conference 2017

CyberSecurity4Rail

October 4th · Hotel Thon EU · Brussels

Are your services protected against cyber criminals?

This Conference will prepare you!

hitrail

european railway IT & data communications

Table of contents

The threat of digital crime in a digitized railway world

Are railways ready to fight digital crime, protect their systems effectively and rapidly recover services?

The European Railway Area is increasingly dependent on computer systems and their interconnected networks for the safe and effective delivery of services.

Connectivity has become key to critical business applications and functions and the railway industry is now supported by a diversity of complex technologies and interconnected communication networks that make it, like the entire transport sector, fully dependent on digital technologies.

Despite the obvious benefits, digitization has created new security risks that could be exploited by parties with dubious intentions. Criminals and other forces increasingly target digital systems and launch online attacks to access precious data, disrupt services, hold institutions to ransom, or access information to locate and access precious goods.

Digital crime is becoming more sophisticated and better organised. Hackers are constantly finding ways to break digital security.

It is just a question of time before your system may become victim to a cyber attack, possibly resulting in important reputational damage and a substantial loss of revenue.

The key to effective digital security? Cooperation in a connected world

Analysts report a 50% increase in attempted fraudulent logins in the past year alone.

Recent world-wide ransomware attacks have exposed the vulnerabilities of our connected world. Rail and other transport modes were also hit and will continue to be targeted and so must work together to put robust solutions in place to protect data and networks from further attacks.

Analysts report a 50% increase in attempted fraudulent logins in the past year alone.

Railways deliver essential services including carrying passengers safely, as well as precious goods and dangerous goods which are transported near to, and even through, urbanised areas. This makes them a specific target that requires our protection. Many companies across the transport industry are not well prepared for the digital security challenges of today and the near future.

Railways as businesses must adapt to protect their systems and data, and the most effective way to adapt is through cooperation. Working with policy makers, regulators, peers within the railway industry, companies in other transport sectors and experts in digital security, the railway industry can protect itself against digital crime.

Protecting digital systems and data - the challenges

- *Where are the potential areas of weakness?*
- *How do we assess the risks?*
- *Which services are critical to keep the railways running?*
- *Which services need higher levels of security?*
- *What can railways do to better protect themselves, their services, and their customers from cybercrime?*
- *Are there any standards which help?*

Safeguarding interconnectivity in the railways

As specialists in the provision of interoperability and cross border communications solutions in the railway sector, Hit Rail's objective has always been to ensure the safety and security of the data and messaging handled through its systems.

Established in 1990, the company is jointly owned by 12 of Europe's major railways and is responsible for managing international private data communications infrastructure and message brokering services on behalf of its shareholders and customers. Its services are used by more than 50 railway companies from 21 countries. All Hit Rail customers' data centres and company networks are interconnected by a pan-European IP-based VPN (Virtual Private Network) named Hermes VPN. In addition, the Hit Rail HEROS platform, launched in 2013, enables message interoperability across disparate IT platforms between railway applications in passenger, freight and infrastructure.

The security and integrity of networks for collaborative services such as those required by the Single European Rail Area (SERA) and the implementation of TSI Regulations are of paramount importance and Hit Rail, through its work with railways across Europe and the detailed knowledge and expertise it has acquired in European regulatory frameworks and secure communications systems and networks, continues to encourage debate and cooperation on cybersecurity as the way forward in combatting the growing threat of cybercrime.

The CyberSecurity4Rail conference: objectives and target audience

The CyberSecurity4Rail conference will bring together experts in cybercrime and digital security, leaders in ICT, representatives from transport and railway companies, European organisations and international bodies. The aim will be to address the threats of cybercrime and to share a vision for safer, more secure digital communications and data networks in the transport industry.

The positions of policy makers, major international railway organisations and various actors in the field will be presented by their senior representatives. Major developments to date, the challenges ahead and the critical issues to be solved will be discussed.

The conference will provide:

- An open, neutral forum for the stakeholders to exchange opinions on strategies to reduce risks and the best way to protect their systems and data
- A unique opportunity to directly engage with and pose questions to policy makers
- A high level networking opportunity for all participants

Target audience

- European Commission officials (DG MOVE and DG CONNECT)
- Regulators (ERA and ENISA)
- European and international railway association senior representatives (CER, UIC, EIM, ERFA, UIP, TSGA, etc.)
- Railway management and senior technical staff (RUs, IMs and their business partners and customers)
- Other companies in the transport sector (SITA/IATA on air transport)
- Experts in the digital security industry

Convergence…Connecting Europe…Cooperation

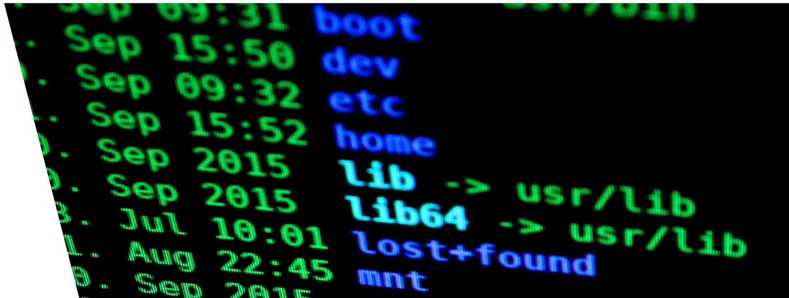
The Conference will address the following cyber security structures and associated initiatives in Europe.

- ***Single European Railway Area (SERA)[1]:*** As part of the European single market, the SERA supports harmonisation of technical, administrative and safety rules for interoperability between national rail systems. Technical specifications for interoperability (TSI) support interchange of precious data to ensure efficient operation of services for passengers and freight, but TSI interchange requires secure exchange strategies to avoid cybercrime.

- ***Railway Community Modernisation:*** Following the separation of operations and infrastructure in our modern railway systems, IT interconnections are increasingly complex. On-going railway operations, as well as the adoption of TSIs, require a safe and secure network strategy to protect data interchange, and to ensure identification, authentication and trust. Each set of national railway actors must ensure its own integrity against cybercrime. In addition, each railway must ensure that cross-border connections with other networks for interoperability do not compromise safety and security. We are all part of a European Railway Ecosystem whose resistance to cybercrime relies on cooperation.

- ***NIS Directive[2];*** Is the first piece of EU-wide legislation on cyber security. It was adopted in July 2016, and will be transposed by Member States by June 2018 to include creation of a Computer Security Incident Response Team (CSIRT) / Computer Emergency Response Team (CERT) and cooperation network. Railways, as operators of "essential services", will have to take appropriate security measures and to notify serious incidents to the relevant national authority, and are encouraged to develop an ISAC (Information Sharing & Analysis Centre). ISACs already operate in industries such as Energy[3] and so provide operational examples of how cooperation between Railway IT experts could be implemented as support for our own discussion.

Cybercrime can be combatted through collaboration

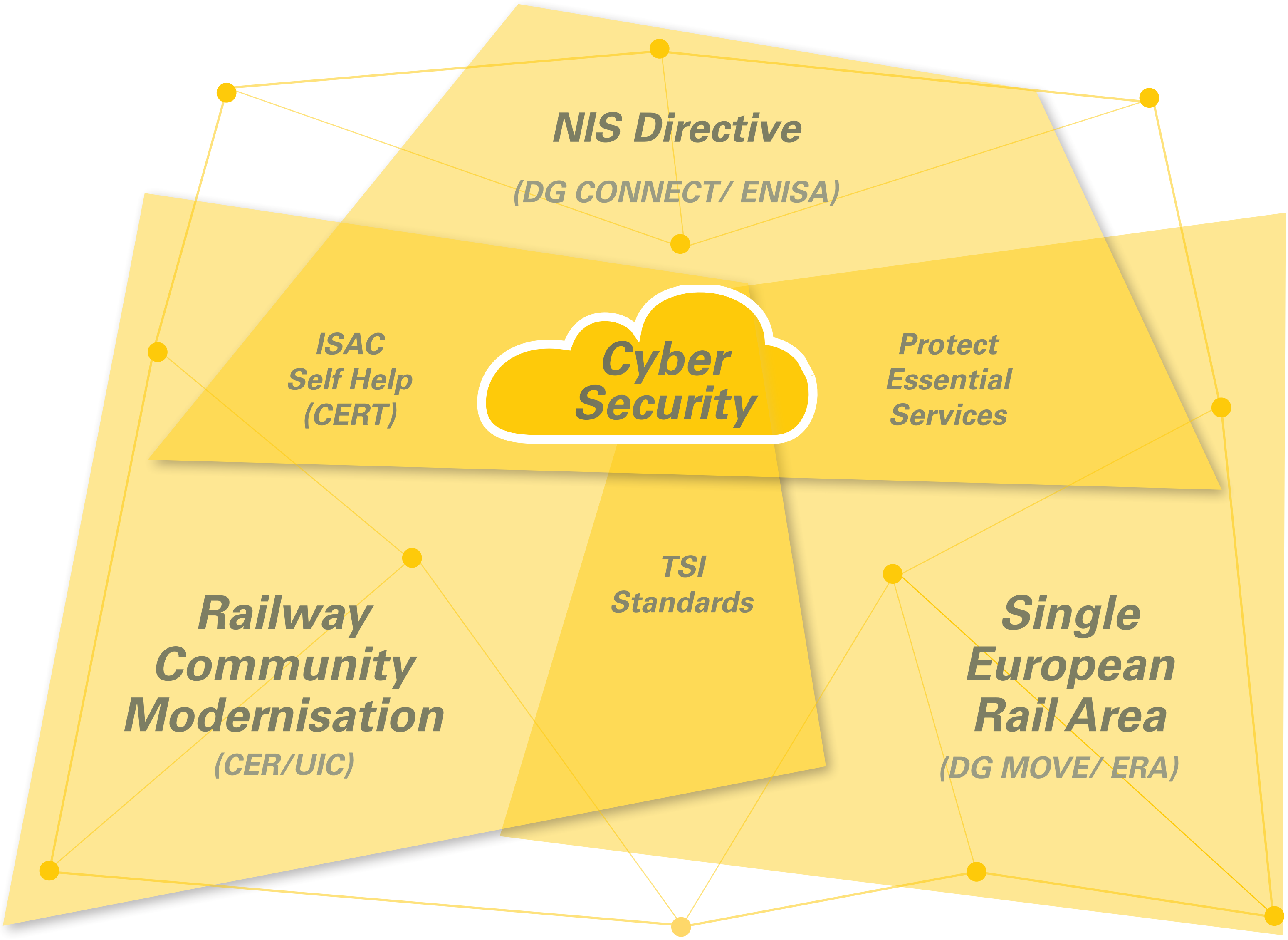


```
Sep 09:31 boot            usr/bin
Sep 15:50 dev
Sep 09:32 etc
Sep 15:52 home
Sep 2015  lib -> usr/lib
Sep 2015  lib64 -> usr/lib
Jul 10:01 lost+found
Aug 22:45 mnt
Sep 2015
```

[1] SERA: http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuld=FTU_5.6.6.html

[2] NIS Directive: https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[3] European Energy ISAC: http://www.ee-isac.eu/


NIS Directive
(DG CONNECT/ ENISA)
ISAC
Self Help
(CERT)
Cyber
Security
Protect
Essential
Services
TSI
Standards
Railway
Community
Modernisation
(CER/UIC)
Single
European
Rail Area
(DG MOVE/ ERA)

The Conference will also address the lessons learnt from the Police, the Connecting Europe initiative and Hit Rail.

- ***Lessons from Police and Cybercrime Investigation:*** ccollaboration between Member States security services and agencies such as EUROPOL ensures cooperation at a high level, to combat the current loss of around 270 Billion Euro per annum to the European economy[4]. IT experts give their technical advice to support these agencies, and have numerous examples of how cybercrime operates, and what avoidance strategies can be considered.

- ***Lessons from Connecting Europe[5]:*** the Connecting Europe programme from DG CONNECT, which also supports implementing the NIS Directive, ensures safe and secure Government Service ecosystems, and facilitates cross-border delivery of Government services for mobile citizens and business, using secured networks to connect Member States nodes so as to limit opportunities for cyber intrusion. CE also provides service-interoperability building blocks (BBs), using common specifications (like TSIs) some of which arise from the eIDAS[6] Regulation, and needs cooperation potentially using a secure common network strategy (supported by BBs) - deployed by trusted communities of stakeholders: a model relevant to Rail.

- ***Hit Rail's experience and strategies for secure networking:*** Hit Rail will describe how it has adopted increased security measures in its network offer and how these measures have ensured its 100% record of providing rail with a virus and intrusion free network.

Are railways ready to fight digital crime?

[4] *EUROPOL Unit EC3: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3*

[5] *Connecting Europe Digital examples: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Digital+Home*

[6] *eIDAS regulation: https://ec.europa.eu/digital-single-market/en/trust-services-and-eid*

The conference programme

Morning: 09.00 to 13.00
Convergence in Cyber Security – a European perspective
Chair: Dr. Josef Doppelbauer (ERA)

Welcome and Introduction	09.00 –09.10	***Helmut Grohmann*** Chair of Hit Rail Supervisory Board Welcome and introduction
Keynotes: Policy Overview and Strategic Issues	09.10 – 09.35	***Corrado Giustozzi*** Senior Cyber Security Strategist, SELTA SpA Cyber security – don't be a victim!
	09.35 – 10.00	***Dr Josef Doppelbauer*** European Union Agency for Railways (ERA) The regulators' view on cyber security
	10.00 – 10.25	***Carlos Mestre-Zamarreno*** Head of Unit, DG MOVE A.5 Security Security in the Single European Railway Area – policy considerations
	10.25 – 10.50	***Dr Florent Frederix*** DG CONNECT H1, European Commission The Network and Information Security Directive (NIS) and the requirement for railway collaboration
		COFFEE
Keynotes: Policy Overview and Strategic Issues	11.20 – 11.45	***Dr Libor Lochman*** Executive Director, CER The railway sector perspective on cyber security
	11.45 – 12.10	***Philippe-Emmanuel Maulion*** SITA CISO How airlines protect against cyber attack
	12.10 – 12.35	***Mick Haynes*** Technical Director, Hit Rail Secure networks for collaborative services

Panel Discussion	12.35 –13.00	***All morning speakers as panellists*** Chaired by **Mick Haynes** Technical Director, Hit Rail

LUNCH

Afternoon: 14.00 to 17.00
Cooperation in Cyber Security – The Way Forward
Chair: Carlo Borghini (Shift2Rail)

Case Studies and best practices	14.00 – 14.20	***Rossella Mattioli*** Security and Resilience of Communication Networks Officer, ENISA Cyber security and resilience of transport infrastructure
	14.20 – 14.40	***Lies Alderlieste-de Wit*** Chief Information Security Officer, NS Perspectives of a European railway operator
	14.40 – 15.00	***Marie Hélène Bonneau*** Senior Technical Adviser of International Union of Railways UIC Lessons learned from the CYRAIL Project
	15.00 – 15.20	***Christian Schlehuber*** Responsible for the IT-Security of the CCS and operational telecommunication systems, DB Netz AG Perspectives of a railway infrastructure manager

COFFEE

Case Studies and best practices	15.40 – 16.00	**Guus Van Es** General Manager, British Telecom Global Security Consulting The telco view
	16.00 – 16:20	**Romolo Buonfiglio** Senior Executive in Information Security, Almaviva The IT provider view
Panel Discussion	16.20 – 16.35	All afternoon speakers as panellists Chaired by **Antonio E. López** General Manager, Hit Rail
Keynote Closure	16.35 – 17.00	**Carlo Borghini** Executive Director, Shift2Rail Joint Undertaking Closing keynote address

The speakers

Dr Josef Doppelbauer
Executive Director of European Union Agency for Railways ERA

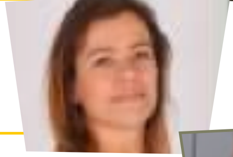
Carlos Mestre-Zamarreno
Head of Unit, DG MOVE A.5 Security

Dr Florent Frederix
DG CONNECT H1, European Commission

Dr Libor Lochman
Executive Director of Community of European Railway and Infrastructure Companies CER

Carlo Borghini
Executive Director of Shift2Rail Joint Undertaking

Lies Alderlieste-de Wit
Chief Information Security Officer of Nederlandse Spoorwegen



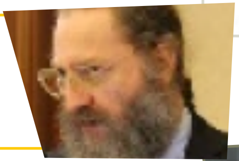
Christian Schlehuber
Responsible for the IT-Security of the CCS and operational telecommunication systems of DB Netz AG

Philippe-Emmanuel Maulion
Chief Information Security Officer of SITA, the air transport ITC company

Rossella Mattioli
Security and Resilience of Communication Networks Officer, ENISA

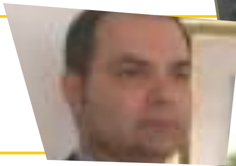
Guus van Es
General Manager for BT's Global Security Consulting

Corrado Giustozzi
Senior Cyber Security Strategist, SELTA SpA

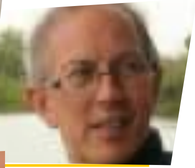


Marie-Hélène Bonneau
Senior Technical Adviser of International Union of Railways UIC

Romolo Buonfiglio
Senior Executive in Information Security of Almaviva



Mick Haynes
Technical Director of Hit Rail

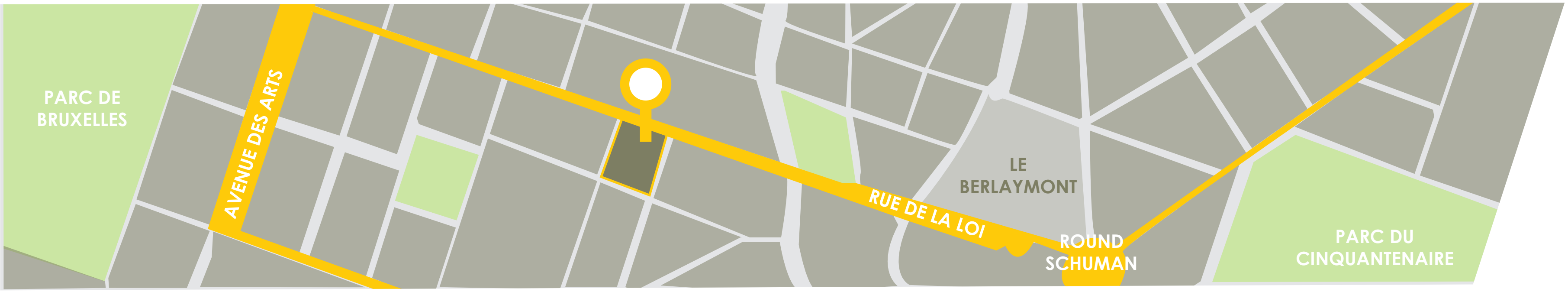


Antonio E. Lopez
General Manager of Hit Rail

Venue & logistics

Venue

Hotel Thon EU
Rue de la Loi 75, 1040 Brussels.



The Hotel is easily accessible from the Maelbeek metro station and from the Schuman railway station in Brussels.

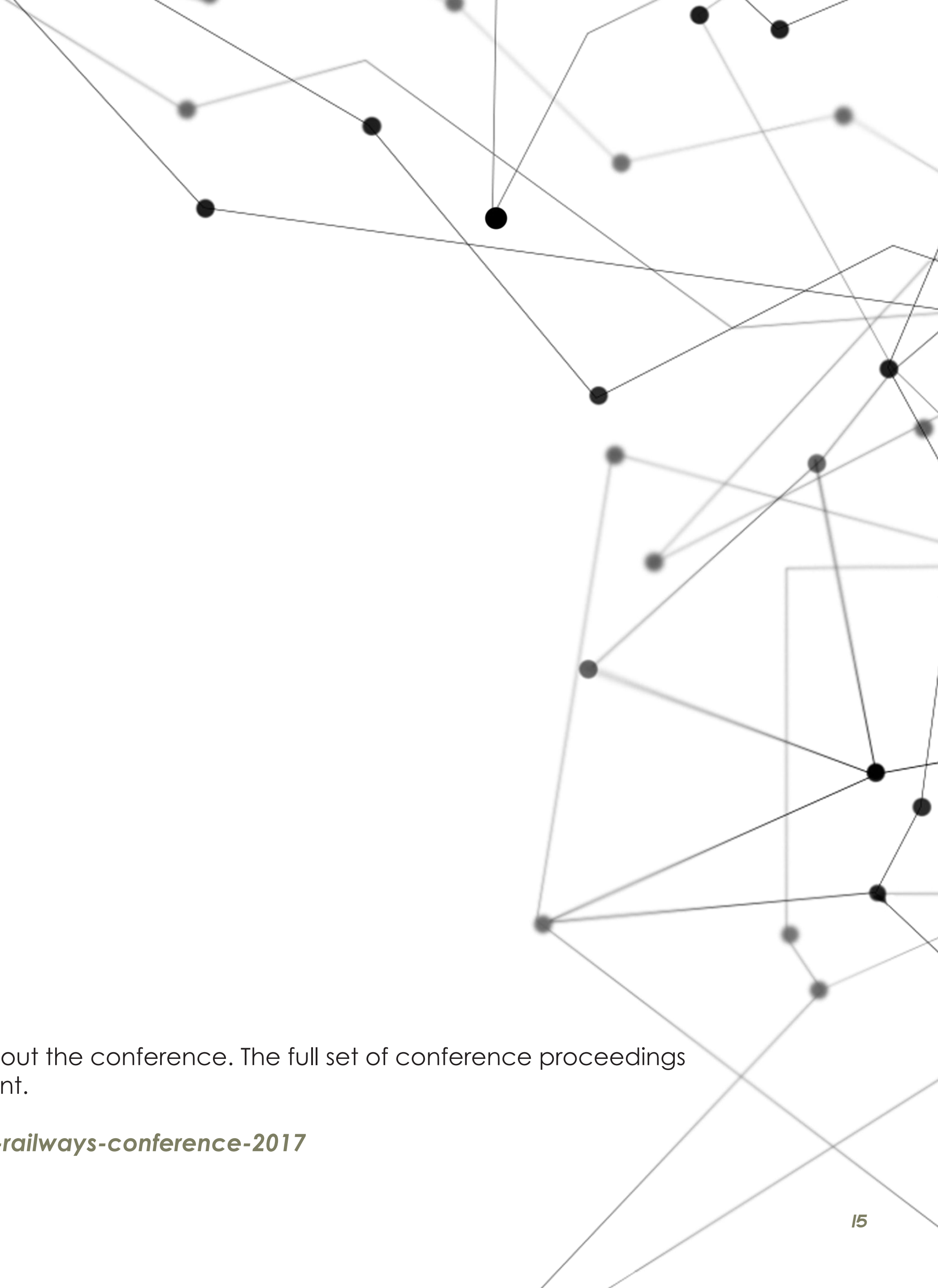
The Conference Reception Desk will be open from 08.30 on 4th October 2017.

Registration

Participation in the conference, which includes entrance, documentation, refreshments and lunch, is free of charge.

All participants must **register in advance** of the conference. Given the capacity of the venue, please register early to avoid disappointment.

Registration must be carried out online using the registration form available from the conference website at:
http://www.hitrail.com/events/cyber-security-for-railways-2017-registration



Conference Administration

Hit Rail BV
Postbus 2202
3500 GE Utrecht
The Netherlands
www.hitrail.com
conference@hitrail.com

Contact

Antonio E. López
General Manager
Hit Rail BV
alopez@hitrail.com

Please visit the Conference Website for the most current information about the conference. The full set of conference proceedings and a conference report will be published on the website after the event.

Conference Website: ***http://www.hitrail.com/events/cyber-security-for-railways-conference-2017***

hitrail

www.hitrail.com