Written evidence submitted by Prover Technology (RTC0029)

Executive summary

- Prover Technology is a leading supplier of software products that are used for reducing effort and calendar time in development and safety approval of rail control systems. A number of railway infrastructure managers have standardized on using the company's software products for certain types of rail control systems (e.g. Swedish Rail, Norwegian Rail, freight railroad Canadian Pacific and the metros of Paris, New York and Stockholm). The products are used for rail control systems by most of the larger suppliers in on-going projects in North America, Europe and Asia.
- The schedule targets formulated by the Digital Railway pose several challenges. This document is primarily concerned with schedule challenges for track-side rail control systems (interlocking and RBC) for the Digital Railway, thus excluding challenges specific to on-board (ETCS) and traffic management (TMS).
- The Digital Railway plans to install new train control systems to increase traffic capacity. The choice to install ERTMS rather than conventional signalling technology may be the most efficient option, at least long-term, while there are many question marks related to the success of the ERTMS initiative to date, and the efficiency with which such systems can be commissioned.
- To deliver the Digital Railway, the traditional narrative for development and safety assessment of train control systems has to be abandoned. Traditional methods are too labour-intensive and time-consuming to meet the objectives and schedule for the Digital Railway.
- The processes by which new products and systems are approved for revenue service are critical for the success and schedule targets of the Digital Railway. Especially, the Digital Railway requires software-automated creation of safety evidence for new train control systems based on mathematical proof, to dramatically reduce the effort and calendar time required for safety assessment and certification of sub systems/components. This is a generic method for efficient and reliable creation of safety cases, reducing the work required to establish the safety evidence for each implementation to a minimum. Traditional safety assessment carried out by 'principles testers' constitute a bottleneck and source of uncertainty, due to differing interpretations of what is required, creating significant risks for cost increase and schedule delay.
- The success of the Digital Railway requires that modern methods are used for development and safety approval of new train control systems. This is mature technology that is commercially available, as presented at the IRSE Presidential Programme meeting on Dec 8, 2015; once non-recurring engineering work has been completed, generation of a specific interlocking including testing and proof-based safety evidence creation can be completed in just one day. This is significantly more efficient than traditional methods, which typically consume calendar months up to a year or more to accomplish the same result.

Proposals

The following proposals are intended to assist in letting go of the traditional narrative for development and safety assessment, and to achieve significant savings in cost and commissioning time in parallel with large improvements in safety. To this end, the Digital Railway should ensure that:

1. UK legislation allows for safety assessment and certification of train control sub systems to be based on mathematical proof of safety requirements, with such safety evidence being created by trusted software products.
2. Standard interfaces and safety requirements for interchangeable wayside train control system equipment (from different vendors) are established, to benefit from automatically created safety evidence based on proof of safety requirements and automated design.
3. A strong central engineering group is established to co-ordinate and maintain signalling system principle specification standards for the Digital Railway, including standard interfaces and vendor-neutral safety requirement specifications. This group's specifications should establish the design of the signalling systems, required to ensure there is one national solution for signalling and train control, with the risk of multiple variations being managed out. This group's work should benefit from modern, vendor-neutral software automation tools and practices, as well as experts in applying such modern software engineering tools and methods.

May, 2016