

Building power grid cyber-resilience through the application of IEC 62443 across the OT asset base

5-Day Conference, Exhibition & Networking Forum

Monday 13th to Friday 17th June 2022 | Edinburgh, UK

Programme Highlights Include:

Regulation – understanding how the regulatory environment is evolving to drive the take-up of IEC 62443 in conjunction with ISO 27001 to meet the cybersecurity demands of power grid OT infrastructure

Business Case – creating a compelling business case to secure long-term investment in IEC 62443 expertise, application and infrastructure development

Framework – breaking down the standard and understanding its components and application for power grid operators, product and solution suppliers, and system integrators

Application – optimising the application of IEC 62443 to key domains such as the substation, control centre, smart meter infrastructure, IIOT, supply chain and more

Testing – developing a rigorous testing regime to ensure ease of certification for IEC 62443 enabled products, solutions and system installations

Upskilling – defining an effective internal training programme to upskill established and new technical staff with IEC 62443 skills and competence

Event Highlights Include:

Case-Study Programme – hear lessons learnt from 20+ utility implementations of IEC 62443 in TSO and DSO organisations across Europe and beyond

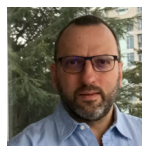
Technology Innovation Discussions – understand the IEC 62443 implementation strategies of solution providers and systems integrators

Roundtable Debates – participate in intimate discussions, where you bring your IEC 62443 challenges to the table and benefit from the insights of the whole ecosystem

Solution Zone – technology scout through a focused display of 10+ IEC 62443 enabled product and service providers

Facilitated Networking - join the networking evening reception where you will meet with IEC 62443 leads from across the European utility sector in a relaxed and informal setting

30+ Speakers Including:



Gabriel Faifman
Co-convenor
TC65 WG10



Jón Elías Práinsson
CISO
Landsnet



Michael Knuchel
Head of SAS
Engineering
Swissgrid



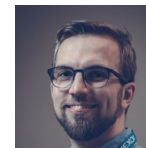
Michael Ebner
CISO
ENBW



Siv Hilde Houmb
Senior Advisor
Statnett



Tahir Saleem
OT Cybersecurity
Manager
DEWA



Sampo Turunen
Specialist
Secondary Systems
Fingrid Oyj



Deniz Tugcu
Senior OT Cybersecurity
Specialist
Vattenfall



James Cole
Secondary Systems
Manager
Evoenergy



Jan Munkejord
Author & Philosopher
within IACS
Equinor



Cevn Vibert
Senior Cyber
Compliance Manager
Ofgem



Frances Cleveland
Convener
TC57 WG15



Pedro Marin Fernandes
IEC National Committee
Expert Member
TC65 WG10



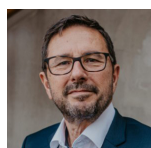
Samuel Ubido
Information
Security Manager,
OT
Uniper



Janne Hagen
Special Advisor
Contingency Planning
NVE



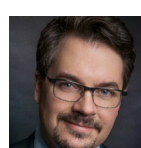
Carlos Montes Portela
ISA/IEC-62443 Certified
Trainer
Dicarma Coaching,
Training & Consulting



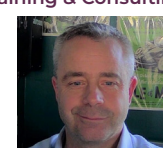
Pierre Kobes
Consultant for
Industrial Cybersecurity
Dr. Kobes Consulting



Andre Ristaino
Managing Director
ISA



Jens Wiesner
Head of Section
BSI



Christopher Thompson
Enterprise Architect
Operational Technology
SCN

Strategic Partner:

Media Partners:

Gold Sponsor:

Silver Sponsor:

Exhibitors:

Produced By:



Conference, Exhibition & Networking Forum

Dear Colleague,

Welcome to the premier IEC 62443 Week 2022 conference, exhibition and networking forum. This series of standards provides power grid operators with a robust framework to manage and mitigate security vulnerabilities in industrial control systems. Implementing IEC 62443 is now everyone's responsibility and must be fully understood and embraced by power grid operators, technology suppliers and system integrators alike, to realise its full benefits.

This week-long event provides power grid cybersecurity leaders with a thorough exploration of IEC 62443 concepts, frameworks and controls with an accurate representation of cybersecurity risk to the operations. This well-balanced programme combines a fundamentals of IEC 62443 workshop, with a utility-driven implementation main conference, and a future focused offensive cybersecurity briefing on day five.

By the end of the week, power grid cybersecurity leaders will be equipped and prepared to adopt IEC 62443 as part of their broader security management system, to work more collaboratively, systematically and cost effectively to minimise their security risks, and to strengthen the defence posture with a more proactive cybersecurity approach.

Monday 13th June – Fundamentals of IEC 62443 Workshop

The week begins with this comprehensive yet in-depth workshop on the fundamental building blocks of IEC 62443. Whether you are new to the subject matter or experienced and in need of a refresher, this is your opportunity to gain all the foundational knowledge you need to make sense of the case-study reviews that follow during the main conference.

Tuesday 14th to Thursday 16th June – Implementation Case-Study Conference & Exhibition

During the 3-day conference and exhibition, grid operators, solution providers and system integrators explore IEC 62443 concepts, frameworks and controls with an accurate representation of the cybersecurity risk to their operations. Case-study reviews are shared of recent applications of the standard in conjunction with ISO 27001 in a wide range of power grid environments.

Friday 17th June – Offensive Cybersecurity Briefing

On the final day of the event this leading-edge briefing provides new insights into how the standard can be leveraged to safely drive offensive cybersecurity strategies in the OT environment.

We look forward to welcoming you to Edinburgh in the UK, in June 2022!

Kind Regards,

Mandana White
CEO | Smart Grid Forums

Workshop Leaders:



Carlos Montes Portela
OT Security Manager & ISA/IEC-62443 Subject Matter Expert & Certified Trainer
Dicarma Coaching, Training & Consulting

Carlos has over 25 years of experience in different roles within the power grid sector: software engineer, technical and functional designer, IT architect, EAI/SOA architect, team leader, senior smart grid innovator and senior OT security officer. Currently, Carlos is an independent coach, trainer and consultant on cybersecurity related topics. As a TOGAF, CISSP and CISM certified OT Security Manager, Carlos is currently contracted by a Dutch DSO where he is responsible for OT ISO-27001 and ISA/IEC-62443 based ISMS. Carlos is a Certified Trainer and Subject Matter Experts for the ISA/IEC62443 training program. Carlos received a B.Sc. degree in Software Engineering and a 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.



Gabriel Faifman
Co-Convener
TC65 WG10

Gabriel Faifman is a highly qualified individual with diverse experience as Director, Manager and Senior Consultant in Information Systems and Network Security on multiple projects within Schneider Electric. He also serves as an expert for the TC65 working group on the IEC 62443-2-4 international standards project. Previously he has held similar positions at GE, Wurldtech, BC Hydro, YVR (Vancouver International Airport), France Telecom, BellSouth, Deloitte & Touche, and Coca Cola Company. Gabriel excels at communication by acting as liaison between the user community and Engineering staff to ensure that products, systems and business processes are adapted to customers' requirement. He speaks multiple languages including English, Spanish, and Portuguese. Gabriel specialises in: Overall Cyber-Security, Audit, Governance Model, System integration, OT, SOA Security, Microservices & IIoT Secure Architecture.

Pre-Conference Workshop

Fundamentals of IEC 62443

Monday 13th June 2022

Workshop Format:


This one-day practical workshop provides both experienced power grid cybersecurity practitioners and those who are new to the profession with an efficient way to learn about the fundamental building blocks of the IEC 62443 series of standards. Participants will obtain knowledge of how the standard can best be applied to the power grid environment. The day starts with an overview of concepts, terminology and models, and goes on to review the application of the different parts of the standard. Through discussions the participants will learn on how IEC 62443 can be used at different stages of the lifecycle of Industrial and Automation Control Systems (IACS) and how knowledge applies to the power grid. The day wraps up with an analysis of how IEC 62443 can be leveraged to strengthen risk management and defence in depth strategies.

The programme consists of a series of speaker-led presentations, group problem solving exercises and discussions, and frequent Q&As. Participation is limited to 30 individuals, to ensure a hands-on interactive learning experience.

Workshop Agenda:

08:30	Welcome address and introduction to the Workshop
	Session 1: Concept – understanding the ISA/IEC 62443-1-1 terminology, concepts and models <ul style="list-style-type: none">Introduction to cybersecurity for Industrial Automation and Control Systems (IACS)Trends in cybersecurity and analysis of cybersecurity incidents in the power grid domainBreaking down the framework and understanding how the concepts and models apply to the power grid environment
10:00	Session 2: Utility Application – establishing an industrial automation and control system security programme (CSMS) <ul style="list-style-type: none">Understanding your risk profile, how it is evolving, and how best to apply IEC 62443 in your environmentDeveloping a CSMS programme that gains management buy-in and can be easily mobilised across the workforce and organisationManaging cybersecurity lifecycles and patch management programmes
11:00	Morning refreshments and networking
11:30	Session 3: Risk Analysis (part 1) – implementing a defence in depth approach to power grid cybersecurity within the framework of IEC 62443 <ul style="list-style-type: none">Usage of IEC-62443 for risk assessment following a step-by-step approach provided in part IEC-62443-3-2Interworking the cybersecurity strategy for IT and OT assetsDetermining the optimal layers of security for different parts of the gridBalancing segmentation and security with operational efficiency
12:30	Lunch and networking
13:30	Session 4: Risk Analysis (part 2) – implementing a defence in depth approach to power grid cybersecurity within the framework of IEC 62443 <ul style="list-style-type: none">Usage of IEC-62443 for risk assessments following a step-by-step approach provided in part IEC-62443-3-2Interworking the cybersecurity strategy for IT and OT assetsDetermining the optimal layers of security for different parts of the gridBalancing segmentation and security with operational efficiency
14:30	Session 5: Supplier Application – developing products and systems that are secure by design through the optimal application of IEC 62443 <ul style="list-style-type: none">Understanding the implications of IEC 62443 for suppliers of power grid products and systemsWorking with lifecycle and patch management constraints of the power grid environmentEnsuring ease of IEC 62443 certification for products and systems
15:30	Afternoon refreshments and networking
16:00	Session 6: System Integrator Application – leveraging IEC 62443 to achieve seamless integration of new products and systems and ease the quality assurance process <ul style="list-style-type: none">Understanding the implications of IEC 62443 for systems integratorsWorking seamlessly with power grid operators and technology suppliers to ensure the seamless interworking of the standardAchieving best practice in system validation to achieve certification
17:00	Close of Workshop

Conference Day One: Tuesday 14th June

08:00	Registration and refreshments	14:15	ISO 27001 - Implementing IEC 62443 in an ISO 27001/2 series-oriented organisation to achieve measurable, technical security in the OT environment <ul style="list-style-type: none">· Clarifying the benefits of IEC 62443 implementation over ISO 27001 in the OT environment to help drive adoption· Determining how regulatory support for IEC 62443 must evolve to help drive adoption· Matching IACS specific requirements in IEC 62443 to 27001/2 based ISMS to achieve common controls where possible· Overcoming challenges related to antivirus incompatibility, patching disruption and network traffic impacts on safety controls· Achieving secure remote access to OT assets and a holistic defence-in-depth strategy to protect operational assets Pierre Kobes , Consultant for Industrial Cybersecurity – Dr. Kobes Consulting
08:20	Welcome address from the Chair	15:00	Afternoon refreshments, networking & exhibition
08:30	Energy Transition - Adopting a forward-looking OT cybersecurity posture to enable energy system change at speed and scale <ul style="list-style-type: none">· Adopting IEC 62443 to provide structure for widespread technology uptake and increased connectivity across the grid driven by the move to dependence on microservices supporting the transition to clean energy· Understanding the ramifications of simple, connected IIOT devices being implemented on large scale platforms and the increased use of APIs and containers· How does the sector need to redefine OT product lifecycles to bring concepts of agility, modularisation and easily changeable hardware and software into the OT space? What will the implications for OEMs, Integrators and Operators be?· Reviewing how the standard will need to evolve to keep up with the pace of change· Reducing security complexity to effect more rapid organisational and substantive energy system change Cevn Vibert , Senior Cyber Compliance Manager - Ofgem	15:30	Risk Assessment - Enabling business continuity and organisational change through effective security risk management and governance based on IEC 62443-3-2 Security risk assessment for system and solution design <ul style="list-style-type: none">· Raising the level of understanding to align the protection of operational environments to threats, impacts, appetite for risk and budgets within your organisation· Enabling change owners to conduct risk assessments in an IT/OT converged environment· Establishing the link between governance processes and audit controls· Ensuring the rigour of testing and certification processes beyond the scope of the standard· Creating a coherent strategy to achieve tangible, measurable technical security Michael Knuchel , Head of SAS Engineering - Swissgrid
09:15	Threat Landscape - Understanding the evolving threat landscape and mapping to IEC 62443 defined security levels to effectively mitigate threats using a risk-based approach <ul style="list-style-type: none">· Obtaining a true picture of the APT and cyber-criminal threat landscape· Establishing a realistic baseline for designing and building achievable and appropriate system security levels, based on the maturity of your security organisation· Prioritising threat mitigation based on the probability and impact of an attack· Overcoming practical limitations in OT systems of securing above level 2· Optimising your security posture to accurately address the varying levels of threat Andy Bochman , Senior Grid Strategist, Defender - Idaho National Laboratory	16:15	Security Lifecycle - Applying IEC 62443-4-1 Secure Development Lifecycle (SDLC) requirements to achieve a sustainable full-life-cycle approach to security engineering <ul style="list-style-type: none">· Determining how operators can apply specific standards documents to each phase within the security lifecycle· Tracking controls, embedding them into day-to-day monitoring, and building them into a continuous audit· Defining IACS principal roles and responsibilities· Mapping with complimentary ISO 27000 approaches· Conducting risk assessment prior to any system changes on a continuous basis to identify gaps, show traceability, and prove effective risk mitigation· Ensuring the ongoing continuous security of products and systems in a traceable, and sustainable manner Samuel Ubido , Information Security Manager, Operational Technology - Uniper
10:00	Morning refreshments, networking & exhibition	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 cybersecurity community to ensure a well-rounded and holistic discussion. Key issues raised, and solutions proposed will be collated for
10:30	Utility Panel: Cyber Security Management System (CSMS) - Establishing a framework for a cybersecurity management system with IEC 62443-2 to define policies, procedures, and guidelines for operators <ul style="list-style-type: none">· Using IEC 62443 as an umbrella for harmonising relevant standards with Governance, Risk and Compliance (GRC) within your organisation· Deciding on the most appropriate combination of standards for organisational requirements as defined in the appendix of IEC 62443 including ISO 27001, NIST, NERC CIP and CAF· Taking the time to adequately assess the entire organisational picture of people, process and technology to get a holistic view of risk· Assigning roles, responsibilities, and accountability for cyber risk within the organisation· Aligning the protection of your operational environment to threats, impacts, risk appetite, and budget Jón Elías Þráinsson , CISO - Landsnet Michael Ebner , CISO - ENBW Santitos Garcia Zamora , High Voltage Substation Project Engineering - ENEL Distribution Peru	18:30	Networking Reception - time to relax and unwind after an intensive day of presentations and discussion! 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 smart grid technical community.
12:00	Lunch, networking & exhibition	20:30	Close of conference day one
13:30	Evolving Standard – Securing the development of an increasingly diversified and interconnected energy network with IEC 62443 <ul style="list-style-type: none">· Determining what the assignment of horizontality means for the standard and its application in the power grid· How will the interworking of IEC 62443 as a horizontal OT standard, and ISO 27000 as a horizontal IT standard help to shape the future of grid security?· Reviewing the technical report on IIOT and results of the gap analysis· Clarifying which grid-specific developments to sections of the standard are on the roadmap of TC65 WG10· Reporting on the development of rules to establish energy sector specific profiles and an update on individual profile development· Creating a common language between OT and IT and enabling the evolution of a smarter more sustainable energy grid Gabriel Faifman , Co-convenor - TC65 WG10		

Conference Day Two: Wednesday 15th June

08:00	Registration and refreshments	
08:20	Welcome back from the Chair	
08:30	Access Control - Applying IEC 62443 alongside IEC 62351 to manage the risk brought about by increased data exchange and the evolution of distributed microservices <ul style="list-style-type: none">· Enabling increased data exchange between distributed renewables assets, EVs and secondary substations using IEC 62443 defence in depth in conjunction with IEC 62351· Understanding the complimentary application of IEC 62351 and IEC 62443 in managing access control and OT resource permissions· Evolving the 62443-4-2 definition of “component” to reflect the architecture of modern cyber-physical systems and match with appropriate levels of cybersecurity· Obtaining a holistic view of risk to move from asset level attack path modelling to a systems approach in an increasingly decentralised network· Establishing a common language between diverse stakeholders to facilitate a holistic approach to OT cybersecurity Frances Cleveland , President – TC57 WG15 Gabriel Faifman , Co-convenor – TC65 WG10	<ul style="list-style-type: none">· Assessing the effectiveness of the standard in defining how conduits between zones can be protected to ensure that lateral movement is restricted· Overcoming complexity to improve your security posture and developing a playbook for segregating and protecting critical assets Siv Hilde Houmb , Senior Advisor - Statnett
09:15	Supply Chain – Utilising IEC 62443 2-1 and 2-4 as part of a strategy to manage increased complexity in supply chain security <ul style="list-style-type: none">· Utilising IEC 62443 help to manage the increasingly complex mesh of relationships, contracts and privileges brought about by cloud, analytics, SOC, maintenance and system development outsourcing trends and remote access· Taking a collaborative approach to developing vendor specifications is facilitating achievable and consistent product security, and the impact of horizontality of the standard· Identifying the current limitations of the standard, and how it could evolve to help better manage challenges such as supply chain traceability and 3rd party access management· Complimenting the work of regulators on 62443 supply chain security and applying it in conjunction with other relevant standards such as NIST and NERC CIP part 13 as part of a robust supply chain security posture· Developing a holistic understanding of supply chain risk, and how standards can help to define an effective risk mitigation strategy in line with the realities of an expanding attack surface Pedro Marin Fernandes , IEC National Committee Expert Member – TC65 WG10	14:15 Substation Security Profile – Defining substation specific security requirements to facilitate IEC 62443 implementations <ul style="list-style-type: none">· Establishing a cybersecurity programme for critical systems to manage the complexities of IEC 62443 implementation in the substation environment· Understanding business as usual with current controls to establish a baseline against which to assess risk when approaching security enhancements· Engaging the entire supply chain and considering operator, integrator, and vendor requirements to develop a system of systems view of substation security· Developing secure remote access controls to manage increased remote operation and maintenance· Creating a practical roadmap for 62443 configurations in the substation Tahir Saleem , OT Cybersecurity Manager - DEWA
10:00	Morning refreshments, networking & exhibition	15:00 Afternoon refreshments, networking & exhibition
10:30	Technology Innovation Panel – Adopting IEC 62443 across a wider range of power grid industrial automation control systems <p>During this session 3-4 power grid system and cybersecurity suppliers explain how they are adopting IEC 62443 into their product suite. This is your opportunity to benchmark compliant suppliers, query their product development strategies, and gain new insights to help you plan your own system development with state-of-the-art IEC 62443 enabled products and systems in mind.</p> Mark Clemens , Connectivity Architect & Security Strategist – COPADATA	15:30 Secondary Systems – Overcoming complexity with a balanced approach to secondary systems cybersecurity in the substation environment <ul style="list-style-type: none">· Conducting feasibility assessments to clearly prioritise practically achievable security management practices· Developing practical strategies to overcome specific challenges around remote access, patching management and legacy systems· Implementing the correct security controls to ensure the cyber resilience and security of secondary systems without degrading or disrupting performance with reference to IEC 62443 parts 3 and 4-2· Developing a recommended practice report on cybersecurity of protection devices with a consortium of Nordic TSOs· Managing increased complexity to ensure secure, reliable operation and regulatory compliance Sampo Turunen , Specialist Secondary Systems - Fingrid Oyj
12:00	Lunch, networking & exhibition	16:15 Certification and Testing – Understanding the current scope of testing and certification of components, products, and systems based on IEC 62443 and the improvements required to fully meet the needs of utilities, system integrators and suppliers <ul style="list-style-type: none">· Understanding how IEC 62443 product certification is successfully enabling a collaborative approach to security and the challenges that still remain for suppliers, integrators and operators· Extending certification to cover component security, and the applicability of the IEC 62443 series of standards and certifications to commercial off-the-shelf (COTS), IIoT components, and gateways· Integrating product certification into a security scheme and addressing issues with configuration at security level 2 and above· Managing additional pen testing requirements outside of certification and feeding back new assessment requirements· Instilling confidence in all stakeholders, simplifying specifications and go-to-market strategy, and providing assurance of system resilience Andre Ristaino , Managing Director - ISA Anjos Nijk , Managing Director - ENCS
13:30	Zones and Conduits - Applying IEC 62443 to design and implement standardised security zoning architecture in a geographically dispersed grid <ul style="list-style-type: none">· Developing a systems view of multiple multi-layered and diverse systems to identify critical assets and establish acceptable levels of risk· Creating a common understanding of the meaning of zones and conduits among enterprise architects, business service owners, technicians, and engineers, and establishing a centralised team to determine the right governance and blueprints for critical sites· Establishing permissions, authentication, passive monitoring and accountability for vendors and operators with zero trust principles	17:00 Close of conference Day Two

Conference Day Three: Thursday 16th June

08:00 **Registration and refreshments**

08:20 **Welcome address from the Chair**

08:30 **Functional Security – Creating simple, functional IACS cybersecurity controls to align with utility end-user needs**

- Refining the set of requirements informed by the end user perspective to empower non-IT stakeholders on the potential of the IEC 62443 series
- Thoroughly incorporating functional threats and risk factors into 3-2 risk assessment
- Finding the correct balance around simplicity and security in user authentication where availability is a priority
- Preventing disruption by taking operational realities into consideration when using a 2-3 approach to patch management
- Mitigating the problem of a shortage of cybersecurity skills and enabling safety, reliability, and security

Deniz Tugcu, Senior OT Cyber Security Specialist - **Vattenfall**

09:15 **Smart Metering – Securing electronic access points and perimeters to mitigate threats from smart-metering infrastructure vulnerabilities**

- Applying IEC 62443 to the unique challenges of smart metering cyber security involving bi-directional communication between the consumer and the grid and insecure grid connected devices
- Mitigating low visibility of and ease of ingress to smart metering infrastructure in people's homes, public and private clouds by monitoring and defending entry points and conduits
- Leveraging 2-3 system security requirements to understand the risk to your systems and inform your perimeter defence strategy accordingly
- Understanding the interplay with other standards such as NIST, ISO 27001/2 and NERC CIP to holistically address smart-meter security risk
- Facilitating efficiency, measurability, and sustainability of energy consumption while protecting critical

Jon Wells, Chairman Committee - **OSGP Alliance**

10:00 **Morning refreshments, networking & exhibition**

10:30 **Regulatory Panel – To what extent is regulation driving IEC 62443 adoption and does it go far enough in doing so?**

- Identifying the benefits of IEC 62443 as a means of achieving compliance to OT cybersecurity regulation
- Is IEC 62443 on a trajectory to gaining similar recognition as an OT standard to that of ISO 27001 as an IT standard for critical infrastructure?
- Addressing challenges around differing national approaches to regulating the security of supranational infrastructure
- What lessons can be learned from the impact of developments in NERC CIP and other recent US regulation of energy sector security?
- Understanding how IEC 62443 may be leveraged by asset owners to manage increased levels of accountability under the NIS 2 Directive and gain visibility on regulators' view of the standard

Cevn Vibert, Senior Cyber Compliance Manager - **Ofgem**
Janne Hagen, Special Advisor Contingency Planning - **NVE**
Jens Wiesner, Head of Section - **BSI**

12:00 **Lunch refreshments, networking & exhibition**

13:30 **IIOT Security – Utilising IEC 62443 to overcome the additional security complexities introduced by the large-scale deployment of IIOT and Edge devices**

- Adopting and adapting methodologies in 4-2, 2-4, and 3-3 to meet the specific requirements of securing IIOT components and systems
- Future proofing security and operability by adopting new hardware architecture and software defined everything (SDx)
- Reconsidering the appropriateness of security levels when applying the standard to securing systems incorporating several levels of the Purdue model
- Managing and reducing the complexity brought about by varying protocols in IoT devices and APIs running in the cloud or at the grid edge
- Considerations given to 62443 guidance in development of NCSC and industry guidelines for securing IIOT.

Mo Javadi, Co-Founder and COO - **delatflare**
Christopher Thompson, Enterprise Architect, Operational Technology – **SGN**

14:15

Aligning Safety and Security – Developing a common barrier model with IEC 62443 and IEC 61508/11 to drive interoperability across the industry 4.0 value chain

- Conducting a 5-year research project to develop new knowledge, methods and guidance to secure industrial control and safety systems against cyberattacks
- Understanding the application of barrier management principles for functional safety and cybersecurity in the oil and gas sector to assess applicability to smart grid use cases
- Assessing the viability of the development of digital twins of control systems and safety instrumented systems
- Maturing towards international standards to achieve digital twin interoperability
- Facilitating the modernization of IACS to meet the requirements of the changing energy system and drive interoperability

Jan Munkejord, Author & Philosopher within IACS - **Equinor**

15:00

Afternoon refreshments, networking & exhibition

15:30

Remote access – Implementing IEC 62443 to manage the risk brought about by increased remote access

- Understanding Part 2-4: Security programme requirements for IACS service providers to manage remote access of contractors and third parties
- Ensuring you have the right architecture and segmentation in place to prevent lateral movement within your systems
- Implementing role-based and multi-factor authentication and session monitoring for employees as well as external providers based on zero trust principles
- Meeting the foundational requirement for data to be handled, encrypted, and secured with IPSEC based on IEC 62443 implementation guidance
- Enabling remote operation and maintenance and demonstrating clear value to the business

James Cole, Secondary Systems Manager - **Evoenergy**

16:15

Skills and Training – Accelerating development of the OT cybersecurity workforce as an industry to develop a suitably qualified OT cybersecurity workforce

- Leveraging IEC 62443 as a bridge between people with distinct IT and OT skillsets using real implementable models governing technology, people, and process
- Enabling change by raising cyber awareness in an ageing operational workforce
- Managing the complexity of IT/OT converged environments when training new engineers
- How can the industry focus its resources to extend and revitalise OT cybersecurity training and apprenticeship schemes to equip the next generation in line with the evolution of the energy sector?
- Ensuring that your organisation retains the deep body of operational knowledge needed to maintain critical infrastructure while adapting to the new reality of a hyper-connected OT environment

Samuel Ubido, Information Security Manager, Operational Technology - **Uniper**

Michael Knuchel, Head of SAS Engineering - **Swissgrid**
Janne Hagen, Special Advisor Contingency Planning - **NVE**

17:00

Close of conference day three

Testimonials from Past Events

“Smart Grid Forums is on the leading edge of grid security.”
Don Miller, Chief Technology Evangelist - **Network Perception**

“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**

“Useful and dynamic format to go quickly through a number of topics.”
Mait Sagarra, Cybersecurity services - **Naturgy**

“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**

Conference, Exhibition & Networking Forum

Post-Conference Briefing Offensive Cybersecurity Briefing

Friday 17th June 2022

Briefing Format:

This one-day briefing provides a comprehensive introduction to the opportunities and challenges posed by offensive cybersecurity strategies for the power grid. The day begins with a deep-dive into how the threat landscape is evolving and the tactics, techniques and procedures being employed by cybercriminals and nation state actors specifically targeting the power grid. We explore the application of the Mitra Att@ck framework, the different detection tools and techniques, and the optimal interworking of red and blue teams to maximise awareness and speed up response.

The programme consists of a series of speaker-led presentations, group problem solving exercises, practical simulations, and frequent Q&As. Participation is limited to 30 individuals, to ensure a practical and interactive learning environment.

Briefing Agenda:

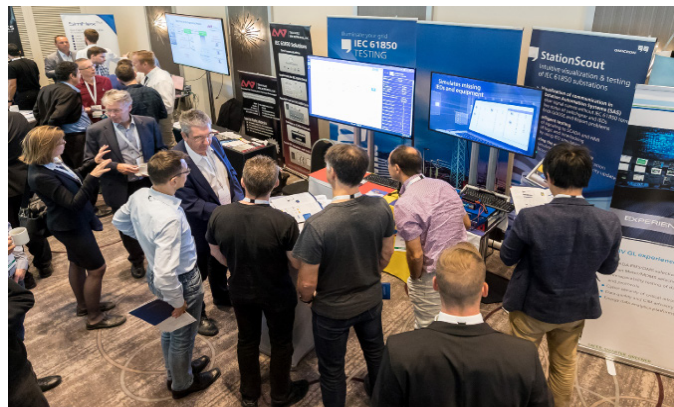
08:30	Welcome address and introduction to the Briefing
	Session 1: Threat Landscape – understanding how the threat landscape is evolving and the risk posed to a rapidly changing power grid environment <ul style="list-style-type: none">Identifying the key cyber criminal and nation state groups currently disrupting and degrading the power gridEvaluating their tactics, techniques and procedures and how these are likely to develop in the near futureDetermining the mix of defensive and offensive cybersecurity strategies required to get ahead and stay ahead of the threat
10:00	Session 2: Utility Case-Study – successfully applying offensive cybersecurity techniques to the OT environment <ul style="list-style-type: none">Determining the regulatory, organisational, operational drivers for employing offensive cybersecurity strategiesSelecting the offensive tools and techniques that will deliver the best return on effort and investmentManaging the application of offensive techniques to minimise risk to operations
11:00	Morning refreshments and networking
11:30	Session 3: Mitre Att@ck – demystifying the framework and optimising its application in the power grid <ul style="list-style-type: none">Understanding the fundamental building blocks of the Mitre Att@ck frameworkLeveraging the framework to understand how different adversary groups are likely to move through the power grid environmentUtilising the database to develop threat models and methodologies to effectively guard the power grid and its ecosystem
12:30	Lunch and networking
13:30	Session 4: Threat Detection – utilising detection tools and techniques to identify legitimate events, correlate alerts across complex attack chains and speed up threat response <ul style="list-style-type: none">Carrying out a thorough risk assessment to ensure the optimal choice of detection tools and techniques against your risk profileExamining the range of detection tools available on the market and fit for purpose for the power gridApplying sophisticated detection techniques that accurately break down the vulnerability and map the attack path
14:30	Session 5: Team set-up – Red-team, Blue-team, Purple-team <ul style="list-style-type: none">Understanding the distinct roles and responsibilities of each teamIdentifying the vulnerabilities that are most likely to be exploited by adversariesDeveloping an action plan that effectively interworks the teams and stimulates effective thought processes
15:30	Afternoon refreshments and networking
16:00	Session 6: Practical Exercise – during this session the groups splits into several smaller groups in order to solve a problem arising from the day's presentations and discussions. This will be followed by a simulation exercise and the day will be concluded with a thorough Q&A session.
17:00	Close of Briefing

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 power grid Cybersecurity leaders and specialists?

Our in-person exhibition area provides the perfect opportunity for you to do this and more! Capped at 10 booths, we ensure a focused and relevant display of state-of-the-art IEC 62443-enabled products and services for our audience, and maximum visibility and interaction levels for each of our exhibitors.

To find out more contact us at: registration@smartgrid-forums.com



Venue

Radisson Blu Hotel, Edinburgh City Centre

The Radisson Blu Hotel, Edinburgh City Centre is located in the heart of the historic Royal Mile in Edinburgh's old town, just a short walk to major city center attractions. Walk to the iconic Edinburgh Castle, National Museum of Scotland, the Scottish Parliament, and Edinburgh's famous shopping thoroughfare, Princes street. The hotel is also within easy reach of Holyrood Palace and Holyrood Park. Arthur's Seat, the park's highest point, has stunning views of the Scottish capital.

Location & website

80 High Street, The Royal Mile, Edinburgh, EH1 1TH, United Kingdom
<https://www.radissonhotels.com/en-us/hotels/radisson-blu-edinburgh>

Accommodation

Email: reservations.edinburgh@radissonblu.com
Telephone: +44 131 557 9797

Briefing Leader:



Phil Tonkin
Senior Director of Strategy
Dragos

Phil Tonkin has worked in the Energy sector for 23 years, starting in the Electricity Transmission sector as a substation engineer. During his career Phil has worked in Electricity Transmission, Distribution & Generation, Gas Transmission, Distribution and Storage as well as in IT. Phil joined Dragos as Senior Director of Strategy in January 2022, before which he led the OT Security Program at National Grid for the UK and US for 5 years. He is a keen contributor to advance cyber security and resilience in the energy sector.

Gold Sponsor:



SUBNET offers cybersecurity software solutions making critical infrastructure more secure & intelligent. We provide innovative solutions that combine the latest in SUBstation technologies with modern-day NETWORKING and computing technologies, enabling electrical utilities to build a smarter, more effective grid. Through our Unified Grid Intelligence (UGI) software solutions, SUBNET will improve the utility's NERC CIP compliance, overall grid reliability, and future-proofing infrastructure for anticipated growth in grid monitoring. SUBNET's Unified Grid Intelligence solutions are based on our 4 flagship products: PowerSYSTEM Center™ | PowerSYSTEM Server™ SubSTATION Server™ | SubSTATION Explorer™

Find out more at: www.subnet.com/

Silver Sponsor:



COPA-DATA is an independent software manufacturer that specializes in digitalization for the manufacturing industry and energy sector. Its zenon® software platform enables users worldwide to automate, manage, monitor, integrate and optimize machines, equipment, buildings and power grids. COPA-DATA combines decades of experience in automation with the potential of digital transformation. In this way, the company supports its customers to achieve their objectives more easily, faster and more efficiently. The family-owned business was founded by Thomas Punzenberger in 1987 in Salzburg, Austria. In 2020, with more than 300 employees worldwide, it generated revenue of EUR 54 million. A sales network of international distributors and 13 subsidiaries ensures that the software is marketed worldwide. More than 300 certified partner companies further support end users with the efficient implementation of the software, particularly in the key industries of food & beverage, energy & infrastructure, automotive and pharmaceutical.

Find out more at: www.copadata.com

Exhibitors:



When it comes to application development, security is paramount. With IriusRisk's automated, scalable and easy-to-use threat modeling platform, your engineers can iron out architectural security flaws before writing code, helping you avoid costly re-design and get to market faster with secure products your customers can rely on.

Find out more at: www.irusrisk.com/



DNV is an independent assurance and risk management provider, operating in more than 100 countries. Through its broad experience and deep expertise DNV advances safety and sustainable performance, sets industry standards, and inspires and invents solutions. DNV combines specialist sector knowledge of with engineering expertise and information system best practice to keep critical infrastructure projects and operations confidently cyber secure. It provides many of the world's most successful and forward-thinking companies with clear and practical advice to uncover their cyber risks, build a powerful force of defence against threats, recover from attacks, and unite stakeholders behind cyber security programmes that everyone can believe in.

Find out more at: dnv.com/cybersecurity



Founded in 2007, the ISASecure Program's mission is to provide the highest level of assurance possible for the cybersecurity of automation control systems. The ISASecure Program has been conducting certifications on automation and control systems since 2011 through its network of ISO/IEC 17065 accredited certification bodies. Founders and key supporters of ISASecure® include BP, Chevron, ExxonMobil, Saudi Aramco, Shell, Honeywell, Johnson Controls, Schneider Electric, Yokogawa, Siemens, exida, TUV Rheinland, CSSC, FM Approvals, Synopsys, DNV-GL, Applied Risk, Trust CB, Security Compass, SGS Espanola de Control, BYHON, TUV SUD, WisePlant HQ, and Bureau Veritas.

Find out more at: <https://www.isasecure.org/en-US/>

Strategic Partner:



The IEC (International Electrotechnical Commission) brings together 173 countries and 20 000 experts who cooperate on the global IEC platform to ensure that products work everywhere safely with each other. The IEC is the world's leading organization that prepares and publishes globally relevant international standards for the whole energy chain, including all electrical, electronic and related technologies, devices and systems. The IEC administers four conformity assessment systems that certify that components, equipment and systems used in homes, offices, healthcare facilities, public spaces, transportation, manufacturing, explosive environments and energy generation are safe, energy efficient and perform to the required standards. IEC work covers a vast range of technologies: power generation (including all renewable energy sources), transmission, distribution, smart grid & smart cities, batteries, home appliances, office and medical equipment, all public and private transportation, semiconductors, fibre optics, nanotechnology, multimedia, information technology, and more.

Find out more at: www.iec.ch/homepage

Media Partners:



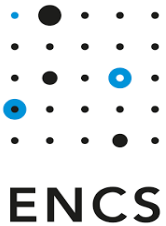
The OSGP Alliance is the global non-profit association dedicated to promoting the adoption of the Open Smart Grid Protocol (OSGP) and infrastructure for smart grid applications towards a future proof modern smart grid. With a key focus on security, smart metering, smart grid, grid analytics, distribution network management and smart cities our members, including utilities, hardware manufacturers, service providers and system integrators, all share a common goal and vision: promoting open standards for energy demand side management, smart grid and smart metering systems.

Find out more at: www.osgp.org/en



Global Smart Energy Federation (GSEF) established in 2010 and formerly known as Global Smart Grid Federation (GSGF), is a global stakeholder organization of national smart grid associations, forward-looking utilities, and think tanks from around the globe working in the domains of energy transition and clean transportation. By linking the major public-private stakeholders and initiatives of participating countries, the federation shares practices, identifies barriers and solutions, fosters innovation, and addresses key technology standards and policy issues. The activities of GSEF help our member organizations and their member utilities in their energy transition and grid modernization initiatives that enhance access to affordable clean energy and increase the security, flexibility and resiliency of the power system while reducing the emissions. GSEF has 16 member countries including India, Indonesia, Mexico, Malaysia, Thailand, Mozambique, South Africa, Botswana, Saint Lucia, USA, Japan, France, South Korea. European Distribution System Operators (E.DSO), an organization promoted by European Commission; and several think-thanks of global repute in also a member of GSEF.

Find out more at: www.globalsmartenergy.org/



The European Network for Cyber Security (ENCS) is a non-profit membership organisation that brings together critical infrastructure stakeholders and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training. ENCS uses its network in academia, government and business to provide cyber security solutions and counsel dedicated to the needs of national Distribution System Operators (DSO), Transport System Operators (TSOs) and regulators.

Find out more at: <https://encs.eu/>



IoT Now - How to run an IoT enabled business. With exclusive analyst reports and specialist journalists, IoT Now is the leading global brand covering the Internet of Things, machine-to-machine communications (M2M), embedded devices and connected consumer devices. Delivering webinars, quarterly magazines, white-papers, daily news and expert opinion pieces and podcasts, IoT Now focuses on the deployment of these technologies across the enterprise, automotive, logistics, healthcare, utilities, travel, security and smart city verticals. To join our community, register at: www.iot-now.com For more information, contact: Cherisse Jameson: c.jameson@wkm-global.com

Find out more at: www.iot-now.com



At Cybersecurity Magazine we first and foremost aim to bring cybersecurity associated information in language accessible to everyone. We feature weekly articles, written and reviewed by experts, and podcasts in various topics around the latest cybersecurity news and developments. We aim to bring quality topical articles that will help professionals and experts in the field, decision makers, and all users of technology. Our monthly podcast features episodes from our editors, with special guest experts, discussing the latest news and relevant topics of cybersecurity.

Find out more at: <https://cybersecurity-magazine.com/>



Energy Digital connects the world's largest energy brands and their most senior executives with the latest trends, industry insight, and influential projects as the world embraces technology and digital transformation. Energy Digital is an established, trusted, and leading voice on all things energy – engaging with a highly targeted audience of global executives. We provide the perfect platform for you to showcase your products and services, share your achievements, and enhance your reputation in the industry.

Find out more at: <https://energydigital.com/>



Infosec-Conferences.com is the community's most popular cybersecurity event directory. Launched in 2013, we list 1,000's of conferences, podcasts, webinars and training events. Join our newsletter to receive event alerts and discount coupons.

Find out more at: <https://infosec-conferences.com/>

Booking Form



Building power grid cyber-resilience through the application of IEC 62443 across the OT asset base

5-Day Conference, Exhibition & Networking Forum
Monday 13th to Friday 17th June 2022 | Edinburgh, UK

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: www.smartgrid-forums.com/iec-62443-week

Delegate Pricing & Discounts

	Very Early Bird Rate Until Friday 25 th March 2022	Early Bird Rate Until Friday 29 th April 2022	Standard Rate After Friday 29 th April 2022
5-Day Delegate - Conference + Fundamentals + Offensive	£3,695 + VAT @ 20% = £4,434	£4,095 + VAT @ 20% = £4,914	£4,495 + VAT @ 20% = £5,394
4-Day Delegate – Conference + Fundamentals Workshop	£2,895 + VAT @ 20% = £3,474	£3,195 + VAT @ 20% = £3,834	£3,495 + VAT @ 20% = £4,194
4-Day Delegate – Conference + Offensive Briefing	£2,895 + VAT @ 20% = £3,474	£3,195 + VAT @ 20% = £3,834	£3,495 + VAT @ 20% = £4,194
3-Day Delegate – Main Conference & Exhibition	£2,195 + VAT @ 20% = £2,634	£2,395 + VAT @ 20% = £2,874	£2,595 + VAT @ 20% = £3,114
1-Day Delegate - Fundamentals of IEC 62443 Workshop	£795 + VAT @ 20% = £954	£895 + VAT @ 20% = £1,074	£995 + VAT @ 20% = £1,194
1-Day Delegate – Offensive Cybersecurity Briefing	£795 + VAT @ 20% = £954	£895 + VAT @ 20% = £1,074	£995 + VAT @ 20% = £1,194
Exhibitor (with 2 x Main Conference Passes)	£5,000 + VAT @ 20% = £6,000	£6,000 + VAT @ 20% = £7,200	£7,000 + VAT @ 20% = £8,400

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 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.