

## SECURELY AVAILABLE INFORMATION

When you are using a number of disconnected systems to manage critical infrastructure, none of which talk to each other by design, you need to get information out of these systems without the risk of introducing anything nasty.



### THE CLIENT

A European Rail Network.



### THE CHALLENGE

Our client uses a number of disconnected systems to manage its signalling. These systems have been in use for some time and although they are reliable, it is difficult to interface them.

Information about the current location of trains is held within these signalling systems and is used to manage the whole signalling process. This information is extremely valuable and the Rail Network needs to extract it for reporting purposes.

The signalling systems must be unaffected by this extraction – they are essential for both the efficient running of the rail network and for the safety of passengers and crew. Any solution developed must be able to guarantee that nothing can be changed within the signalling systems using the connection that is created in order to extract the reporting data.



### THE SOLUTION

The solution we developed and configured featured a set of Nexor Data Diodes to solve the challenge.

Information from the trains is already captured on the signalling network as the train passes through the area it controls. This information from the signalling network is then sent to a server that is part of the same secure network.

This (signalling network) server is connected to a second (management) server in a different network using a Nexor Data Diode. This guarantees that data is physically only permitted to flow in a single direction, thereby enabling secure data transfer, as no data can go back into the isolated signalling network.

For each individual secure signalling network a combination of an initial server; a data diode; and an additional (destination) server was configured; with the destination server in each case being part of the same (management) network. Information can then be stored and processed on the management server, as needed, by the Rail Network.



## TRUSTING THE SOLUTION

Nexor developed the solution using our accredited professionals, CyberShield Secure® methodology and industry-leading SIXA® technology portfolio.

Using a data diode in the connection between the systems allows information about the trains to be passed to the management network, secure in the knowledge that it is physically impossible for the same connection to be used to modify signalling information or to introduce any malware.

The Nexor Data Diodes are assured to the highest Common Criteria Evaluation possible: EAL7+.

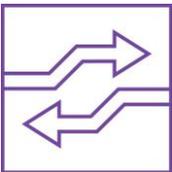
Our staff development programme is aligned to the Skills Framework for the Information Age, SFIA, the industry's most widely adopted and relevant best-practice benchmark for IT skills, training and development.

Our CyberShield Secure® process framework is underpinned by a secure model that builds in trust throughout the whole production process not just in the components. We follow industry best-practice and have the accreditations to prove it. We hold TickITplus, Cyber Essentials, ISO 9001, ISO 27001 and Investors in People Gold.



## THE IMPACT

Useful management information from the secure systems can be accessed and collated without the need for staff to physically visit and connect to the various domains. This has provided significant time and cost savings for the Rail Network.



## NEXOR CAPABILITIES

Nexor provides solutions to get information in to and out of secure networks. This enables organisations to perform more efficiently and effectively. The connection of secure networks is achieved by using people, process and technologies that align to best cyber security practice established by national authorities.