TRAINING SERIES

SMART GRID FORUMS

Fundamentals of IEC 62443 Sept 2023

Early Bird: Friday 28th July 2023

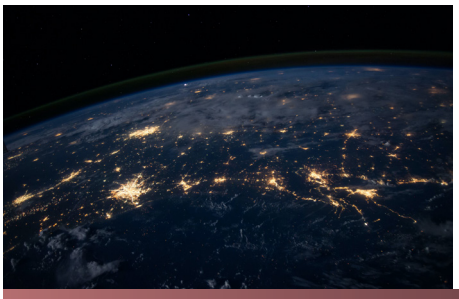
12-Week Online Training for Power Grid Cyber Security Leaders and Specialists

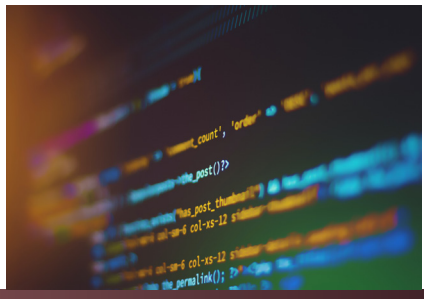
Modules 1-12: 16:00 to 17:30 CET Every Tuesday

Tuesday 5th September to 28th November 2023

Final Exam: Tuesday 5th December 2023

Group Booking Discounts!
Save 10% on 3+ delegates
Save 20% on 5+ delegates
Save 30% on 10+ delegates
Booked from the same organisation at the same time!





Programme Themes Include:

- **Overview:** Understanding the core components of the IEC 62443 family of standards, and how they can be applied as the basis for securing IACS in grid environments alongside overlapping standards such as the ISO 27000 series
- **Resilience:** Getting to grips with key 62443 resilience concepts, technical requirements, and foundational requirements, then practically applying them to define security levels and implement security controls based on criticality
- **Risk Management:** Learning how to conduct high level and detailed risk assessment, provide ongoing security lifecycle development, and demonstrate security to regulators and board
- **Security by Design:** Understanding the technical requirements for components and systems, and developing strategies for communicating with your partner ecosystem

Programme Format Includes:

- **Programme:** 12 x 90-min weekly modules each Tuesday afternoon
- **Modules:** Speaker presentation, practical problem-solving exercise, Q&A, multiple choice quiz
- **Certification:** Weekly 10-question quiz plus final exam to achieve CPD certification

Module Leaders Incude:

Gabriel Faifman
Co-Convenor
TC65 WG10

Siv Houmb
Senior Advisor
Statnett

Michael Knuchel
Head of SAS Engineering
Swissgrid

Rishikesh Sahay
Assistant Professor in Cybersecurity,
Oregon Institute of Technology

Deniz Tugcu
Lead OT Security Specialist
Vattenfall

Tahir Saleem
Senior Specialist OT Security
DEWA

Christopher Robinson
Principal Consultant
Applied Risk

Dale Geach
Head of Digitalisation, IoT and Cybersecurity
Siemens

Maarten Hoeve
Researcher
ENCS

Kelly Stich
Chief Cyber Security Architect
SUBNET Solutions Inc.

Hariharan Ramachandran
Principal Security Assurance
OFGEM

Strategic Partner: IEC

Certification Partner: CPD MEMBER The CPD Certification Service

Produced By: SMART GRID FORUMS Driving Clean Energy

TRAINING SERIES

Dear Colleague,

We are delighted to bring you this Fundamentals of IEC 62443 online training programme. This 12-week community-based learning event has been developed in collaboration with 20+ IEC 62443 specialists from across the smart grid sector, to ensure that your cyber security teams have all the theoretical and practical knowledge they need to embark on their IEC 62443 journey with confidence.

As an international, horizontal series of standards addressing cybersecurity for operational technology in automation and control systems, IEC 62443 is gaining traction as an indispensable tool for securing people, processes, and technology in converged grid environments. Providing technical and process security for operators, component and system manufacturers, and integration and maintenance service providers, IEC 62443 establishes a common language between IACS stakeholders needed to define and implement risk-based security controls across the entire lifecycle of grid assets and systems.

Through 12 x 90-minute modules delivered over 12 weeks, this programme provides a thorough, up-to-date understanding of IEC 61850, including:

• **Resilience:** Getting to grips with key 62443 resilience concepts, technical requirements, and foundational requirements, practically applying them to define security levels and implement security controls based on criticality

• **Risk Management:** Learning how to conduct high level detailed risk assessment, provide ongoing security lifecycle development, and demonstrate security to regulators and board

• **Security by Design:** Understanding the technical requirements for components and systems, and developing strategies for communicating with your partner ecosystem

Each module is comprised of a speaker-led presentation, break-out group problem solving exercise, reporting back and Q&A, and a 10-question quiz. Participants accumulate points during the course of the 12 weeks and take a final exam to achieve CPD certification.

The programme is overseen by Gabriel Faifman, Co-convenor of TC65 WG10, delivered by leading IEC 62443 experts from utilities, consultancies, OEMs, and grid-cybersecurity industry organisations, and certified by the CPD. Places are strictly limited to 30 to ensure an interactive learning environment.

Don't delay! Book your places today and ensure that you and your colleagues are equipped with the crucial IEC 62443 skills and knowledge you need to ensure security over the lifecycle of your assets and systems in support of organisational objectives and the energy transition.

Kind Regards,

Mandana White
CEO | Smart Grid Forums

PS: Very Early Bird – Save up to €1,000 on Delegate places by booking before Friday 26th May 2023

PSS: Group Booking Discount - 10% discount for 3+ delegates, 20% discount for 5+ delegates and 30% discount for 10+ delegates booked from the same organisation at the same time!

Learnworlds Platform

The 12-week programme and final exam will be conducted on the Learnworlds platform which is optimised for training, learning, and examination.

Participants will receive their unique login details the day that the programme begins so that they may set up their user profile and familiarise with the platform features and functionalities in advance of the programme commencing.

All speaker presentations, break-out problem solving sessions, group Q&A sessions, the weekly multiple-choice quiz, and final examination will be conducted on this platform.

Programme Format

This programme is independently produced by Smart Grid Forums, supported by the IEC, and certified by the CPD.

Each module will be led by a different speaker, and consist of:

- 30-min speaker presentation
- 30-min problem solving exercise
- 20-min Q&A session
- 10-min multiple choice quiz

Final Exam & Certification

To achieve CPD certification participants must:

- Attend 70% or more of the modules live
- Review recordings of all missed modules
- Take the 90-min final exam and achieve 70% pass

Testimonials of our Past Cybersecurity Events

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

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

"It was a relief to realise that SGN are not alone in their struggle to implement IEC 62443 requirements. The delegates attending the event were incredibly supportive and patient."

Jayne Crowley, E&I Engineering Policy Manager, **SGN**

"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**

PROGRAMME

Module 1: Tuesday 5th September 2023	Module 2: Tuesday 12th September 2023	Module 3: Tuesday 19th September 2023
Core Components of the Standard - Gaining an overview of the 62443 family of standards to provide a foundation for a risk-based approach to securing IACS in the smart grid environment • Understanding the basic concepts and terminology laid out in IEC 62443-1-1 • Learning the foundational requirements of IEC 62443 to understand methods for securing IACS encompassing People, Processes and Technology • Applying IEC 62443 concepts and models to real-life grid scenarios • Gaining insight into the activities of Working Group TC65 and the roadmap for the ongoing development of IEC 62443 **Gabriel Faifman,** Co-Convenor, **TC65 WG10**	**Understanding IT and OT Requirements - Achieving visibility of OT assets and interdependencies with IT systems to understand how IEC 62443 can provide the basis for OT cybersecurity governance** • Understanding the demands of converged IT and OT architecture and IoT connectivity to apply cybersecurity principles across the grid environment • Determining key cybersecurity objectives and setting policies in line with business and safety drivers and the evolving priorities of availability, confidentiality, and integrity • Applying IEC 62443 to help overcome the nuances of secure data exchange in OT environments with legacy assets and their connectivity with IT systems • Preparing your asset register in readiness for IEC 62443 Risk Assessment **Michael Knuchel,** Head of SAS Engineering, **Swissgrid**	**Key Resilience Concepts - Understanding concepts of defence in depth, zones, and conduits as a basis for grid systems security** • Practically applying the principle of security zones and conduits to grid architecture based on criticality and securing communication between zones • Achieving layered protection based on the military concept of defence in depth by applying cybersecurity countermeasures to people, processes, and technologies • Gaining insight into information exchange requirements to determine appropriate solutions for securing systems, zones, and conduits • Applying operable security by developing a coherent architecture based on IEC 62443 principles • Overcoming common vulnerabilities of IACS operating on a flat network, without segregation to mitigate external threats and avoid communication degradation **Rishikesh Sahay,** Senior OT Security Engineer, **Ørsted**
Module 4: Tuesday 26th September 2023	**Module 5: Tuesday 3rd October 2023**	**Module 6: Tuesday 10th October 2023**
Applying 62443 with other Standards - Mapping IEC 62443 to ISO 27000, NIST, NERC CIP and IEC 62351 to understand the role that various standards play in the development of a cybersecurity management system • Gaining an appreciation of the combination of the key standards needed to manage the complexity and diversity of interconnected smart grid systems • Understanding the overlap between IEC 62443 and ISO 27000 series standards, where they can be applied to complement one another, and the organisational challenges that arise in their joint application • Appreciating the role that each standard plays on a high general level, high energy-specific level, and detailed technical level • Finding the appropriate balance of standards for your organisational priorities based on common requirements in the NIST cybersecurity framework • Developing a CSMS based on an optimal combination of IEC 62443 with other standards to ensure compliance to national and transnational cybersecurity regulations **Maarten Hoeve,** Researcher, **ENCS**	**Conducting 62443 risk Assessment - Applying IEC 62443 3-2 to conduct a risk assessment in support of organisational goals and regulatory compliance** • Understanding criticality and taking a balanced approach to risk, likelihood, and consequence • Defining boundaries of systems under consideration and integrating operational, and safety considerations when assessing IACS risk • Conducting high level risk assessment to support the business case and rationale • Performing detailed risk assessment in alignment with IEC 62443 3-2 • Demonstrating compliance against organisational and regulatory requirements using risk assessment methodologies and frameworks **Tahir Saleem,** Senior Specialist, OT Security, **DEWA**	**Technical Requirements for Products or Components - Gaining an appreciation of IEC 62443 4-2 vendor requirements to establish a common language with your partner ecosystem** • Learning the seven foundational requirements for each component type detailed in IEC 62443 4-2 • Evaluating security by design principles against real software applications, embedded devices, host devices, and network devices • Leveraging the NIST secure software development framework requirements mapped to IEC 62443 controls • Developing a collaborative approach with vendors to set achievable technical specifications for the security level of components and simplify product selection • Creating security documentation for all components in your system to tangible, measurable, demonstrable compliance **Dale Geach,** Head of Digitalisation, IoT and Cybersecurity, **Siemens**
Module 7: Tuesday 24th October 2023	**Module 8: Tuesday 31st October 2023**	**Module 9: Tuesday 7th November 2023**
Requirements for Integrators - Leveraging IEC 62443 2-4, Technical requirements for systems to support the secure design and implementation of grid systems • Classifying security, confidentiality, availability, integrity and safety from the beginning of a partnership with an integrator to gain oversight of systems and avoid the need to retrofit controls • Contextualising overall system security with the likelihood and impact of threat and vulnerabilities across IT, OT, IoT and Cloud architecture • Utilizing zones and conduits to implement security · Effectively quantifying, communicating, and managing risk for the purposes of system design • Providing confidence in each phase of the implementation journey with the systematic use of IEC 62443 to ensure lifecycle operability and security **Kelly Stich,** Chief Cyber Security Architect, **SUBNET Solutions Inc.**	**Security Lifecycle Development - Lifecycle development framework to manage patching and lifecycle demands of industrial control systems** • Using the NIST secure lifecycle development framework - Identify, detect, protect, respond, and recover as a basis for applying IEC 62443 across your systems' lifecycle • Leveraging IEC 62443 2-1 CSMS requirements to develop a cost-effective and secure approach to patch management and maintenance of PLCs and IACS devices and legacy operating systems • Overcoming challenges of continuously improving from a relatively low level of maturity after IEC 62443 certification • Developing a continuous system monitoring capability to conduct effective forensic analysis and enhance visibility • Using IEC 62443 4-1 secure system development to engrain security by design • Hardening your incident response and recovery capabilities **Hariharan Ramachandran,** Principal Security, Assurance, **OFGEM**	**Defining Security Levels - Using IEC 62443 to define security levels based on the criticality of assets mapped with threat and adversarial capability** • Assessing criticality and applying security levels to zones, conduits, and products • Grouping assets and systems into security zones within your architecture and defining countermeasures to meet the required security level • Mapping foundational requirements to security level requirements to inform your defence-in-depth strategy • Aligning asset vulnerabilities to real threat and adversarial levels • Practically applying security levels in line with organisational risk acceptance and budgetary constraint **Deniz Tugcu,** Lead OT Security Specialist, **Vattenfall**
Module 10: Tuesday 14th November 2023	**Module 11: Tuesday 21st November 2023**	**Module 12: Tuesday 28th November 2023**
Setting Security Controls in Specific Grid Environments - Using IEC 62443 3-3 technical requirements and suggestions for countermeasures to apply specific security measures in key grid domains • Evaluating existing countermeasures and selecting additional countermeasures based on criticality, cost, complexity, and effectiveness • Conducting IEC 62443 3-3 gap analysis • Developing a plan to address unacceptable risk, considering the foundational requirements of use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability • Learning how to apply controls in specific DSO and TSO environments within real operational, budgetary and system constraints **Siv Houmb,** Senior Adviser, **Statnett**	**Maturity Level - Including IEC 62443 specifications in procurement documentation to ensure the maturity level of component providers and capability of integrators** • Learning the requirements throughout product development and integration to assess IEC 62443 maturity levels • Understanding the documentation required to demonstrate security throughout the product lifecycle, support, quality control, performance validation, and vulnerability response requirements under IEC 62443 • Combining Security Levels and Maturity Levels to define security protection ratings and effectively communicate specifications to partners in tendering documents • Providing clarity on internal security requirements, and effectively communicating with partners to drive efficiency, support regulatory compliance, and enable security by design **Gabriel Faifman,** Co-Convenor, **TC65 WG10**	**Certification and Testing - Using IEC 62443 certification to provide demonstrable security for regulators and the board** • Defining a methodology for validating the authenticity of testing and certification institutions to guarantee trust in component certification • Overcoming supply chain visibility challenges on a sub-component level and defining mitigation where there is any uncertainty • Collaborating with integrators to ensure demonstrable testing and certification of components and systems and developing adequate tools to document the processes • Simplifying and accelerating the process of providing evidence of methods used to continuously ensure IACS security to regulators **Christopher Robinson,** Principal Consultant, **Applied Risk**

MODULE SPEAKERS

Gabriel Faifman, Co-convener**, TC65 WG10**

Highly qualified with diverse experience as Director, Manager and Senior Consultant in Information Systems and Network Security on many projects within Schneider Electric; Wurldtech; GE; Accenture; BC Hydro; YVR (Vancouver International Airport); France Telecom; BellSouth; Deloitte & Touche, and Coca Cola. US Patented Invention for 'Automated Certification Based on Role'. Product & System Security Office member, in charge of the Cybersecurity Strategic Domain at Schneider Electric;
Formerly Director of Strategic Programs and Principal Technical Product Manager with Wurldtech (acquired by GE Digital) for over 7 years. Electronic Engineer UBA, specialized in Industrial Automation; CSS1 Infosec professional; Advanced trained at INL. Serving as co-convenor for IEC TC 65 WG 10 since 2020. Serving as an SME for the TC65 working group on the IEC 62443 international standards project since 2011, representing Canada (Canadian Delegate). Created and executed the original conformance criteria adopted by IECEE on the current IEC 62443-2-4 certification program. IEC 62443-2-4 certifier for: Schneider Electric's substation automation solution; Siemens Substation Automation; Siemens PCS7; Emerson DeltaV & SIS; Yokogawa Centum VP among others. ISASecure – Steering committee member, representing Schneider Electric since 2019.

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

Michael Knuchel graduated in Electronics Engineering and has a Master at the ETH in Management, Technology and Economics. He is working as Head of Engineering SAS for Swissgrid and is additionally responsible for the Cyber Security Projects in the OT environment. He was Project Manager and one of the Authors of the Cyber Security Framework of Swissgrid for substations. Michael Knuchel has gathered experience in the OT field leading international commissioning teams for Substation Automation Systems for five years for ABB worldwide. He is Chairman of the cyber security task force of the Electricity Industry Association.

Rishikesh Sahay, Assistant Professor in Cybersecurity, **Oregon Institute of Technology**

Rishikesh Sahay is an Assistant professor in Cybersecurity at Oregon Institute of Technology, USA. He is a certified IEC/ISA 62443 Cyber Risk Assessment Specialist. Before moving to academia in the US he has worked in industry with companies like Orsted and MAN Energy Solutions as a cybersecurity specialist in Denmark. There he has worked in cyber risk assessment & mitigation and compliance according to the IEC 62443 cybersecurity and NERC-CIP. He did his Postdoctoral research at the Technical University of Denmark (DTU). At the DTU, he developed a cyber risk assessment framework for critical infrastructures.
He did his PhD from Sorbonne University in France in 2017. His PhD thesis was focused on autonomic cyber defense using software-defined networking.
His interests include Cyber risk assessment & mitigation, compliance, autonomic cyber defense, policy-based network management, software-defined networking, cyber resilience, and network security.

Maarten Hoeve, Researcher**, ENCS**

Maarten Hoeve works at ENCS, a cooperative owned by different TSOs and DSOs to share knowledge on cybersecurity. He has helped many of ENCS's members with performing risk assessments for their OT systems, and with setting security requirements in procurement projects. He was part of the drafting team for the upcoming network code on cybersecurity, where he worked on supply chain security and risk management.

Tahir Saleem, Senior Specialist, OT Security, **DEWA**

Tahir commands over a decade of professional experience in OT/ ICS domains with proven expertise in security strategy development, architecture design & engineering, mission-critical operation support, commissioning and maintenance of security services for owners and operators of critical infrastructure services covering: power & water, mining, transport (rail), and oil & gas products.
Tahir is currently working with the Dubai Electricity & Water Authority to build, develop and continually improve the OT security capability for the organization.

MODULE SPEAKERS

Dale Geach, Technology and Innovation Manager, **Siemens**

Dale is a business lead with an engineering background and over 29 years' experience within the energy sector, working with industry customers and partners to understand the challenges faced in delivering a secure and sustainable transition to a cleaner, distributed, and digitalised energy system. As Head of Digitalisation, IOT and Cybersecurity for the Electrification and Automation unit within the Siemens Smart Infrastructure business, Dale is responsible for secure portfolio and services development which serves not only the current needs of industry, but more importantly the technology and service needs of the evolving digitalised and cyber resilient Smart Grid.

Hariharan Ramachandran, Principal Security Assurance, **OFGEM**

Hari is a professional chartered Engineer with 20 years of experience in Engineering, Operations Management, Compliance, and Regulations. He has worked on a multitude of high-profile global engineering projects from conceptual, through FEED and detailed design, to site construction, commissioning, and follow-on operational support, in a wide range of highly critical industrial sectors. His special field of expertise comprises Instrumentation, Functional Safety, and Cyber security of Industrial Automation and Control systems. He is a member of the Cyber Special Interest group, InstMC, and a member of the IEC 62443 standards working group(WG) 10 and 20. He is currently pursuing his Doctorate in Industrial CyberSecurity at De-Montfort University, UK.

Deniz Tugcu, Lead OT Security Specialist**, Vattenfall**

Lead Senior Principal Security Consultant, trapped first cyber criminals (industry spies) back in 1994 by building his own dual bastion host with a breadcrumb honey net. Created (OT Security) results in various business sectors and companies, ranging from finance, United Nations to Global Renewable Energy. Eclectic and curious, looking for new ways to grow and improve security and the world. Currently piloting "FacOTry" enabling Security Automation and Orchestration, for scalable and efficient defence and operation of OT assets. Lives in Copenhagen, enjoys: running , exploration of craftsmanship (ha-ha. Known by co-workers as the CPH pitbull).

Siv Houmb, Senior Advisor, **Statnett**

Dr. Siv Hilde Houmb has a PhD in cybersecurity and decision theory and more than 25 years' experience in cybersecurity and critical infrastructure. She has a long and extensive industry background (more than 20 years), and her experience covers risk assessment, security protocols development, attack protection strategies, ethical hacking (penetration testing) and monitoring and surveillance technology for cybersecurity. She has engineered several security protocols and technical security solutions covering hardware, operating systems, applications and communications. She has worked as a security researcher both nationally and internationally and has published more than 50 scientific papers and articles on information security and risk assessment. Dr. Houmb has over the last 10 years focused on cybersecurity challenges for critical infrastructure, including Advanced Persistent Threats (APT) and how they could be used to severely impact a Nation's core infrastructure.

Christopher Robinson, Principal Consultant, **Applied Risk**

Chris is a Principal Consultant at Applied Risk/DNV where he applies his expertise to various ICS cybersecurity projects to ensure solutions meet the needs of a modern industrial control system. In addition, Chris performs various red team activities such penetration testing, network architecture reviews, and firewall configurations. Chris holds both a Bachelor and Master of Science in Computer Science and maintains multiple certifications, including the GICSP, OSCP, GPEN, CISSP, GISP, GISF, and CEH. Chris has taught SANS MGT414, MGT415, and ICS410 courses and is one of the co-authors of ICS612. He currently resides in London, UK.

Kelly Stich, Chief Cyber Security Architect, **SUBNET Solutions Inc.**

Kelly Stich is a registered Professional Engineer in British Columbia, Canada. Kelly has expertise in the domains of protection, control, automation, and OT cybersecurity. He worked at BC Hydro for over 16 years where he held roles such as Technical Lead for Transmission NERC CIP compliance and Specialist Engineer in Protection and Control Planning. Kelly has developed system architectures for secure remote access, arc flash mitigation, distribution protection and automation using GOOSE messaging, and established the programs for substation security patching and change management. At SUBNET, he is currently supporting NERC CIP, IEC 62443, and NIST CSF implementations for our utility partners.

REGISTRATION

SMART GRID FORUMS

Fundamentals of IEC 62443 Sept 2023

Early Bird: Friday 28th July 2023

12-Week Online Training for Power Grid Cyber Security Leaders and Specialists

Modules 1-12: 16:00 to 17:30 CET Every Tuesday

Tuesday 5th September to 28th November 2023

Final Exam: Tuesday 5th December 2023

Group Booking Discounts!
Save 10% on 3+ delegates
Save 20% on 5+ delegates
Save 30% on 10+ delegates
Booked from the same organisation at the same time!

To find out how you can participate as a Delegate:

Call: +44 (0)20 8057 1700
Email: registration@smartgrid-forums.com
Visit: www.smartgrid-forums.com/fundamentals-iec62443

Pricing & Discounts

Packages & Prices	~~Very Early Bird Rate Until Friday 26th May 2023~~	Early Bird Rate Until Friday 28th July 2023	Standard Rate
Delegate Ticket 12 weeks + final exam	~~€3,995.00~~	€4,495.00	€4,995.00
Delegate Ticket 3+ at 10% discount	~~€3,595.50~~	€4,045.50	€4,495.50
Delegate ticket 5+ at 20% discount	~~€3,196.00~~	€3,596.00	€3,996.00
Delegate Ticket 10+ at 30% discount	~~€2,796.50~~	€3,146.50	€3,496.50

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.