Taking cybersecurity challenges into account in railway safety

With the collaboration of

TLP: WHITE

Foreword

Note written in the framework of a think tank consisting of:

- Laurent CÉBULSKI, Managing Director, EPSF
- Sadio BA, Transport Sector Coordinator, ANSSI
- Thomas CHATELET, ERTMS Project Officer, ERA
- Yseult GARNIER, Head of Industrial CyberSecurity (RCS-I), SNCF RÉSEAU
- Quentin RIVETTE, Head of Industrial CyberSecurity (RCS-I) for Equipment, SNCF VOYAGEURS

Contents

Introduction

The generalisation of electronic components and information and communication technologies, both at the levels of infrastructure and rolling stock (and notably for the control-command part), creates new risks within the railway sector for which the boundary between what concerns cybersecurity and what concerns railway operating safety is increasingly tenuous.

The total control taken remotely over a car by two researchers in 2015 – several other demonstrations have been made since then – is a perfect illustration of the importance that we must attach to this "cyber" risk in the transport sector.

Over the last few years, the railway system has suffered several attacks that have essentially impacted the passenger information and ticketing systems. On 29 November 2016, a hacker attacked the San Francisco public transport network's ticketing system during *Thanksgiving* ("ransomware" type attack[1]), providing free access to the network for several days. More recently, the passenger information system in Germany was altered by the Wannacry ransomware in 2017[2].

The UK railway network was attacked four times between 2015 and 2016. These attacks were regarded as being "exploratory", but the hackers could access vaster information management systems that control the signals[3].

These "cyber" risks cannot be dissociated from railway risks: taking control of a control centre - covered by an authorisation for entry into service issued by the railway safety authority on the basis of operating security standards -, could have serious consequences for operation safety. The current railway technical standards hardly take cyberthreats into account at all. The boundary between railway safety and cybersecurity has yet to be determined whether in technical terms, regarding the scope of intervention and competencies between the various safety authorities, or in organisational terms. It is essential to clarify the functioning at the interface between the two "worlds": articulation between the safety management system and the information systems of the railway operators concerned.

These "cyber" risks cannot be dissociated from railway risks

The increasing degree of connectivity of the infrastructure and rolling stock is creating a significant increase of their attack surface. Nevertheless, this connectivity offers higher levels of performance in terms of supervision and updating, but must be perfectly controlled and cyber-secured by the manufacturers, equipment manufacturers and operators.

The time aspect is a challenge: "cyber" time requires rapid measures for applying corrections to the systems (signalling, maintenance, etc.) in order to address any vulnerabilities, but railway safety time requires a non-regression analysis of the system, and the guarantee that the update made will not make

[1] A malware program that encrypts the data contained in a computer and demands a ransom in exchange for decrypting the data.

[2] Ransomware that impacted a number of companies worldwide in 2017

[3] https://www.independent.co.uk/life-style/gadgets-and-tech/uk-rail-network-railways-hacked-four-times-hackers-trains-a7135026.html

the infrastructure incompatible with the rolling stock running on it, or even degrade the safety level of railway operation.

The goal of this document - jointly written by the European Union Agency for Railways (ERA), French National Cybersecurity Agency (ANSSI), French National Safety Agency for Railways (EPSF), and SNCF Voyageurs and SNCF Réseau - is to:

- remind the reader of the respective scopes of the railway and of the cybersecurity regulatory frameworks;
- draw up an inventory of the ongoing works aiming to build a shared framework between safety and cybersecurity, and to strengthen the way the cybersecurity dimension is taken into account in the railway sector and in the other means of transport;
- highlight the subjects (notably of an operational nature) that have already been identified and that justify the need for a clear operating framework in the area of “overall” safety;
- make recommendations, at this stage of our reflections, stemming from the discussions and exchanges between the authors of this note.

Context: a cyberthreat to be taken into account in railway transport

The The railway transport sector, understood here to include the infrastructure managers, goods and people transport enterprises, as well as their service providers, is a strategic sector. The fact is that the States are increasingly turning towards the development of this means of transport, on the one hand in order to cope with the new challenges relative to network saturation and, on the other hand, to make the most of the technological advances and new economic and environmental outlets brought by the sector. The increase observed in number of players since 2006 (43 railway undertakings and 20 infrastructure managers in France at the end of 2018) should accelerate with the forthcoming opening up of domestic passenger transport to competition. This highly heterogeneous panel of players (size of the companies, traffic, age and maturity, etc.) means that a comprehensive approach is required in terms of railway system safety and cybersecurity, and that particular vigilance is needed regarding the multiple interfaces that exist between all of the stakeholders.

Cyberattacks made for purposes of sabotage by offensive players in response to geopolitical tensions have already been observed abroad. So, geopolitical tensions between France and another State with an offensive cyber-attack capability, could cause cyber-attacks with a view to destabilizing or even sabotaging strategic sectors such as railway transport.

ANSSI has also noted for several years that the railway transport sector, on the worldwide level, is targeted more by attackers motivated by profit. The trend observed regarding ransomware type attacks and personal data exfiltration campaigns against players in the sector is likely to continue. The French railway transport sector may therefore be under threat from these cyber-attacks, some of which could impact the integrity and availability of the data and services it provides.

Furthermore ANSSI, along with its partners, have noted a change in the offensive activities of certain players moving towards a pre-positioning[4] in the IT networks of strategic sectors in France and in other countries, without it being clear what the final goal of these breaches actually is.

Lastly, the railway transport sector has for several years seen an increasing digitisation of its activities and services. This means that ever-more interconnections are imposed on the sector's players between their respective networks, which ultimately increases the attack surface.

[4] Pre-positioning: In this case this means preparing a massive attack on or rapid invasion of an IS by positioning "dormant assets" which will be activated on D-day and serve as an entrance door.

1. Applicable regulatory frameworks

Depending on the field of competence in which you place yourself, the terms used and the associated competences are fundamentally different:

- **Railway safety** concerns overall functioning of the system, which in turn consists of sub-systems (infrastructure, rolling stock, control-command / signalling, operations, etc.). The risks are above all technical and environmental.

- **Operating safety** is the ability of the components (doors, brakes, etc.) of a sub-system to meet one or more functions required under given conditions. It is used to establish demonstrations of the safety of technical sub-systems.

- **Cybersecurity** is a set of technologies, processes and practices aiming to protect the networks, computers and data against attacks, damage and unauthorised access. In an IT context, the term “security” encompasses cybersecurity and physical safety.

1.1 The railway regulatory framework

The highly regulated railway sector has safety authorities for verifying, by means of authorisations and controls, that the stakeholders observe the rules that apply to them. In France, it is EPSF (Public Railway Safety Establishment) that is the competent national authority. It was set up further to the transposition of directive 2004/49/EC of the European Parliament and of the Council on safety on the Community’s railways which, in its first article, stipulates the obligatory establishment, in every Member State, of a railway safety authority.

Article L2221-1 of French transport Law states that EPSF ensures compliance with the rules relative to railway transport safety and interoperability. It is the French national safety authority in the sense of directive (EU) 2016/798 of the European Parliament and the Council of 11 May 2016 relative to railway safety. It accomplishes its missions on the railway system (urban metro and tram networks coming under the authority of the Prefects).

Subject to the missions devolved to the European Union Agency for Railways (ERA) stipulated by regulation (EU) 2016/796 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Railways, EPSF is notably responsible for issuing the authorisations required for exercising railway activities and ensuring the supervision activities relative, in particular, to the railway undertakings and infrastructure managers.

The public establishment promotes and disseminates the best practices in the area of railway safety and interoperability on the basis of all the relevant information available, and also organises and contributes to collective thinking on the improvement of railway safety.

More precisely, EPSF’s main missions are to:

- assess the requests for the authorisations required to exercise railway activities that enter into its scope: railway undertakings’ safety certificates, infrastructure managers’ safety approvals, authorisations to place vehicles on the market and infrastructures in service. It administers the French national vehicle registration system, feeds the European Register of Authorised Types of Vehicles and issues the train driver licenses;

- verify compliance with the conditions for maintaining these authorisations, by means of inspections and audits on the operation, infrastructure and internal organisation of the undertakings. In the event of failure, it can restrict the authorisations' field of application, or even suspend or withdraw them;
- monitor the level of safety, thus ensuring the classification, traceability and analysis of the safety-related events occurring on the network;
- organise national feedback in liaison with the sector and steer collective improvement actions;
- draw up and publish technical documents, best practices and recommendations, relative to railway safety, where certain texts may count as "acceptable means of compliance" with the regulations;
- assist the Minister in charge of transport in the drawing up and adaptation of the national and international texts (more particularly European), relative to railway safety and interoperability.

The European technical regulation is above all an interoperability regulation, and includes railway safety issues in a context of gradual liberalisation of the sector that began with the transport of goods in 2006, and will be completed by that of the national transport of passengers in 2020.

Through the gradual harmonisation of the rules and standards, interoperability aims to lift the technical barriers built up between the States during their history. For example, a train going from Berlin to Madrid must still today be capable of running with four different voltages, six signalling systems and two different rail gauges. Harmonisation involves long, arduous and extremely costly works which, to date, only concern some European corridors dedicated to high speed trains and the transport of goods between major terminal facilities.

In order to speed up this interoperability, the implementation of two new European directives and a European regulation of 16 June 2019 in the framework of the "4th railway package"[5] strengthens the role of the European Union Agency for Railways (ERA), which issues the international authorisations for rolling stock and the international safety certificates for the railway undertakings throughout the European Union, in cooperation with the national authorities, which remain fully competent in the area of verification.

The 4th railway package - consisting of a set of five European texts in total comprising the "technical" pillar (ERA, interoperability and railway safety) and the "market" aspect (governance of the players and opening up to competition for passenger transport) - constitutes the most recent step in the liberalisation of the railways, initiated by the previous packages.

Put simply and succinctly, the railway system can be broken down into two types of objects: the technical objects (rolling stock, infrastructure, signalling) and the organisations, which in turn are backed up by the human factors to underpin their functioning.

Each new technical "object", whether it is a train or an infrastructure, must have been authorised by the competent safety authority. In order to obtain this authorisation, the applicant must demonstrate by means of a safety dossier that the object in question complies with the European regulations (called Technical specifications of Interoperability - TSI) and, where applicable, with the national rules (reflecting the specific technical features of the network concerned).

[5] See https://www.ecologique-solidaire.gouv.fr/ouverture-concurrence-du-transport-ferroviaire-paquets-ferroviaires-et-creation-larafer which explains the different railway packages

This regulatory compliance is mandatory. Associated with an analysis of the railway risks, it constitutes the basis of the demonstrations of safety. So, a train or an infrastructure that meets the standards called up by the regulatory framework will be deemed to function safely.

The safety issues must then be dealt with in operation, and also ensured by maintenance and servicing.

Two major players interact on railway networks: the railway undertakings that operate the goods or passenger transport services, and the infrastructure managers, in charge of managing the traffic and of the maintenance of their network.

Like for the technical objects, each operator must be authorised and inspected on the basis of a safety management system (SMS) demonstrating its ability to identify and deal with the railway risks linked to its activity (documentation management, maintenance, skills management, and also the dissemination of a safety culture throughout the undertaking and management of the organisational and human factors).

The basic principle for railway safety is that it is prohibited to degrade the system's overall level of safety (by introducing new items or changes to what already exists).

The risk analysis represents the common denominator between the authorised entities and the safety authorities. It is on the basis of this analysis that it will be possible to identify the risks, then to put in place safety barriers to cover them.

The European regulatory framework is described in implementing regulation No 402/2013 of the European Commission on the common safety method for risk evaluation and assessment that applies in the railway sector. In particular, it indicates three risk acceptance principles:

- **application of codes of practice**, in the first place the regulatory specifications and standards - compliance with which it is accepted would guarantee an acceptable level of safety;
- **comparison with a reference system**, insofar as this system has demonstrated through its functioning that it guarantees an acceptable level of safety;
- **explicit risk estimation,** called up notably when the first two principles cannot be used, and which calls on the operating safety techniques. This principle is used in particular in the framework of disruptive innovations for which no regulatory framework has been defined and when no similar system exists. The growing introduction of new technologies is tending to increase the utilisation of this principle.

➔ **This railway regulation does not, to date, provide any provisions specific to cybersecurity, nor any interfaces with the authorities and organisations that are competent in the area.**

1.2 The regulatory framework in the area of cybersecurity

The French National Cybersecurity Agency (ANSSI) was created by decree No 2009-834 of 7 July 2009 in the form of a department with national competence. It is attached to the secretary-general for national defence and security, under the authority of the Prime Minister.

The French National Cybersecurity Agency is the national authority regarding the security and defence of information systems.

In this respect:

- it designs, makes develop and implements the secure inter-ministerial means of electronic communications necessary for the President of the Republic and the Government;
- it ensures the function of national authority for the defence of information systems. In this capacity and in the framework of the orientations set by the Prime Minister, it decides what measures the State implements to cope with crises affecting or threatening the security of the information systems of the public authorities and of the operators of vital importance and it coordinates government actions;
- it organises and coordinates the inter-ministerial works in the area of information systems security;
- it draws up the information system protection measures proposed to the Prime Minister. It ensures the adopted measures are applied;
- it carries out inspections of the information systems of the State's departments;
- it implements a system for detecting events liable to affect the security of the State's information systems and coordinates the response to such events;
- It collects the technical information relative to incidents affecting the State's information systems;
- it issues the approvals for the security systems and mechanisms designed to protect, in the information systems, the information covered by national defence secrecy;
- it takes part in international negotiations and ensures the liaison with its foreign counterparts;
- it ensures the training of the personnel qualified in the area of information systems security.

The French National Cybersecurity Agency expresses its opinion on the security of the systems and services, offered by service providers, that are required for the protection of information systems.

In particular, by delegation from the Prime Minister, the Agency is in charge of the following:

- certification of the security of the systems used to create and verify electronic signatures;
- approving the centres that assess and certify the security provided by information technology products and systems;
- issuing authorisations and managing declarations relative to the cryptology means and services.

The European Network and Information Security Agency. – ENISA – is a European Union agency that was set up on 10 March 2004 by a European Union regulation.

In this respect:

- it advises and assists the Commission and the Member States in the area of information security and helps them, in consultation with the sector, to deal with hardware and software security issues;
- it collects and analyses the data relative to security-related incidents in Europe and emerging risks;
- it promotes risk assessment and management methods in order to improve the capacity to cope with the threats weighing on information security;
- it encourages the exchange of best practices in the area of awareness-raising and cooperation with the different stakeholders in the information security sector, notably by creating partnerships between the public and private sectors with specialised companies;
- it follows up the elaboration of the standards for the products and services in the area of network and information security.

Regulation (EU) 2019/881 of 17 April 2019 on ENISA – now called the European Union Agency for Cybersecurity – and on information and communications technology cybersecurity certification, strengthens its role and broadens its missions. Indeed, it has been granted a permanent mandate along with additional resources. It is also responsible for developing a European cybersecurity certification framework for products, processes and services that will be valid throughout the European Union.

Faced with the increase in the number and sophistication of IT attacks, and their potentially destructive impacts, ANSSI's mission is to help the operators of vital importance (OVI) to make their sensitive information systems secure. The cybersecurity of OVIs is part of the broader inter-ministerial system regarding the security of activities of vital importance (SAVI) mentioned in French Defence Law. These activities are distributed by sector of activity attached to a coordinating ministry. As the prime contact for all the "skill" issues, the ministry is responsible for providing its expertise regarding the sector of activity that it is in charge of. This system has made it possible to identify the OVIs, both private and public, that operate or use installations considered to be vital for the survival of the Nation.

In order to face up to the new cyber-related threats, article 22 of the Military Programme Law (or LPM, law No 2013-1168 of 18 December 2013), that follows on from the recommendations of the White Paper on defence and national security of 2013, adds another brick to the edifice by obliging the OVIs to strengthen the security of the critical information systems they operate: the information systems of vital importance (ISVI). Ensuring this security notably involves the application of a certain number of security rules stipulated by ANSSI, thus positioned in the role of regulator. They must notify ANSSI immediately should an incident affect the functioning or security of an ISVI and they may be submitted to inspections. **This system has been fully operational since October 2016 for certain operators in the railway sector.**

Adopted on 6 July 2016, directive (EU) 2016/1148 on security of network and information systems, the NIS directive was transposed into National Law in 2018. The operators of services that are essential (OES) for the functioning of the economy and society are obliged to secure their most sensitive information systems by complying with the security rules imposed by ANSSI. They must notify ANSSI immediately should an incident affect the functioning or security of these information systems and they

may be submitted to inspections. **This system has been fully operational since September 2018 for certain operators in the railway sector.**

These two systems aim to raise the level of cybersecurity for critical infrastructures, in particular railway transport infrastructure. **However, not all of the information systems required for the functioning of the railway system are concerned by these regulations which are limited to the critical infrastructures.** Furthermore, the different approaches adopted by the member States do not always contribute to guaranteeing an equivalent level that is shared between the different players.

➔ **"Cyber" interoperability is therefore not currently fully ensured on the European scale.**

2. Challenges

2.1 The ongoing works and initiatives[6]

2.1.1. In rail transport

A variety of initiatives designed to better define and delimit the way cybersecurity is taken into account in rail transport have proliferated over the last two years. So, whether it is at the level of research, in the area of the standards, regulations, or of partnerships, the concerned stakeholders are seeking to structure themselves in order to attempt to better articulate railway safety and cybersecurity and thereby strengthen the way cybersecurity is taken into account. Conferences are regularly organised on this subject on the national and European levels.

Although it is difficult to envisage being exhaustive on this subject, the following initiatives can be considered significant.

- At the French national level, EPSF and ANSSI signed a letter of intent on 20 March 2018, relative to cooperation in the area of the security of information systems. In concrete terms, this means the two entities must exchange information concerning incidents affecting the information systems of operators entering into EPSF's area of competence, work on identifying and articulating the railway safety requirements and security requirements associated with malicious acts concerning the communication equipment and the software (of which this note is the first deliverable), and collaborate in a general way in the area of the security of information systems (notably through awareness-raising and training actions). This work is still very much emerging and aims in particular to arrive at a French vision of these subjects, before proposing positions shared on the European scale, in the framework of revisions of the regulations - whose adoption procedures are complex - and that are the subject of serious disagreements between the States on the subject of cybersecurity.

  EPSF and ANSSI signed a letter of intent relative to cooperation in the area of the security of information systems.

- Since 2014, joint works have been carried out between SNCF and ANSSI, encouraged by the above-mentioned regulatory corpus (LPM / NIS directive). These works are materialised by technical and organisational support, audits and more formal partnerships around innovative projects such as the Autonomous Train.

- The players are also seeking to federate. Thus, on the initiative of Infrabel (Belgian infrastructure manager), DB Netz (German infrastructure manager) and with the support of ENISA, several European stakeholders from the railway sector (Infrastructure Managers and Railway Undertakings in France, Belgium, Germany and the Netherlands) launched a platform in 2019 for exchanging information on cyber risks: ER-ISAC (*European Railway - Information Sharing and Analysis Centre*). The purpose of this platform is to form a trusted group capable of circulating relevant information on ongoing cyber risks and on the level of reliability of certain products or services and, more generally speaking, of ensuring the promotion of this topic at institutional level. The information and best practices provided by this platform could be considered as being contributions to the regulatory framework or to

[6] The approach does not claim to be exhaustive

drawing up standards. In addition to the members (European railway undertakings and infrastructure managers), other partners can contribute, such as industrial companies in the railway sector, national or European administrations in the area of cybersecurity or of railways, research institutes and lastly other ISACs.

- In the area of research and innovation, the European public-private Shift2Rail partnership which aims to offer a collaboration platform for research and innovation for the Single European Railway Area, covers cybersecurity in one of its Innovation Programs. In particular, a specific technical demonstrator is in place aiming to establish a complete analysis of the cybersecurity risks relative to the ERTMS control-command system, and protection measures for each sub-system, as well as an appropriate architecture (notably establishing zones with differentiated security levels). Different railway sector stakeholders (manufacturers, equipment manufacturers, operators, etc.) are represented in the working group and discussions are ongoing with the European Union Agency for Railways to reflect, in the future versions of the Technical Specifications for Interoperability, the needs for harmonisation of certain interfaces ensuring interoperability: radio interface, encryption of the ETCS signalling messages, etc.

- Regarding standards, the CEN/CENELEC working group dedicated to information system security and cybersecurity (WG 26) aims to establish a European technical specification (TS 50701) relative to cybersecurity applied to the railway sector, and this specification should eventually become a standard. The works are based on the international standard IEC 62443 – “Industrial communication networks - Network and system security”. The working group brings together major stakeholders from the railway sector (manufacturers, equipment manufacturers, operators). This specification will notably propose architecture models, the main cybersecurity risk assessment principles, sets of cybersecurity measures applicable per cyber-criticality zone, and the cybersecurity activities carried out during the product’s lifetime (cf. §2.2.2 Maintaining in Secure Condition). This future standard, which could serve as a recommendation for encouraging the operators and industrial companies to take a closer look at the question of cybersecurity, is still under review.

- The International Union of Railways (UIC) develops railway telecommunication specifications and, in particular, a programme for the successor of the GSM-R ground-train radio called *Future Railway Mobile Communication System* (FRMCS). This new telecommunications system should be based on the 5G telephony standard and natively integrate elements for protecting against cyber-threats compared with the possibilities offered by the old telecommunications systems. As telecommunications are a major lever for the digitisation of railway technologies, the measures for protecting them will be essential.

2.1.2. Example of functioning in other sectors

It appears difficult to be exhaustive so varied are the sectors concerned by cybersecurity, and the maturity in the face of the cybersecurity risks is not the same in every sector of activity.

Air transport was quick to take an interest in this subject. This can doubtless be explained by the existence of a culture firmly rooted in safety and security, by the organisation of the sector that was effective right from the first developments of international transport which makes it possible to ensure homogeneous practices and effective joint working on the worldwide level.

Today, on the European level, the European Union Aviation Safety Agency's mission is to coordinate the cyber issues globally for the aviation sector. In collaboration with all of the sector's stakeholders, it ensures that the cyber risks for the European air navigation systems are taken into consideration during the design and maintenance in operating condition phase. To achieve these goals, it regularly organises workshops to strengthen cooperation, to include cybersecurity in the concept of air safety.

In France, the recent creation of a Council for Cybersecurity in Air Transport (CCTA) under the aegis of the DGAC (French Civil Aviation Authority), the body that coordinates the services of the State, manufacturers, equipment manufacturers and operators and civil aviation professional federations, aims to supervise, structure and coordinate the initiatives concerning cybersecurity in the French aviation sector and to make France's voice heard in the European and international technical working groups.

The Council is organised around three technical committees:

- CT1: "cyber risks", responsible for updating the hierarchy of the risks that could affect the air transport sector;
- CT2: "impact", responsible for proposing measures for mitigating these risks, taking the impact of these measures (security, economy, etc.) into account;
- CT3: "regulations", responsible for drawing up draft national texts and deploying a strategy for influencing the international bodies.

A similar initiative was launched in the automotive sector in May 2019 with CSTA30.

ENISA organised the first conference on cybersecurity in transport in January 2019 in Lisbon, with the support of the European Commission, European Union Aviation Safety Agency, European Maritime Safety Agency and the European Union Agency for Railways. This event marked the fact that the subject of cybersecurity is being taken into account at the highest level and opens new perspectives regarding the relationship between safety in transport activities and cybersecurity. Eventually, these reflections should also contribute to establishing the cyber certification framework promoted by ENISA for the aspects specific to transport.

2.2 Railway safety and cybersecurity: a porous border

2.2.1. New technologies, new connectivities, new risks

The railway industrial information systems, whether they are used for maintenance or control-command, on the ground or on-board, are increasingly computerised. In addition to this there are a number of on-board comfort or entertainment systems whose aim is to improve the customers' travelling experience.

They all now use increasingly standardised technologies, stemming from the world of conventional IT; whereas, in the past, the systems were generally proprietary and specific. Thus the IP networks and non-specific software distribution now take up a significant place on-board trains, and in the ground infrastructures.

This situation is dual; it facilitates functional developments (easier connectivity to be envisaged) and the taking into account of cybersecurity (technologies benefiting from a community of users, cybersecurity products available on the market); but it also leads to an increased probability of malevolent cyberattacks (standard protocol and software layers, public vulnerabilities).

In order to cope with this situation, a certain number of sensitive points (see below) must be brought under control from the cybersecurity viewpoint; more particularly on the industrial ISs that can contribute to the operating safety of the railway system.

- **Access for maintenance**:

  The first of the connectivities that must be brought under control is the one relative to physical accesses, and in particular the access required by maintenance staff (fault reporting operations, visualisation) and the system administrator (advanced reprogramming and parameter configuration operations).

  There is a significant challenge regarding the control of connected devices (IT workstations and tools), access to data (principle of least privilege) above all if they contain software secrets, personal data, or logs of operations performed (traceability) notably when programming or parameter configuring is concerned.

  The utilisation of mobile terminals increases sensitivity; indeed the cybersecurity of a nomad terminal is by default difficult to control, access via these nomad terminals increases the risk of security being compromised and thus offers a potential entry point for a hacker.

  The control of these challenges involves technical (hardening, partitioning, rights management, etc.) and organisational (awareness-raising, training, etc.) measures.

  Remote maintenance and other remote operations (sometimes outsourced), that rely on connected objects currently being deployed massively on the railway network, must be classified in this category, with the installation of on-board/ground links (in other words links between the rolling stock and the ground), and the installation of sensors positioned on the industrial ISs.

  Remote access considerably increases a system's attack surface.

The coverage of the risks inherent to these deployments relies on a combination of technical (partitioning, authentication, encryption, etc.) and organisational (security contractualisation with the partners, etc.) measures.

Besides the application-related vulnerabilities, the low-layer vulnerabilities (electronic, firmware, etc.) will have to be considered in the coming years. The physical and logical protection pair will then be essential for controlling the associated risks.

❖ **Deployment of wireless connectivities**:

Wireless connectivity between IT components is burgeoning and is in the process of imposing itself on the functioning of the railway system thanks to the possibilities it offers in terms of remote diagnosis, geolocation, or the collection of data of use for maintenance. Likewise, improving the "customer experience" will involve these new possibilities (real-time passenger information, on-board internet, etc.). Cybersecurity measures are essential on these particularly exposed links; all the more so as the critical flows can pass through them, such as signalling and steering information, or remote programming functionalities.

Encouraged by society's digitisation and hyper-connectivity, the interactions between trains and customers are developing and are also creating an increased exposure surface to cyberattacks.

In these cases, the physical protection of the systems and networks (first barrier in the defence of railway systems) is not effective. It is vital to envisage a cybersecurity integrated in the system *by design* to meet these challenges. Partitioning, filtering, authentication, surveillance and logging are all measures that are needed for the resilience of such solutions in service.

➔ **Not all of these aspects are subject to an assessment in the framework of the issuing of railway operator authorisations, because they are not integrated in the regulations relative to the railway safety management systems.**

Although intrinsically designed to react functionally in safety-compatible fall-back modes (in the sense of railway safety), **the Industrial ISs including safety functions can no longer ignore cybersecurity.**

As mentioned, the implementation of new technologies leaving a large place for digital technology, and the increase in the attack surfaces that they generate highlights the **vital need to more closely articulate railway safety and cybersecurity**. **Beyond these aspects, meeting the availability goals** (the fall-back of a system often being synonymous with unavailability) **is also a significant challenge** for operators subjected to a security event.

2.2.2. Two antagonistic logics: the demonstration of railway safety and maintaining in secure condition (cyber)

The railway regulations require that, for any information system on-board rolling stock or equipping an infrastructure (signalling – control-command), an analysis should be performed which, according to its importance, may give rise to an authorisation from the Safety Authority. Each change made to an existing system (hardware or software update) requires this type of analysis, which must be traced and appended to the technical dossier for the system concerned. In the case of a software update, often considered as not requiring a new authorisation, the analysis often takes several days to several weeks in order to ensure the non-regression of the updated system, in other words that it will not cause any malfunctions that would be detrimental for safety. Traceability is essential, notably to take account of the additionality criterion (a succession of several minor updates may in the longer term constitute a major change regarding safety).

As for **Maintaining in Secure Condition** ("MSC") it defines all of the organisational and technical measures contributing to maintaining the level of cybersecurity all along a system's lifetime. In particular, it relies on:

- control of the cartography (technical, physical) of the hardware and software components, and of the related organisational processes;
- monitoring of the latter's vulnerabilities;
- processing of the latter via patches or circumvention measures (technical or organisational) making it possible to maintain the level of cybersecurity over time.

Railway time (analysis and non-regression test time) and cyber time are asynchronous:

- a system in its version authorised by the safety authority remains dependable in railway safety terms all along its lifetime (between 15 and 25 years) as long as it is not modified in any significant way. But each modification, even minor, must be the subject of an analysis;
- any given cyber-secured system in its version on day D may become non cyber-secured on day D+1, and must therefore be permanently maintained secure (by the application of patches in particular), which appears to be difficult to reconcile with the time required to analyse the impact of the modification on railway safety.

The main challenge is therefore to successfully define processes enabling an agile and rational MSC at the service of a railway safety system that continues to be compliant with the terms under which it was authorised.

2.2.3. Are the requirements in the area of cybersecurity going to tighten the conditions for admitting[7] rolling stock on the infrastructures?

Regarding railway safety, any train that has previously been authorised must be the subject of a verification of its compatibility with the infrastructure on which it is going to run. This verification is due to the historical specific features of the national networks (characteristics of the tracks, signalling, catenaries, etc.) which mean that these verifications must be carried out on the rolling stock, even if it complies with the applicable regulations.

The technical specifications for interoperability gradually blur these specific features, as the lines concerned are renewed or upgraded. In order to carry out this verification, which is incumbent on the railway undertakings, each infrastructure manager is obliged to publish a register of railway infrastructure, describing the characteristics of its network. This register is harmonised on the European scale.

To date, there are no criteria related to cybersecurity in the compatibility verification process: an infrastructure manager therefore cannot impose any requirements relative to cybersecurity, even if it considers that running a train could constitute a threat in terms of cyberattacks.

The potential angles of attack can be multidirectional: from a train to the infrastructure, from an infrastructure to a train, but also between two trains or two infrastructures operated by different operators.

The introduction of requirements that are potentially very different and divergent by the infrastructure managers to admit trains on their network would have a negative effect on railway interoperability. Inversely, what guarantees do the operators have that the infrastructure would not constitute a vector of attack on their rolling stock?

2.2.4. The railway system's availability challenges

The processes contributing to railway operating safety have for a long time been based on a triptych [human - organisation - technical processes independent from the information systems].

For several years, encouraged by the sector's digital transformation, and thanks to the functional opportunities offered, these processes are increasingly reliant on information systems; thus creating an "IS dependence".

In the case of a malevolent act directed against an information system subject to these dependencies, all or part of the operation could be degraded or interrupted.

[7] By admission, we mean the overall procedure for putting a train into service on an infrastructure (authorisation, verification of compatibility, etc.)

A denial of service on these information systems would directly impact on the railway system's operating capability.

The approach to control operating security, notably for systems ensuring safety functions, involves deterministic states and foreseen degraded modes.

In the case of a malevolent act leading the system to an unforeseen state, the fall-back mode implemented will generally be a system shutdown (e.g.: emergency braking, closed signalling, etc.).

In this logic where robustness is ensured by a switchover to fall-back mode making it possible to guarantee the control of operating security, a cyberattack could easily cause system unavailability.

3. Recommendations (actions and implementation methods)

Given the findings of this note, it would be appropriate to adopt a convergent approach (technical and regulatory) to guarantee the safety of railway systems, whether in the sense of operating safety or of the availability and integrity of information systems.

At this stage of our work, several recommendations can be made:

Recommendation R1: **Intensify the cooperation between EPSF and ANSSI to tend towards a French position on the articulation between railway safety and cybersecurity**

The letter of intent signed between EPSF and ANSSI in 2018 has made it possible to initiate a dialogue between the two authorities, of which this note constitutes the first concrete result, in association with SNCF and ERA.

On the basis of this note, it is a question of building a “French” position on the subjects highlighted here that would constitute the roadmap that could be proposed in a coordinated way in the European bodies in the framework of the forthcoming regulations.

This work could be developed further on the question of means, competences and processes to be put in place to provide a clear, inclusive outline for the issues relative to safety, whether this concerns railway safety or cybersecurity.

It will also be a question of prioritising the challenges: existing systems, innovations requiring the widespread use of digital technology, match between the players’ means with respect to their exposure to risk, etc.

Lastly, increased sharing around safety events and analysis of the associated risks, possibly on simulated cases of railway cyberattacks, would make it possible to test the proposed outlines.

***

Recommendation R2: Have a European overview of the articulation between cybersecurity and railway safety

---

Proposed by ERA in coordination with ENISA, it will be a question of obtaining a European overview of the positions of the Member States on the issues raised in this note, even of identifying other topics that are preoccupying our counterparts.

This overview would serve as input data for preparing a future harmonised European regulatory framework converging on taking railway cybersecurity into account, and to define the future roles of the assessment bodies and of the safety authorities regarding

certifications and authorisations, or even simple declarations from the players to deliver and delimit everyone's perimeters of responsibility.

It would also be a question of getting a better understanding of ENISA's roadmap and of the nature of the relationship and breakdown of actions between ERA and ENISA.

***

Recommendation R3: Facilitate the sharing of information and coordinate the actions of the French railway sector on cybersecurity

---

Over the last few years, faced with the increased cyberthreat, France has put a regulatory system in place to partially meet the need for security because its scope remains insufficient (see §1.2). As the subject of cybersecurity continues to grow in importance, a number of discussion forums have been put in place where different visions can be confronted. These visions are insufficiently shared, and the increased development and deployment of new digital technologies could be braked in the case of events impacting the overall safety of the system.

Furthermore, the railway system aims for the interoperability of its networks and of the rolling stock running on them, and the constraints relative to protection in the area of cybersecurity could hinder this interoperability (see §2.2.3) by introducing criteria that could restrict the train movement possibilities. A "comprehensive" approach to these constraints reinforces the need to coordinate all the players concerned.

So, the creation of a space dedicated to railway sector cybersecurity, bringing together all the stakeholders - institutional, industrial, equipment manufacturers, operators, federations - similar to the aviation sector's CCTA, would make it possible to better structure the sector, examine the "system" issues in order to provide collaborative solutions, and would contribute to synchronising the positions to be defended at the European or international level.

***

Recommendation R4: Integrate the cybersecurity dimension right from the beginning of projects

---

It is essential that cybersecurity should be closely taken into account in order to guarantee an acceptable level of safety at the time of entry into service, and then all along the life cycle.

So, it would appear important to:

– integrate cybersecurity from the moment that projects emerge (in the specifications, in the technological and architectural choices) in order to reduce the costs of cybersecurity and facilitate the integration effort;

– standardise and systematise the approach relative to cybersecurity within the organisations, in order to ensure overall coherence;
– keep up to date a macro-cartography of the cybersecurity risks, stemming from these accompanying actions.

This recommendation concerns all the stakeholders (operators and industrial companies) in charge of designing or modifying single components or complex systems.

***

Recommendation R5: Implement a rational MSC (Maintain in Secure Condition) while reducing as much as possible the impacts on the safety demonstrations (in the sense of operating safety)

Paragraph 2.2.2 of this note highlights the time-related divergences between cybersecurity (MSC requiring quick execution) and operating safety (demonstration of stabilised safety).

The approach for aligning the MSC and the safety demonstration could be based on the following elements:

- Adopt a *secure by design* approach for defining the train network architecture calling on modular bricks aiming to separate the SIS bricks from the application layer; and effective in-depth defence on the most sensitive attack paths;
- Define a perimeter over which the MSC aims to take priority, by drawing up an inventory of the components considered to be the most critical with respect to the system's overall MSC (equipment ensuring the cybersecurity functions, systems in direct interaction with potential illegitimate accesses);
- Define upstream application rules: strategy of generic MSC and breakdown into systems according to their specific features (architectures, technologies, components, exposures, etc.) making it possible to delimit the vulnerability monitoring, contextualised calculation of their criticality, and decision model for deployment;
- Contractualise the MSC activities with the industrial companies for the specific products (vulnerability bulletins and supply of patches/corrections/circumvention measures);
- Implement test and acceptance platforms.

This type of approach should be shared with all the players in the stakeholders sector and, on the basis of a consensus, be applied at the level of guidelines and sector-based standards.

***

Recommendation R6: Identify the repercussions that cybersecurity could have on interoperability in a sector where the number of players and the amount of cross-border traffic is growing

---

Paragraph 2.2.3 of this note highlights the possibility of constraints appearing in the future linked to the requirements of cybersecurity that could be different from one operator to another. Such a situation would impact all of the operators at their interfaces and notably the crossed admission between Rolling Stock and Infrastructure.

In order to avoid such an obstacle, it would be advisable to:

- identify the technologies / systems / interfaces that could in the longer term lead to such a situation and analyse the risks caused by these interfaces. Determine whether, for the cases identified, technologies would be available to enable an operator to protect their own interfaces without impacting the stakeholders with exported constraints;
- assess whether, for the cases identified, shared specifications would make it possible to standardise these interfaces with a level of safety that is sufficient and/or demonstrable (Technical Specification for Interoperability; standard; etc.);
- determine whether, for the cases identified, the certification approach currently being examined at the European level could be a response to the amortizing of exported constraints.

The stakeholders (industrial companies, equipment manufacturers, certification organisations, etc.) could make their contribution to this standardisation / certification approach, in order to contribute to achieving the single market for railway transport services.

***

Recommendation R7: Increase the robustness of the information systems essential for operating the railway system in the face of the "cyber" type threat

---

Paragraph 2.2.4 of this note highlights a growing dependence on information systems for ensuring the operation of the railway system. Beyond the perimeter relative to railway safety, the availability of the information systems that also contribute to operational functioning should be guaranteed.

In order to make the system more resilient, it would be necessary:

- to design information systems and the dependences linking them, while protecting them from the risks of denial-of-service type attacks;
- in the case where a malevolent act succeeds, to anticipate what actions must be taken by means of:

- activity continuity plans (or “how can I continue to operate without my information system, or with a degraded information system? “),
- activity resumption plans (or “how can I effectively and quickly return my information system to nominal service? “).

Établissement public de sécurité ferroviaire

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