

Rail Partners conference at BCRRE puts train software and cybersecurity in the spotlight

March 8, 2024



Rail Partners has hosted its first conference on fleet software and cyber security at The **Birmingham Centre for Railway Research and Education (BCRRE)**, with speakers from across the rail industry.

BCRRE, part of Birmingham University, is also home to the UK Rail Research and Innovation Network Centre of Excellence in Digital Systems (UKRRIN CEDS) which supports the rail industry as it transitions to a more connected, digital railway.

A keynote address was given by Dr George Bearfield, Director of Health, Safety and Cyber Security at Rock Rail, and former director at RSSB with responsibility for rail safety and standards.

He focused on how software has developed in rail to date, the interface between IT and Operational Technology, how rail software could develop in future and what this means for cyber security.

Rail Partners Operator Services division welcomed around 70 industry professionals to the event, which

was split into two sessions. The morning session focused on fleet software assurance, and what more can be done to ensure systems from a variety of suppliers work well together, delivering both high levels of performance and safety, while the afternoon looked at cyber security including what operators' obligations are, and what can be learned from incidents in elsewhere in rail and other sectors.

The conference also welcomed several exhibitors in addition to a BCRRE stand: Libusa Academy which helps businesses manage the evolving risks of technology and regulation through online training including on railway software safety; Modux, who offer research, software development and consultancy services in cyber security; and RazorSecure who specialise in cyber security for rolling stock, railway signalling, and infrastructure systems.

Neil Ovenden, head of engineering at Rail Partners, said: "As the trains we travel on increasingly rely on a range of software from multiple suppliers, to deliver better customer and staff on-train amenities, information and comfort, it adds a level of complexity for maintenance, safety and for security as well.

"The conference was an important moment to share best practice on managing fleets and other systems that require expertise and support from third parties. This includes making sure that every precaution has been taken to protect train software and systems from outside interference so we can continue to run one of the safest railways in the world, even as technology evolves."

Dr John Easton, Associate Professor in Railway Data Science, BCRRE, University of Birmingham, said: "Cyber security provides a unique challenge in established industries such as rail. As one of the most visible elements of the railway system, rolling stock represents an attractive target to hackers, with successful exploits likely to result in national headlines.

"Delivering an adequate response to the ever-evolving cyber risk requires to joined up response from the industry; attackers share information and so to effectively counter them, so must we.

"As an academic body working in the cyber security field, UKRRIN offers the industry a 'safe space' for sensitive discussions that might be difficult in more commercial environments. In return, UKRRIN researchers benefit from the exchange of knowledge with industry professionals on topics such as governance, and the commercial appetite for novel solutions, that enable their research to deliver real world impact in the industry.

"The digitalisation of our railways will transform our industry, providing Great Britain with a green, sustainable transport backbone for decades to come. Thanks to events such as today's, that connected future will also be secure."

Rail Partners' Operator services team produces industry guidance for its members on a range of technical issues across operations and fleet engineering, including on cyber security working practices for rolling stock.

For more information about similar upcoming events, email support@railpartners.co.uk.