Report 17/2019: Loss of safety critical signalling data on the Cambrian Coast lines, 20 October 2017

On publication of RAIB's report concerning the loss of safety critical signalling data on the Cambrian Coast lines, 20 October 2017, Simon French, Chief Inspector of Rail Accidents, said:

"The pilot installation of the European Rail Traffic Management System (ERTMS) on the Cambrian lines has provided valuable experience for engineers and operators of how this system might perform when it is extended to other parts of the national network in the UK. Much of this experience has been positive, but there have been some incidents which have led to disruption to services and some, including the events covered by this investigation, which were potentially dangerous.

"The lessons that have come out of this investigation are important ones for the railway industry. It is fundamental that the process of digital design is robust enough to ensure that software-based systems are of the necessary integrity. In this case, the people operating the railway did not know that there was anything amiss. Digital railways need to detect when they have failed and report this to those who need to know – in this case the signallers.

"The safety of a digital system can be difficult to assess. A system is often made up of a number of 'black boxes' which perform particular tasks. It can be hard to know how each of these boxes really works or to fully understand their potential failure modes – particularly when the box has been bought 'off-the-shelf' or imported from another application entirely. Once our black boxes have been plugged together, do we really know how they will interact with each other, and with the human operator? Digital systems don't often breakdown – safety critical failures tend to be related to the way they are designed or the way that design has been translated into a working system.

"So, assessing the safety of digital systems is often seen as 'tricky' or 'too difficult'. That doesn't mean that we shouldn't try to master the problem. Existing industry guidance helps us by breaking the problem down into distinct steps: specification; definition of requirements; design, checking and testing; and validation against the original specification and requirements.

"How does the industry know whether it has got this process of safety assurance right? Is it fit for purpose as we move into the digital age? We are recommending that the industry comes together to develop a safety assurance procedure for its role as a client for high integrity software-based systems. This will involve learning from other industries and co-operation between many different bodies. The railway industry must not shrink from the challenges that this will present, as it will be vital for establishing and maintaining public confidence in the digital railway of the future."