Taking into account safety issues through the innovation process

Laurent CEBULSKI

Authorizations Director

Etablissement Public de Sécurité Ferroviaire (France)

Summary

The original roles of national safety authorities are regulatory in nature, and the two components of their task are checking compliance on the one hand, and checking that stakeholders understand risks on the other hand. In the case of both authorisation and inspections, these checks take place after the innovation process, where it has often been remarked that safety requirements are not adequately taken into account during the development of a new product or service. In the past, this has led to a mutual lack of understanding between actor-innovators on the one hand, who are keen to push back barriers, and the safety authority, which is responsible for checking that uncontrolled new risks are not brought into the system, and that the regulatory requirements that apply to everyone are not distorted in order to establish special cases which could potentially cause dangers. As a result, safety resulted in a time to market which was too long to allow industrialists to turn their ideas into reality.

Of course, regulation does not overshadow the concept of innovation, which is very much present in European legislation and more specifically technical specifications for interoperability, as well as the European regulation on the common safety method for risk evaluation and assessment. However, the various departments that are involved in the innovation chain (research and development, design, industrialisation and procurement, which are sometimes multi-site and multi-company) are not fully cognisant of all of the mandatory regulatory provisions, beyond strictly technical and commercial matters. The lack of applicable standards, for a disruptive innovation, can also add a certain degree of complexity to the evidence of safety to be provided, with the use of explicit demonstrations which are generally the preserve of those who are knowledgeable about operating reliability. Moreover, for actors who innovate, safety is one of a number of factors between which a balance must be struck, such as in the case of expansions or optimisation of capacity in densely-populated areas for which maintenance of the initial safety level is a prerequisite.

Introduction

The *Etablissement Public de Sécurité Ferroviaire* (EPSF), which was established in 2006, is the French railway safety authority whose role is to guarantee system consistency and safety and to contribute to the interoperability of European networks while ensuring that actors are treated fairly. Its area of intervention encompasses the national rail network (NRN).

The original roles of national safety authorities are regulatory in nature, and the main components of their task are checking compliance by way of permits and inspections, checking authorised actors' understanding of risks, and informing the sector of the applicable regulations and amendments to them.

The challenges are manifold: for different actors of different sizes and ages (35 railway companies, 15 infrastructure managers) to work well together, there needs to be strict compliance with rules which must be harmonised in order to minimise the risks associated with the design, operation and maintenance of rolling stock and transport networks.

These risks are themselves numerous and take multiple forms. A double-decker high-speed train carries 1,000 passengers at a speed of 320 km/h and weighs more than 1,000 tonnes, the "Transilien" network (Paris region) transports more than 3 million passengers daily, and a freight train can pass through several countries with 3,000 tonnes of hazardous materials in its wagons.

The need for safety is thus constant, but it must be put into perspective with other factors which are essential to the viability of businesses in the sector: availability, profitability and capacity, all of which spur them to innovate in all fields, both technological and organisational.

The gap between safety and innovation is often too large

From the point of view of a safety authority, for both authorisation and inspections, it has often been remarked that safety requirements are not adequately taken into account during the development of a new product or service, since safety and interoperability aspects which arise after the innovation process.

From the brainstorming session that is supposed to lead to innovative ideas to the process of regulatory authorisation, the large number of stages and parties involved tends to push back the analysis of the technical (or organisational) rules that apply to everyone to the end of the cycle.

Indeed, the original idea behind innovation, especially disruptive innovation, is to think outside the box, to get away from standards, or at least to forget them so as not to create any barriers to the emergence of ideas. Risks and compliance are not the priority at that time, especially if the company is operating in an international context where different standards and different rules apply to different markets.

In very broad terms, the idea that is selected gives rise to a research/development project, which includes design, prototyping, testing, and potentially industrialisation if the process leads to a definite outcome. It is then that the integration stage comes, and this gives rise to questions of regulatory obligations. And this happens too late. On the Technology Readiness Levels (TRL) scale, which has 9 levels, safety is usually taken into account at level 6 at best (which entails demonstration of a prototype

or model of a system/subsystem in a representative environment, where the risks in the environment should be understood from the first level upwards.

This can lead to a mutual lack of understanding between actor-innovators on the one hand, who want to break down barriers, and the safety authority, which is responsible for ensuring that uncontrolled new risks are not brought into the system, and that the regulatory provisions that apply to everyone are not distorted in order to establish special cases which could potentially cause dangers. As a result, safety results in a time to market which is too long to allow industrialists to turn their ideas into reality.

Innovation versus regulation: striking the right balance

Of course, regulation does not overshadow the concept of innovation, which is very much present in European legislation and more specifically technical specifications for interoperability, as well as the European regulation on the common safety method for risk evaluation and assessment. The latter invites reflection on the impact on safety of the innovativeness of a change, but it would benefit from identifying more clearly how the analysis should be conducted.

In any case, the various departments that form part of the innovation chain are not cognisant of all of the mandatory regulatory provisions, beyond strictly technical and commercial matters. It is quite rare for a research and development department to have a safety engineer who has a keen interest in regulatory matters. Furthermore, if there are no standards that apply to a disruptive innovation, this can also add a degree of complexity to the evidence of safety that needs to be provided, with the use of explicit demonstrations which are generally the preserve of those who are knowledgeable about operational safety.

Nonetheless, from the research/development phase onwards, certain questions should form an integral part of all of the factors that are considered: performance, cost, lifetime… and safety. The following questions should be considered:

- Whether the idea that is created fits into the existing regulatory framework
- Whether the product that is developed should be incorporated into a railway sub-system
- Whether the product that is developed will bring new safety risks

In other words, a preliminary risk and regulatory analysis is essential at the research/development stage.

In the light of this, EPSF has decided to narrow the gap between the emergence of new concepts and the approval of applications for safety approval by inviting the actors to talk to each other from the design stage onwards, and particularly when the risks inherent in any innovation, whether technical or organisational, are analysed. These upstream exchanges of information, which take place even before the pre-engagement phase, which is already too late, bring several advantages:

- They enable the industrialist to present its project, or even its options, so that it can obtain the external perspective of an authority which has a systemic view of the railway network;

- They enable the safety authority to be on the look-out for applications which could be complex due to the atypical nature of the proposed developments;

- They remind industrialists of the applicable regulations;
- They identify regulatory gaps, changes that may be required in the field, or exceptions that may be necessary;
- They identify new risks which are entailed by a new component or service;
- They enable the industrialist to consolidate its schedule by giving thorough consideration to safety milestones.

It should not be forgotten that the safety permit that is issued is often regarded as a technical and legal guarantee, and important evidence of trust in the relationship between a client who invests in an innovation and their supplier.

The special case of densely-populated areas

By 2050, 66% of the world's population, or 2.5 billion people, will live in urban areas. This level of population density generates impacts which are unique to densely-populated areas, where infrastructures are already heavily constrained by the intense strain placed on them and their age. In densely-populated areas, availability is the cornerstone of a system, so maintenance must be prompt and efficient, and responsiveness to safety incidents must be optimal so that impacts on operation are minimised.

So there are many potential pathways for innovation, particularly in terms of organisation: responsiveness to incidents will be all the more efficient if the operator's safety management system is robust – the most fertile area being control over the human factor, either within the company or in terms of system users.

Several incidents in the Paris region can be taken as examples:

- On 19 July 2016, the explosion of a transformer caused delays to over 500 services including 24 cancellations over a period of 9 hours, and also halted several trains due to the lack of power. This incident also resulted in passengers having to get out onto the tracks.
- On 29 October 2015, an employee of the infrastructure manager felt a big jolt while on board a passenger train. He then informed the maintenance engineer's local manager, whose teams found that two fishplates close to a switch were broken. Their intervention affected 64 services and the situation was restored to normal 13 hours later.
- On 27 July 2015, the driver of a passenger train which was moving along a line on which track renewal and ballast (TRB) works had taken place detected instability of the track. Track repair works began, and the incident affected 73 services (51 of which were withdrawn) for 17 hours.

These incidents were handled in accordance with the provisions of the safety management system of the operators who were affected, and only impacted the availability of rolling stock. However, these

incidents invite reflection on the way in which the passengers who got out onto the tracks were dealt with, the optimisation of maintenance in terms of the relationship between quality and time taken, the communication of information in emergencies, and the role of the human factor both as a cause of incidents and as a safety loop.

Innovating by considering what already exists

A unique aspect of the railway system is the indissoluble link between infrastructures and the trains that move along them. Although these infrastructures are renewed or redeveloped over time, they constitute a legacy of technology and operating practices which were built up over a period of more than a century. The multitude of technological components of different types and ages (overhead lines, switches, points, etc.) are a heavy constraint on the implementation of innovations, whether they are “disruptive” or “push” innovations, by a tier *n* supplier. The dissemination of a new development, whether it is technological or organisational in nature, should not create any special cases that overlap or substitute the existing system, be incompatible with its possible interfaces, or deviate from mandatory interoperability rules. The most current example is the implementation of the European signalling system ERTMS, the harmonisation of which is being impacted by the specific national characteristics of railway networks within the European Union.

In all cases, non-regression of the system is the rule for safety, and this tends to lead actors to tighten up their approach by distorting the general principle of “globally at least equivalent”, the premise of which is that any new system or any change to a working system must provide an overall level of safety which is at least equivalent to that of existing systems which offer comparable services. Some can lose sight of the concepts of “globality” and “system” (“globally” then becomes “locally”, and does not allow for the safety level to be reduced on an ad-hoc basis in a targeted and measured fashion insofar as this reduction is compensated for in order to maintain the overall safety level of the system. This situation generally stems from the fear that rules and historic practices which have been tested but whose reasons for implementation ceased to exist as the railway system developed will be called into question.

The safety authority as a driver of innovation

It is essential for a safety authority to take an overall view of changes in the railway system so that it can understand their impact.

In addition, through the 30,000 safety incidents that are recorded each year in its database, the safety authority is able to identify opportunities for progress and areas where industrialists and operators need to focus their efforts. It can then give impetus to the sector, or even initiate or contribute to certain research topics.

In 2015 and 2016, EPSF initiated two topics in relation to railway safety. The first, which is organisational in nature, involves creating a tool to gauge how robust operators’ safety management systems are by relying on stress tests derived from accident scenarios.

The aim of the second one, which is technical and connected with industrialists within the sector and academic actors, is to minimise risks associated with the phenomenon of train deshunting.

Other topics are being researched, including optimisation of infrastructure maintenance, in order to improve the analysis of applications for safety approval which relate to ERTMS, or the virtualisation of certain tests which are required for sub-systems to be authorised.

The emerging topics are also being discussed with the “RAILENIUM” Technology Research Institute, the purpose of which is to drive innovative projects of all kinds with the railway sector, and which is now a favoured partner of EPSF in relation to several safety-related issues.

Conclusion

Few accidents are caused by intrinsic technical failures: the human factor is dominant in all safety incidents. As a result, many innovation projects focus on the need to increase the capacity and availability of infrastructures, regulate traffic, reduce costs and standardise products. In these projects, improving safety is not an end in itself, and the maintenance of safety is a factor which is considered through the applicable regulations, often after the development process.

Safety and innovation should not stand in opposition to each other, they should complement one another. To that end, it is essential to consider risks as soon as new concepts, whether they are technological or organisational, emerge. Of course, safety and interoperability should be put into perspective with other factors which are essential for project viability: economic, societal and environmental aspects should be subject to equal scrutiny.

The safety authority, which has an overall view of the system and developments in it, and also its weaknesses due to safety incidents, must be proactive in improving the overall safety level. It has two important roles to play: on the one hand, it must act as an initiator or catalyst for research/development projects which concern safety. On the other hand, it must make actors within the system aware of the need to consider safety in their innovative projects, both by reminding them of the applicable standards and rules and also by inviting them to think as early as possible about the risks in the system. In all cases, anticipation is the key.