Digital transformation of the rail sector: what impact on the regulator?

Laurent CEBULSKI – Authorization Director – October 2019

Etablissement Public de Sécurité Ferroviaire (EPSF) – France

1. Introduction

With two centuries of history, the railroad has accompanied the various industrial revolutions, while retaining its original operating principles, modernized as technological advances.

In France, with 30,000 kilometers of operated railway lines (including 2,800 km of high-speed lines), France has the second-largest rail network in Europe after Germany.

Rail transport, whether dedicated to the transport of passengers or goods, is now threatened by new modes of mobility. The autonomous car, the “uberisation” in practices, the liberalized coaches and the truck platooning are all competitors that fit into the MaaS ("Mobility as a Service") from which the rail mode could be excluded. The same is true for freight: rail must be fully integrated into a multimodal logistics that aims to minimize the cost of the "last mile".

Mostly based on return of experience essentially accumulated by historic operators, railway companies are convinced that increasing productivity and competitiveness can no longer rely on traditional methods but must rely on the opportunities offered by digital technologies. Several major projects have already emerged: autonomous train, connected infrastructure, digital twin, MOOC for operator training, augmented reality for maintenance interventions ...

The common denominator for all these projects is that they must be assessed, certified, or even authorized, by demonstrating that they do not reduce the level of safety of the rail networks on which they are implemented and then checked during their actual operation, to ensure that it remains securely sustainable for users.

The rail system has an immutable principle: it is forbidden to degrade its safety level. To this principle is added a second imposed by Europe: it is forbidden to curb the interoperability of networks, in other words to put technical, organizational or human barriers that would prevent the movement of people and goods.

In each Member State of the European Union, safety authorities are responsible for ensuring that these principles are respected. They must, therefore, also closely monitor developments, innovations, transformations in progress to be able to assess their impact on the network global safety level, but also to change their practices accordingly.

On a technical level, the rise of digital technologies has accelerated over the past two years. The possibilities offered by these new tools are numerous and the actors are developing them more and more in order to rationalize the costs (material and human), to improve the availability of the systems by anticipating their failures, and to minimize the long and costly field tests to demonstrate the safety of a technical object.

This paradigm shift still affects the safety authority: the treatment of the "traditional" risks of the railway domain by the triptych [humans - technics - rules] deployed within the organizations is jostled by the innovations under development, of which the often disruptive nature no longer makes it possible to rely on pure experience, and introduces new logics of safety demonstration based on barriers for which no feedback is available. For example, no rail accident data is available to evaluate the conduct of an autonomous train by an artificial intelligence (AI) module, or obstacle detection by lidars.

For the regulator, it is therefore a question of being ready to apprehend these changes, to identify them, to know them, to understand them, to better assess them when it is necessary to authorize, control or even change rules that have become incomplete or obsolete.

2. Using massive data to influence safety

All technologies and domains currently being developed have a common denominator: collecting (connected objects), analyzing, exploiting (virtual certification, digital model and twin), and even stealing and modifying (cybersecurity) data.

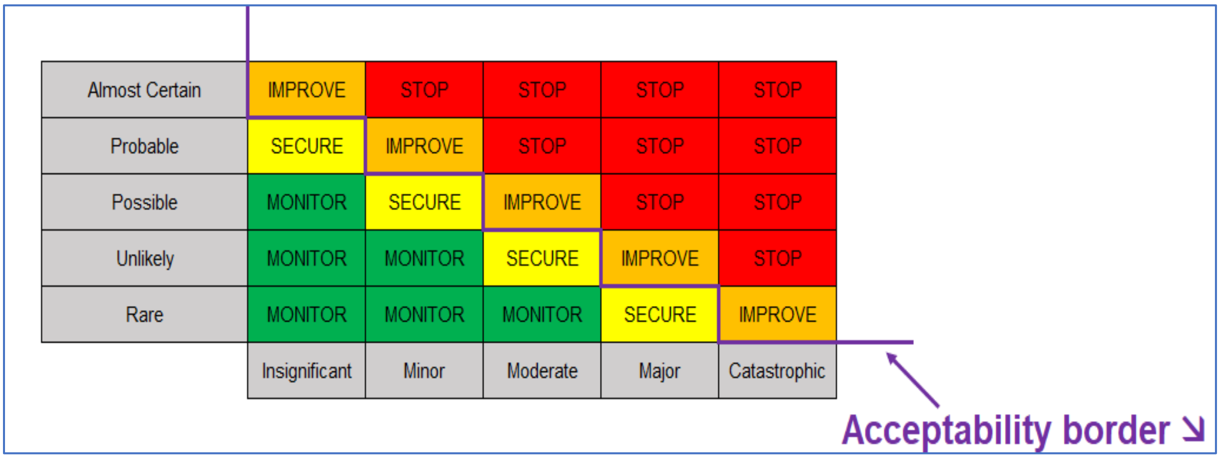
This is not new: as in other areas, rail companies have always had multiple and very diverse databases. The novelty lies in the possibilities offered by new technologies to have massive data quickly exploitable and make it a strategic issue of operation for these companies.

Of a system composed of multiple non-interconnected bases, often operated manually (not to say "artisanally" because of the unstructured nature of the data that composes them), the industry has become aware of the importance of having a real policy of governance of its data, now considered as intangible assets.

The use of AI now makes it possible to meet challenges such as the identification of a root cause to a safety problem, and the search for the most appropriate corrective action to be implemented for the operator. Today, the algorithms are capable of extracting tons of operational data and indicating the actions recommended for most unforeseen maintenance problems.

Traditionally, risk analyses are based on an "event - frequency - severity" triplet. It is a question of attributing a frequency to a dreaded event, as well as a gravity, which constitutes a difficulty for the RAMS engineer because of a certain subjectivity: an event has not the same gravity according to the spectrum of the one who analyses it.

The most classic representation of these criteria is in the form of a risk representation matrix.



Almost Certain	IMPROVE	STOP	STOP	STOP	STOP
Probable	SECURE	IMPROVE	STOP	STOP	STOP
Possible	MONITOR	SECURE	IMPROVE	STOP	STOP
Unlikely	MONITOR	MONITOR	SECURE	IMPROVE	STOP
Rare	MONITOR	MONITOR	MONITOR	SECURE	IMPROVE
	Insignificant	Minor	Moderate	Major	Catastrophic

Acceptability border ↘

Risk representation matrix

The relative subjectivity of the criteria that feed this matrix has always generated expert debates around the sole acceptability of the identified risk. Two views can oppose:

- that of the producer of the analysis, which relies on the accumulated data on products of the same nature of which he has knowledge (rate of failure, lifetime, etc.) as well as on his feedback (methods of failure, operating environment);

- that of the regulator, which must assess the assumptions presented by the applicant, based on its own data, experience feedback (including safety events related to similar products), the standards established on the basis of this return experience, and the expertise of the engineer in charge of evaluating the analysis.

The more reliable and sufficient data available to the parties to position the frequency / severity slider as accurately as possible, the better is the level of precision and the easier is the consensus on the acceptability threshold to be set. The goal is to achieve enough confidence to consider that a product can be safely licensed.

The increasing integration of sensors (30 billion connected devices expected in the world in 2020) in vehicles and infrastructure will increase the number of data available to operators and therefore the level of precision of their analyses, by better traceability of the life of potentially failing components. The technical object management tools will make it possible to know in real time the entire lifecycle of a part, from its design to its replacement.

This availability of a large mass of data (concentrated in a few major players or diluted within the sector) likely to feed the safety analysis can be seen as the specter of a threat, or an opportunity.

The previous projections lead to the following observations:

- In threats:

    - The entity with the most data integrity and robust analysis algorithms could reverse the balance of power and be regarded as holding the "truth" in safety: it is the transposition of the model "winner takes all ", where the one who offers the best service picks up everything. The growing complexity of AI, which is a real black box, precludes its being evaluated by a human brain: only the AI can monitor and evaluate AI. The report to the authority then moves from the assessment of the risks towards the level of confidence in the integrity of the data on the one hand, and towards the relevance of the models used on the other hand, and would then call other competences than those strictly related to railway safety, as well as the development of its own algorithms.

    - Thus, in the area of control, an auditor should ask himself questions other than those relating to railway operations and safety, such as: is the algorithm sufficiently transparent (and therefore modifiable, in the sense of improvable "of the term) for end users? Is it likely to be used in a socially acceptable way? Could it inadvertently produce / exploit weaknesses inherent in the human factor? Is the algorithm used for a misleading purpose, or simply based on bad assumptions? Is there evidence of internal bias or incompetence in its design? Does it adequately indicate how it achieves its recommendations and indicates its level of trust?

- Recent books on the subject highlight a recurring error in constructing models that confuse causality and correlation. But if two events are correlated (in time or space), that does not mean that one has caused the other. The shortcuts that are taken obscure the third-party elements that may contribute to having an effect on the result found.

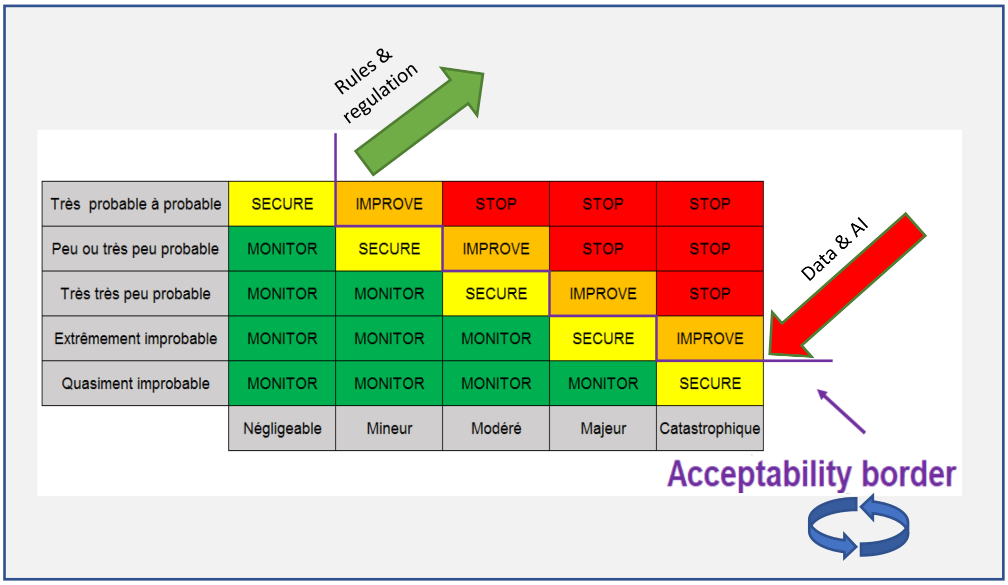
- The adverse effect could be the arbitration justification against safety (for financial reasons for example), especially if it is shown that securing an equipment requires an amount deemed prohibitive in relation to the risk probabilities accident data from predicted data analyzes and predictive models.

- More misleading, the misuse of data available but not used, in a logic of "dark analysis", could skew the analysis and disrupt the operation of the system.

- In opportunities:

- The acceptability of a risk with respect to the [severity - occurrence] pair in the safety demonstrations would be less debatable and could lead to finer evaluations, since it is based on a set of precise data to replace the experience acquired. (and often lost) over the years.

- The breadth of technical knowledge in the rail sector, many of which are cross-functional and based on experience that companies have difficulty in tracing and exploiting, remains an opportunity for those with a systemic vision and expertise proven technique to continue to "criticize" the analyzes produced.



Très probable à probable	SECURE	IMPROVE	STOP	STOP	STOP
Peu ou très peu probable	MONITOR	SECURE	IMPROVE	STOP	STOP
Très très peu probable	MONITOR	MONITOR	SECURE	IMPROVE	STOP
Extrêmement improbable	MONITOR	MONITOR	MONITOR	SECURE	IMPROVE
Quasiment improbable	MONITOR	MONITOR	MONITOR	MONITOR	SECURE
	Négligeable	Mineur	Modéré	Majeur	Catastrophique

3. The New Paradigm

Currently in the acceleration phase, the digital transformation of the rail sector will ultimately change the way of approaching safety. The multiplication of data thanks to connected objects, and their processing by the use of algorithms, will constitute the keystone of the risk evaluation system, and will be able to change normative references and regulations.

In a context of opening to competition, multiplication of actors and rationalization of operating costs, the safety management systems of railway operators (infrastructure managers and railway undertakings) and maintenance organizations will have to evolve to take into account the impact of these new uses on organizational and human factors: increased role of intelligent technological systems providing a massive influx of information to be processed, evolution of the trades to maintain control over the systems processing this information, and consequently, different decisions because guided by machine analysis.

In other more advanced sectors, the need for evaluation (compliance, fairness, loyalty, neutrality, transparency, etc.) of platforms and algorithms becomes a subject of society, subject to debate and regulation.

For the regulator, new strategic issues appear:

- A training challenge, as the digital tools and practices will require a deep adaptation of the expertise of the assessors, whose acculturation must already begin, in order to be able to interrogate new practices, new tools and finer analysis fed by more and more data;

- An information issue, for which it is important to question the collection of data essential to maintaining a global view of the level of rail safety;

- An authorization issue, with the underlying development of testing and verification protocols that prevent machines from being designed to meet these tests, obscuring the goal of ensuring system safety;

- A supervisory issue, because the process and procedure controls in force today will have to combine the human factor and the "intelligent machine" factor, with other modes of questioning and probably auditing approaches that remain to be built;

- Finally, a regulatory challenge: a digital system must remain in line with its specifications, and its specifications must comply with the legislation. It will therefore have to take into account these developments, which could lead to a redistribution of the responsibilities of all stakeholders.

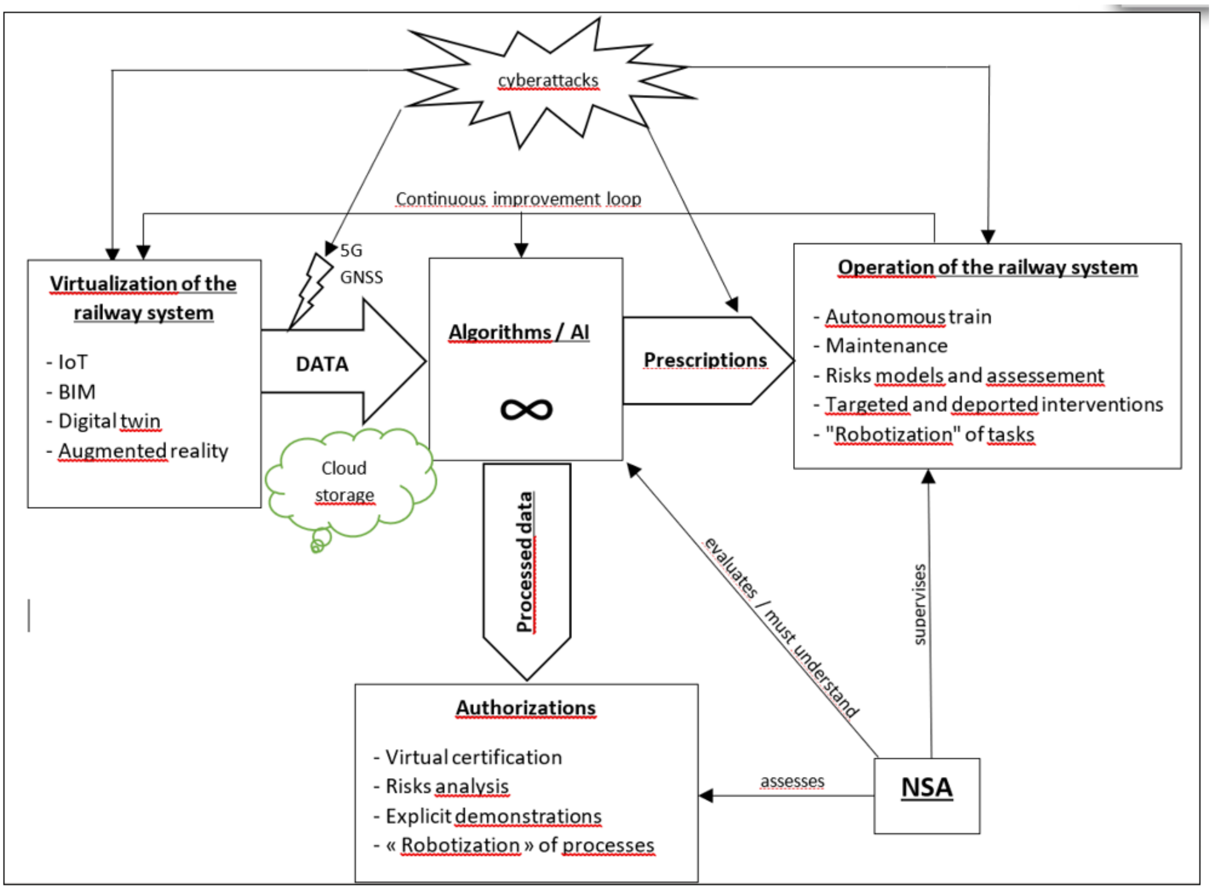
The finding is important: the regulator, like the companies of the sector, must set up a strategy around the « safety » data: inventory, collection, selection, appropriation, structuration and scheduling, use (including data available in "open data"), understanding, processing, exploitation are all actions on which it is necessary to question. The data has a value and, when used, creates value, including the value "safety". Still need to dispose of it and know how to use it!

Located in the heart of new technologies in the deployment phase, the implementation of a strategy around data is not enough: it is also appropriate to be able to appropriate the operation of the technical objects that generate them, and that adapt their behavior according to them through a learning loop. This understanding must accompany the evolution of comptrollership and be supported by strong regulatory provisions that the authority needs to build upon.

Finally, given the speed of evolution of technologies, work in community is essential, to avoid the effect of "shipwrecked digital", with on the one hand companies with significant resources to take full advantage of these new tools, and on the other hand the "small" companies that could benefit from them but can not afford them, on the understanding that the search for the best level of safety is everyone's business. This work in community could be organized in the form of a platform, without neglecting the oral exchanges which make the efficiency of the sharing during the meetings around the experience feedback organized by the EPSF.

The operators interviewed expressed their wish to have an open and up-to-date authority on these subjects in order to avoid being refused initiatives and innovations because they are poorly understood in terms of their functioning apprehended in terms of impact on railway safety.

The diagram below presents the new paradigm of a digitized railway world.


cyberattacks
Continuous improvement loop
5G
GNSS
Virtualization of the railway system
- IoT
- BIM
- Digital twin
- Augmented reality
DATA
Cloud storage
Algorithms / AI
∞
Prescriptions
Operation of the railway system
- Autonomous train
- Maintenance
- Risks models and assessement
- Targeted and deported interventions
- "Robotization" of tasks
Processed data
evaluates / must understand
supervises
Authorizations
- Virtual certification
- Risks analysis
- Explicit demonstrations
- « Robotization » of processes
assesses
NSA