training@sans.org 020 3384 3470 www.sans.org/ics-london-2016

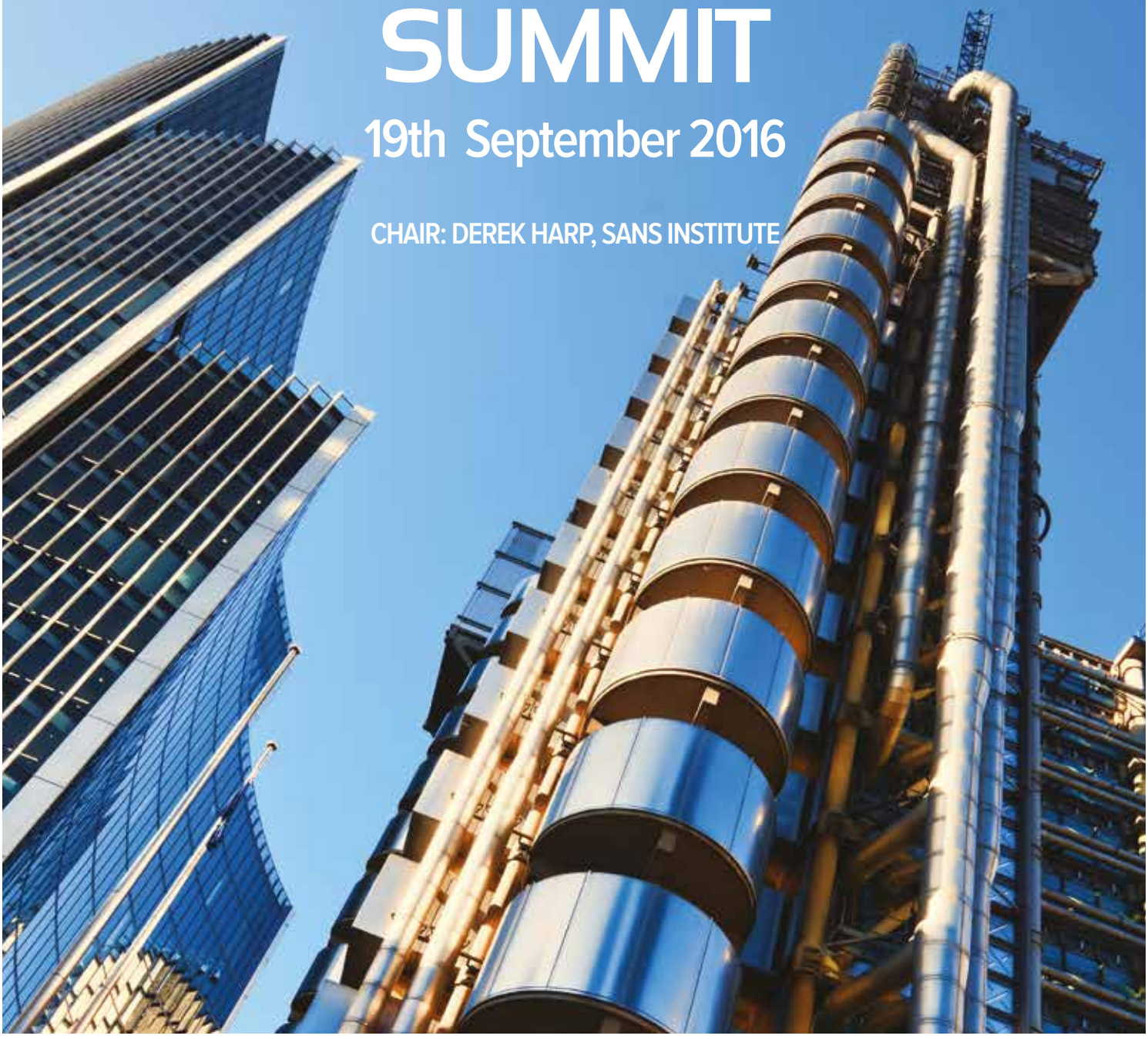
SANS EMEA

Grand Connaught Rooms, 61-65 Great Queen Street, London, WC2B 5DA

SANS EUROPEAN ICS SECURITY SUMMIT

19th September 2016

CHAIR: DEREK HARP, SANS INSTITUTE



Monday 19 September, 2016

8:30 – 8:50 am	**Coffee and Registration**
9:00 – 9:25 am	**Welcome and Introduction** To include key highlights from the SANS ICS 2016 Security Survey **Derek Harp:** *SANS Institute*
9:25 – 9:55 am	**How do you know if you are doing enough?** Cyber Security discussions often gravitate quickly towards technical topics and trying to find solutions to problems aligned with the engineering mind-set. However, how do we communicate the value of cyber security programs and cyber security spending to our leadership? When asked the questions "are we doing the right things?" and "are we doing them fast enough?" are we able to articulate that story and present the value of a mature security capability in business terms, to our most senior leadership? This presentation will show the journey that started in a board room and the steps taken by the cyber security organization to answer what seemed to be simple questions. The presentation will not only feature the insights and lessons learned from ABB but also the views and challenges as seen by KPMG, the external experts that were brought in to help assess ABB's global cyber security initiative. **Davide Zanetti:** *ABB* **Jano Bermudes:** *KPMG*
9:55 – 10:25 am	**Cyber Security in a Heterogeneous Critical OT Environment** Keeping the London Underground safe and reliable requires the continual operation of multiple diverse Operational Systems and Assets simultaneously. Establishing a unified approach for managing the cyber security risk throughout the entire Operational Technology lifecycle requires embedding cyber security into the organisation culture and the procurement, assurance, handover, operations and maintenance regimes. A realistic starting point is a cyber security framework focused on balancing the implementation of fit-for-operation cyber security technical controls and processes. This supports the achievement of the operational railway performance, availability, maintainability and safety targets/objectives whilst using the existing London Underground operational capabilities and its employees as the core factor for starting to build the solutions and arrangements. This session will introduce the practices, principles, thoughts and lessons learnt experienced during the journey to protect London Underground Operational Systems and Engineering Assets. **Luis Parrondo:** *TFL*

10:25 – 10:55 am	**Coffee Break**
10:55 – 11:25 am	**The Stale Data Problem – A look at a CyberPhysical Weakness** For the last couple of decades, defending industrial systems from cyber attack was really about defending the electronic infrastructure that ran the industrial process. What the process was actually doing only entered into the thought process when assigning the potential damage that could be caused if a particular device was compromised. A paint factory and an oil refinery were defended in the same way. With the rise of CyberPhysical systems we have come to realize that the electronics running the process can no longer be studied separately from the physics of the process itself. Defenders can now legitimately choose between adding additional monitoring to a device or adding a physical protection such as an overspeed interrupter to mitigate a possible attack strategy. While viewing a process as a CyberPhysical system enables better defense, it also allows for new attacks. The presentation will cover the "Stale Data Problem". The most common algorithm for controlling a feedback loop is a PID controller. A PID loop will often cycle at a rate much faster than the data arrives from the field. A common setup is for the loop to operate on the last known good value instead of the algorithm blocking until a full set of new data arrives. On the other hand, the design of the algorithm makes assumptions about the timeliness of the data and the response time of the process once the data has changed. In this presentation, an example weakness will be shown where the timing of the arrival of the data is manipulated by the attacker to influence the function of the PID loop and therefore the target process. This will serve as an example of a weakness that can only be studied as a CyberPhysical system and not as separate cyber and physics problems. **Jason Larsen:** *IO Active*
11:25 – 11:55 am	**Industrial Defence In-Depth** This presentation will look at a specific example, the features of industrial customers, the difference between the Defence In-Depth concept for industrial objects, and what kind of cyber security products and services should be used. What organizational measures should be taken and, most importantly, how to find a balance between ensuring cyber security and technological process continuity. **Andrey Doukhvalov & Andrey Nikishin:** *Kaspersky Lab*
11:55 am – 12:25 pm	**Creating and Sustaining ICS Cyber Forensics Programs** This presentation covers the process of creating an effective incident response capability in the ICS environment. Key takeaways include understanding the differences in performing IR in the ICS environment and the additional data that needs to be collected to compensate for the lack of tools available for doing this work. **Eric Cornelius:** *Cylance*

12:25 – 1:25 pm	**Lunch**
1:25 – 1:55 pm	**The Auto Industry's Paradigm Shift** The move from gas to electric engines, autonomous driving, and car sharing instead of car ownership are very fundamental paradigm shifts that will significantly alter personal transportation and the auto industry. All of these changes are driven by the disruptive forces of information technology and thus we find ourselves in a situation where a very regulated and settled down industry is on a head-on collision with the „Web 2.0" style of creating products that never really leave the beta stage. Stunt hacks that exploit vulnerabilities in vehicles and automation systems that overpromise and underdeliver are beginning to force knee jerk reactions from legislators. Add to that the ever growing hunger for the data generated by vehicles about driver behavior as one example, we are facing some interesting challenges down the road. This presentation will focus on some of the safety and security issues caused by these fundamental changes to car design and operation and look at some of the open questions and possible answers to deal with these challenges. **Kai Thomsen:** *Audi*
1:55 – 2:50 pm	**Audience Interactive Session – What's Important to You?** **Doug Wylie:** *NexDefense*
2:50 – 3:20 pm	**Coffee Break**
3:20 – 3:50 pm	**Fail to Plan – Plan to Fail** Preparation is the poor cousin of all of the steps involved in the incident handling process. This talk should make you rethink how your business can prepare and avoid common "show-stoppers" that kill your ability to handle an incident. We then examine an irreverent case study about how "bad" can get "worse". **Don Reynolds:** *CRH*
3:50 – 4:25 pm	**The GICSP: A Cornerstone Certification** At two years of age, the Global Industrial Cyber Security Professional (GICSP) is now well established as the leading ICS security certification. This brief session will discuss the origins of the credential and its ongoing development. Included will be information on the whitepaper which the GICSP Steering Committee, in collaboration with SANS Institute, are issuing to mark the issuance of the 1,000th GICSP certification, and a preliminary look at research into how certification has affected and empowered its holders to be more effective in their jobs, how practitioners value to their company and industry has increased, and how certified professionals are moving their careers forward. **Doug Wylie:** *NexDefense* **Derek Harp:** *SANS ICS*

4:25 – 5:10 pm	**Analysis of the Cyber Attack on the Ukrainian Power Grid** On Dec 23, 2015 the Ukrainian power grid suffered outages to roughly 230,000 customers due to a cyber attack. This was the first ever public cyber attack on a power grid that led to outages and holds lessons for a wide variety of communities. The SANS ICS team broke the news on the malware uncovered and later confirmed the cyber attack. Of particular note was that the malware enabled the attack but did not cause the outage. In this presentation learn about the investigation, the analysis, and the lessons learned for the larger community. **Robert M. Lee:** *SANS Institute* **Mike Assante:** *SANS Institute*
5:10 – 5:20 pm	**CLOSING**
5:30 – 7:30 pm	**Networking Drinks**

Speaker Bios:

Andrey Doukhvalov

Chief Strategy Architect, Head of Future Technologies at Kaspersky Lab. Working in the software business for almost 30 years, Andrey has been employed in various roles – from software engineer to software project leader – in system and application-level software development projects. For the last 17 years Andrey has been developing security software at Kaspersky Lab. One of Andrey's key current projects is the radically new secure operating system being developed as a platform dedicated to a wide range of specialized solutions where trust is of paramount importance.

Andrey Nikishin

In a career that stretches back to the early days of Kaspersky Lab, Andrey worked as a Senior Software Engineer and Architect before moving to the Strategic Marketing Department as a Product Strategy Manager. Prior to his present role, Andrey headed the Cloud and Content Technologies Research and Development Department. Before joining Kaspersky Lab, Andrey had several years of experience developing his own antivirus programs. Andrey has a degree from the Baltic State Technical University in St. Petersburg and received his MBA from the London Business School.

Davide Zanetti

Davide Zanetti is Cyber Security Program Manager at ABB Group.

In his current position, Davide is responsible for driving and implementing global cyber security initiatives that help to ensure ABB offerings - product, systems, and services - support customers' cyber security needs and requirements.

Davide also supports the ABB Group Cyber Security Council, which is a global, cross-functional organization that works with all ABB divisions and group functions, in defining and implementing ABB's cyber security strategy, governance, and assurance.

Prior to joining ABB, he held several R&D and cyber security positions in the telecommunication and healthcare sectors.

Davide holds a Ph.D. in Computer Science (research focused on system security) from the Federal Institute of Technology (ETH) in Zurich, Switzerland.

Derek Harp

Derek Harp is the Director for ICS Strategic Programs at SANS and the GICSP Steering Committee Chair. He is responsible for organising events, resources and initiatives that educate and enable increased collaboration within the entire ICS security community. Mr. Harp has served as a founder, CEO, or advisor of early-stage companies for the last 18 years with a focus on cybersecurity. Derek is also a co-founder and a board member of NexDefense, Inc., a company focused on the security technology needs of ICS asset owners. Previously, he was the CEO and co-founder of LogiKeep, Inc., where he was the co-inventor of Intellishield™, a pioneer IT security product which was subsequently acquired. Mr. Harp is a former U.S. Navy Officer with experience in combat information management, communications security, and intelligence.

Don Reynolds

Don works as the technical security lead for a fortune 500 multinational construction materials group, Cement Roadstone Holdings. His background is commercial incident handling, having worked in the telecommunications, power and finance sectors. He is a passionate believer in real security and is allergic to hype and advanced persistent marketing.

Doug Wylie

Doug Wylie is a seasoned business practitioner, industry thought leader and certified security professional with extensive experience as a global market-maker for industrial products, open technologies and contemporary solutions used in mission-critical applications.

In his current role, Doug directs and promotes NexDefense's position and perspective on emerging market demands, industrial networking, and the ever-evolving security trends that affect customers across an array of industries and applications. His focus includes identifying and solving real-world customer challenges, while similarly establishing relevant solutions that increase visibility and operational knowledge to counteract risks that may impact safety, integrity, information security and productivity.

Prior to NexDefense, Doug worked for Rockwell Automation and performed most recently as Director, Product Security Risk Management reporting to the Office of General Counsel and CISO. He earned the prestigious 2013 SANS People Who Made a Difference in Cybersecurity award and actively maintains his Certified Information Systems Security Professional certification (CISSP® 435349). Doug holds his Bachelor of Science in Business Administration from John Carroll University in Cleveland, Ohio and numerous internationally-recognized patents related to industrial communications, control and software technologies.

Eric Cornelius

Eric Cornelius is the Director of Critical Infrastructure and Industrial Control Systems (ICS) at Cylance, Inc. He is responsible for the thought leadership, architecture and consulting implementations for the Company. His leadership keeps organizations safe, secure and resilient against advanced attackers.

Previously, Eric served as the Deputy Director and Chief Technical Analyst for the Control Systems Security Program at the US Department of Homeland Security. Eric brings a wealth of ICS knowledge to the Cylance team. In addition to his years of technical leadership, Eric literally wrote the book on incident response in the ICS arena. Eric's extensive knowledge of critical infrastructure and those who attack it will be brought to bear at Cylance as he leads a team of experts in securing America's critical systems.

Eric is the co-author of "Recommended Practice: Creating Cyber Forensics Plans for Control Systems" as part of the DHS National Cyber Security Division, Control Systems Security Program, 2008.

He is also a frequent speaker and instructor at ICS events across the globe.

Cornelius earned a bachelor's degree from the New Mexico Institute of Mining and Technology where he was the recipient of many scholarships and awards including the National Science Foundation's Scholarship for Service. Cornelius went on to work at the Army Research Laboratory's Survivability/Lethality Analysis Directorate where he worked to secure field deployable combat technologies. It was at ARL that Cornelius became interested in non-traditional computing systems, an interest which ultimately led him to the Idaho National Laboratory.

While at INL, Cornelius participated in deep-dive vulnerability assessments of a wide range of ICS systems. After attacking these systems for several years, Cornelius began to develop methodologies for detecting attacks and performing incident response in the ICS environment.

Cornelius has continually improved these methodologies through extensive field testing and close partnership with asset owner/operators in nearly all sectors of critical infrastructure. Through this experience, Cornelius will help keep Cylance on the forefront of ICS security to better protect America's critical assets.

Jano Bermudes

Jano is a Director in KPMG's Cyber Security Practice and leader of the Industrial Security Controls Capability Group. He is a consultant, developer, network engineer and security solutions architect with 15+ years of experience helping clients designing, building operating and securing critical infrastructure. In addition to the Industrial Security Capability Group he also heads up the Strategy Risk and Architecture Capability Groups at KPMG and support clients with complex security transformations that help them recover from major security breaches that have impacted several industries in recent years. Jano has led

transformation engagements across numerous industry sectors such as Oil & Gas, Industrial Manufacturing, Pharma and Telco's, where he has held senior operational positions and led multi-million pound engagements.

Jason Larson

Jason Larsen is a professional hacker that specializes in critical infrastructure. He was a founding member of the industrial control system program at the Idaho National Labs and has tested devices from most of the major industrial control systems. Previously he's worked on a wide variety of topics from radiation therapy for cancer to anonymous relay networks. When he's not speaking at conferences, Jason spends his time doing focused research into practical remote physical damage for IOActive.

Kai Thomsen

Kai has been working in various IT Security roles for more than fifteen years, most of the time in what nowadays is called Incident Response. He has been working at AUDI AG since 2013. In his first role there as IT Service Continuity Manager he developed and established a Business Continuity organization in the IT department. Since 2015 he is back to his DFIR roots, tasked with developing an Incident Response Team and working as IR team lead and forensicator.

Prior to Audi, he worked for twelve years at SMS group, an engineering company for steel manufacturing plants. There he was responsible for network security and forensics.

Kai is very passionate about learning and teaching security methodologies that actually help defenders make a difference and sometimes even win one fight or the other. On rainy days in the office he likes to make the never ending supply of sales droids eat their own words.

Luis Parrondo

Luis Parrondo is the Principal Cyber Security Architect of London Underground, Transport for London. He is responsible for continuously managing the Operational Systems and Engineering Assets Cyber Security risk which requires capital delivery & supply chain Cyber Security assurance, legacy assets Cyber Security improvement and the Cyber Security integration with the Operations & Maintenance processes.

Prior to joining London Underground, he served as Principal Security Consultant for the world's largest company purely focused on automation and controls as well as different consultancy entities. Throughout his career, he has worked on most Critical Infrastructure sectors, engaging with asset owners on the delivery of greenfield/brownfield projects and developing Industrial Cyber Security programmes & operations assurance frameworks.

Luis holds various Cyber Security certifications including CISSP, CISM, CISA, GICSP and a degree from the University of Oviedo. Parallel, he is collaborating with ENISA (European Union Agency for Network and Information Security) as an Expert on the Security and resilience of Intelligent Public Transports in the context of Smart Cities.

Michael Assante

Michael Assante is currently the SANS lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security and co-founder of NexDefense an Atlanta-based ICS security company. He served as Vice President and Chief Security Officer of the North American Electric Reliability (NERC) Corporation, where he oversaw industry-wide implementation of cyber security standards across the continent. Prior to joining NERC, Mr. Assante held a number of high-level positions at Idaho National Labs and served as Vice President and Chief Security Officer for American Electric Power. Mr. Assante's work in ICS security has been widely recognized and he was selected by his peers as the winner of Information Security Magazine's security leadership award for his efforts as a strategic thinker. The RSA 2005 Conference awarded him its outstanding achievement award in the practice of security within an organization.

He has testified before the US Senate and House and was an initial member of the Commission on Cyber Security for the 44th Presidency. Before his career in security, Mr. Assante served in various naval intelligence and information warfare roles. He developed and gave presentations on the latest technology and security threats to the Chairman of the Joint Chiefs of Staff, Director of the National Security Agency, and other leading government officials. In 1997, he was honoured as a Naval Intelligence Officer of the Year.

Robert M. Lee

Robert M. Lee is a co-founder at the critical infrastructure cyber security company Dragos Security LLC where he has a passion for control system packet analysis, digital forensics, and threat intelligence research. He is the course author of SANS ICS515 - "Active Defense and

Incident Response" and the co-author of SANS FOR578 - "Cyber Threat Intelligence." He is a passionate educator although he should not be confused with the other Rob Lee at SANS - that Rob Lee is cooler but has less hair.

Robert obtained his start in cyber security in the U.S. Air Force where he currently serves as a Cyber Warfare Operations Officer. He has performed defense, intelligence, and attack missions in various government organizations including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Robert routinely writes articles and journals in publications such as Control Engineering, Air and Space Power Journal, Wired, and Passcode. He is also a frequent speaker at conferences and is currently pursuing his PhD at Kings College London with research into the cyber security of control systems. Robert is also the author of the book "SCADA and Me" and the web-comic www.LittleBobbyComic.com

NB This agenda should be considered a draft and the organisers will continue to make amendments to content and line up.