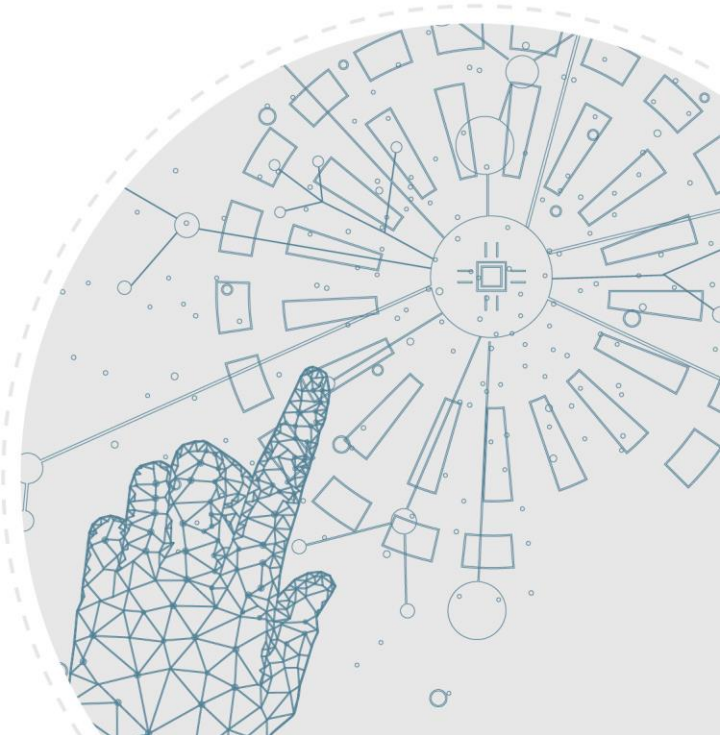
SYS DOCT 002 V1

Doctrine

Considerations concerning connected objects in the railway sector

23/10/2023



Contents

1. Introduction

1.1. Foreword

This document is the result of the work initiated by a focus group organised by the Etablissement public de sécurité ferroviaire (EPSF) on connected objects. The intention is that it be continually updated in line with advances in this field. It fits into a dynamic period of digitalisation in the railway sector, during which the use of connected objects is likely to increase.

Information can be transmitted in near-real time

This document sets out to identify the issues and risks associated with these specific components and to deliberate on safety impact, especially in the railway context, and to put forward recommendations.

This document does not provide specific instructions on the appropriate safety level for each connected object.

1.2. Scope of application of this document

This document is not intended for is use in a connected object engineering process ranging from design to certification. Its purpose is rather to ensure that the use made of connected objects provides every guarantee that results will match the behaviour expected from them in service.

1.3. Definition of a connected object

As defined by the International Telecommunication Union, a connected object is an equipment with the capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

2. Background to connected objects in the railway sector

The gradual decrease in the long-term cost of components such as circuits, along with the spread of the Internet and telecommunications networks, the development of high-density batteries, the development of artificial intelligence, of low-consumption sensors, of low-energy long-distance communication protocols, etc. all contribute to the development of connected objects. This trend makes it easier to install a large number of these devices, offering better understanding of the state of the system.

2.1. What connected objects offer

Connected objects have the ability to transmit information from areas previously inaccessible to humans. This enables more accurate mapping of the environment, which can potentially be reproduced in a “digital twin”. Existing components can be fitted with these communication devices. Moreover, information can be transmitted in near-real time.

In the railway sector, the use of sensors and communication networks is nothing new. Previously, however, functions were compartmentalised, operating in isolated sub-systems. The information gathered by respective sub-systems was not shared. Also, for any given component, sensor data was analysed independently without aggregation.

The use of connected objects enables real-time maintenance, with the ability to intervene immediately in the event of a fault or failure, and the implementation of predictive maintenance. Repairs to equipment can be scheduled at the most opportune time, i.e., when they have the least impact on production.

2.2. Use of connected objects in the railway sector

As far as the railway sector is concerned, a large number of potential safety-related applications have been identified to date:

- for rolling stock, connected object can be used in analysis doorways that retrieve information from onboard sensors in order to prompt maintenance in real time, fire detection, detection of flat spots on wheels, detection of overheating in bearings or electrical components, factoring mileage travelled into maintenance, detection of coupling shocks, installation of sensors on the bogie to identify abnormal vibrations or temperature rises, detection of open doors, etc.
- for operations, connected objects can be used to automatically switch on lights when approaching a train or a level crossing, detect congested platforms, review suitability for transport, detect flapping tarpaulins or parts inside the running gauge, detect intruders, locate trains, detect applied brakes (digital braking), etc.
- for infrastructure, connected objects can be used to supervise the state of points and give early detection of point switching failure, to monitor electrical and IT installations, faulty track geometry, presence of vehicles or pedestrians at level crossings, temperatures affecting rail expansion, engineering structures, bridges, etc., the running gauge, floods, rising water tables, landslides, to protect operators working on the track, etc.

2.3. Constraints and limitations of connected objects

2.3.1 Environmental constraints

Connected objects are generally located close to the components they monitor (*in situ*), in environmental conditions that may be unusual for railway electronics, and which are liable to cause premature deterioration.

These devices are often designed with limited computing and memory capacity, to minimise their energy consumption and preserve the battery, especially when they are not connected to a continuous source of electricity.

In addition, they can use specific protocols that consume very little energy and limit bandwidth.

2.3.2 Location/constraints

The measurements made have uncertainties (notably linked to the distance separating the sensor from the measured source) and may be sensitive to ageing. The measurements and information must come

from the source we want to measure. Some connected objects will be spread out in areas that are potentially difficult to access.

Connected objects can be powered by the electricity grid, by batteries, by harvesting energy from their environment, or by several of these sources. The batteries may not last long enough to remain functional for the intended period of use. If a connected object harvests energy from the environment (solar, vibration, etc.), there are periods when these energy sources will not be available.

2.3.3. Telecommunications

The sensors are able to communicate with servers that have significant data processing and storage capacity, commonly located in the cloud. There are a number of risks: a possible broken link, significant transmission delays, and potentially inadequate bandwidth.

The frequency and transmission rate are sometimes intentionally reduced to control energy consumption, which may prove insufficient to perform the desired function. Communications over the airwaves have specific limitations and constraints. These constraints are typical of telecommunication networks: attenuation, range, directions, bandwidth, frequencies, presence of obstacles, congestion, disconnection, time to connect, etc.

It is essential to establish a reliable link between the transmitter and the receiver, which creates constraints in terms of polarisation, directionality, and gain between the components. These requirements translate into design and installation constraints.

2.3.4. Compatibility and interoperability

Equipment compatibility is an important aspect, especially at the interfaces between rolling stock and infrastructure. Therefore, as far as connected objects are concerned, the equipment must take account their interaction with vehicles using the rail network. The information produced may be ambiguous. For example, a speed could be the speed of the train, the rotation speed of an axle, etc.

2.3.5. Data management

Connected objects, by their very nature, produce a wealth of data. It is therefore imperative that the system in place as well as the agents assigned to this task are able to manage this information efficiently. Moreover, close attention must be paid to verifying the accuracy of this information, especially in terms of its timely relevance or its vulnerability in terms of cybersecurity. It is therefore important to bear in mind the potential difficulties associated with the use of multiple reported data points, sometimes in a very precise way, which could prove difficult to exploit. Processing noise and distinguishing it from anomalies is a major issue in signal analysis. A function should not be activated in response to background noise.

2.4. Specifics of connected objects in the railway sector

In terms of technology, connected objects do not come with any radically new innovations. The fields of electronics, software, and telecommunications have been well established for decades. However, their

planned integration into the railway sector has specific characteristics that could give rise to new risks. At this stage, the following potential peculiarities have been identified:

- use of components in an outdoor environment
- use of artificial intelligence
- high scale
- evolution of maintenance protocols (maintenance assisted by connected objects, implementation of predictive maintenance)
- replacing human surveillance with automatic devices

The majority of connected objects available on the market are not automatically compliant with standards specific to the railway sector. Furthermore, it is essential to ensure that connected objects can be integrated into the railway environment without creating new risks, such as electromagnetic interference or falling parts.

Connected objects are often built using commercial components with a relatively short lifespan (hardware and/or software), generally a few years, whereas railway applications have lifespans extending over several decades.

It will therefore be necessary for these objects to exist alongside equipment having a much longer life cycle. As a result, obsolescence (whether in the hardware and/or software) will be an ongoing issue.

3. Regulatory framework for connected objects

3.1. The European regulatory framework

Digital technological developments give rise to issues of compatibility and market access, safety, confidentiality, and liability. These issues can be tackled at European level when common solutions are needed, especially in the context of the internal market.

Although connected objects are a recent field for which the regulatory approach remains limited for the time being, since 2015 the European Commission has published analytical and strategic documents and pot forward more specific legislative initiatives in several areas that have an impact in their own way on the development of connected objects.

The connected object safety issue is not addressed as such, but is *de facto* covered by more generic regulations that also apply to connected objects. It can also be seen that, when horizontal legislation is proposed on these subjects, the Commission takes account of possible sector specifics and of the legislation/structures/organisations/procedures already in place in certain sectors, which are already subject to rules concerning their market introduction and the monitoring of systems and components (such as railways). Of special relevance is the monitoring of developments in areas such as cybersecurity, artificial intelligence (AI), and liability rules. Legislative procedures are under way at the European Parliament and the Council of the European Union on legislative acts that introduce a horizontal approach to these issues, but which have or could have consequences at sectoral level.

3.2. The standardisation framework

Many standards can be applied to connected objects. First of all, railway standards must be taken into account. However, standards from other fields may also apply (telecommunications, etc.). The entity will have to analyse the potentially applicable standards, in terms of environment, technology, and scope.

3.3. Consequences for the EPSF of the connected object regulations

Regulations relating to cybersecurity, AI, and information systems have and will undeniably give rise to major consequences for the railway sector stakeholders. However, as the regulatory texts currently stand, the impact remains limited for EPSF in the scope of its missions. In the absence of prescriptive regulations specific to the Internet of Things (IoT), the traditional authorisation scheme based on reports from notified bodies (Nobo), designated bodies (DeBo) and risk analysis assessment bodies (Asbo), and also based on a demonstration of safety, would be applicable in this area. The central regulatory text for the EPSF thus remains Commission Regulation (EU) No 402/2013 of 30th April, 2013 *on the common safety method for risk evaluation and assessment*.

4. Fault and failure management

The risks associated with the use of connected objects can be of various kinds. They can be functional, i.e., linked to the complexity of developing these components, or dysfunctional, i.e. associated with failures.

4.1. Understanding and detecting faults

The faults to be analysed concern both the supervised object (such as an axle) and the connected object itself.

The use of connected objects will not necessarily identify all the failure modes of the component being monitored. Some of the information provided by connected objects may be lost (due to electromagnetic interference, power outage, etc.).

To guarantee that a connected object will provide the appropriate information, it will be necessary to analyse the failure modes and understand the deterioration phenomena of the supervised components. This approach is based on an analysis of these failure modes (a dependability-type approach).

Detecting faults or failures in the connected objects themselves is a major challenge. Some are not used continuously, so their failure will potentially only be detected when they are in use.

4.2. Fail Safe modes

The use of a large number of components is likely to lead to increased rates of failure, which can lead to significant system downtime. The loss of a link with a sensor will lead, for example, to a declaration of a fault on an axle and therefore potentially to a halt in traffic. The definition of fail safe modes requires

further thought at both component and system level. And during all this, an appropriate safety level must be maintained.

On the upside, connected objects can be used to identify faults that were not previously identified, thereby improving safety levels. In this case, which fail safe mode should be adopted?

The design must consider the system's worst-case operating states, without necessarily linking these states to a component failure. The implementation of limitations or boundaries may be necessary to minimise the effect of a failure. These limitations can be local (close to the component) and/or global (at system level).

4.3. System of systems

The complexity of systems based on connected objects multiplies the risk of failures that are difficult to manage. The failure of a connected object can affect several functions. A sensor can be used in several systems and/or successively integrated into several functions. Complexity makes the system less predictable. Systems become so complex that they are difficult to apprehend, and an agent's ability to understand them is reduced. Modelling these systems is a growing issue. Bearing in mind that simpler systems are often already difficult to model.

General risks

General risks are not always included in technological analyses and fall outside the scope traditionally covered by the EPSF. Nonetheless, the following themes have been identified as those most likely to affect connected objects: sovereignty, climate risks, and energy consumption.

5. Human and organisational factors and safety management

5.1. Loss of information

The adoption of connected objects means that operators will be less present in the field. However, when working on site, operatives can observe elements that the sensors do not detect (signs of leaks, odours, etc.). Operators thus have a global view of the environment. An agent can easily identify a fire, whereas sensors must identify deformation, temperature increase, short-circuits, etc.

5.2. Crisis management

Systems using connected objects can either act autonomously or prompt an operator to initiate an action, based on raw or pre-processed information provided by the interface. The operator interacts with the system when a particular situation arises, detects an abnormal situation, appraises the situation using the available information to identify or anticipate the state of the system. They then develop a solution based on the constraints and risks involved.

Maintenance or operational staff can be overwhelmed by too much information or too many alarms, which can even be contradictory. If the system is available and reliable, breakdowns with a major impact on operations will become increasingly rare. The operator will have to be ready to react very quickly to faults that it very rarely encounters. It will be necessary to determine whether operators will be able to take control of the system in such situations, and what training they will need to be able to deal with them when the time comes.

5.3. Skills

Connected objects are an emerging technology. There is a consequent shortage of qualified professionals in this field. This can create a rift between the technology implemented and the ability of employees to use it. This challenge is made all the more complex insofar as several areas of proficiency are required, especially in metrology, telecommunications, and digital technology. Maintaining these sophisticated systems could prove a major challenge. It is also essential to incorporate the need for ongoing training, given the constant evolution of these technologies.

5.4. Organisation/Responsibilities

The implementation of connected objects could lead to a risk of worker disconnect, with their feeling less involved in tasks such as maintenance. In the event of a fault or failure, maintenance will have to intervene, disrupting conventional maintenance methods in the railway sector, which are mainly based on regular maintenance operations.

5.5. Consequences on safety management

The incorporation of connected objects is influencing safety system management. The affected areas include skills management, asset management, document management, and supervision.

6. Cybersecurity

This note does not set out to deal with cybersecurity in the railway sector. Nevertheless, this paragraph sets out a number of points to bear in mind in this respect.
Cybersecurity aspects are never far off when deliberating about connected objects. On the basis of Regulation (EU) 2019/881 of the European Parliament and the Council of 17th April, 2019 *on ENISA (the European Union Agency for cybersecurity) and on the certification of information and communication technologies* with respect to cybersecurity, ENISA has been given a central role in setting up a cybersecurity certification model.

Also concerning cybersecurity certification, another stakeholder could come into play as the regulations envisage an important role for national cybersecurity certification authorities. EPSF will have to collaborate and exchange with this authority.

In 2021, the French National Agency for Information Systems Security (ANSSI) published a guide with the title “ *Recommandations relatives à la sécurité des (systèmes d’)objets connectés* (ANSSI-PA-087)”

(recommendations for the security of connected objects or systems thereof) . The recommendations apply to all connected objects. They must be tailored to the application's required security level.
EPSF has published a document drawn up in collaboration with ANSSI, " Prise en compte des enjeux de cybersécurité au sein de la sécurité ferroviaire" (Consideration of cybersecurity issues in railway safety). This document sets out cybersecurity recommendations tailored to the railway sector.

7. Recommendations

In view of the findings set out in this note, a number of recommendations can be made at this stage.

Recommendation for EPSF

The EPSF must have a complete grasp of the risks inherent in the use of these technologies, from their presentation in authorisation submission files to their use when contributing to a safety process. Attention must notably be focused on the probable constant evolution of these components. A detailed understanding of how connected objects work could be followed by introducing specific training courses to enhance employees' skills. The impact on the safety management system needs to be analysed, especially with regard to the skills required to carry out these safety tasks.

***

Identification of critical failures

All potential faults and failures must be considered, in particular those of the connected object itself and those of the equipment being monitored. One of the biggest risks is not being able to detect a fault that is considered to be detectable. The entity must ensure that it has taken proper account of this in its organisation and risk models.

***

Fail Safe modes

It is recommended that fail safe modes be designed in the knowledge that not all faults will necessarily be detected. The implementation of restrictions or boundaries may be necessary to ensure effective management of these situations.

***

Location

It should be firmly borne in mind that sensors may require precise positioning, that calibration and possibly recalibration may be necessary, and that sensors may lose accuracy over time. Accessibility to the sensors needs to be analysed. In addition, the impact of these components on the railway environment must be taken into account (electromagnetic interference, falling, etc.).

***

Responsibilities

The roles and responsibilities of each player must be clearly established to ensure that all the actions required to maintain the safety level of connected object-based systems are carried out.

***

Crisis management

The organisation's ability to manage potential crisis situations should be verified, notably by ensuring the reported information can be used by the operators and that they are prepared and capable of managing these situations effectively.

***

Skills

The organisation must ensure that its operators have the requisite skills to operate and maintain connected objects that include various cutting-edge technologies.

***

Data processing

The organisation must make sure it is able to manage the information provided by connected objects. This relates to the potentially large volume of data received, possible difficulties in using the reported information, and the assurance that this information is adequate for execution of the required task.

***

Interoperability

The use of connected objects must not give rise to interoperability issues (for example, connected objects present in carriages or wagons that are assembled to form a train).

***

Energy consumption

There must be an assurance that connected objects have enough energy to perform their function, or that their loss of energy does not compromise safety.

***

Resilience to general risks

The implementation of connected objects must be based on an analysis of the system's resilience, i.e., its ability to withstand shocks. This analysis must include the risks associated with a disruption in supply, a loss of sovereignty, a subcontractor failing, or the obsolescence of a component. Action must be taken to mitigate these risk (stockpiling, interchangeable components, etc.).

***

Safety management system

The entity must ensure that its safety management system is appropriate to the implementation of connected objects. This especially concerns staff and management training and the management of the configuration and hierarchy of these objects.

***

8. Acknowledgements

This report is based on an extensive review of related literature. In addition to that, many interviews were conducted with design offices, infrastructure managers, start-ups, maintainers, connected object manufacturers, etc., mainly from the railway sector.

EPSF would like to thank all the contributors.

Établissement public de sécurité ferroviaire (French railway safety authority)

60, rue de la Vallée – CS 11758 – 80017 AMIENS Cedex 1, France