Case Study | Intelligence on Wheels

Making Rail Travel Safer with a CodeMeter-Protected Collision Avoidance System

TrainCAS, the collision warning system developed by Intelligence on Wheels (IoW), helps save the lives of rail passengers with a smart three-pronged safety solution. The groundbreaking technologies built into the system and the potential for criminal misuse make security, but also IP protection a paramount concern.

The Challenge

The TrainCAS system is a case study in cyber-attack prevention, IP protection, and licensing needs: A sophisticated hardware, software, and data combination that not only has to be protected against threats from hackers or other malicious actors for safe and secure rail travel purposes, but also against undue attention and exploitation by competitors, less ethical users, or simply overly curious third parties. In the railroad industry, a model of robust engineering and regulatory oversight, solutions for safeguarding intellectual property and software license management must navigate the technical landscape and stringent mandates, especially considering the sector's key role in today's mass mobility infrastructure.

The Solution

IoW opted for the proven CodeMeter IP protection and licensing technology with its impressive track record of providing security-by-design solutions for critical infrastructure. A combination of AxProtector and CodeMeter Core API helps encrypt and protect the bespoke embedded software. CodeMeter Cards (CmCards), chosen for their robustness against interference and reliability at high temperatures, act as the license containers limiting access to the software and data such as trackmaps and as safe havens for running the crypto code.

The Result

With a keen focus on "security-for-safety", IoW has selected CodeMeter for its proven hardware reliability. Integrated directly into the TrainCAS system, the CodeMeter CFast cards provide advanced hardware cryptography. These secure modules are essential for ensuring that both software and critical trackmaps are accessible only with the correct licenses, effectively preventing unauthorized code execution. During operations, sensitive code is decrypted only momentarily as needed. Furthermore, train data exchanges are reinforced with cryptographic signatures from the private keys stored on the CmCards, which, while inaccessible to unauthorized users, allow for widespread public verification. This system guarantees the authenticity and integrity of the data. In a significant technological stride, IoW has integrated an Android-based platform into this architecture. Utilizing CmCard/microSD, this new addition adheres to the same rigorous security protocols, marking a substantial progression in developing secure and interconnected rail ecosystems.

Dr. Thomas Strang
CEO, Intelligence on Wheels GmbH

"For us, security-for-safety has two meanings: protecting the IP that makes our business possible and protecting trains out on the tracks against cyber-attacks. Working with our likeminded partners at Wibu-Systems was a pleasure, and holding the CodeMeter hardware in my hands gives me the same feeling of reassurance I get when I see our TrainCAS systems in action."

intelligence on wheels

The Company

Intelligence on Wheels was born in 2012 as an offshoot of Germany's aerospace pioneers DLR with the mission to commercialize its advanced train collision avoidance systems. With three core elements – train-to-train communication, track-selective self-localization, and situation analysis and decision support – its TrainCAS systems lift railroad safety to a new level and is already being used by train operators in Germany, Czech Republic, Italy and elsewhere.

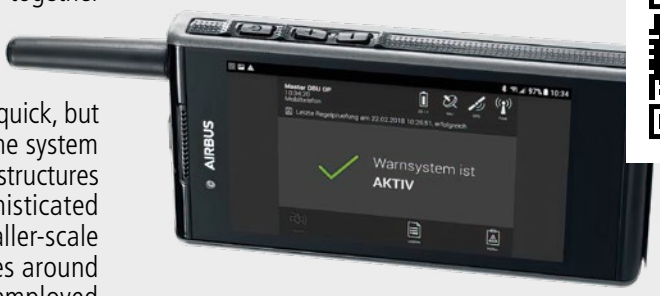
TrainCAS Secured: IoW's CodeMeter Shields Rail Tech from Cyber Threats

Rolling stock collisions are among the rarest, but also the most dramatic and certainly the most newsworthy of accidents and disasters in modern rail operations. Unlike the more common collisions with road vehicles at level crossings or other objects on the track, and unlike cases of trains coming off the tracks where pure chance or catastrophic technical failures are easily identified culprits, train-on-train collisions can come down to a vast variety of factors from human error to hardware or software malfunction.

In the hybrid world of rail transport, combining almost two centuries of legacy infrastructure with cutting-edge technology and record-breaking performance, rail operators must contend with a mix of modern, interconnected rail operating systems, tracks and rolling stock with decades of working life already behind them, and a vast variety of rolling stock on their lines at the same time. This is where Intelligence on Wheels, an offshoot of Germany's pioneering aerospace innovators DLR, comes in with its collision avoidance system. As three-pronged solution, TrainCAS brings together train-to-train communication, accurate self-localization, and situation analysis and decision support systems to empower rail operators and their staff on the ground to keep their trains running routinely and safely or to make quick, but well-informed decisions to avoid impending collisions. The system is designed to work alongside established rail safety infrastructures and is particularly suited as an added and more sophisticated safety system for modern regional routes as well as smaller-scale operators that have to engineer their routes and services around complex, often single-track lines. It is already being employed by regional rail services in Germany, as a common denominator in the heavily regionalized, diverse Czech rail landscape, and elsewhere.

With a system whose raison d'etre is protecting the lives of passengers, technical and IT security means more than in most other cases. For its principle of "security-for-safety", Intelligence on Wheels places equal emphasis on the reliability of its safety systems as it does on the security of its IP and the system's protection from tampering and sabotage. This is why Intelligence on Wheels turned to Wibu-Systems for its award-winning CodeMeter technology to encrypt and protect its software and provide the hardware-based cryptographic security components to be built into the TrainCAS onboard techno-logy in the field.

Cooperating with Intelligence on Wheels meant crossing new frontiers for CodeMeter. The unique nature of the rail world with its heavy-duty facilities operating under some of the toughest conditions imaginable, the usual CodeMeter hardware had to be adjusted specifically to these new requirements, such as high-temperature usage. Thanks to its robustness to accommodate the up to 10W transmit power of the TrainCAS train-to-train communication, CmCards were selected as license repositories and safe havens for executing the crypto code during runtime for added protection against hackers and overly curious users. The solution required further labor-intensive adjustments, but produced a tough and particularly tamperproof hardware that is built into the onboard TrainCAS systems. It fits with the entire design philosophy of the TrainCAS system, whose latest expression is a ruggedized phone for provable and uncompromised train-to-train and train-to-trackwork data exchange, designed by Airbus to work reliably even under adverse conditions.



The TrainCAS software and the constituent trackmaps that enable highly reliable situation detection in the first place are secured by a combination of AxProtector and CodeMeter Core API, chosen specifically to match the mixed embedded systems used by Intelligence on Wheels. This prevents both unauthorized use by unlicensed users and tampering, intentional or unintentional, by people trying to manipulate the system. Each fragment of code is decrypted within the CmCards on the fly and only when it is actively needed, which makes any attempt to physically access the systems worthless for hackers, unethical competitors, or simply techcurious users. Protecting critical infrastructure against cybersecurity threats, securing IP against theft, and creating a new business model for safety services: TrainCAS by Intelligence on Wheels shows the abilities of CodeMeter in action.

About Wibu-Systems:

Wibu-Systems is a global leader in cutting-edge cybersecurity and software license lifecycle management. We are committed to delivering unparalleled, award-winning, and internationally patented security solutions that protect the intellectual property embedded in digital assets and amplify the monetization opportunities of technical know-how. Catering to software publishers and intelligent device manufacturers, the interoperable hardware and software modules of our comprehensive CodeMeter suite safeguard against piracy, reverse engineering, tampering, sabotage, and cyberattacks across mainstream platforms and diverse industries.

WIBU-SYSTEMS AG | Zimmerstrasse 5 | 76137 Karlsruhe, Germany
Tel.: +49 721 931 72-0 | sales@wibu.com | www.wibu.com