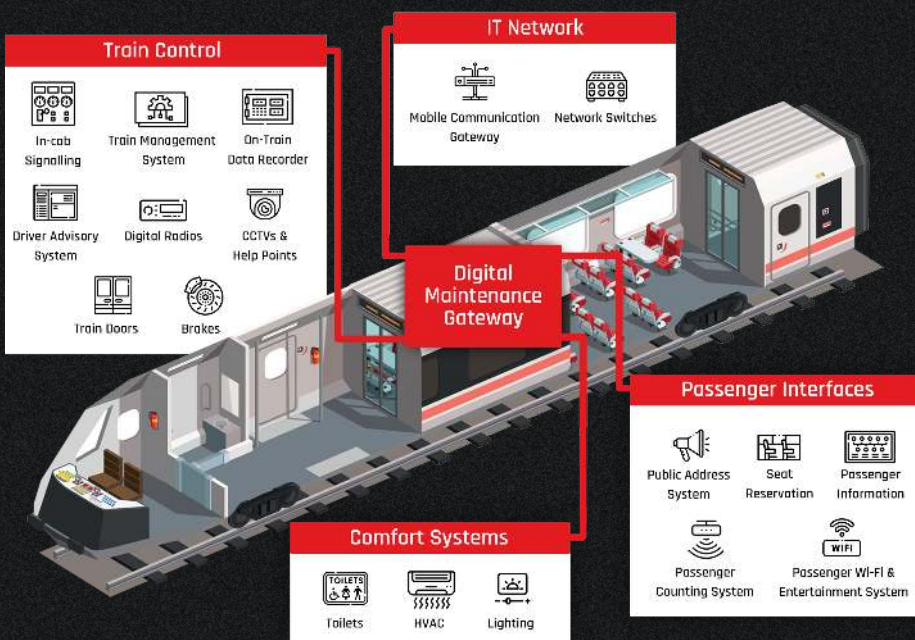


Reduce maintenance time and cost, and enhance cyber security.

RazorSecure's Digital Maintenance Gateway is an Access Control solution that adds multiple layers of security to the process of updating on-board and wayside systems. It improves security and saves time and money by enabling remote updates and making the update process more efficient. A dedicated system is deployed on-board the train that provides a managed point of access and a secure environment to run maintenance applications, eliminating dedicated service laptops.

The RazorSecure Digital Maintenance Gateway (DMG) is designed to meet the maintenance requirements of modern digital trains by enabling engineers to complete tasks quickly and efficiently through automation, reducing the potential for human error and eliminating dedicated service laptops and USB sticks. The DMG is a comprehensive digital maintenance solution, hosting software maintenance tools and updating files. Engineers login to a familiar and consistent working environment with update files that they need to complete their tasks and remote assistance from skilled engineers at the click of a button. Through a direct integration with the train systems, the DMG enables secure local and remote access, with unique credentials for each engineer and Multi Factor Authentication support. Remote access can be provided through a direct LTE connection or through existing connectivity solutions. The DMG enhances our portfolio of holistic cyber security solutions for rolling stock, helps meet IEC-62443 cybersecurity standards and provides a secure, modern user interface to engineers.



BENEFITS

AUDIT ACTIVITY

Full monitoring and traceability of maintenance activity improves compliance, captures learning outcomes and allows quick diagnosis of issues.

USE RESOURCES EFFICIENTLY

A faster update process and controlled distribution of firmware & configuration files means less time in the depot and fewer operational issues due to configuration mismatch.

CONTROL ACCESS

Identify users connecting to the on-board network and authenticate them securely with unique credentials, preventing anonymous or unauthorised access.

REDUCE MAINTENANCE COST

Eliminate reliance on specialist electronic tools, freeing up skilled maintenance staff to work more effectively and deploy updates faster.

ELIMINATE CYBER VULNERABILITIES

Isolate service laptops from potentially insecure on-board systems, remove the use of USB sticks, prevent addition of unauthorised applications or malware.

KEY CAPABILITIES

SECURE REMOTE ACCESS

Remote access is limited to authorised engineers who may only connect to specific assets in an agreed time frame. Local access is possible via a physical network interface.

SECURE DIGITAL ENVIRONMENT

Engineers interact with existing maintenance applications in a familiar desktop environment. Every session starts in a clean state ensuring users cannot add applications or malware.

ACTIVITY MONITORING

Monitor user activity to improve compliance, capture learning outcomes, quickly diagnose and fix issues, and improve maintenance processes.

FLEET-WIDE FILE DISTRIBUTION

Files for digital maintenance are centrally managed, checked for integrity, and synchronised to an on-board file store, making them available on the vehicle at the point of use.

TASK AUTOMATION

Repetitive or manually intensive maintenance processes can be automated. Updates can be performed in parallel on several train units at the same time.

USER AUTHENTICATION & AUTHORISATION

Identify individual users and authenticate them securely with unique credentials, preventing anonymous access and providing full traceability & auditing of user sessions.

FLEXIBLE DEPLOYMENT

Deployed on an EN50155 edge compute platform or virtually, with managed IP connectivity to on-board network and wayside services running on customer on-premise infrastructure or hosted by RazorSecure.

LIMIT EXPOSURE OF ON-BOARD SYSTEMS

Isolate laptops from potentially insecure on-board systems, substantially reducing the cyber attack surface.

RAZORSECURE APPROACH

We recognise that each train fleet is different and requires a holistic approach due to differences in system and network architecture. By understanding your cyber risks, we can advise on security best practices and appropriate risk mitigations. We will then work with you to design, integrate, homologate and deploy the RazorSecure solutions as appropriate. Our flexible approach is customised to manage the unique challenges and requirements of each customer. We will work closely with you to find a solution for any challenge you may have. The first step towards improved cyber security is simply to begin a conversation with us, and our team will be happy to guide you through the process.

