SMARTSEC EUROPE 2016

Advanced cyber-security strategies to achieve smart grid resilience

2-Day Conference | 29th – 30th November 2016
Hotel Casa 400, Amsterdam, The Netherlands

Very Early Bird Discounts!
Save €200
on Delegate places
Save €1000
on Exhibitor
by booking before
Friday 30th September 2016

Hear detailed insights on:

- ✓ **Strategy & Investment** – understanding the impact of emerging trends such as IoT, renewables, and electric vehicles on utility infrastructure vulnerabilities, and the cyber-security strategy and investment priorities that will ensure cyber resilience
- ✓ **Risk Management** – getting to grips with how the threat landscape is evolving, the changing profile of cyber-criminals, and how you can integrate your internal mitigation with external collaboration to achieve a holistic approach to smart utility cyber-security
- ✓ **End-to-End Cyber-Security** – evaluating the latest technologies, innovative processes and high impact policies that will establish and reinforce unbreakable end-to-end cyber-security in the smart utility environment
- ✓ **Domain Specific Cyber-Security** – evaluating a range of embedded and bolt-on cyber-security solutions that will support high levels of security and functionality in the most vulnerable parts of the grid, such as digital substations, integrated SCADA systems, AMI infrastructures
- ✓ **Future Applications** – leveraging the potential of new technologies such as anomaly-based intrusion detection systems and quantum computing in the fight against the next wave of smart utility cyber-crime
- ✓ **Regulation & Standards** – determining how European level regulation and more robust standards are being developed to better meet the cyber-security needs of next generation smart utilities

Utility Case-Studies from:

Aurelio Blanquet
Director, Division of Automation and Telecommunications & Chair EE-ISAC
EDP Distribuição

Walter van Boven
Digital Grid Department Manager & Acting CIO - **Alliander**

Johan Rambi
Corporate Privacy & Security Advisor
Alliander

Kimmo Juntunen
ICT Infrastructure Manager and CISO
Caruna

Carlos Montes Portela
OT Security Officer - **Enexis**

Piotr Szarwas
Head of IT - **RWE IT**

Michal Maciejewski
Utilities & Grid Solutions Manager
RWE IT

Francois Chevalier
Head of Control Centre and Telecommunication - **Sibelga**

Lhoussain Lhassani
Senior Specialist Asset Management
Stedin

Nuno Medeiros
ICT and Smart Grids Security Officer
EDP Distribuição

Andro Kul
IT Risk Manager - **Eesti Energia**

Live Demo Labs

Don't miss the opportunity to get hands-on experience with the latest utility cyber-security tools and technologies during a dedicated 1:1 meeting.
Call us to arrange!

Expert Advice From:

Maurice Snoeren
Head of Section, Cyber Security - **DNV GL**

Michael John
Director - **ENCS**

Martin Gilje Jaatun
Senior Scientist - **SINTEF**

Paul Smith
Senior Scientist - **AIT Austrian Institute of Technology**

Bart de Wijs
Head of Cyber Security, Power Grids Division - **ABB**

Andreas Hülsing
Post-Doctoral Researcher
TU Eindhoven for PQCrypto

Philip Irschik
Senior Executive Advisor
E-Control

Harm van den Brink
IT Architect – **ElaadNL**

Media Partners:

Silver Sponsor:

Produced by:

Dear Colleague,

Welcome to the 3rd annual **SmartSec Europe 2016.** This case-study driven technical cyber-security conference for smart utility IT and OT professionals, provides all the practical insights you need to help drive your cyber-security policies, procedures and new technology implementation plans to the next level.

Over two intensive days you will hear from 12+ leading utilities, get up to speed with the latest technologies and services, and understand how regulatory and standardisation activity is being developed to better support future implementation programmes.

Just some of the programme benefits include:

- ✓ **Strategic Drivers Discussions** - hear from utility senior management on how they are prioritising investment and supporting the drive toward next generation cyber-secure smart utility IT/OT infrastructures
- ✓ **Technical Case-Studies** - understand the lessons learnt by utility technical teams from actual implementations of cyber-security within the end-to-end smart utility environment
- ✓ **Roundtable Discussions** - taking place at the end of day one, the opportunity to discuss emerging themes in small working groups, brain storm and problem solve, and report back findings to the wider group
- ✓ **Technology Innovation Panel** - hear how the leading solution providers are developing and deploying next generation cyber-security solutions tailored to the specific needs of smart utilities
- ✓ **Solution Zone** - running alongside the conference, this focused display of state of the art cyber-security technologies and services has experts on hand to discuss your specific challenges and provide tailored advice to help propel your implementation plans to the next level
- ✓ **Live Demo Labs** - a 1:1 private demonstration, providing you with the opportunity to gain hands-on experience with the most advanced and forward looking cyber-security technologies and services on the market
- ✓ **Networking Evening Reception** - taking place the evening of conference day one, this complementary networking event provides the opportunity to relax and unwind, meet with colleagues from across the European smart grid cyber-security community, allow new ideas to cement and new partnership opportunities to emerge

We look forward to welcoming you to the event in November.

Kind Regards,

Mandana White
Director | **Phoenix Forums**

PS: Very Early Bird Rate! Save €200 on Delegate places and €1,000 on Exhibitor spaces by booking your place before Friday 30th September 2016!

PPS: Group Booking Discount! Save a further 10% when you book 3 or more Delegates from the same organisation at the same time!

Who Should Attend?

Directors, Heads and Managers of:

- Cyber-Security
- Smart Grid
- Substation Automation
- SCADA Systems
- Telecoms
- AMI

Within TSOs, DSOs, Power System Suppliers, Cyber-Security Suppliers, Testing & Certification Labs, System Integrators.

"SmartSec Europe 2014 provided me with the information and contacts to plan my cyber-security roadmap for the next 12-24 months"
Noel Comerford
Security Analyst - **ESB**

"Excellent conference, with very relevant topics, good presentations and possibilities for networking"
Jorgen Fangel Jensen
Manager ICS-Infrastructure - **DONG Energy**

"A great opportunity to learn what is out there today and will be coming tomorrow concerning smart grid security solutions"
Steven Frere
Senior Smart Meter Communication Specialist - **Eandis**

"Very well organised and great to be able to interact with security expert colleagues on many topics"
Carlos Montes Portela
IT Architect, **Smart Grids - Enexis**

Sponsors:

In DNV GL we unite the strengths of DNV, KEMA, Garrad Hassan, and GL Renewables Certification. With 2,500 energy experts we support customers around the globe in delivering a safe, reliable, efficient, and sustainable energy supply by delivering world-renowned testing, certification and advisory services to the energy value chain. Our Intelligent Networks and Communication department is global thought leader on and specialized in SCADA EMS/DMS, smart meter, data communication infrastructures and protocols and cyber security projects. We have successfully completed more than 300 SCADA EMS/DMS projects around the globe. We have worked with all major vendors in numerous projects, and are intimately familiar with their systems, their staff, and their record in implementing systems. In addition, several DNV GL staff members are actively involved in several International Standardization groups defining the new generation of EMS and DMS systems. Visit: www.dnvgl.com

RAD provides Service Assured Networking (SAN) solutions for power utilities. RAD's Cyber Shield solution isolates industrial control systems – ICS – and automation devices from attack vectors. It protects not only from attacks on SCADA traffic, but also serves as a NERC-CIP Intermediate System to shield the management plane from malicious actions. RAD also enables seamless migration to packet-switched communication networks and applications. Founded in 1981, RAD has an installed base of more than 15 million units, and works closely with Critical Infrastructure network operators and partners around the globe. RAD is a member of the $1.25 billion RAD Group. Visit: www.rad.com

Exhibitors:

"Highly informative conference, well-structured and organised"
Simon Rodriguez, *International Sales Manager* - **SUBNET**

Sponsorship and Exhibition Opportunities

Would you like the opportunity to raise your brand profile, demonstrate your products and services, and share your expertise with a highly concentrated and influential group of utility cyber-security implementation experts and decision makers?

Our adjoining exhibition area provides the perfect platform for you to do this and more! Capped at 10 stands we ensure a focused and relevant display of the latest cyber-security technologies and services for our audience and maximum visibility for each exhibitor.

To find out more about the various sponsorship and exhibition opportunities:

Call: **+44 (0)20 8349 6360** | Email: **registration@phoenix-forums.com**



Conference Day One | Tuesday 29th November 2016

08:30 **Registration and refreshments**

09:00 **Chairman's welcome address**

09:15 **Strategic Drivers Panel - assessing the emerging IoT landscape, its implications for smart utilities, and how cyber-resilience can be achieved**

- Defining IoT in the context of the smart utility and determining how it will impact future cyber-security policies and procedures
- Creating a vision of resilience in terms of preparedness, risk management, security, protection, and crisis management
- Identifying the factors driving large-scale investment in end-to-end cyber-security among the leading European smart utilities
- Bridging the gap between IT and OT skill sets in an increasingly connected smart utility environment

Aurélio Blanquet, *Director, Division of Automation and Telecommunications & Chair EE-ISAC* - **EDP Distribuição**
Walter van Boven, *Digital Grid Department Manager & Acting CIO* - **Alliander**
Kimmo Juntunen, *ICT Infrastructure Manager and CISO* - **Caruna**

10:00 **Ecosystem Collaboration - establishing a framework for the seamless interworking of all stakeholders of the power market to speed up the implementation of next generation cyber-security within the smart utility**

- Determining the drivers for setting up more formal collaboration of utilities with suppliers, system integrators, and other parties in the supply chain
- Evaluating the benefits of sharing information in terms of incident data, technology requirements, standards developments, and regulatory guidance
- Working effectively with the supplier community to translate evolving utility requirements into robust and cost-effective cyber-security solutions
- Driving the end-to-end deployment of multi-vendor cyber-security solutions

Johan Rambi, *Corporate Privacy & Security Advisor* - **Alliander**

10:30 **Emerging Threats - implementing a cyber-security strategy that guards against the increasingly organised and sophisticated nature of utility cyber-attackers**

- Reviewing lessons learnt from recent utility cyber-attacks such as the Ukraine attacks
- Examining the changing mind-sets, tools, and tactics being used by organised cyber-attackers and how this translates into future threats
- Determining how utility policies, procedures, and people must evolve to better guard against more organised attacks
- Applying advanced monitoring techniques to continuously survey vulnerable sections of the grid
- Developing a response and recovery plan that provides preparedness for sophisticated multi-layered attacks

Paul Smith, *Senior Scientist* - **Austrian Institute of Technology**

11:00 **Morning refreshments and exhibits**

11:30 **TSO Cyber-Security - achieving end-to-end cyber-security in a complex transmission system environment**

- Identifying the key points of system vulnerability to prioritise investment in new cyber-security solutions in order to guard against modern attacks
- Cost-effectively securing legacy infrastructure whilst maintaining functionality and maximising the value gained across the infrastructure's lifecycle
- Defining an IT security architecture that leverages multi-layered Defence-in-Depth structures that combat known and unknown threats
- Determining the potential of innovative bolt-on solutions that are on the market and in development
- Proactively collaborating with partners such as DSOs and power generators to share incident data and gain a more comprehensive view of the grid, its vulnerabilities, and new opportunities for security enhancement
- Leveraging evolving standards to ease the implementation of TSO specific security solutions

Speaker to be confirmed

12:00 **DSO Cyber-Security - achieving end-to-end cyber-security in an increasingly automated and connected distribution system environment**

- Determining how DSO cyber-security requirements are intensifying with accelerated rates of distribution automation
- Overcoming the challenges of effectively securing high volumes of equipment in the distribution grid
- Managing the security of many more grid connections to LV and MV substations, smart meters, renewable energy sources, and EV charging points
- Safeguarding customer data privacy while ensuring operational security is not compromised
- Optimising the IT security architecture whilst taking into account the rapidly changing distribution system environment

Carlos Montes Portela, *OT Security Officer* - **Enexis**

12:30 **DSO Cyber-Security - effectively upgrading legacy SCADA systems with bolt-on security solutions to ensure robust security against modern threats**

- Identifying the security pressures placed on legacy SCADA systems as interconnectivity increases
- Striking the balance between enforcing adequate security whilst maintaining high levels of system functionality
- Overcoming the challenges of securing legacy systems characterized by limited system resources
- Comparing the pros and cons of proprietary and off-the-shelf security solutions for legacy SCADA systems in terms of system functionality, efficiency, and cost-effectiveness
- Seamlessly integrating IT solutions in a traditionally OT-oriented environment
- Determining the level of monitoring required for legacy SCADA systems and applying a cost-effective solution

Piotr Szarwas, *Head of IT* - **RWE IT**
Michal Maciejewski, *Utilities & Grid Solutions Manager* - **RWE IT**

13:00 **Lunch and exhibits**

14:00 **Advanced SCADA Security - optimising the security by design of new SCADA implementations to ensure a flexible and future-proofed SCADA environment**

- Determining the functional and design priorities for new SCADA systems based on the evolving grid and changing market dynamics
- Defining the extent of SCADA interconnectivity required with other IT and OT systems such as EMS, OMS, GIS, and the security implications to consider
- Designing with future loopholes in mind to ensure a flexible and easily upgradeable SCADA system
- Effectively collaborating with vendors to ensure the optimal level of security by design, enabling a secure patching process, and working towards developing multi-vendor solutions
- Interworking IT and OT teams in the implementation and maintenance of new SCADA systems
- Monitoring systems can further enhance new SCADA systems

François Chevalier, *Head of Control Centre and Telecommunication* - **Sibelga**

14:30 **Testing & Validation - establishing a framework for the effective testing and validation of critical infrastructure cyber-security**

- Determining how the threat landscape is shifting and the implications for testing and validation priorities and procedures
- Establishing a robust methodology for assessing security levels for critical infrastructure and benchmarking vendor solutions
- Identifying the cyber security maturity levels that are appropriate to the energy sector and determining how these will evolve over time
- Building up the internal skills required to accurately judge validation results

Michael John, *Director* - **ENCS**

15:00 **Afternoon refreshments and exhibits**

15:30 **Integrated Substation Security - developing a combined cyber and physical security strategy to protect geographically dispersed substations**

- Defining the all-digital substation and identifying the new points of security vulnerability
- Determining how physical and cyber security are complementary
- Establishing an in-depth cyber-security process to supplement physical security measures
- Forming a disaster recovery strategy that considers physical and cyber-security breaches in tandem
- Effectively integrating IT and OT processes to ensure combined physical and cyber-security
- Leveraging monitoring techniques to survey data traffic between the substation and control centre

Lhoussain Lhassani, *Senior Specialist Asset Management* - **Stedin**

16:00 **AMI Security - defining the scale of potential cyber-attacks through the metering infrastructure and implementing measures to achieve comprehensive resilience**

- Ascertaining the range and scale of cyber-attacks possible through the smart meter and its implications for the wider power grid
- Balancing smart meter functionality and security, and working effectively with vendors to ensure cost-effective security by design and regular updating
- Establishing the potential for monitoring data concentrators to further bolster the security of the smart meter infrastructure
- Evaluating emerging IoT based security solutions and effectively interworking them with established OT procedures
- Ensuring that smart meter deployment pressures do not undermine the quality of the cyber-security measures and putting in place a programme of continuous updating to ensure future loopholes are effectively dealt with
- Employing robust testing procedures to ensure the longevity of smart meter security solutions

Nuno Medeiros, *ICT and Smart Grids Security Officer* - **EDP Distribuição**

16:30 **Roundtable Discussions** - during this 90 minute session the audience splits into several smaller working groups, each focused on a specific theme arising from the day's presentations. This is the ideal opportunity to bring your specific cyber-security challenges to the table and brainstorm and problem solve solutions with the entire utility cyber-security ecosystem. At the end of the session each working group will feed back a summary of their discussions and recommendations to the wider audience.

18:30 Networking Evening Reception - take this opportunity to relax and unwind with colleagues from across the European cyber-security ecosystem. The perfect way to round of an intensive day of presentations and discussions.

21:00 **End of conference day one**

Conference Day Two | Wednesday 30th November 2016

09:00 **Registration and refreshments**

09:15 **Chairman's welcome back**

09:15 **Regulatory Developments Panel - determining how European level regulation must evolve to better support smart utility cyber-security investments, priorities, and implementation plans**

- Understanding the current state of EU legislation, such as the NIS Directive, and its implications on the utilities
- Translating EU cyber-security regulations into tangible guidance for utilities and their vendors
- Leveraging appropriate elements of US regulations and translating them into effective European wide guidance
- Developing a common set of standards for Europe that unite individual country regulations
- Improving the clarity of regulatory guidance so it can be easily implemented and maintained
- Providing concrete guidance on thorny issues such as customer data protection
- Ensuring regulatory guidance does not conflict with utility business objectives

Aurélio Blanquet, *Director, Division of Automation and Telecommunications & Chair EE-ISAC* - **EDP Distribuição**
Philip Irschik, *Senior Executive Advisor* - **E-Control**

10:00 **Standards Developments - evaluating a range of standards being developed to support the cost-effective implementation of smart utility cyber-security**

- Updating on the latest developments with leading utility cyber-security standards: ISO 27000 family, IEEE, IEC 62443, IEC 62351
- Evaluating the potential of US based standards such as NERC and NIST for European utilities
- Determining the implications of establishing a diverse set of standards, as opposed to a common standard, from a security perspective
- Facilitating the adoption of standards by vendors to support ease of system integration and pave the way towards multi-vendor solutions
- Determining how regulatory bodies can better direct the take-up of standards whilst allowing room for flexibility

Bart de Wijs, *Head of Cyber Security, Power Grids Division* - **ABB**

10:30 **Risk Management - defining a comprehensive risk assessment strategy to effectively manage internal vulnerabilities and adjust to external threats**

- Integrating corporate objectives into the risk assessment process to ensure effective prioritising of actions and investments
- Ensuring cooperation of IT and OT and the integration of their risk management strategies.
- Examining how external market trends and changing hacker profiles are pressurising the risk management process
- Determining how internal infrastructure developments and interconnectivity are rendering the risk environment more complex
- Overcoming the challenges of investing in new technologies with ambiguous embedded security
- Working around the inherent limitations of equipment which prevent straightforward and accurate vulnerability assessments
- Prioritising which equipment should be secured based on the likelihood and scale of external threats and internal organisational objectives
- Identifying techniques for validating the risk assessment such as attack simulations and external data sources
- Reaching the optimal risk mitigation strategy without compromising functionality and operational efficiency

Andro Kull, *IT Risk Manager* - **Eesti Energia**
Maurice Snoeren, *Head of Section, Cyber-Security* - **DNV GL**

11:30 **Morning refreshments and exhibits**

12:00 **Technology Innovation Panel - understanding how next generation cyber-security solutions are being developed to better meet smart utility requirements**

During this session, key solution providers will present their latest thinking, product strategies, and innovation pipelines to promote security and resilience in the smart grid. Various solutions will be discussed handling encryption, detection, firewalls, and cloud computing. Each speaker will present for 15 minutes and there will be a 30 minutes for Q&A and panel debate.
Dr. Martin Gilje Jaatun, *Senior Scientist* - **SINTEF**

13:00 **Lunch and exhibits**

14:00 **Renewables Integration - assessing the specific security needs of renewables integration into the grid and working with renewables partners to ensure end-to-end cyber-security**

- Reviewing the types of cyber-attacks that have resulted from renewables integration and predicting the scale and scope of future attacks as the number of renewables integration points increase
- Working around the limited cyber-security resource available within renewables organisations and determining how utilities can off-set the inherent risks
- Establishing a coordinated procedure between utilities and renewables organisation to ensure effective and swift detection, prevention, and response
- How are standards and regulatory guidelines developing to support more robust cyber-security for the renewables environment

Speaker to be confirmed

14:30 **EV Security - balancing privacy, security, and functionality in the integration of electric vehicles into the power system**

- Determining the key vulnerabilities of EV charging points and the potential impact of a security breach
- Working with the limited system resources available in the charging points for improved security measures
- Implementing open standard (OCPP) to create a common security profile and secure communication between charging points and deck offices
- Defining a cost-effective patching procedure to keep charging points up to date
- Evaluating the feasibility of monitoring charging points
- Working with vendors to improve the security by design of future charging point technology
- Protecting the privacy of drivers whilst preventing fraud and ensuring robust security

Harm van den Brink, *IT Architect* - **ElaadNL & Enexis**

15:00 **Afternoon refreshments and exhibits**

15:30 **Anomaly-Based Intrusion Detection System - leveraging advanced detection and prevention techniques to more rapidly respond to new and unpredictable threats**

- Comparing the potential of self-learning anomaly-based monitoring systems with conventional certificate and rule-based monitoring
- Defining how the ability to detect and adapt to new and unpredictable threats via pattern correlation and traffic behaviour will pave the way for new and innovative methods of securing the grid
- Prioritising where in the grid self-learning monitoring systems should be integrated to gain maximum value and return on investment prior to larger-scale deployment
- Refining the integration of self-learning monitoring systems into the broader security infrastructure and how it could complement existing layers of defence
- Evaluating the potential scale of deployment and ascertaining the feasibility of end-to-end deployment
- Effectively synchronising prevention mechanisms with detection and facilitating swift response capabilities
- Benchmarking system on the market and in development vis-á-vis features, functionalities, robustness, scalability, and cost-efficiency

Speaker to be confirmed

16:00 **Post Quantum Security - understanding the potential of quantum computing as a tool for cyber-attackers. Determining the risks and counter-measures**

- Examining the feasibility of quantum computing and forecasting when it will likely reach the market
- Determining how quantum computing can be leveraged to enact devastating attacks on critical infrastructures
- Assessing the vulnerabilities of asymmetric / public key algorithms in a post-quantum environment as well as the challenges in transitioning towards quantum-safe cryptosystems
- Ascertaining the state of symmetric / private key algorithms in a post-quantum environment and the opportunity costs in making them quantum-safe.
- Evaluating the potential of post-quantum encryption and other security solutions to guard against quantum attacks
- Predicting how quantum computing can be leveraged by smart utilities to bolster their cyber-security strategy

Andreas Huelsing, *Post-Doctoral Researcher* - **TU Eindhoven for PQCrypto**

16:30 **Chairman's summary and close**

16:45 **End of conference**

Download 2014 Presentation Highlights

Hacker Trends from a Smart Grid Perspective
Erwin Kooi, Alliander

Smart Substation Security
Kris Hallaert, Elia

Smart Charging of Electric Vehicles
Carlos Montes Portelo, Enexis &
Johan Rambi, Alliander

Failure Scenarios for the Electric Sector
Annabelle Lee, EPRI

Striking the Balance Between Security and Cost in the Large Scale Deployment of Smart Meters
Steven Frere, Eandis

Speaker Biographies

(in order of appearance)

Aurélio Blanquet
Director, Division of Automation and Telecommunications & Chair EE-ISAC
EDP Distribuição

Aurélio Blanquet is graduated in Electronics Engineering and MBA in business administration. Since 2007, he is Director for Automation and Telecommunications in the Portuguese DSO EDP Distribuicao. Mr. Blanquet was also former Project Leader in the InovGrid Project development, the Portuguese Smart Grid's innovation initiative pursuing the upgrade of the Distribution Network to face the new needs and challenges of the electricity market. Actually he is the responsible for the Distribution Automation, Telecommunications and Cyber Security projects within this Program. He is also Board Member at EUTC - European Telecom Utilities Telecom Council, and member at Eurelectric's WG Distribution System Design.

Walter van Boven
Digital Grid Department Manager & Acting CIO
Alliander

Walter van Boven is the responsible manager of the Digital Grids department within the Alliander. Digital Grids acts as service integrator for the complete data value chain form sensor in the field up to real-time control and analytics systems. Cyber security lies within Walter's responsibility. During his working period at KPMG Walter has been responsible for several IT security audits and assignments.

Kimmo Juntunen
ICT Infrastructure Manager and CISO
Caruna

Kimmo Juntunen is the ICT Infrastructure Manager and CISO at Caruna Group. Caruna is the largest electricity distribution company in Finland. Kimmo has over 20 years working experience in information technology and information security area. He has worked in several industrial sectors. Current role in Caruna he lead a team which main responsibilities are information security, architecture solutions, system integrations, server and capacity services, end user services and communication services.

Johan Rambi
Corporate Privacy & Security Advisor
Alliander

Johan Rambi is Corporate Privacy & Security Advisor within the department Governance, Risk and Compliance (GRC) and he is responsible for the development and monitoring of corporate Privacy & Security policies and guidelines within Alliander. Furthermore Johan supports the organization with Privacy & Security (Impact) assessments, requirements and measures in the role of subject matter expert. As former Privacy & Security officer Johan implemented the controls of the Privacy Audit Proof certification for the Smart Metering processes in the organization. Johan is active in several European expert groups (European Energy Cyber Security Platform, Network and Information Security platform, Data Protection Impact Assessment template) for the European Commission and standardization committees on Privacy and Cyber Security. Johan is a well-known speaker at European and US conferences to disseminate best practices on Privacy, Smart Meter- and Smart Grid Cyber Security and as co-founder Johan has launched the European Energy-ISAC in December 2015 to promote international collaboration and information sharing through PPP. Before Johan joined Alliander, he worked as security architect and consultant at different organizations for the last 18 years.

Paul Smith
Senior Scientist
Austrian Institute of Technology

Dr Paul Smith is a Senior Scientist in the Digital Safety and Security Department of the AIT Austrian Institute of Technology. Previous to this appointment he was a Senior Research Associate at Lancaster University, UK. He received his PhD in September 2003 and graduated in 1999 with an honours degree in Computer Science from Lancaster. Paul's research interests are focused on the security and resilience of critical information infrastructures. Currently, he is the coordinator of the EU-funded SPARKS project, which is considering these aspects for the smart grid. He has participated in a number of international research projects in this area, and has published articles on numerous aspects that relate to his core interests.

Carlos Montes Portela
OT Security Officer
Enexis

Carlos Montes Portela received the M.Sc. degree in Business Process Management and IT (cum laude). His master thesis focused on the design space of the ICT architecture of the Smart Grid taking into account security and privacy issues. Currently, Carlos is an OT Security Officer at the Innovation Department within Asset Management at Enexis B.V., a large Dutch Distribution Grid Operator. As a TOGAF, CISSP and CISM certified OT Security Officer, Carlos contributes to the evolution of Enexis from a DNO into a DSO embedding security into the different stages of OT related initiatives. He has been involved in projects related to Smart Metering, RTU's / Station Automation, Smart Charging of EV's and incentive based Smart Grid Demand / Response scenarios with home consumers.

François Chevalier
Head of Control Centre and Telecommunication
Sibelga

François Chevalier has a master in electricity engineering (1984) from Louvain-la-Neuve University (Belgium) and a master in management from the university of Leuven (1985). Since 1989, he has been working for distribution network operators in Belgium first in wallonia (south of Belgium) and since 1997 for Sibelga (Brussels). He was during the major part of his career responsible of gridoperation but also of long term griddevelopment and head of training center. Since 2014, he is head of the control center and telecommunication department, in charge of several Smartgrid projects. One of these projects consists in the replacement of the Scada system in order to be ready for a more active grid control.

Michael John
Director
ENCS

Michael John is the Director of Consulting Services at the European Network for Cyber Security (ENCS). The mission of ENCS is to improve the resilience of European critical infrastructures. With his work at ENCS, Michael is fully committed to enhancing the Smart Grid and Smart Metering security and privacy landscape. Additionally, Michael is involved in the European Commission's work on privacy, data protection and cyber security with in the Smart Grid environment. He is also engaged in several related work groups at Member State level in Europe. Furthermore, Michael holds the role of the Security Coordinator for The PRIME Alliance, whose goal is the development of a global power-line standard to enable truly flexible and efficient Smart Grid networks. Prior to this role at ENCS, Michael worked at Elster, one of the world's leading Smart Meter manufacturers, where he was responsible for ensuring Elster's Smart Metering applications are secure by design and fully compliant with the latest EU standards. Michael John has a deep telecommunications and information security background. Prior to working in the utilities sector, he was a Network Engineer at Nortel. Michael holds an MSc in Computer Science.

Lhoussain Lhassani
Senior Specialist Asset Management
Stedin

Dr Lhoussain Lhassani is senior asset manager within Stedin. Stedin is the grid owner in the west and centre of the Netherlands. One of his focuses is the implementation of IP network for the communication for the Electric Power Utilities. Stedin is now implementing the protocols IEC-104 and the IEC-61850, based on TCP/IP and Ethernet in the substations and to communicate with the control centers. One of his challenges is the further optimization through the use of All-IP or Ethernet for the communication in the world of high voltage (telemetry, telecommand and teleprotection). Another interest is the optimization of the IT-technology to support the business requirements.

Nuno Medeiros
ICT and Smart Grids Security Officer
EDP Distribuição

Nuno Medeiros holds an MSc degree on Electrical and Computers Engineering from the University of Porto and an MSc degree on Master of Science in Information Technology - Information Security (MSIT-IS) from Carnegie Mellon University. Before December 2011, he was responsible for managing and leading projects for the SCADA/DMS infrastructure of the EDP DistribuicÃ£o. He is currently working as a Cybersecurity and Privacy Officer for SCADA/DMS and Smart Grid projects. He is also an industry representative in several European working groups and projects, and is frequently invited as speaker in European Conferences on the topics of security and privacy.

Philip Irschik
Senior Executive Advisor
E-Control

Philipp Irschik is a Senior Executive Advisor to the Board of Directors at the Austrian National Regulatory Authority E-Control. He advises and supports the Board on operational and strategic issues spanning from core regulatory activities such as network regulation, tariff design and electricity distribution to policy questions concerning the Austrian and European energy market design. On a European level he chairs the taskforce on ICT and cybersecurity at the Council of European Energy Regulators (CEER). In addition he is a member of the recently founded Energy Expert Group on Cybersecurity by the European Commission (DG ENER). In 2015 he was identified as a Future Energy Leader by the World Energy Council (WEC).

Bart de Wijs
Head of Cyber Security, Power Grids Division
ABB

In this capacity, Bart represent this division in the ABB Group Cyber Security Council which is a cross-disciplinary team staffed with resources from various corporate functions. Additionally, he is a member of the ABB Cyber Security Response Team handling vulnerabilities and incidents. Within the division he leads a team of cyber security specialists dealing with the different aspect of all the security related concerns potentially affecting ABB customers. He is a member of various cyber security expert groups as well as an ABB representative in public private partnerships and information sharing initiatives. Between 2007 and 2010 he was responsible for cyber security in ABB's Power Generation business unit.

Andro Kull
IT Risk Manager
Eesti Energia

Dr. Andro Kull received his PhD degree from University of Tampere (Finland) in 2012. During 2012-2015 he worked part time at Tallinn University, Institute of Informatics as a lecturer preparing and leading IT risk management and information security courses for IT management master students. Starting 2015, he joined Tallinn University of Technology as a lecturer for course Information and Cyber Security Assurance in Organisations under international cyber security master program. His research interests are connected with information security management discipline and include IT risk analysis, information security governance, IT auditing and information security assurance aspects, but also business continuity planning and critical infrastructure protection. Andro has around 15 years practical work experience in public sector as IT specialist and IT manager, in financial sector as IT auditor and in energy sector as IT risk manager. Right now he is working for biggest energy company in Estonia and deals with IT/OT risk management process development for group company (energy production and distribution).

Maurice Snoeren
Head of Section, Cyber-Security
DNV GL

Maurice has an electrical engineering background and graduated from the Eindhoven University of Technology. More than 14 years of experience in electrical engineering of embedded systems and software development. The last six years, responsible for the centralized process automation (OT) for the Benelux for RWE. Developed together with IT, the IT and OT organization and governance to improve IT/OT integration and cyber security. He performed cyber security audits, risk assessments and technical reviews of the OT landscape. Besides his role to coordinate the Benelux cyber security activities, he was responsible for the centralized automation landscape and applications for the Benelux.

Dr. Martin Gilje Jaatun
Senior Scientist
SINTEF

Martin received the Sivilingeniør degree in Telematics from the Norwegian Institute of Technology (NTH) in 1992, and the Dr.Philos. degree from the University of Stavanger in 2015. Previous positions include scientist at the Norwegian Defence Research Establishment (FFI), and Senior Lecturer in information security at the Bodø Graduate School of Business. His research interests include software security, security in cloud computing, and security of critical information infrastructures. He is vice chairman of the Cloud Computing Association (cloudcom.org), President of Cloud Security Alliance Norway, and a Senior Member of the IEEE.

Harm van den Brink
IT Architect
ElaadNL & Enexis

Harm van den Brink is an IT Architect at ElaadNL (Dutch knowledge and innovation center on electric mobility) and Dutch DSO Enexis. ElaadNL is known for open standards like OCPP, OCHP, OSCP etc. Van den Brink is a specialist in IT and security and is responsible for the IT architectures of smart grids and electric mobility. The main focus is on requirements for IT security, the implementation of IT security and the development of innovative Smart Charging features within the EV infrastructure, the smart grid and between all parties involved in the smart grid system.

Andreas Huelsing
Post-Doctoral Researcher
TU Eindhoven for PQCrypto

Andreas is a postdoctoral researcher at TU Eindhoven working with Tanja Lange in the PQCRYPTO project. His research focuses on post-quantum cryptography - cryptography secure against quantum computer-aided attacks. Andreas' goal is to get post-quantum cryptography into practice. To achieve this, he works on developing schemes for which reliable security estimates can be made and that meet practical performance requirements. A lot of his research focused on hash-based signatures leading to a recent IRTF Internet draft on this topic. Before his current position, Andreas was a postdoctoral researcher in the cryptographic implementations group at TU Eindhoven, working with Daniel J. Bernstein. He did his PhD in the cryptography and computer algebra group at TU Darmstadt under the supervision of Johannes Buchmann. Before starting his PhD, he worked as a research fellow at Fraunhofer SIT in Darmstadt. Andreas holds a Diploma in computer science from TU Darmstadt.

SMARTSEC EUROPE 2016

Advanced cyber-security strategies to achieve smart grid resilience

2-Day Conference | 29th – 30th November 2016
Hotel Casa 400, Amsterdam, The Netherlands

Participation Fees & Discounts

	Very Early Bird Rate Until Friday 30th September 2016	Early Bird Rate Until Friday 28th October 2016	Standard Rate
☐ Conference	€1,395 + VAT @ 21% = €1,687.95	€1,495 + VAT @ 21% = €1,808.95	€1,595 + VAT @ 21% = €1,929.95
☐ Exhibitor (incl. conference pass)	€4,000 + VAT @ 21% = €4,840	€4,500 + VAT @ 21% = €5,445	€5,000 + VAT @ 21% = €6,050

Delegate Details

Title | First Name
Last Name
Job title
Company
Company VAT
Address
Postcode | Town/City
Country
Switchboard Number
Direct Line Number
Mobile Number
Email Address

Delegate Questions

1. How did you hear about this conference?

2. What is the nature of your company's business?

Venue & Accomodation

Hotel Casa 400

Eerste Ringdijkstraat 4
NL-1097 BC
Amsterdam
The Netherlands

Tel: +31 (0)20 665 1171
Fax: +31 (0)20 663 0379

Email: info@casa400.nl
www.hotelcasa400.com

Room Reservations

To book your room at the preferential rate reserved for attendees of this conference, please contact Casa 400 directly on: +31 20 665 1171 quoting **SmartSec Europe 2016.**

Enquiries

Call: +44 (0)20 8349 6360
Email: registration@phoenix-forums.com

Registration & Payment Methods

1. Credit Card, Invoice and Bank Transfer, go online at: www.smartsec-europe.com
2. Cheque payments, fill in the delegate details above, attach EURO cheque made payable to: Phoenix Forums Ltd, and post to: Registrations, Phoenix Forums Ltd, Winston House, 2 Dollis Parks, London, N3 1HF, United Kingdom.

Terms & Conditions

Payment: payment must be made at the time of booking to guarantee your place, either by credit card, or invoice which must be settled within 7 days and prior to the first day of the conference. If payment has not been received by the first day of the conference then credit card details will be requested onsite and payment will be taken before entry to the conference. Bookings made within 14 days of the conference require payment by credit card on booking.

Delegate Inclusions: the delegate fee covers attendance of conference sessions, speaker presentation materials, lunch and refreshments during the course of the conference, and the networking canal cruise. It does not cover the cost of flights, hotel rooms, room service or evening meals. If after booking your place you are unable to attend you may nominate, in writing, another delegate to take your place at any time prior to the start of the conference. Two or more delegates may not 'share' a place at the conference. Please make separate bookings for each delegate.

Exhibitors: the exhibition is located in the networking and catering area alongside the conference room to ensure maximum footfall and visibility for all exhibitors. Each exhibitor will be allocated a 3m x 2m space with table, 2 chairs, power sockets and WiFi access. The exact location of each exhibitor will be determined 4 weeks prior to the conference. Exhibitor set-up commences at 7am on the first day of the main conference, and break-down takes place after 4pm on the last day of the main conference. Exhibitor packages include 2 conference passes. Additional passes may be purchased at 10% discount on the published rates.

Cancellations: regretfully cancellations cannot be facilitated but transfer to a future conference is permissible. We will provide the speaker presentation materials to any delegate who has paid but is unable to attend for any reason. If we have to cancel an event for any reason, we will make a full refund immediately, but disclaim any further liability.

Alterations: it may be necessary for us to make alterations to the content, speakers, timing, venue or date of the event compared with the original programme.

Data Protection: Phoenix Forums gathers personal data in accordance with the UK Data Protection Act 1998 and we may use this to contact you by post, email, telephone, fax, sms to tell you about other products and services. We may also share your data with carefully selected third parties offering complementary products or services. If you do not wish to receive information about other Phoenix Forums events or products from selected third parties please write to us at: **database@phoenix-forums.com**