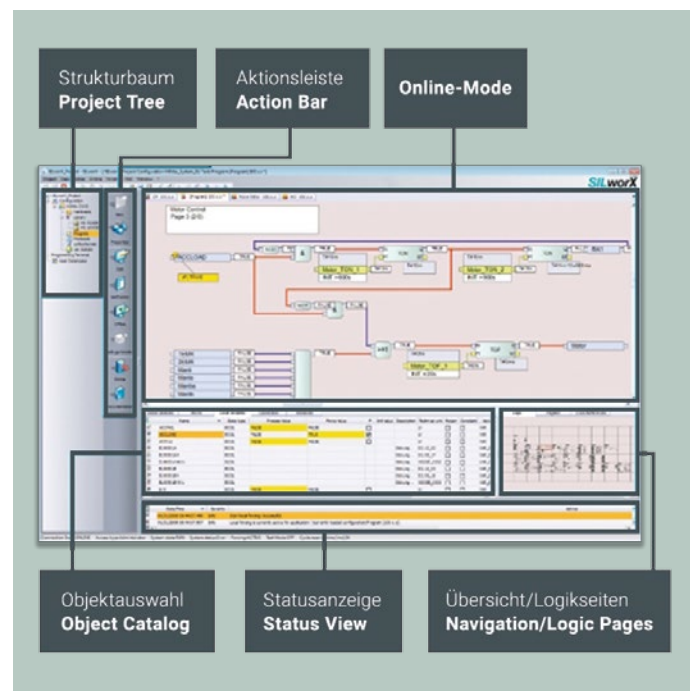


### 3.6 Interoperability

Openness, scalability and modularity are important aspects of interoperability, particularly for interlockings and signaling systems. A key requirement for the COTS system should therefore be that it can support needs-oriented configuration based on a standard operating system and can be deployed as an autonomous controller or as part of a centralized or distributed system. That allows all system parameters of interlockings and applications to be implemented flexibly, extending from locally operated points through control with remote I/O modules close to the field components to central control in a redundant architecture.

The COTS software also plays an important role in networking and interoperability. Ideally it should take the form of a fully integrated configuration, programming and diagnostic tool and utilize industry-standard programming languages compliant with EN 61131. Modern software should also employ function modules and sequential control, as well as C language programming, to facilitate easily understandable programming as well as manufacturer-independent, open interface programming. In this case, testing and commissioning costs can be reduced by creating validated function modules or generic programs. That also simplifies the integration of third-party components – an important consideration in light of the heterogeneous technology of railway infrastructures.

**Figure 5: Modern COTS software (in this case SILworX) should combine configuration, programming and diagnostic functions in a single solution**



### 3.7 Cybersecurity

With the rising degree of automation and increasing relocation of functions to the cloud, there is a growing risk of cyber attacks. That makes cybersecurity increasingly important in railway safety technology. Safety controllers are vital targets of cyber attacks, but equally form an effective line of defense against the hazards to people, railway vehicles and systems, and the environment arising from cyber attacks. Important security enhancement measures in this regard consist of restricting opportunities for human access and setting up autonomous, self-contained security systems.

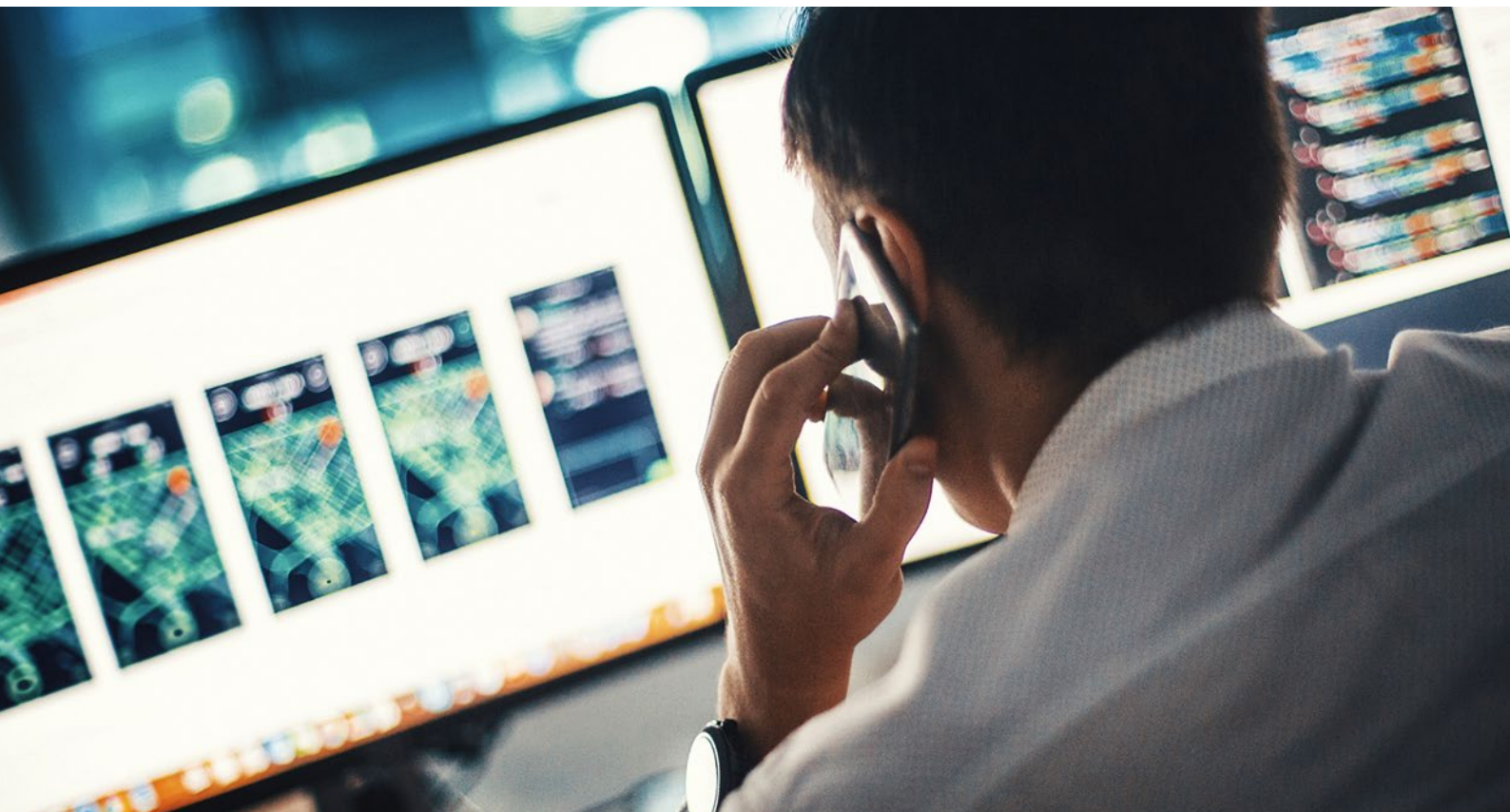
A COTS safety controller for deployment in rail transport should therefore ideally have an operating system which is specifically designed for safety-oriented applications. However, it should also be freely programmable (unlike proprietary systems). Such an operating system includes all functions of a safety PLC but omits all other functions. That renders typical attacks on IT systems ineffective.

For especially effective protection, IT security should be directly integrated into the operating systems of COTS controllers. The HIMatrix and HIMax controllers, for example, are tested for resistance to cyber attacks as part of the development process. By contrast, operators who use conventional PC-based PLC systems must regularly update the operating software of these PCs

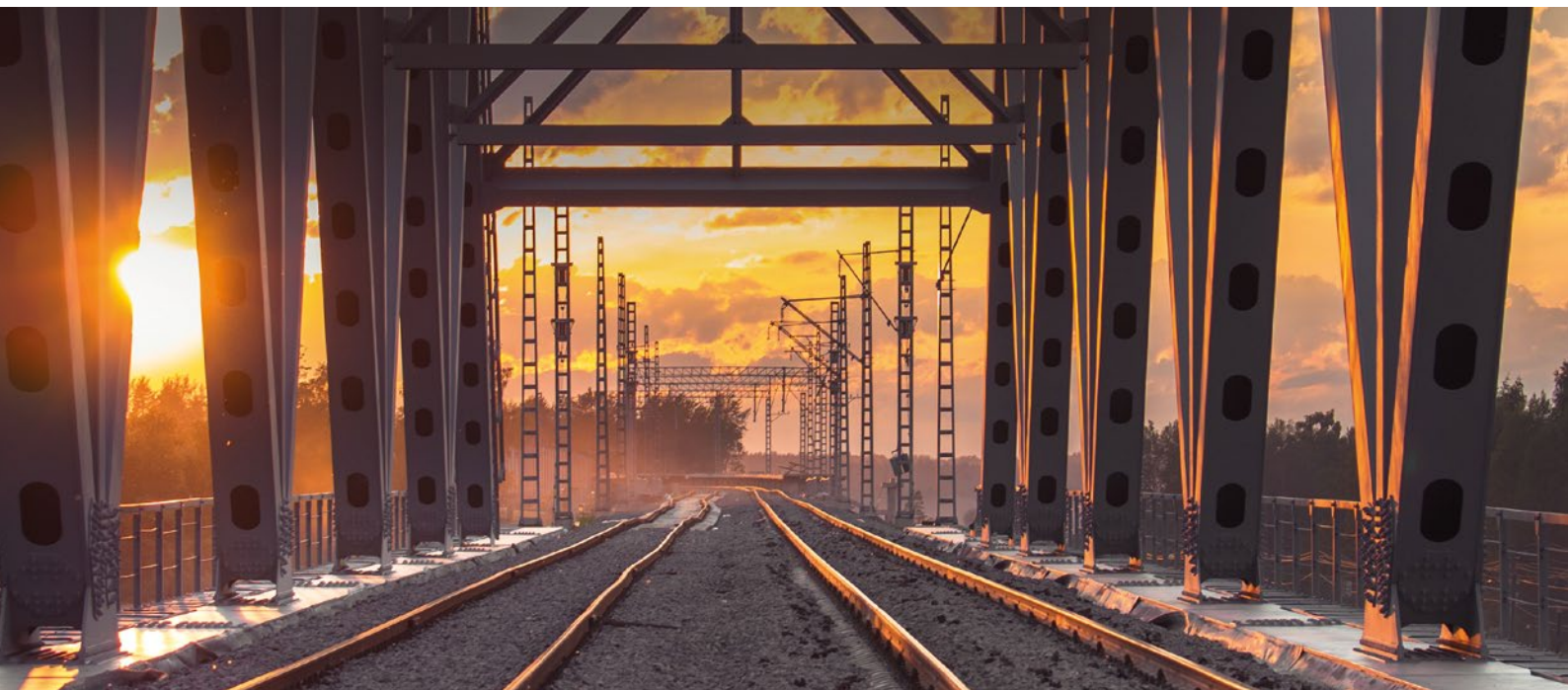
in order to effectively protect them against attacks. However, every update of the operating software by the operator puts the safety case and/or approval at risk.

COTS controllers should preferably have separate system processors (CPUs) and communication processors, in order to ensure high operational reliability even in the event of a cyber attack on the communication processor. This also allows several different and physically separate networks to be operated with a single communication processor or processor module. In the interest of cybersecurity, it is also desirable to be able to individually disable unused interfaces so that the safety controllers are limited to the communication functions which are actually needed.

COTS software should also support multi-level user management which allows user permissions to be set individually, in order to optimally protect the application and the safety system. That eliminates the need for a new patch or recertification of the system in the event of a password change.







## Guideline

---

# 4. Conclusion

---

Proprietary safety-related electronic systems are still predominant in the railway industry. However, there is a clearly visible trend toward COTS controllers as the new standard, due to their deployment versatility and their distinctly lower acquisition and life cycle costs in comparison to proprietary technology. A comparison of the key requirements and properties of modern safety controllers in light of current standards and socio-economic factors shows that railway operators, rolling stock manufacturers and system integrators who use COTS systems benefit from higher flexibility and future viability, easier maintenance and optimal cost-effectiveness over the entire lifetime of rolling stock or infrastructure applications.

COTS systems differ in their details. The main aspects which railway operators, rolling stock manufacturers and system integrators should consider in their purchasing decisions are certification (are the controllers certified in compliance with CENELEC, and what SIL level do they support?), scalability, flexibility, interoperability, easy maintenance, and ease of use of the software. Particularly in light of the increasing number of cyber attacks and a growing degree of networking, users should also always ask what features and functions the COTS solution in question offers for effective protection against such attacks.

Along with the technical aspects, the ability of the COTS supplier to provide worldwide support in addition to hardware, software and tools is also crucial for the global railway industry. The supplier must be able to guarantee spare parts and retrofits over periods of 30 years or more.

COTS systems represent the future of railway technology. They are scalable, modular and easily adaptable. Even new functions can usually be integrated without difficulty. In other words, they grow with the infrastructure or the automation architecture. Long-used rolling stock with many updates and diverse vehicle variants can therefore be implemented easily and economically with the aid of COTS solutions. There is additionally a greater degree of freedom in the selection of component suppliers. Furthermore, spare parts are available worldwide at short notice and can be installed easily. All this is leading to ever greater numbers of major players in the railway industry opting for COTS solutions.

## GUIDELINE

# HIMA COTS SYSTEMS FOR THE RAIL INDUSTRY

---

For further information please contact:

### **HIMA Rail Segment Team**

Phone: +49 6202 709-411

E-mail: [rail@hima.com](mailto:rail@hima.com)

Find out more online:

 <https://www.hima.com/en/industries-solutions/rail>

The content provided in this white paper is intended solely for general information purposes, and is provided with the understanding that the authors and publishers are not herein engaged in rendering engineering or other professional advice or services. Given the complexity of circumstances of each specific case and the site-specific circumstances unique to each project any use of information contained in this white paper should be done only in consultation with a qualified professional who can take into account all relevant factors and desired outcomes. This white paper has been prepared with reasonable care and attention. However, it is possible that some information in this white paper is incomplete, incorrect, or inapplicable to particular circumstances or conditions. Neither HIMA nor any of its affiliates, directors, officers or employees nor any other person accepts any liability whatsoever for any loss howsoever resulting from using, relying or acting upon information in this white paper or otherwise arising in connection with this white paper." Any modification of the content, duplication or reprinting of this white paper, as well as any distribution to third parties –even in parts- shall require the express written approval of HIMA.



[www.hima.com](http://www.hima.com)