PROTECTRAIL

White Paper

Key Lessons for the Railway Sector
on PROTECTRAIL Security Architecture

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 242270

Abbreviations

CAP	Common Alerting Protocol
CBRNE	Chemical Biological Radioactive and Nuclear Explosives
CMS	Crisis Management System
DPWS	Devices Profile for Web Services
EDA	Event-Driven Architecture
EDGE	Enhanced Data Rates for GSM Evolution
eSOP	electronic Standard Operational Procedures
GPRS	General Packet Radio Service
GUI	Graphical User Interface
HSPA	High Speed Packet Access
ICT	Information and Communications Technology
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
LCIM	Levels of Conceptual Interoperability Model
LTE	Long-Term Evolution communication standard
MPLS	Multiprotocol Label Switching
NTP-server	Network Time Protocol server
ONVIF	Open Network Video Interface Forum
RTP/RTSP	Real Time Streaming Protocol
SOA	Service-Oriented Architecture
SOCC	Security Command and Control Centre
UTC	Coordinated Universal Time
VPN	Virtual Private Network
WS Notification	Web-Services Notification specifications allowing event-driven programming between web services

© José Pires/UIC

SECURITY IS A CORNERSTONE OF ANY SUSTAINABLE MOBILITY POLICY AND MOBILITY SYSTEM. MAKING RAIL TRANSPORT SECURE IS COMPLEX AS IT MUST BE OPEN AND ACCESSIBLE AND ENABLE AN EFFICIENT FLOW OF PASSENGERS AND GOODS. AT THE SAME TIME, A RAIL, LIKE ANY OTHER TRANSPORT SYSTEM, FACES A BROAD SPECTRUM OF THREATS, RANGING FROM LOW-PROBABILITY-HIGH-IMPACT EVENTS (E.G. TERRORIST ATTACK) TO HIGH-PROBABILITY-LOW-IMPACT (E.G. VANDALISM) THAT MAKE DIFFERENT SECURITY TECHNOLOGIES NECESSARY (E.G. CHEMICAL SENSORS, INTRUSION DETECTION SYSTEMS, VIDEO MANAGEMENT SYSTEMS). THIS LEADS TO THE CHALLENGE OF INTEGRATING THE VARIOUS SECURITY TECHNOLOGIES INTO A COHERENT AND EASILY MANAGEABLE SYSTEM.

The PROTECTRAIL consortium and its 29 members, consisting of railway operators, railway manufacturers, security technology providers, research organisations, and major railway associations, came together to improve railway security in the light of the challenges outline above. PROTECTRAIL objective was to integrate the growing influx of security technologies into rail operations and make them interoperable to improve security. For this reason, PROTECTRAIL designed an *interoperability framework* built on a system-of-systems approach.

This is a modular architectural framework into which asset-specific and interoperable security solutions can be “plugged”, giving operators and infrastructure managers the possibility to continuously adapt their security systems to the changing security needs with minimal non-recurring engineering costs.

This framework basically consists of a set of rules and standards which facilitate the integration and communication amongst various security technologies. It is based on three key ideas:

1. interoperability is improved through standardisation,
2. re-use of existing and relevant international standards is preferred,
3. simplicity is key to long-term adoption.

PROTECTRAIL tested this interoperability framework during field demonstrations concentrating on four priority facets: Event-Driven Service-Oriented Architecture, Network Communications, Video Management, and Security Technology.

In the course of PROTECTRAIL it became clear that security systems need to be designed in a future-proof manner. For this to happen, the operator or infrastructure manager implementing a security system must devise a security master plan that contains fundamental ICT principles and an overarching IT architecture. *This master plan should not focus on what technology to deploy but on how to deploy it*.

It also became clear that railway security will be enhanced if the multitude of actors in the field will adopt international interoperability standards for security. The rail sector today includes various independent actors. Until these international standards are promulgated, railway security actors should not adhere independently to the principles of this White Paper but also agree on a common implementation.

The following will give an outline on the lessons learnt during the PROTECTRAIL project.

The PROTECTRAIL approach and its reusability

PROTECTRAIL based its interoperability framework on design patterns which are successfully used in other industries. These include the following elements:

- A reusable **Service-Oriented Architecture** (SOA);
- An **Event-Based Architecture** for data exchange between various security components and decouple the components from each other;
- Reusing of well-established and proven **standards** which reduce the non-recurring cost of software integration;
- Planning of an **extendable** architecture for the future to extend the framework with upcoming standards;
- Building **modular** components with web services;
- Supporting **discoverable** components to reduce the configuration effort and improve the reusability;
- Building on an **IP network** (cabled or wireless) which is dimensioned to support consistently the **video surveillance streams** necessary to assess, confirm and investigate security incidents.

Figure 1: Interoperability Framework: a design pattern to integrate the capacities
Basics of the interoperability framework

Event-Driven Architecture (EDA) consists of numerous event producers and event consumers from various locations and various stakeholders of public transport operations. Security **sensors and devices** from on-board and wayside (i.e. sensors and devices like CBRNE detectors, intrusion detection, laser scanners and devices like video cameras and recorders, person tracking) send events ranging from basic alerts with limited environmental information to more complicated alerts with various information and resource fields which are vital for a better understanding of the situation on the ground. These sensors and devices are called event producers.

PROTECTRAIL identified the need for a common **Event Format** which includes location (and in all probability the affected area), absolute occurrence time (in UTC), a unique event identifier and type, attached resources as well as source and contact information. PROTECTRAIL chose the Common Alerting Protocol (CAP) of OASIS as the best existing standard for the public transport sector. The OASIS specifications define a data model for a wide range of applications like safety, security, health, weather and environmental threats, telecommunication and cyber security. PROTECTRAIL adopted the XML Schema representation of CAP to implement the event providers and consumers based on that standard.

The proposed event format inherited the following CAP standard features:

- Multi-operational and multilingual messages;
- Three dimensional and flexible geographic description;
- Message update and cancellation;
- Links to further information such as images, reports and videos.

Today CAP is used extensively for weather and earthquake warnings in public and commercial Emergency Alert Systems like Google Public Alerts; it remains to be endorsed by the international security standards.

Interoperability relies on both, a common data model and shared representation. **Shared representation** is important for all stakeholders to collaborate based on the same information assets. It starts with the same wording, shared facility information and ends in common geographical maps.

For a reliable message interchange, PROTECTRAIL recommends the implementation of the **Event Broker** as key element in the interoperability framework. PROTECTRAIL used the Eventing Framework specification **WS-Notification** which can contain any type of XML data format. A **Message Server** manages all incoming and outgoing messages and can deliver and handle high performance, clustering, transactions and a wide range of cross-language clients and protocols. If an event consumer is not available the message server can store undelivered messages and retry delivery out of a message queue. The PROTECTRAIL implementation of the event broker was based on the most popular open source message server, called Apache ActiveMQ, and supported three different data structures for events, namely the **Common Alerting Protocol** (CAP), a project specific resource and the ONVIF format.

In future, new event frameworks and data structures can be **easily extended**. This is normally done by adding new web service endpoints. Endpoints are unique URL's for providing public accessible and reusable Web Services which can be used for service composition and orchestration.

The role of the **Security Command and Control Centre (SOCC)** is to ingest and correlate various event sources into a single platform and thus improves the situational awareness among those persons that need to work with the information, for instance security operators or first responders. Several SOCC's can share a situation and cooperate. Typically such a system visualises the events in a GIS map and shows related video cameras, recorded videos and it provides operational and security related procedures. Simple events can be correlated to a major incident which means that the event contains additional information on for instance a responsible person, severity, certainty, and urgency. The SOCC system helps the operator in his daily work to suppress nuisance alarms, to group similar alarms, and to relate the event with other information and sensors. The SOCC guides the operator through a stressful situation through electronic Standard Operational Procedures (eSOP). These procedures are programmed today but can be executed as a graphical business process in the future. To allow for a continuous improvement of the eSOPs during operation, the decisions and actions of the operator can be recorded. With such a system the operator can be trained with simulated operational situations.

A Crisis Management System (CMS) is a solution to manage a crisis with various responders and any class of requested stakeholders. A CMS has to handle multiple operators, transportation modes and locations. A crisis manager has to act and make decisions based on all available real time information. This information can come from external experts and external media types like news feeds, live and recorded, as well as fixed and mobile video that need to be integrated. As situations evolve, hand-over from CMS to CMS may prove to be necessary.

In PROTECTRAIL the information abstracted from the events was standardised, processed and eventually disseminated by the SOCC and the CMS to passengers and other relevant stakeholders using various sources like **Passenger Information Displays and Announcement Systems**.

© Philippe Fraysseix

The flow of information follows the process depicted in Figure 2.

Figure 2: Participants in a global security context

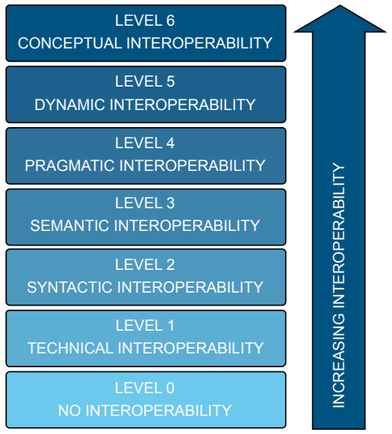
PROTECTRAIL is only at the beginning of a process which will require further standardisation, but the proposed interoperability scheme is prepared to integrate upcoming standards which have been identified, such as: for investigations ISO22311, for IP-based security products like ONVIF Profile S (a subset of IEC 62676), or IEC 62580-1 for on-board embedded devices based on DPWS.

Enabling security solutions

The challenge of combining a large variety of technological and procedural security solutions lies in the technical integration of the various systems and in the ability to combine the strength of these devices in a global and coherent system. This section provides theoretical background information on interoperability.

The PROTECTRAIL approach allows for technical, syntactic and semantic interoperability of the different systems as defined in the Levels of Conceptual Interoperability Model (LCIM):

- Technical interoperability is achieved using standardised common communication protocols in order to exchange data between the participating systems,
- Syntactic interoperability is achieved using a common data model such as the Common Alerting Protocol (CAP) of the Oasis Consortium in the PROTECTRAIL demonstration and
- Finally semantic interoperability is achieved by defining the content of the information exchanged in restricting the data model used.



In order to achieve a higher level of interoperability, shared methods and procedures are required in order to efficiently use the available information in the context of a security incident. With this goal in mind, Security Operation Control Centre solutions from different partners can be integrated in a global security system.

These control centres actively share contextual information during the development of security incidents using the interoperability framework and also apply predefined and agreed security methods and procedures in response to the different security threats. These procedures and methods can be applied separately in the different security control centres hence providing a high level of interoperability between such heterogeneous systems.

Future implementers may benefit of the lessons learned from PROTECTRAIL:

- Interoperability is to be achieved block by block and needs to be built on strong foundations; technical interoperability is not enough to guaranty system level interoperability.
- The use of open standards or documented norms facilitates the adoption of an interoperability framework, especially when a large number of partners with different objectives are involved.
- The end-user of the system should be involved in the definition of an interoperability framework in order to achieve high level interoperability.
- Real interoperability can only be achieved if all actors in railway security can agree on a common implementation of security interoperability standards.

Network communication

Providing diversified railway security and infotainment applications, including video surveillance, voice communications, system maintenance, e-booking, and other broadband services, mandates high a quality IP-based Ethernet network. While wired networks are already mature enough to support these applications, wireless networks have proven to be a challenge due to the non-deterministic nature of radio signals when the train moves at high speed.

PROTECTRAIL HAS PROVEN THE IMPORTANCE OF A STATE OF THE ART NETWORK ARCHITECTURE FOR RAILWAY SECURITY APPLICATIONS. IN LINE WITH THE GENERAL REQUIREMENTS FOR INTEROPERABILITY AND MODULARITY, PROTECTRAIL CONFIRMED THAT THE VISIBILITY OF TRAIN AND OTHER RAILWAY FACILITIES CAN BE IMPROVED USING VARIOUS SECURITY APPLICATIONS. THESE APPLICATIONS REQUIRE HIGH BANDWIDTH BI-DIRECTIONAL COMMUNICATION LINKS TO BE ABLE TO EXCHANGE MESSAGES WITH EACH OTHER.

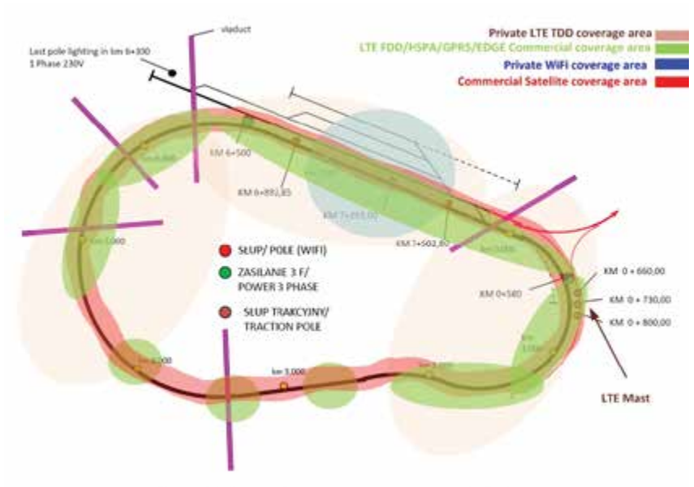


Figure 3 Wireless Coverage on the test track in Zmigrod

PROTECTRAIL members installed various security solutions with many geographically distributed data collection points, both stationary and mobile. These capacities were connected via various communication channels such as high speed optical networks, coaxial cables, and wireless links. The data collected from various sources were preserved with full consistency by using NTP-based time synchronisation with geo-location.

When designing a network for on-board and wayside applications, the following best practises should be considered:

» Train to wayside communication links form a crucial subsystem in delivering diversified railway security and infotainment applications on-board. Delivering such a communication subsystem and fulfilling the QoS requirements of a broad range of applications is always going to be a challenge. PROTECTRAIL succeeded in showcasing a multi-modal Train to Wayside Communication System (TWCS), using various modern wireless technologies. This TWCS make use of existing commercial telecom infrastructure (i.e. LTE, HSPA+, HSPA, etc) and optionally, it combines these networks with private wireless technologies (i.e. 802.11 n Wi-Fi). As it provides redundancy between commercial and private network it increases the end-to-end throughput by combining both networks when available.

» For real-time video streaming, a case by case trade-off between UNICAST and MULTICAST must be made. While UNICAST may be beneficial when there is only one or few consumers, MULITCAST helps preserve scarce bandwidth when there are multiple consumers scattered over different locations. An on-board Network Video Recorder (NVR) server with MULTICAST streaming feature could be used. Adaptive variable bit rate streaming could also be beneficial for preserving scarce bandwidth but there is no mature solution due to a lack of standards.

» Cyber security is of growing importance for the railway sector. The railway industry needs to establish security standards and best practices for information security management like the ISO 27000 series. In this context security technologies like VPN for secure collaboration in distributed locations and MPLS for high-performance routing in large networks and redundant network connections in case of a failure or an attack, virtual LANs for a secure segregation and guarantee a quality of service for safety related applications.

Figure 4 Cyber security for the railway network

Modern and practical approaches to video and video-based analytics


© José Pires/UIC

In line with the general requirement for interoperability and modularity stated above, PROTECTRAIL integration confirmed that the sole implementation of the video-surveillance industry standards (IEC 62676-1&2 and even ONVIF profiles) is not enough. This is further complicated by the regulatory need for stability and trustworthiness as well as privacy protection imposed on security video systems.

The lessons learned from PROTECTRAIL are recommendations for:

- A generalised use of RTP/RTSP streams carrying video H264 compressed metadata time stamped at the frame level, consistently with the security events described above
- Full modularity of the basic services associated to video, independently of their physical implementation
- Video-surveillance systems are networks of distributed PC's; as such they are potential targets of cyber-attacks, against which they must be protected (physically, by training staff or with software)
- Digital video, especially when live information with low latency is required, has stringent needs for communications channels (no buffering is allowed); this implies a good quality of service for the communication but also an optimised set-up in the network architecture to minimise throughput at any point of the network in all circumstances (typically a case by case trade-off between UNICAST and MULTICAST)
- The system must preserve full consistency between time and metadata associated with the streams, the events produced by the analytics (see below) and the supervision tools.
- By law the operators generally cannot access the recorded video files for **privacy protection** reasons. If the operator wants to use the video for operational security or training, they have to remove the privacy related attributes for instance by using face blurring.
- If the control centre wants to access the on-board videos in real time, the infrastructure is not prepared to get a constant video streams today. ONVIF and RTSP are made for networks with a constant bitrate. For videos streaming on wireless networks the solution is an **adaptive bitrate** for video streaming depending on the existing wireless infrastructure.

Several video analytics solutions have reached a reasonable level of maturity, such as:

Video tracking:

Video tracking is the process of locating an object (or more than one) that moves in time, using a camera. An algorithm analyses the video frame and gives as output the position of the target objects. The main difficulty in video tracking is to capture the correct position of targets in consecutive frames, especially when objects see their aspect change over the time and move at a higher frequency than the frame rate. Semi-automatic tracking is a tool provided to video-surveillance operators to support them in doing more efficiently a task performed today manually, after appropriate training. This function can be activated locally for benign events, but can also be run at the security control centre in real-time in case of more complex situations, before the situation is handed over to the police, or after the event to help selecting the appropriate video sections requested by the police for forensic investigations.

Crowd Detection:

Crowd density detection provides information that may be relevant for safety. It is also a key parameter for making the right decisions in several security-related crisis situations. It must be noted however that in many large cities crowds as such are not considered a situation critical to detect for security reasons. Similarly multiple individuals collapsing in a station must be detected to confirm a chemical attack in a given area.

Face recognition:

A face recognition system is a biometric technology which is well-accepted by the population as it is close to a human recognition process and is almost non-intrusive. Therefore, many systems include biometry in order to identify or confirm the identity of a person. Nevertheless, this technology may be difficult to implement as it is sensitive to many variations (aging, facial expression, lighting, face orientation, beard, hair, clothing, etc.).

Intrusion detection:

To detect objects existing in restricted areas, it is necessary to extract objects in video frames. Object extraction consists of background generation, configuration of region of interest (ROI), extraction of object candidates based on background subtraction and contour labelling, noise elimination, and calculation of object information such as size and position. Algorithms of intrusion detection can help in:

- Detection of persons in areas that are supposed to be empty;
- Perimeter anti-intrusion (including in-service tracks);
- Graffiti prevention.

Regarding such analytic applications, the lessons learned in PROTECTRAIL are recommendations for:

A minimum configuration required for analytics: For example many analytics require an initial calibration for each camera (e.g. to determine its 3D location and orientation or to adjust to internal lighting conditions). To make larger setups (50+ cameras) manageable it is recommended to either automate these calibration procedures with sufficient quality or to use solutions that do not require such configuration.

Using analytics for decision support and not as fully-automated security solutions: Complex systems are never 100% fail safe or fail in unexpected conditions. An interactive system provides functionality to support an operator who is the human-in-the-loop.

Metadata standardisation: Full consistency for video analytics remains an open issue as there are no well-established industry standards and video analytics are a quickly evolving market. Maintaining consistent metadata definitions will require attention when solutions are integrated, especially when a new solution needs to fit into a legacy system. In this situation, the most future-proof approach is to stick on the minimum criteria for events outlined above and rely on associated URLs for details.

Wider system (e.g. Storage/Playback/GUI/other) requirements: Video analytics usually need more performance or have wider requirements than basic video solutions. Some analytics require for instance high frame rates/high resolution playback of stored data instead of a lower resolution, lower frame rate data. Other analytics might need an extra monitor because they require certain user interactions or provide information that cannot be displayed on a video stream. It is recommended that the video-surveillance systems that might be extended at a later time with analytics are designed for upgrade, typically to support analytics (e.g. room for servers or extra monitors, etc.).

In addition to the real-time (or near real-time) solutions described above, collected videos must be usable for forensic analysis. This implies minimum video quality (sometimes mandated by law), proper and unambiguous identification of the scenes, time of occurrence and the ability to be decoded by police systems. ISO 22311, recently promulgated, addresses these requirements.

PROTECTRAIL also recognises that video-surveillance can be extremely useful for security management and crime investigation, but that it also might result in an unnecessary intrusion into citizen privacy. When video surveillance is used a balanced guided by regulations complemented by common sense needs to be struck.

Conclusion

Looking back at four years of PROTECTRAIL, it becomes clear that PROTECTRAIL was not a security project like others but an integration project. The objective of PROTECTRAIL was to define a security system and reach a level of standardisation for ICT in rail that has already been achieved in other industries. The methodology for the integration of security technologies has worked and shown to be adequate to the scope, efficient, scalable and able to evolve in time thanks to its simplicity, non-proprietary nature and standardisation. It can accordingly be recommended for new systems. It is important to note that the integration of security technologies in the railway sector is difficult but achievable even within the current European and national legislative framework and with existing standards.

Key lessons of the security architecture recommended by PROTECTRAIL are:

- with the minimum set of information available in an event (time, nature and geo-location) together with smart services like discovery it is possible to efficiently and flexibly manage situational awareness in both fixed and mobile security applications;
- the SOA-based architectural framework and the information content of the standard events are much more important than the SOA tools to implement the framework and the envelope that contains the event (concepts and information are resilient to evolution, changes or obsolescence of information technologies tools and solutions);
- the seamless resilient integration of different wired (Ethernet and MPLS) and wireless (LTE, ZigBee, WiFi) communication technologies has proved to be a key success factor.

© José Pires/UIC

By establishing standardised events and SOA principles in security and rail infrastructures, the industry achieves a better interoperability, and the time to integrate new security solutions, the cost to develop and test new solutions is reduced drastically, and security stakeholders understand each other during security events and crisis situations.

If implemented in the railway sector, the PROTECTRAIL results will help the rail sector to advance and to catch up with security in other fields. In the railway sector too security needs to be approached in a comprehensive and coherent manner and must be based on a system that is able to integrate new security solutions, be it to minimise the risk of a terrorist attack or reduce costly everyday forms of crime such as metal theft. When looking further into the future however it becomes evident that PROTECTRAIL can only be a first step. Slowly but surely the ICT world is moving towards an “Internet of Things” and the railway sector needs to be part of this development.

As always when discussing security it must be kept in mind that even though security is a fundamental value in our society, it does come with economic costs (for investment, deployment, operation and maintenance) and social costs, in terms of potentially reduced freedom and privacy for citizens. When prioritising one over the other, a careful balance needs to be struck.

All in all, PROTECTRAIL with its future-proof methods and recommendations is clearly a success for the railway sector and the European Commission can be thanked for the efficiency of its financial commitment. PROTECTRAIL will help railway transport play an irreplaceable role in mobility by making it even safer against petty acts of vandalism and sophisticated terrorists attacks. This is particularly important during a time when the complexity in the sector grows due to new technologies and new and more actors.

Name: PROTECTRAIL
Grant Agreement Number: 242270
Total Cost: EUR 21,775,289
EU Contribution: EUR 13,115,064
Start Date: 1 September 2010
Duration: 46 months

Coordinator:
Ansaldo STS S.p.A.
Via P. Mantovani 3-5 | 16151 Genova, Italia

Coordinator contact:
Vito Siciliano
T: +39 010 6552976
E: vito.siciliano.prof110@ansaldo-sts.com

Dissemination contacts:
Marie-Hélène Bonneau
T: +33 1 44 49 21 43
E: bonneau@uic.org

Jan Steinkohl
T: +32 2 626 12 69
E: jan.steinkohl@unife.org

The PROTECTRAIL Consortium

Ansaldo STS S.p.A.
www.ansaldo-sts.com
IT

PKP Polskie Linie Kolejowe S.A.
www.pkp-sa.pl
PL

Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO
www.tno.nl
NL

D'Appolonia S.p.A.
www.dappolonia.it
IT

Selex ES S.p.A. (formerly SelexElsag S.p.A.)
www.selexelsag.com
IT

Elbit Systems Ltd.
www.elbitsystems.com
IL

Union Internationale des Chemins de fer
www.uic.org
FR

Facultés Universitaires Notre-Dame de la Paix
www.fundp.ac.be
BE

Bombardier Transportation GmbH
www.bombardier.com
DE

EPPRA
www.eppra.com
FR

Alstom Transport S.A.
www.alstom.com
FR

Kingston University Higher Education Corporation
www.kingston.ac.uk
UK

Thales Communication and Security S.A.
www.thalesgroup.com
FR

SODERN S.A.
www.sodern.com
FR

Sarad GmbH
www.sarad.de
DE

Smiths Heimann S.A.S.
www.smithsdetection.com
FR

UNIFE – The European Rail Industry
www.unife.org
BE

Instytut Kolejnictwa
www.ikolej.pl
PL

Morpho S.A.
www.morpho.com
FR

CEA Commissariat à l'Énergie Atomique
www.cea.fr
FR

Ductis GmbH
www.ductis.de
DE

Institut Franco-Allemand de Recherches de Saint-Louis
www.isl.eu
FR

Železničná spoločnosť Slovensko a.s.
www.zssk.sk
SK

TCDD - Turkish State Railways
www.tcdd.gov.tr
TR

Joint Stock Company Lithuanian Railways
www.litrail.lt
LT

MER MEC S.p.A.
www.mermecgroup.com
IT

RFI Rete Ferroviaria Italiana S.p.A.
www.rfi.it
IT

Société Nationale des Chemins de fer Français
www.sncf.com
FR

June 2014 | Published by UIC | Design: Marina Grzanka