5-Day Conference, Exhibition & Networking Forum

SMART GRID FORUMS

SGF-Cybersecurity Week 2023

Early Bird: Friday 31st March 2023

Delivering next-level cybersecurity and cyber-resilience to the power grid to enable the acceleration of the energy transition

5-Day Conference, Exhibition & Networking Forum
15-19 May 2023 | Amsterdam, The Netherlands

Group Booking Discounts!
Save 10% on 3+ delegates
Save 30% on 5+ delegates
Save 50% on 10+ delegates
Booked from the same organisation at the same time!

Discussion Themes Include:

Risk Management - establishing a framework to drive next generation cybersecurity strategies customised to the power grid

Regulation - leveraging multiple regulatory frameworks and harmonising compliance to ensure a solid foundation for cybersecurity delivery and development

Standardisation - leveraging standardisation and ensuring its effective adoption and implementation across the cybersecurity organisation

IT-OT Integration - establishing cybersecurity policies, processes, and practices to ensure end-to-end cybersecurity of the entire smart utility organisation

Advanced Solutions - implementing solutions to drive cybersecurity advancement across the power grid

Cloud Cybersecurity - supporting the business case for Cloud migration across the power grid

Event Highlights Include:

Utility Case-study Driven Agenda - showcasing 20+ TSO and DSO techno-commercial implementations of prevention, detection and response strategies

Technology Innovation Discussions - enabling you to influence the direction of cybersecurity supplier product development roadmaps

End-User Roundtable Discussions - enabling you to bring your real-world grid cybersecurity challenges to the table and benefit from the insights and advice of the entire power grid ecosystem

Hands-on Practical Workshop - enabling you to get under the skin of Cloud security and enable you to make the business case and drive the implementation of new solutions

Solution Zone - displaying 30+ suppliers of IT and OT cybersecurity solutions customised to the power grid environment

Facilitated Networking Programme - including a Networking Evening Reception on the evening of conference day one, welcoming all participants

Speakers Include:

Hanne Hansen
CISO
Energinet

Annilisa Arge Klevang
CISO
SEV

Catherine Buhler
CISO
Energy Australia

Erki Guhse
CISO
Enefit

Barry Coatsworth
Director and Cybersecurity Leader
Guidehouse

Indrek Kunapuu
CISO
Elektrilevi

Jeremi Gryka
Deputy CIO/IT Security
PSE

Phil Litherland
Cyber Security - OT Security Product Manager
National Grid

Michael Ring
Information Security Officer (ISO) GFO
TenneT

Michael Knuchel
Head of SAS Engineering
Swissgrid

Janus Ahrensbach
ICS Security Architect
Energinet

Sampo Turunen
Secondary Systems Manager
Fingrid

Olivier Clement
Head of Cybersecurity Anticipation & External Affairs
Enedis

Deniz Tugcu
Lead Senior OT Cybersecurity Specialist
Vattenfall

Shawn McBurnie
Director IT/OT Cybersecurity and Compliance
Northland Power

Siv Houmb
Senior Adviser
Statnett

Ruben Figueiredo,
Cyber Security GRC Manager
E-REDES

Salim Bouramman
Expert OT Cyber Reslience and Cyber Range
E.ON

Greg Blezard
Head of Information Security
ENWL

Luka Mocnik
ICT Infrastructure Architect
Elektro Gorenjska

Strategic Partners: IEC, EE-ISAC
Media Partner: OSGP Alliance
Gold Sponsors: FORESCOUT, SEL Schweitzer Engineering Laboratories
Silver Sponsors: Rhebo a Landis+Gyr company, OMICRON
LDL Sponsor: SUBNET Solutions Inc.
Exhibitors: DNV, WATERFALL Stronger Than Firewalls
Produced by: Smart Grid Forums

www.smartgrid-forums.com/cybersecurity-week

Dear Colleague,

Welcome to the inaugural **SGF-Cybersecurity Week 2023**. The last couple of years have seen power grid cybersecurity teams stretched to their limits. The pressure to support grid innovation at the speed of the digital age, the impact of Covid on remote working and increased grid vulnerabilities, and the demands of multiple regulatory frameworks working at odds with each other, has created a perfect storm that only true IT-OT integrated cybersecurity strategies can resolve.

SGF-Cybersecurity Week 2023 provides a highly focused and impactful forum for power grid cybersecurity leaders, specialists and decision makers from both IT and OT backgrounds to come together in a safe, secure and fully vetted environment, to collaborate and cooperate on new strategies and implementation plans, and to get the grid ahead of the threat.

The programme breaks down as follows:

Monday 15th May 2023: Risk Management Briefing

The week begins with a briefing on the Risk Management priorities of utility CISOs, with presentations shared on the current regulatory landscape, cybersecurity standards, securing on-going cybersecurity budget, driving workforce development, and spearheading collaboration. Participants will come away with a clear understanding of the strategic priorities of cybersecurity leaders, and how the entire cybersecurity team and the supplier ecosystem must align to get the power grid ahead of the threat.

Tuesday 16th to Thursday 18th May 2023: IT & OT Cybersecurity Conference & Exhibition

The main conference is comprised of morning plenary sessions addressing macro issues such as regulation, workforce development, and data management, and afternoon technical tracks focused on the specific implementation issues impacting IT and OT cybersecurity teams. A combined programme of facilitated networking activities enable IT and OT colleagues to come together and share experience and expertise, and gain insights into each other's priorities. Running alongside the conference is a Solution Zone with a focused display of IT and OT cybersecurity solutions proven in the power grid environment.

Friday 19th May 2023: Cloud Cybersecurity Workshop

The week wraps up with this Cloud cybersecurity workshop to clarify the risks and opportunities of cloud solutions for the power grid. Participants will come away from this day with a clear action plan for gaining investment, managing regulatory compliance, and driving the implementation of cloud solutions across the power grid.

There is no better place for Europe's power grid IT and OT cybersecurity community to convene, collaborate, and cooperate on new projects and strategies that will strengthen grid security and get overly stretched cybersecurity teams ahead of the threat!

We look forward to welcoming you to this safe, secure and fully vetted forum in May 2023!

Kind Regards,

MWhite

Mandana White
CEO | **Smart Grid Forums**

PS: Very Early Bird – Save up to €800 on Delegate places and €2,000 on Exhibitor spaces by booking before Friday 31st March 2023

PPS: Group Booking Discount – 10% discount for 3+ delegates, 30% discount for 5+ delegates and 50% discount for 10+ delegates from the same organisation at the same time – contact us today to arrange!

Join the Solution Zone

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 Cybersecurity leaders and decision makers?

Our adjoining exhibition area provides the perfect environment for you to do this and more! Capped at 30 stands we ensure a focused and relevant display of the latest IT and OT Cybersecurity solutions for our audience and maximum visibility and interaction levels for our exhibitors.

Testimonials from Past Cybersecurity Events

"Great opportunity to learn from others how they handle the common problems allowing us to find the most effective and efficient solution. This is added value at its best!"

Michael Knuchel, Head of SAS Engineering, **Swissgrid**

"This was a great opportunity to learn about the IEC 62443 concepts, controls and framework."

Anja Ivanovska, Info Sec Specialist, **EVN**

"A refreshing insight and different angle on cyberthreats and possible measures for the OT domain."

Bas Mulder, Technologist OT, **TenneT**

"Very informative to see how cyber-criminal activity is becoming very organised, which makes them even more dangerous."

John Milor, Cybersecurity Risk Consultant Expert
Pacific Gas & Electric

"The overall presentation and subject matter discussed was awesome. I have enjoyed the in-depth insightful discussion of the presenters thoroughly."

Aninda Chatterjee, Project Engineer, **Siemens**

Monday 15th May 2023 - Cybersecurity Governance Briefing

08:00 **Registration and Refreshments**

08:20 **Welcome from the Chair**

08:30 **European Cybersecurity Regulation - Developing a strategic view of the latest European regulations for power grid cybersecurity to implement an integrated governance, risk, and compliance strategy**

- Understanding how European CNI, and Energy Sector cybersecurity regulations interact with one another and with domestic regulation to develop an effective approach to compliance
- Integrating NIS 2 and the NCCS into existing GRC frameworks to fully benefit from their intended effect
- Reducing time and cost of compliance activities, minimizing risk and providing the foundation for an effective holistic approach to cybersecurity governance

Anjos Nijk, Managing Director, **ENCS**

09:15 **Network Code on Cybersecurity - Understanding how the Network Code on Cyber Security will help utilities to become more resilient**

- Establishing a common maturity level for European utilities to address systemic risk across the connected grid
- Overcoming challenges of transposing the legislation into domestic law and combining compliance activities with other European legislation such as NIS D to avoid unnecessary duplication of effort
- Improving risk assessment mechanisms and omnidirectional information sharing between utilities, national CSIRTs, and EU institutions, to provide collective threat intelligence

Olivier Clement, Head of Cyber Security Anticipation & External Affairs, **Enedis**

10:00 **Morning Refreshments and Networking**

10:30 **Supply Chain Risk - Gaining oversight of legal, procurement, privacy, and technical concerns to reduce exposure to supply chain risk**

- Taking a lifecycle approach to manage reputational, legal, technical, regulatory, and business risks from procurement to operation
- Working with legal and procurement functions to ensure technical requirements are adequately represented in supplier contracts
- Avoiding falling foul of regulations and proactively ensuring security and operability

Chris Kubecka, CEO, **Hypasec**

11:15 **Gaining Board Commitment – Communicating continuously evolving security requirements to the board to drive awareness and budget alignment**

- This is a drill - Holding the board to ransom to simulate direct attacks on senior leadership
- Creating awareness of attack vectors, likelihood, and impact to obtain support for risk acceptance
- Preparing the board to lead an effective response to serious cyberattacks and mitigate organisational damage

Annilisa Arge Klevang, CISO, **SEV**

12:00 **Lunch and Networking**

13:00 **Skillsets for a Converged Security Team - Defining roles and responsibilities of the next generation of security experts to foster the development of an aligned technology organisation**

- Developing a full understanding of the skills that will be required to manage the security requirements of converged environments in the increasingly distributed grid ecosystem
- Pre-empting organisational risks to help define workforce development opportunities
- Developing training, skills development, and recruitment policies to fully support the changing requirements for security

Barry Coatesworth, Director and Cybersecurity Leader, **Guidehouse**
Hanne Hansen, CISO, **Energinet**

13:45 **Influencing Down - Taking leadership to instil a cohesive security culture across IT and OT teams**

- Gaining a comprehensive oversight of your systems and applications to develop a strategy for optimising technology teams and managing external stakeholders
- Overcoming resource scarcity to manage challenges around legacy infrastructure and increasingly converged IT and OT environments
- Inspiring confidence from the top-down to support a unified, resilient, and sustainable security organisation

Annilisa Arge Klevang, CISO, **SEV**
Erki Guhse, CISO, **Enefit**
Shawn McBurnie, Director IT/OT Cybersecurity and Compliance, **Northland Power**

14:30 **NIS 2 Supply Chain Cybersecurity - Understanding the applications of the NIS 2 directive towards addressing supply chain risk**

- Using guidance from cybersecurity frameworks such as CAF and NIST to implement the changes to governance needed to harden supply chain resilience
- Managing increased enforcement risk, and a reduction of reporting time to improve incident detection, response, and recovery, and drive support for security projects that align and enable the business
- Harnessing NIS 2 to improve demonstrable resilience through increased organisational security focus, executive accountability, and better preparedness

Ivo Maritz, Senior Adviser Cybersecurity, **Maritz Consulting**
Suzanne Rijnbergen MBA, Managing Director Cyber Resilience Gallia, **Accenture**

15:15 **Afternoon Refreshments and Networking**

15:45 **Risk Mitigation - Developing strategies to ensure the cybersecurity of the control room of the future**

- Using the Control Room of the Future (CRoF) Technology Centre to manage disruption and support the development of an intelligent, resilient and cyber secure power grid needed to support the transition to clean energy
- Understanding how utilities can use the CRoF Technology Centre to research, develop and demonstrate intelligent technologies for cyber security of the future power grids
- Safely test cyber attack / defence scenarios and jointly train system operators and CSIRT in real-time using an IT-OT cyber range and digital twin of the power grid to become resilient to threats to power system stability and mitigate the risk of cascading failures and a blackout

Alex Stefanov, Director, **Control Room of the Future**

16:30 **Cybersecurity Standards to Support IT/OT Convergence - Consolidating cybersecurity standards to develop frameworks that will support your organisation's transformation requirements**

- Gaining a comprehensive understanding of the role standards such as IEC 62443, ISO 27000 and IEC 62351 play in the development of a cybersecurity management system that meets your organisational requirements
- Overcoming resistance to change to gain acceptance of the framework of standards most appropriate to the security needs of your organisation
- Establishing a common language with external providers, integrators and your entire organisation to facilitate security by design in grid transformation

Siv Houmb, Senior Adviser, **Statnett**

17:15 **Spearheading Collaboration - Improving information sharing with grid companies nationally and regionally to establish a culture of responsible disclosure across your security organisation and drive collective security**

- Understanding the necessity for the energy utilities to exchange information on cybersecurity in a trusted circle like the EE-ISAC to become more resilient to threats to grid security
- Establishing the governance needed to overcome the complexities and challenges that come with increased volume of information exchange and regulatory compliance requirements
- Reaping the benefits of information sharing and being part of the EE-ISAC

Aurelio Blanquet, Secretary General, **EE-ISAC**

18:00 **Close of Briefing**

Tuesday 16th May 2023 - IT-OT Cybersecurity Conference Day One

08:00 **Registration and Refreshments**

08:20 **Welcome from the Chair**

08:30 **Outcome Focused Regulation - Taking a proportionate and balanced approach to risk, governance, and compliance to ensure cybersecurity maturity across the connected grid**

- Gaining a holistic perspective of how the regulatory landscape is adapting to meet the challenges of IT/OT convergence, supply chain dependencies and evolving threats to grid security
- Moving beyond a compliance-based approach towards an integrated outcome-focused model to increase capability, maturity and resilience
- Raising awareness throughout the supply chain to drive economies of scale and ensure an adequate level of collective grid security

Janne Hagen, Special Adviser Contingency Planning, **NVE**
Phil Litherland, Cyber Security - OT Security Product Manager, **National Grid**

Hanne Hansen, CISO, **Energinet**

09:15 **Regulatory Compliance - Developing an integrated view of data privacy and information security regulations to support a holistic approach to compliance**

- Obtaining oversight of European and domestic regulation and operational need to strike the correct balance between effective information flow and regulatory requirements around the sharing of information
- Overcoming the complexity of meeting physical security, safety, data privacy and cybersecurity requirements to develop an efficient approach to compliance in line with operational need
- Employing a holistic approach beyond the requirements of individual authorities to reduce the risk of being impacted by cyber attacks

Janne Hagen, Special Adviser Contingency Planning, **NVE**

10:00 **Morning Refreshments, Exhibition and Networking**

10:30 **Information Sharing - Creating robust and trusted information sharing mechanisms to support responsible disclosure and real-time threat intelligence across the entire grid ecosystem**

- Proactively leading your organisation's information sharing regionally and globally to create aligned, and responsive threat intelligence and disclosure program
- Striking the correct balance between managing risk, and compliance to data privacy regulations with the benefits of improved and expanded information sharing across the grid supply chain
- Establishing trusted and effective information sharing mechanisms to help drive end-to-end grid security and become more responsive to active threats

Massimo Rocca, Board Member, **EE-ISAC**

11:15 **Network Code on Cybersecurity - Preparing to implement the Network Code on Cybersecurity as part of a consolidated approach with critical infrastructure regulations to achieving sector-wide operational resilience**

- Understanding the overlap between the requirements for information sharing in NIS 2 and the NCCS to take a coherent approach to compliance
- Improving the flow of information between Utilities, National CSIRTs and European institutions to create active feedback and responsiveness across all entities
- Raising the level of maturity across all European utilities to develop a more resilient grid ecosystem that is responsive to evolving threats

Anjos Nijk, Managing Director, **ENCS**
Barry Coatesworth, Director and Cybersecurity Leader, **Guidehouse**

Olivier Clement, Head of Cyber Security Anticipation & External Affairs, **Enedis**

12:00 **Lunch, Exhibition and Networking**

IT Security Track

13:30 **Detection - Conducting unannounced penetration testing to understand how hackers can bypass your detection systems**

- Demonstrating system vulnerabilities and the limitations of compliance to raise awareness of threat actors' methodologies and capabilities
- Developing scripts to bypass detection systems, conducting reconnaissance, and looking for credentials to show practical paths that can be used to exploit vulnerabilities
- Understanding how risk assessment, compliance and configuration need to be improved, and detection algorithms hardened to mitigate threat

Tom Jøran Sønstebyseter Rønning, Team Leader of Operational Security, **Statnett**

14:15 **Attack Paths - Modelling the path of attacks to understand vulnerabilities and become more resilient**

- Building a special Hardware in the Loop Digital Substation environment a spart of the CybWin power grid research project in order to test different offensive and defensive security actions
- Implementing 14 different cyber attacks against the target substation to cover the general steps of offensive actions against power substations, such as reconnaissance activities, operation failure attacks by spoofed commands or denial of service type of attacks
- Raising awareness of IEC 60870-5-104 Scada protocol attacks against power grid substations for grid asset owners to better protect their infrastructures.

Laszlo Erdodi, Associate Professor, **NTNU**

15:00 **Afternoon Refreshments, Exhibition and Networking**

15:30 **Secure Edge Solutions - Applying secure development life cycle and standards to adequately secure edge solutions**

- Securing the entire IoT ecosystem to manage the exponential increase in data generation and transfer
- Overcoming organisational complexity to deploy an OT Edge security platform at a substation level
- Developing a sustainable approach to edge security to support smart grid transformation

Phil Litherland, Cyber Security - OT Security Product Manager, **National Grid**

16:15 **Risk-based Vulnerability Management – Overcoming complexity to quantify the probability and impact of specific attacks and inform your vulnerability management strategy**

- Gaining visibility of all of your assets to conduct thorough continuous vulnerability assessment across the entire attack surface
- Providing success metrics to help overcome organisational and individual resistance to comprehensively tackling vulnerability management
- Automating and simplifying the process of prioritising vulnerabilities based on threat intelligence, impact, likelihood and difficulty to inform a cohesive risk acceptance strategy

Deniz Tugcu, Lead Senior OT Cybersecurity Specialist, **Vattenfall**

OT Security Track

13:30 **Threats and Vulnerabilities - Highlighting threats to and vulnerabilities of cyberphysical systems to ensure reliability, security and privacy of the smart grid**

- Gaining an understanding of the overlapping demands of reliability, security and privacy in cyberphysical systems as a basis for a coherent strategy
- Developing safety, security, and privacy systems that can resist machine learning attacks and optimize performance levels
- Integrating advanced computing, networking, and communication techniques and capabilities into the smart grid to improve reliability and productivity

Leandros Maglaras, Professor of Cybersecurity, **De Montfort University**

14:15 **Asset Vulnerability Management - Understanding OT asset vulnerabilities to develop more effective asset management practices**

- Demonstrating examples of attacks affecting OT systems to raise awareness of vulnerabilities in SCADA systems and common attack vectors
- Deepening knowledge of OT infrastructure to overcome the complexities of patching and updating
- Increasing resilience to minimize the impact of attacks on business IT infrastructure on critical assets

Dmytro Cherkashyn, Head of Cybersecurity Development, **UNISS**

15:00 **Afternoon Refreshments, Exhibition and Networking**

15:30 **Proactive Defence - Learning from attacks to the Ukrainian power grid to implement low-cost measures to become more resilient to persistent threats**

- Uncovering the motivations and methods of patriotic hackers to manage a new type of threat
- Understanding which ICS can be relatively easily exploited to prioritise your defence strategy
- Deploying low or no cost measures to defend against an increased volume and persistence of attacks on critical infrastructure

Chris Kubecka, CEO, **Hypasec**

16:15 **Threat Modelling - Correlating vulnerabilities against threat to create an integrated continuous risk and vendor management process**

- Mapping the threat landscape and emulating OT attacks in a controlled substation environment to understand the full capabilities of threat actors
- Understanding how vendor vulnerabilities from the enterprise network, lack of firmware updates, lack of updates on SCADA systems can be exploited by advanced, persistent threat actors to overcome the weaknesses and limitations of your systems
- Modelling threat from the point of view of how an attacker may exploit your systems to identify, mitigate and proactively defend against attack

Siv Houmb, Senior Adviser, **Statnett**

17:00 **Roundtable Discussions -** during this session the audience breaks out into several smaller working groups, each focused on a specific theme that arose during the day's presentations. Each working group will comprise of representatives of the entire smart grid cybersecurity community to ensure a well-rounded and holistic discussion

18:00 **Roundtable Summaries -** during this session each working group leader will provide a 5-min summary back to the wider group, highlighting the issues raised, the solutions discussed, and the recommendations made to take the matter to the next level

19:00 **Networking Evening Reception -** time to relax after an intensive day of presentations and discussions! All participants are invited to join this networking reception where you will have the opportunity to enjoy the company of colleagues from across the European power grid cybersecurity community, in a relaxed and informal setting

22:00 **Close of Conference Day One**

Wednesday 17th May 2023: IT-OT Cybersecurity Conference Day Two

08:00 **Registration and Refreshments**

08:20 **Welcome from the Chair**

08:30 **Cybersecurity Culture - Developing a cybersecurity ambassadorship programme to embed sustainable cyber-awareness across the organisation**

- Identifying and training office leaders to embed cyber-awareness in every area of the business through an effective communication campaign
- Maintaining the level of engagement among ambassadors needed to create a sustainable, reliable long-term program
- A cost-effective approach to achieving demonstrable resilience to phishing and DDoS attacks and improving reaction times to active threats

Erki Guhse, CISO, **Enefit**

09:15 **Security as an Enabler - Communicating security as an enabler of transformation and business objectives to optimise resource allocation**

- Assessing maturity and risk to determine a proactive communication strategy
- Defining the appropriate scope and timing of engagement, and identifying people with the correct level of technical knowledge to get results
- Achieving cultural alignment with the wider organisation to engrain security in decision making processes, improve efficiency and reduce cost

Catherine Buhler, CISO, **Energy Australia**

10:00 **Morning Refreshments, Exhibition and Networking**

10:30 **Skills Development - Striking the optimal balance in bilateral training of IT and OT experts to develop the capability needed to achieve secure grid modernization and operational resilience**

- Overcoming resource scarcity to embed the level of capability needed to meet the increased need for managing virtualised applications in the OT environment
- Establishing a dedicated OT security team within the IT business unit to provide focused expertise for OT specific requirements while maintaining continuity with enterprise IT functions
- Creating a bridge between IT and OT to ensure security, availability and reliability of substation systems

Michael Knuchel, Head of SAS Engineering, **Swissgrid**

11:15 **Cybersecurity Awareness Training - Integrating security training into existing cultural frameworks to enable organisation-wide cyber-awareness**

- Preparing internal and public-facing teams to work collaboratively towards mitigating cyber-threat
- Developing metrics to demonstrably measure the success of training
- Fostering a culture of positive communication in combination with greater awareness of attack vectors and vulnerabilities to improve preparedness for and responsiveness to cyber incidents

Isabell Neise, Head of Business Development, **UNISS**

12:00 **Lunch, Exhibition, and Networking**

IT Security Track

13:30 **Threat Management - Using automation for effective threat management**

- Automating threat indicator identification, validation and escalation to reduce time and improve confidence
- Migrating OT data into SOC and SIEM to correlate threats across IT and OT environments and establishing confidence levels against each threat
- Creating reliable and robust threat information sharing mechanisms between TSOs, DSOs, Generation, ISACs and Government bodies to drive sector wide security

Shawn McBurnie, Head of IT/OT Security & Compliance, **Northland Power**

14:15 **Systems Configuration - Automating virtualised substation configuration management to improve confidence and reduce complexity**

- Determining the optimal way of managing the complexity and volume of configuration requirements across your assets' lifecycle
- Overcoming difficulties with virtualised automation of backups across multi-vendor systems including legacy technology to improve systems availability
- Reducing manual configuration and limiting the possibility of human error to improve confidence in system backups

Sampo Turunen, Secondary Systems Manager, **Fingrid**

15:00 **Afternoon Refreshments, Exhibition and Networking**

15:30 **Grid Modernization - Securing smart grid transformation to facilitate carbon emission reduction**

- Conducting six pilot projects to drive operational efficiency and customer energy use reduction
- Managing standards, regulation and technical challenges brought about by the integration of new smart instruments, increased data flow and SCADA upgrades
- Optimizing and securing customer facing and internal infrastructure to support the integration of EVs, ADMS and renewables assets

Venkatesh Gollapalli, Security Architect, **EY**

16:15 **IT-OT Communication - Developing a collaborative strategy for overcoming obstacles to critical data exchange between IT to OT**

- Achieving secure and effective two-way data exchange to gain complete visibility in business systems of IT and OT vulnerabilities and communicate updates and materials from SAP to the production environment
- Developing a rock-solid DMZ to validate inputs from IT to OT and ensure confidentiality of critical data
- Creating mutual trust between the business and operations to instil confidence and enable grid optimization

Janus Ahrensbach, ICS Security Architect, **Energinet**

17:00 **Close of Conference Day Two**

OT Security Track

13:30 **Remote Management - Deploying an advanced remote management platform to enable remote, automated configuration, password management, and log management for OT devices in substations**

- Establishing a universal solution to overcome the scale and complexity of current management processes
- Assessing implementation risks and project timeframes to develop fit-for-purpose specifications and procurement requirements for a solution that can effectively manage configuration and password automation across the majority of devices in the substation environment
- Simplifying and accelerating backups, updates, and upgrades of switches, routers, relays and IEDs to drive operational efficiency

Indrek Kunapuu, CISO, **Elektrilevi**

14:15 **Remote Control- Leveraging IEC 62443 to future proof remote control of medium and low voltage substation automation**

- Using IEC 62443 principles to support secure data flows and remote access
- Overcoming resource scarcity, legacy technology and the need to use public communication networks to ensure the secure communication between the control centre and LV/MV substations
- Making the RTU in secondary substations a secure gateway to provide observable data in LV/MV substations in support of advanced analytical, predictive and IIoT applications, grid stability and flexibility for future upgrades

Luka Mocnik, ICT Infrastructure Architect, **Elektro Gorenjska**

15:00 **Afternoon Refreshments, Exhibition and Networking**

15:30 **OT Security in Procurement Projects - Moving targets: Covering OT-Security requirements for Amprion Offshore HVDC projects in a changing regulatory landscape**

- Covering OT Security requirements for offshore HVDC projects in the critical infrastructure domain
- Challenges of changing regulatory OT security requirements in long-running and complex projects
- Lessons learned from large procurement projects over the past ten years and how to avoid common mistakes
- Conducting technical security pre-tests and acceptance testing to meet the need for accelerated system design and project delivery

Stephan Beirer, Team Manager ICS/OT Security, **GAI NetConsult**
Simon Gustafson, Project Engineer Offshore Grid Connection Systems, **Amprion Offshore**

16:15 **AMI Security - Mitigating threats to advanced metering infrastructure to secure data flow in OT environments**

- Getting visibility of the key weaknesses of Advanced Metering Infrastructure and how threat actors may attempt to exploit them
- Conducting penetration tests to verify the resistance of Advanced Metering Infrastructure to cyber threats
- Identifying and eliminating weak points of AMI infrastructure and its elements to increase its cybersecurity resilience

Tomasz Wysztygiel, Cybersecurity Manager, **EY OT/IOT Hub**

17:00 **Close of Conference Day Two**

Thursday 18th May 2023: IT-OT Cybersecurity Conference Day Three

08:00 **Registration and Refreshments**

08:20 **Welcome from the Chair**

08:30 **Systems Resilience - Implementing a systemic security classification of assets to optimise confidentiality, integrity and availability of critical systems**

- Employing a mutual strategy across IT and OT to enable offline operation of the most critical systems in the event of a major attack or catastrophic failure
- Overcoming resource scarcity in a remote island location and reliance on remote vendor access and expertise to ensure secure, reliable operation
- Gaining in depth knowledge of systems and applications to efficiently communicate criticality and prioritise remediation plans

Annilisa Arge Klevang, CISO, **SEV**

09:15 **Integrated IT/OT SOC - Developing an integrated IT and OT SOC capable of a holistic response to threats across converged environments**

- Overcoming cultural and technical barriers to deploying security monitoring solutions in the OT environment
- Gaining full visibility of OT dependencies and vulnerabilities, and modelling use cases to effectively communicate requirements to vendors
- Preparing effective substation and supply chain security measures, incident response plans and playbooks to counter combined threats to your IT and OT systems

Ivo Maritz, Senior Adviser Cybersecurity, **Maritz Consulting**

10:00 **Morning Refreshments, Exhibition and Networking**

10:30 **Cyber-informed Engineering - Establishing a national cyber-informed engineering strategy to embed security in clean energy system transformation**

- Harnessing expertise and insight from energy companies, energy systems and cybersecurity manufacturers, standards bodies, researchers, DOE National Laboratories, and Federal partners in the cybersecurity and engineering mission space to adopt a national strategy towards increasing the security, reliability, and resilience of the US's energy sector
- Leveraging CIA to address gaps in how we train engineers and technicians to provide them with the means to build in security from the ground up
- Establishing the framework to embed cybersecurity into energy systems and avoid the need to retrospectively secure critical systems

Andy Bochman, Senior Grid Strategist, **Idaho National Laboratory**

11:15 **Systems Resilience - Using AI and computational intelligence to detect, prevent, respond and recover from attacks on cyber-physical grid systems**

- Simulating the entire ecosystem of electricity generation, transmission, distribution and consumption to develop strategies for mitigating the threat to critical communication systems and prevent cascading failure
- Developing innovative AI "autopilot" detection systems to manage increased volumes of data and threats to smart grid systems
- Allowing utilities to stress test systems, technology and processes using a digital twin of the end-to-end grid environment to ensure resilience and support innovation

Alex Stefanov, Director, **Control Room of the Future**

12:00 **Lunch, Exhibition, and Networking**

IT Security Track

13:30 **Network Re-segmentation - Establishing trusted and semi-trusted zones to enable large-scale IT architecture transformation**

- Gaining full visibility of your assets to determine criticality and inform your risk acceptance and mitigation strategies
- Developing the governance needed to enable technical solutions such us hybrid cloud to facilitate increased data exchange and reduce cost
- Leveraging standards to ensure compliance and demonstrably manage risk while supporting the business's smart grid transformation

Jeremi Gryka, Deputy CIO/IT Security, **PSE**

14:15 **ISO 27001 - Mapping new ISO 27000 requirements and normative changes to the ISMS of electricity grid providers**

- Understanding how regulatory and normative changes will be transposed into national law to obtain clear guidance on the impact to your management systems
- Mapping and applying new requirements to inform your change management strategy
- Reorganizing your ISMS in line with new norms to reduce complexity

Michael Ring, Information Security Officer (ISO) GFO, **TenneT**

15:00 **Afternoon Refreshments, Exhibition and Networking**

15:30 **Risk Management - Implementing a risk management strategy under an ISO 27000 certified ISMS**

- Using section 5 of ISO 27001 to determine and prevent risk in a cycle of continual improvement
- Developing documentation for identification, assessment, and treatment of risk on an ongoing basis to demonstrate risk tolerance, termination or transfer and to deploy effective controls
- Establishing processes to demonstrate compliance to cybersecurity regulations and become more resilient to cyberattacks

Ruben Figueiredo, Cyber Security GRC Manager, **E-REDES**

16:15 **Cloud Implementation - Implementing trusted cloud architecture to optimise storage and processing of data**

- Accelerating cloud adoption to reach the maturity needed to support energy system and utility business model change
- Tackling technical limitations of legacy OT and achieving the mindset shift needed to support the necessary shift to cloud-based systems
- Reducing cost of traditional on-prem solutions and facilitating the management of the volumes of data needed to operate increasingly distributed grid infrastructure

Kristian Alsing, Independent Consultant

17:00 **Close of Conference Day Three**

OT Security Track

13:30 **OT Standards - Using OT cybersecurity controls to ensure compliance**

- Implementing controls and standards such as ISO 27000 and IEC 62443 to feed effective compliance frameworks
- Measuring success of controls, and managing exceptions and failure in a continuous lifecycle to demonstrate compliance
- Developing a process of continuous improvement to support a collaborative approach with authorities towards system security

Greg Blezard, Head of Information Security, **ENWL**

14:15 **Incident Response - Establishing an incident response and recovery playbook for OT engineers to ensure ongoing operability and resilience of OT networks in the event of a cyber incident**

- Equipping OT engineers with tools and training to enable speedy first response to the incident
- Creating an incident and recovery playbook which is understood and respected by OT engineers
- Maintaining availability while responding to suspicious activity

Lukasz Kisielewski, OT Security Delivery & Senior Manager, **Accenture**

15:00 **Afternoon Refreshments, Exhibition and Networking**

15:30 **OT Modernization - Opening the OT mindset towards IT agility and innovation to enable transformation, achieve cost savings, and drive efficiency**

- Prioritising education to align people, process and technology across all levels of the organisation
- Establishing and developing an integrated framework to map governance, risk, compliance, technical security controls and audit and establish a common language
- Defining effective KPIs for management, budget holders, engineers, and IT to support tangible security

Deniz Tugcu, Lead Senior OT Cybersecurity Specialist, **Vattenfall**

16:15 **OT Supplier Security Assessment - Taking a criticality-based assessment approach to establish a secure and resilient OT-Supplier pool**

- Implementing standards and procedures to provide transparent requirements for OT-suppliers
- Collaborating with suppliers on a continuous basis to develop trust and collectively ensure control of risk
- Applying best practice for grid operators to proactively optimize cyber security resilience, and ensure a reliable level of trust in components of OT systems and services

Salim Bouramman, Expert OT Cyber Resilience and Cyber Range, **E.ON**

17:00 **Close of Conference Day Three**

Cloud Cybersecurity Workshop

Registration: 08:00

Programme: 08:30 to 16:00

This Cloud cybersecurity workshop helps participants clarify the opportunities and risks associated with cloud and hybrid-cloud solutions for the power grid. Participants will come away from this day with a clear action plan for gaining investment, aligning the workforce, and driving the implementation of cloud solutions across the power grid.

Workshop Leader:

Kristian Alsing, Cybersecurity Executive **- Independent**

Kristian has developed cyber security and resilience capabilities for 20 years. He is a business-driven leader, with experience in end-to-end security solutions; delivery and operations across a variety of highly regulated industry sectors. Last two years he's driven transformative security programmes in an energy, utilities and natural resources cyber business in a major global Systems Integrator and consultancy. Here he covered cyber transformation, MSS and consulting including in most areas of the smart grid. Kristian blogs and speaks on a variety of cyber topics. Kristian holds a number of security certifications, a Master's and Bachelors in Business Studies/ Comms. and a Diploma in BCM. He has spent 12 years freelancing in music journalism.

Workshop Programme:

Business Case - Developing a business case for hybrid cloud security for the electric grid

- Understanding how changes in electricity provision such as prosumer, EVs, and new energy system entities are driving strategic imperatives
- Understanding the long-term benefits of adopting cloud and edge computing to enable grid-change
- Overcoming the challenges around aligning on-prem and cloud security into one framework
- Assessing the risks and opportunities of open data for the electricity sector
- Managing new timelines for capital programmes needed to support accelerated cloud adoption
- Leveraging hyperscaler cybersecurity investment and developing a road map

Regulation - Managing demands of regulation and data privacy laws in the cloud environment

- Understanding how Cyber-resilience regulations are impacting the drivers and inhibitors of cloud adoption for the smart grid
- Gaining oversight of the impact of NIS2
- Assessing the impact of US industry focused, trickle down executive order approach to regulation
- Focusing on a risk driven, secure-by-design compliance approach to enable cloud adoption
- Using privacy by design to build client legitimacy and trust
- Understanding how privacy and other constraints are holding back industry innovation

Use-Case - IT applications of Cloud in the smart grid

- Understanding the opportunities, benefits and constraints of smart grid cloud applications
- Enabling secure new ecosystem features and methods of delivery
- Identifying and addressing cybersecurity challenges
- Aligning opportunities to business drivers and initiatives

Use-Case - OT applications of Cloud in the smart grid

- Demonstrating cloud use in support of prosumer applications and EVs
- Understanding the demands of the edge computing environment
- Managing increased exposure to risk and taking a secure-by-design approach
- Overcoming cultural barriers to enable innovation and meet the needs of the next-generation smart grid

Demonstration - Practical implementation of secure hybrid cloud

- Demonstrating advanced cloud applications operating in the smart-grid environment
- Gaining insight into implementation challenges to overcome common pitfalls
- Identifying threat vectors and overcoming common security concerns

Gold Sponsors:

Forescout delivers automated cybersecurity across the digital terrain. We empower our customers to achieve continuous alignment of their security frameworks with their digital realities, across all asset types – IT, IoT, OT and IoMT. It is a non-stop journey, managing cyber risk through automation and data-powered insights. The Forescout Continuum Platform provides complete asset visibility of connected devices, continuous compliance, network segmentation, network access control and a strong foundation for zero trust. For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide automated cybersecurity at scale. Forescout customers gain data-powered intelligence to accurately detect risks and quickly remediate cyberthreats without disruption of critical business assets.

Find out more at: www.forescout.com

Schweitzer Engineering Laboratories, Inc. (SEL) works to make electric power safer, more reliable, and more economical. We provide products, solutions, and services for the protection, monitoring, control, automation, security, communications, and metering of electric power systems worldwide.
All SEL products include a ten-year worldwide warranty and exceptional customer support. In the most recent study of the protective relay marketplace by Newton-Evans Research Company, North American electric utilities ranked SEL #1 in technology, price, service and support, ease of use, and cybersecurity.

Find out more at: www.selinc.com

Silver Sponsors:

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The company supports customers with OT security from the initial risk analysis to managed OT monitoring with intrusion & anomaly detection. Since 2021, Rhebo is part of the Landis+Gyr AG, a leading global provider of integrated energy management solutions for the energy industry with around 5,000 employees in over 30 countries worldwide. Rhebo is a partner of the Alliance for Cyber Security of the Federal Office for Information Security (BSI).

Find out more at: www.rhebo.com

OMICRON is the leading supplier of testing and supervision solutions for power utility communication systems utilizing the IEC 61850 standard. OMICRON's products support the whole lifecycle of IEC 61850 Digital Substations from design verification, evaluation, factory testing, commissioning, to operation and maintenance. The applications in protection, automation & control of electrical power systems in connection with IEC 61850 GOOSE, Sampled Values, and Client/Server (MMS) communication are covered by a diverse portfolio of tools. The products range from pure software tools to protection and automation test sets and distributed test, measurement, recording, and supervision systems. OMICRON's intrusion detection system has a special focus on IEC 61850 and serves an important role for the Cybersecurity of Digital Substations. With OMICRON subsidiaries and service centers on every continent, the OMICRON team serves customers world-wide.

Find out more at: www.omicronenergy.com

Live Demo Lab Sponsor:

SUBNET Solutions Inc. (SUBNET) is a software engineering company that provides grid modernization solutions for the global utility industry. Our solutions software provides
"multi-vendor" device support, directly in contrast to the "vendor specific" offerings by most large utility device vendors. SUBNET provides MORE OT Security & Capabilities which will comply with NERC, IEC 62351, IEC 62443, ISO 27002. Through our Unified Grid Intelligence (UGI) software solutions, SUBNET will improve the overall grid reliability, and future-proofing infrastructure for anticipated growth in grid monitoring.
SUBNET's Unified Grid Intelligence solutions are our 4 flagship products:
PowerSYSTEM Center™ | PowerSYSTEM Server™
SubSTATION Server™ | SubSTATION Explorer™

Find out more at: www.subnet.com

Exhibitors:

DNV is the independent expert in risk management and quality assurance, operating in more than 100 countries. Through its broad experience and deep expertise DNV advances safety and sustainable performance, sets industry benchmarks, and inspires and invents solutions. Whether assessing a new ship design, optimizing the performance of a wind farm, analysing sensor data from a gas pipeline or certifying a food company's supply chain, DNV enables its customers and their stakeholders to manage technological and regulatory complexity with confidence. Driven by its purpose, to safeguard life, property, and the environment, DNV helps tackle the challenges and global transformations facing its customers and the world today and is a trusted voice for many of the world's most successful and forward-thinking companies.

In the energy industry

DNV provides assurance to the entire energy value chain through its advisory, monitoring, verification, and certification services. As the world's leading resource of independent energy experts and technical advisors, the assurance provider helps industries and governments to navigate the many complex, interrelated transitions taking place globally and regionally, in the energy industry. DNV is committed to realizing the goals of the Paris Agreement, and supports customers to transition faster to a deeply decarbonized energy system.

Find out more at: www.dnv.co.uk

Unbreachable OT Security, Unlimited OT Connectivity. Waterfall Security Solutions' unbreachable OT cybersecurity technologies keep the world running. For more than 15 years, the most important industries and infrastructure have trusted Waterfall to guarantee safe, secure and reliable operations. The company's growing list of global customers includes national infrastructures, power plants, nuclear generators, onshore and offshore oil and gas facilities, refineries, manufacturing plants, utility companies, and more. Waterfall's patented Unidirectional Gateways and other solutions combine the benefits of impenetrable hardware with unlimited software-based connectivity, enabling 100% safe visibility into industrial operations and automation systems.

Find out more at: www.waterfall-security.com

Booking Form

SGF-Cybersecurity Week 2023

Early Bird:
Friday 31st March 2023

Delivering next-level cybersecurity and cyber-resilience to the power grid to enable the acceleration of the energy transition

5-Day Conference, Exhibition & Networking Forum
15-19 May 2023 | Amsterdam, The Netherlands

Group Booking Discounts!
Save 10% on 3+ delegates
Save 30% on 5+ delegates
Save 50% on 10+ delegates
Booked from the same organisation at the same time!

To find out how you can participate as a Delegate, Exhibitor or Sponsor:

Call: +44 (0)20 8057 1700
Email: registration@smartgrid-forums.com
Visit: https://www.smartgrid-forums.com/cybersecurity-week
Venue: https://www.smartgrid-forums.com/cybersecurity-week-venue

Pricing & Discounts

	~~**Very Early Bird**~~ ~~**Friday 27th January 2023**~~	**Early Bird** **Friday 31st March 2023**	**Standard Rate**
5-Day Delegate - Cloud Cybersecurity Workshop + 3-Day Main Conference + Cybersecurity Governance Briefing	~~€3,695 + 21% VAT~~ ~~= €4,470.95~~	€4,095 + 21% VAT = €4,954.95	€4,495 + 21% VAT = €5,438.95
4-Day Delegate - 3-Day Main Conference + Cloud Cybersecurity Workshop	~~€2,895 + 21% VAT~~ ~~= €3,502.95~~	€3,195 + 21% VAT = €3,865.95	€3,495 + 21% VAT = €4,228.95
4-Day Delegate - 3-Day Main Conference + Cybersecurity Governance Briefing	~~€2,895 + 21% VAT~~ ~~= €3,502.95~~	€3,195 + 21% VAT = €3,865.95	€3,495 + 21% VAT = €4,228.95
3-Day Delegate - 3-Day Main Conference	~~€2,195 + 21% VAT~~ ~~= €2,655.95~~	€2,395 + 21% VAT = €2,897.95	€2,595 + 21% VAT = €3,139.95
1-Day Delegate - Cloud Cybersecurity Workshop	~~€795 + 21% VAT~~ ~~= €961.95~~	€895 + 21% VAT = €1,082.95	€995 + 21% VAT = €1,203.95
1-Day Delegate - Cybersecurity Governance Briefing	~~€795 + 21% VAT~~ ~~= €961.95~~	€895 + 21% VAT = €1,082.95	€995 + 21% VAT = €1,203.95

Terms & Conditions

Payment: for both in-person and virtual event delegate bookings, payment must be made at the time of booking, by credit card or paypal, or within 7 days by invoice and bank transfer, to guarantee your place. For sponsor and exhibitor bookings, the client will be invoiced 100% of the package fee on signature, and this fee must be settled by bank transfer within 7 days or before the first day of the event, whichever falls soonest.

Participant Inclusions: the delegate, exhibitor and sponsor fee for both in-person and virtual events covers attendance of the conference sessions, access to the exhibition area, and receipt of the speaker presentation materials. For in-person events this fee also covers provision of lunch and refreshments during the course of the conference and networking reception. This fee does not cover the cost of flights, hotel rooms, room service or evening meals.

Participant Restrictions: two or more delegates may not 'share' a place at the conference, separate bookings must be made for each delegate. The exhibitor and sponsor benefit structure detailed in the associated order form may not to be sub-divided, shared or distributed with any firm other than the signatory of the order form and therefore excludes but is not limited to partners, affiliates, clients, suppliers and associates. Using the conference as a platform to promote competing events is strictly forbidden, and failure to observe this clause will result in attendees being removed from the event without any entitlement to refunded fees or incurred expenses.

Event Cancellations: once booked delegate, exhibitor and sponsor cancellations cannot be facilitated. You may however nominate in writing, another delegate, exhibitor or sponsor to take your place at any time prior to the start of the conference. In the event that Smart Grid Forums Ltd postpones an event, the delegate, exhibitor or sponsor fee will be credited toward the re-scheduled event. If you are unable to participate in the re-scheduled event, 100% refund of your fees will be made but we disclaim further liability.

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

Fortuitous Events: Smart Grid Forums Ltd shall assume no liability whatsoever if an event is altered, re-scheduled, postponed or cancelled due to a fortuitous event, unforeseen occurrence or any other event that renders performance of this event inadvisable, illegal, impracticable or impossible. For the purposes of this clause, a fortuitous event shall include, but shall not be limited to: an Act of God; government restriction and/or regulations; war or apparent act of war, terrorism or apparent act of terrorism; civil disorder, and/or riots; curtailment, suspension, and/or restriction or transportation facilities/means of transportation; or any other emergency.

Data Protection: Smart Grid Forums Ltd gathers personal data in accordance with EU GDPR 2016 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 and services. If you do not wish to receive information about other Smart Grid Forums Ltd events or products from selected third parties, please write to use at: registration@smartgrid-forums.com

Governing Law: this agreement shall be governed and construed in accordance with the laws of England and the European Union.

VAT Treatment: the customer must supply their VAT number at the point of registration to ensure the correct VAT treatment for in-person and virtual events. For in-person events VAT is charged to all participants at the VAT rate of the country the event is taking place in as that is considered the place of supply. For virtual events VAT is charged only to those customers who reside in the UK since the location of the organiser and the place of supply to the customer are both in the UK. Please note that these VAT rules are specific to 'ticketed b2b events' and that VAT rules for other types of events supplied by other types of organisers will vary.