

3rd edition, June 2009

Original

0

Description of the HERMES System

This leaflet will be published only in English



UNION INTERNATIONALE DES CHEMINS DE FER
INTERNATIONALER EISENBAHNVERBAND
INTERNATIONAL UNION OF RAILWAYS

Leaflet to be classified in Volume:

IX - Information Technology, Miscellaneous

Application:

With effect from 01.06.2009

All members of the International Union of Railways

Record of updates

1st edition, July 1985	First issue
2nd edition, December 2003	Overhaul of Leaflet - Retyped in FrameMaker Adaptation to the editor's guide M1 - New lay-out
3rd edition, June 2009	Overhaul of Leaflet due to migration to a network with enhanced capabilities.

The person responsible for this leaflet is named in the UIC Code

Contents

Summary	1
1 - Introduction	2
1.1 - Brief description of the system.....	2
1.1.1 - Standards and components up to network level	2
1.1.2 - Standards and components above network level	2
1.2 - IT applications using the HERMES system	3
1.3 - Users of the HERMES system.....	3
1.4 - History of the HERMES system.....	4
1.5 - Competence	5
1.6 - Contact	5
2 - The HERMES system	6
2.1 - Basic Principles	6
2.2 - The Network	6
2.2.1 - Principles	6
2.2.2 - Specification.....	7
2.2.3 - Problem Management and User Support	9
2.2.4 - Security Issues.....	10
2.3 - The HOSA Protocols	10
2.3.1 - Principles	10
2.3.2 - Transport.....	11
2.3.3 - Session	12
2.3.4 - Applications.....	18
2.3.5 - Addressing	18
2.3.6 - Administration	19
3 - HERMES Management.....	20
3.1 - HIT Rail B.V.....	20
3.2 - The HERMES Project Group (GPH)	21
3.2.1 - GPH Strategy	21
3.2.2 - GPH Technical.....	21
3.3 - HIT Rail Supervisory Board	22

3.4 - HIT Rail Shareholders Meeting.....	23
Appendix A - The OSI Reference Model / Open Systems Interconnect.....	24
List of abbreviations	25
Bibliography	28

Summary

The purpose of this leaflet is to describe the data transmission system used as carrier for international IT applications of railway organisations (RO)¹ and to define the appropriate standards and components.

This data transmission system is subsequently referred to as the "HERMES system".

In order to make it possible for the ROs to use the HERMES system and to communicate with one another, it is necessary to make obligatory specifications of the connection characteristics for network access and security, of protocols and functions, of regulations at user level, of message structure etc. These regulations must strictly be observed by all users of the HERMES system, as otherwise any data communication between ROs will be impossible or lead to system breakdowns.

1. UIC & OSJD members and other railway-oriented organisations

1 - Introduction

1.1 - Brief description of the system

The HERMES system is a pan-European data communication service mainly built to ensure the communication between international IT applications of ROs operating on different IT platforms.

The IT applications are not part of the system as defined in this context.

The description refers to the OSI Reference model (see Appendix [A - page 24](#) and List of abbreviations - [page 25](#)).

1.1.1 - Standards and components up to network level

The chosen standard on network level is IPv4, later to be migrated to v6.

It is implemented via an international IP service provider.

Connection of ROs is according to the document "HERMES VPN Rules of Connection".

Security definitions are described in the document "HERMES VPN Security Policy" (see also point [2.2.4 - page 10](#)).

For details on components see point [2.2 - page 6](#).

1.1.2 - Standards and components above network level

This leaflet defines the standards for transport and session level for the IT applications using the HERMES system.

The so called "HOSA Protocols" (HERMES Open Systems Architecture) are used

- On transport level: basically TCP.
- On session level: FTP, BQM, HTTP ([see List of abbreviations - page 25](#)), Internet Messaging and other proprietary application protocols (to be defined in the document "HERMES VPN Security Policy").

Each RO ([see List of abbreviations - page 25](#)) is responsible for the implementation of the required HOSA Protocols within its own IT environment according to the document "HOSA Implementation Guidelines". Implementation Guidelines for the HOSA protocols FTP and BQM are available at HIT Rail ([see List of abbreviations - page 25](#)).

Security definitions are described in the document "HERMES VPN Security Policy" (see also point [2.2.4 - page 10](#)).

For details on components, see point [2.3 - page 10](#).

1.2 - IT applications using the HERMES system

The HERMES System can be used by the so called "UIC applications" as well as non-UIC applications. The message formats used in UIC applications are defined by UIC documents while those of "non UIC applications" just comply with bi- or multi lateral arrangements (see also point 2.3.4 - page 18).

It is up to each RO to decide which application it uses.

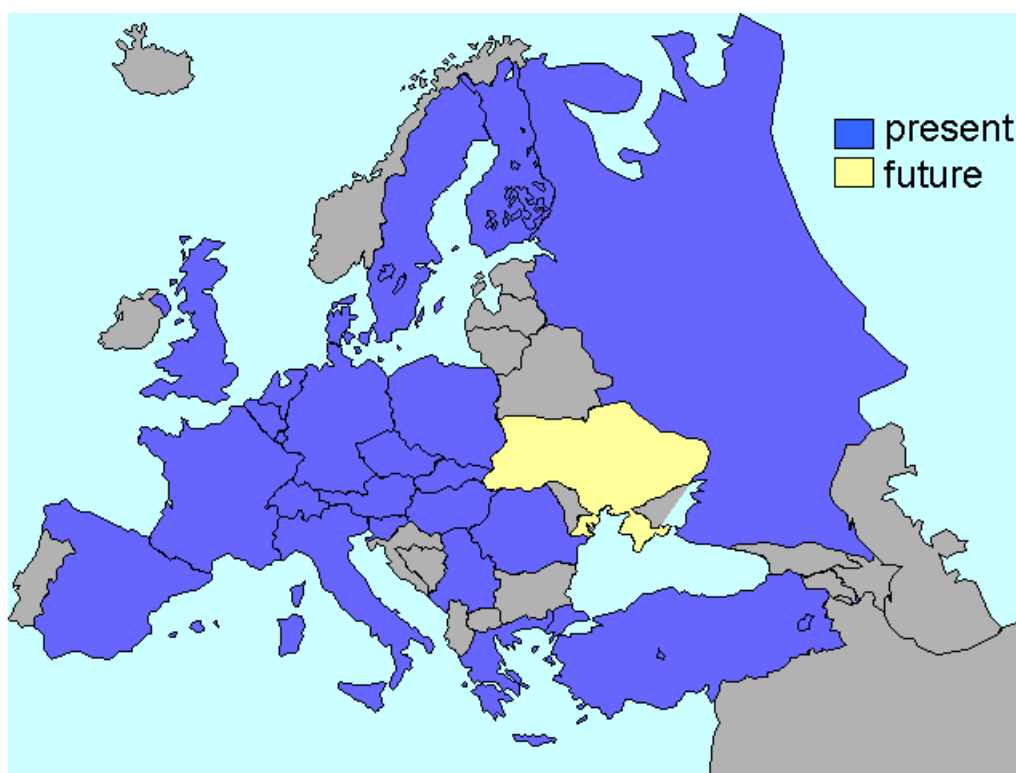
A list of the UIC applications is published in *UIC Leaflet 912, Appendix 5*. More detailed descriptions are available on the HIT Rail web site.

1.3 - Users of the HERMES system

On June 1st 2007 following RO's are connected to the HERMES System: ATOC, CD, CFL, DB, DSB, Eurostar, FS, NS, MAV, ÖBB, PKP, RENFE, RZD, SBB, SJ, SNCB, SNCF, SZ, UIC, VR, ZSR, ICF.

In most countries connected to the Hermes VPN there is a central Hermes connection for all of these countries' ROs. In several cases a Hermes link is owned by one single RO and other ROs within the related country are bound to afford a Hermes connection of their own.

For an up-to-date list, refer to HIT Rail (www.hitrail.com).



1.4 - History of the HERMES system

The European railways have always been in the vanguard of international data communications. HERMES took shape in 1978 when six railways - BR, DB, FS, SBB, SNCB and SNCF - agreed, under the patronage of the UIC, that there was a need to provide a high quality data communications network across railway boundaries. They decided to develop and operate a network supporting a wide range of structured exchanges of information between otherwise incompatible IT platforms serving passenger and freight business.

They commissioned the installation of the "HERMES" network. From the beginning the decision was made to use international standards where possible. This led to the adoption of CCITT X.25 as the network protocol. In the absence of standards for the higher-level protocols, a common set of messages was defined and each national data network had to interpret this message and create a suitable response.

It was envisaged that within the next two years, several other railway companies would be in a position to exchange data with existing HERMES members. HERMES was then extended to include DSB, NS, ÖBB, RENFE and SJ as well as organisations hosted by member railways, such as Interfrigo and Intercontainer.

The expenditure on HERMES and its applications was kept at a modest level. The limiting factor was not the provision of telecommunications support but the effort involved in implementing the data structures and messages required.

By 1990 the network connecting 11 railways had been in use for over ten years and needed renewing. HIT Rail was formed and given this task. The new "HERMES Plus" network used more up-to-date X.25 nodes and managed the migration of the railways' systems to the new extensively meshed network. Continuous management was provided from the Network Management Centre in Nottingham. The inter-application standards developed to communicate over the initial network were still in effect.

Railways cannot in practice define their own information standards and expect their customers and suppliers to accept them. The European railways require that the network should work cost-effectively and to a defined standard of quality. It is obvious that the only way to achieve this goal is to implement published computing standards, like the Open Systems Interconnection (OSI) or market standards (TCP/IP). As a first move to respond to an increasing need of railway partners to communicate using newer network protocols, IP routers for particular applications were connected to the existing X.25 backbone. By doing so contemporary protocols were transmitted over the legacy network.

To reduce the costs inherent to ownership of network nodes and leasing lines while keeping a flexible pan-European network responding faster to future changes in partnerships and the marketplace, in 1999 the railways, represented by HIT Rail decided to **replace the X.25 network by an IP VPN (Virtual Private Network)**. Within the same strategy the partners have also adopted the HERMES Open Systems Architecture (HOSA) using standards drawn from the Internet protocol suite.

After a thorough and complex selection process, the company AT&T was selected in September 2002 to provide the requested VPN service. The service became operational in the beginning of 2003 allowing the connection of many new railway customers and enabling new applications to use the advantages of the Hermes system.

After three years of successful running of the **first** Hermes VPN, HIT Rail started a project to **renew** the network. The intention was to move to a new generation, MPLS (see [List of abbreviations - page 25](#)) based network with the aim to enable new services and reduce costs. Also the steady growth of the traffic volumes was considered, since the capacity of the old VPN could not cover the new needs. In July 2006, British Telecom (BT) was selected as the new VPN provider. After a migration phase between November 2006 and February 2007 the **second Hermes VPN** interconnects today 34 sites (13 duplicated) in 23 countries.

1.5 - Competence

Responsibilities within the HERMES system are as follows:

1. Up to network level

- administration and value added services: HIT Rail
- establishment and operation: VPN provider
- point of contact towards VPN provider: HIT Rail
- security: GPH,
locally RO

2. Transport and session level incl. API (Application Program Interface)

- definition: GPH
- local implementation: RO
- operation: RO
- security: GPH,
locally RO

1.6 - Contact

HIT Rail B.V.

Web: <http://www.hitrail.com>

2 - The HERMES system

2.1 - Basic Principles

- Meet ROs' functionality
- Meet requirement of interoperability - openness

Transport is one of the most important sectors of economic activities. The HERMES ROs believe that the availability of transport applications which support seamless data exchange is decisive for the future of the rail industry. A fundamental requirement is interoperability between the different information and communications technology systems of the HERMES ROs but also openness to third parties, e.g. customers or partners in multimodal traffic, to support the ROs' business processes.

- Be consistent with technological and market developments

The key technological trends focus on Internet technology for universal networking and application connectivity while the Web provides an universal interface for access to applications. In addition, Internet and Web-based protocols are increasingly being implemented for intra-organisational communications ("Intranet"). Many industry communities also apply Internet and Web-based protocols for communications with selected business partners ("Extranet").

- Minimise costs

The use of widely accepted standards dramatically reduces software costs and supplier dependency and also enables outsourcing to service providers benefiting from the competition on the market.

2.2 - The Network

2.2.1 - Principles

For reasons mentioned in point 2.1 the Internet standard IP v4 was selected.

- Paid SLA-based Services (see List of abbreviations - page 25) (why not just use the Internet?)

The HERMES ROs need Reliability, Security and Quality assurance which can only be guaranteed via an SLA-defined service and clear responsibilities. Because the HERMES ROs cannot afford to risk running time- and business-critical applications on an "unreliable" and "anonymous" communication infrastructure, the Internet cannot be used. This is not a situation singular to the railways. Well known examples of other industry sectors using international VPN's are the motor industry (ANX), the banks (Bolero) and the airlines (Open Travel Alliance).

- Services Outsourced

The decision to outsource the network services was principally a matter of cost reduction. Given the competition on the telecom market, it turned out that a reduction of 30 % compared to the costs of the former HERMES Plus Network could be attained. So the services were outsourced to an international IP service provider.

- Meet Service Level and Performance Needs

Service level agreement and performance criteria of the network need to fulfil the requirements of the applications connected to the network.

- Organisational and technical flexibility

The network architecture and the supplier organisation have to be flexible in order to be able to adapt to structural changes, such as amalgamations, demergers and acquisitions. It also has to support access by new HERMES ROs and third parties. Network performance and other services should be easily and flexibly adaptable to the versatile requirements of the users (scalability).

2.2.2 - Specification

A VPN is a private network deployed over a service provider's backbone network providing levels of privacy, security, quality of service, and manageability similar to networks built on dedicated, privately owned or leased facilities.

The pan-European IP-based HERMES VPN provides a flexible, managed and cost efficient communications environment: it aims to bring tangible business value to the HERMES community. The end-to-end data communication services allow flexible railway business process interactions.

Main characteristics of the interfaces between the partners' corporate network and the VPN are:

- IEEE 802.3 10/100 is used as interface to the partners' corporate network
- depending on the end user's requirements, the transmission rate of the access circuits from the Customer Premises Equipment (CPE) to the VPN's Point of Presence (PoP) can be scaled up or down; several connections methods are available (dedicated line, xDSL),
- in case of an outage of the access circuit the connection will be established using DSL, ISDN ([see List of abbreviations - page 25](#)) or Internet tunnel back up if desired;
- some partners dispose of 2 interconnected sites. Both CPEs are connected to the VPN and configured to support Cisco's proprietary Hot Standby Router Protocol (HSRP). If one CPE or access fails the other CPE will be used to provide VPN access. In this case no additional back up capability is installed. HSRP is described by *RFC2281 (March 1998)* ([see Bibliography - page 28](#)). A "Request for Comment" describes an Internet standard handled by the Internet Activities Board (IAB).

The following features allow a VPN to deliver the required data communication services.

Basic network features

- The current network protocol is IP v4. If, in the future, IP v6 becomes mature enough the VPN can migrate to this new version. Should one of the HERMES partners use IP v6 before the network has migrated to the new protocol its data will be transparently transported over the existing infrastructure.