Industrial Control Cybersecurity Europe 2015

Subject to change
For opportunities contact:
James Nesbitt, james.nesbitt@cybersenate.com
+44(0)207 096 1754 UK

29th and 30th September 2015

Pre Conference Workshop September 28th
Crowne Plaza, London, Docklands, UK

CYBER SENATE

Our Key Sponsors

CYLANCE

SIEMENS

paloalto NETWORKS®

LOCKHEED MARTIN

Applied Risk

codenomicon

www.industrialcontrolsecurityeurope.com

To register call +44 (0)20 7096 1754 or email marketing@cybersenate.com

THE GOAL OF THE CONFERENCE

All stakeholders have a new responsibility in ensuring the safety, reliability and stability of our Critical National Infrastructure. Public and Private partnerships are paramount and information sharing on an international level a priority. We will be addressing key areas of vulnerability, threat detection, mitigation, and planning for the Energy, Oil, Gas, Electric and Water Sector.

The Industrial Control Cybersecurity conference consists of presentations and debate from some of the energy industry's leading end users from Operational and IT backgrounds, Government influencers, leading cybersecurity authorities and some of the world's most influential solution providers.

Key topics of discussion will pivot on convergence of operational and information technology transformation, design, implementation, integration and risks associated with enterprise facing architecture.

Further review includes the development of policy, operational and cultural considerations, maturity models, public and private information sharing and the adoption of cybersecurity controls.

2015 will provide further insight into how industry can further develop organisational priorities, effective methodologies, benchmark return on investment for cybersecurity procurement, supplier relationships and how to effectively deploy defense in-depth strategies.

We will introduce discussion on the latest attacks and hear from those who are responsible for identifying them. The conference will further address penetration testing, the art of detection and threat monitoring, incident response and recovery.

Goals of the conference

The goal of the conference – to enhance dialogue and information sharing between public and private sectors, providing participants an opportunity to contribute and engage on some of our country's most pressing security threats surrounding critical national infrastructure. Our vision as a collective to enhance resilience and the adoption of cybersecurity controls within the Energy, Water, Oil, Gas, Electric, Chemical and Nuclear sector.

Why you cannot miss 2015

- Gain further understanding of the risks and opportunities created by the convergence of operational and information technology
- current areas of vulnerability, threat detection, mitigation, maturity capability models and risk management.
- Take away tools to assist in developing organisational priorities, methodologies and how to effectively deploy defense in-depth strategies.
- Hear how your industry counterparts are defining and benchmarking return on investment for cybersecurity procurement, supplier responsibilities and adapting new models for incident response.
- Take part and contribute to the technological transformation IT/OT shift involving design, implementation and integration requiring the collaborative efforts of two unique but historically different skillsets.

Target Audience

The Industrial Control Cybersecurity Europe conference consists of presentations, debate and contribution from some of the energy industry's leading Chief Information Security Officers, Operational and IT Divisional Heads, Government influencers and world leading cybersecurity authorities and solution providers. Our focus is on providing a educational platform to enhance resiliency and public and private information sharing, with a heavy focus on end users and responsibility.

CYLANCE

Cylance is the first company to apply artificial intelligence, algorithmic science and machine learning to cyber security and improve the way companies, governments and end users proactively solve the world's most difficult security problems. Cylance provides the technology and services to be truly predictive and preventive against advanced threats.

www.cylance.com

SIEMENS

Siemens is one of the world's leading suppliers of innovative, environmentally friendly products and solutions for industry customers. We use solid market expertise, technology-based services and software for industrial processes to increase our customers' productivity, efficiency and flexibility. Our globally unmatched offering of automation technology, industrial controls and drive technology as well as industrial software, equip manufacturing enterprises with what they require over their entire value chain. Industrial Cyber Security (ICS) products and services are an important part of the Siemens portfolio and we provide product and engineering support to our customers to ensure critical control systems are protected while achieving full integration of the complete solution. Maximizing information transparency across ICS is now more important than ever but secure architectures and continuous monitoring of the systems has to be a primary consideration for the final solution.

www.siemens.co.uk/industry

paloalto NETWORKS®
the network security company™

Palo Alto Networks has pioneered the next generation of network security. Our innovative platforms allow organisations to identify, control, and productively enable applications whilst simultaneously inspecting all content for all known and unknown threats. Palo Alto Networks is categorised as a Leader in the Gartner Magic Quadrant for Enterprise Firewalls.

www.paloaltonetworks.com

LOCKHEED MARTIN

Company Bio to follow:-
www.lockheedmartin.com

Applied Risk

Applied Risk is a leader in Industrial Automation and Control Systems (IACS) security, specializing in security risk assessments, network security architecture, security training and ICS threat intelligence. Utilizing our extensive process control security expertise, Applied Risk serves numerous major clients including many of the world's top energy and utility companies within the petrochemical, power generation, power transmission and water utilities industries. Applied Risk helps businesses protect assets and reduce security risk. We give organizations ranging from Fortune 500 enterprises to small-to-medium sized businesses the services and solutions they need to transform the way they procure, build, integrate and manage their critical infrastructures.

www.applied-risk.com

codenomicon

Codenomicon provides a suite of next-generation solutions that reveal a better path to total defense. These solutions provide new layers of testing, robustness, intelligence, collaboration and security to deliver strength in visibility to the very Core of today's critical systems, networks and devices. Founded in 2001 in Oulu, Finland, the global company works with leading telecommunications, networking, manufacturing, healthcare, financial services, defense, government, CERT and cyber authorities to strengthen systems and proactively secure customers and connections.

www.codenomicon.com

'Why don't they get it?' Understanding the View from the Other Side of the Firewall

Traditionally, IT and OT teams have been separated by the firewall. However, nowadays with everyone and everything connected to the internet such as theInternet of Things (IoT) in fourth generation SCADA computing and the greater use of COTS in ICS. These two teams, from different technology perspectives need to understand the other's viewpoint and start talking the same language. IT and OT are completely intermingled in our technology driven global business. Even in terms of simple discussions around 'Risk Impact' the IT team may view the worst-case scenario as large loss of data whereas theOT team may consider the worst case as loss of life. Security posture, risks, incident response and recovery are vastly different between the two similar technologies and teams.

It is only when teams come together and begin talking the same language will we be better prepared to face the external and internal threats as well as understanding the full extent of our vulnerabilities. Through discussions and interactive breakout sessions, the workshop will examine common mistakes and misconceptions made by teams when considering the 'other side' and help attendees to leave with a better understanding of how to take this back to their parent companies and put together a strategy for common understanding useable by all. To effectively monitor, report, strategize and respond to every day and emerging threats a good understanding of general risks from both sides of the perimeter and IT vs. ICS must be explored.
Risks, policies, regulations, legal requirements, hardware, protocols, etc…. are different between IT and ICS technologies, although similar and in many cases sharing the same network resources. Each must be approached differently. The current threat landscape has changed, traditional ICS security by obscurity or head in sand IT Security defense is no longer viable. Nor are old fashioned approaches and attack techniques and tools are evolving at a much faster rate than SCADA equipment can be manufactured much less replaced with new hardware capable of facing today's industrial, nation state or cybercriminal or hacktivist threats.

In this workshop, you will be given a taste of what ICS and IT incident response look like on both sides of the firewall.

09:00-09:15	**Introductions**
09:15-10:15	Discussion regarding terms, technologies, risks and risk impact with focus on **Before and IT/OT incident.**
and US/	**Exercise:** 10 minute quick exercise tabletop in the UK, based on EU/UK regulations and in USA changed to NIST North American regulations.
10:25-11:25	Discussion regarding terms, technologies, risks and risk impact withfocus on **During and IT/OT incident.**
and US/	**Exercise:** 10 minute quick exercise tabletop in the UK, based on EU/UK regulations and in USA changed to NIST North American regulations.
11:45-12:45	Discussion regarding terms, technologies, risks and risk impact with focus on **After and IT/OT incident.**
	Exercise: 10 minute quick exercise tabletop in the UK, based on EU/UK regulations and in USA changed to NIST and US/North American regulations
12:55-13:10	Wrap Up

WORKSHOP LEADERS

Tim Harwood, Managing Director, HS and T Consultancy

Tim Harwood is a veteran of the security world and has been providing information security guidance and expertise to corporate clients, the UK Government and the UK military for over 30 years. As Managing Director of Harwood Security and Training Consultancy (HS and TC), he provides strategic direction for the company that he founded in 2013.

Tim's professional background includes security capability strategy planning and development, information security capability framework design and implementation and security awareness strategy design and implementation.

He has developed a security professional development framework for a global top ten oil and gas company, delivers training as a member of the SANS and Firebrand faculties and, as a thought leader, regularly presents at summits and conferences.

In 2013, he participated as a Subject Matter Expert and Steering Committee member for the design of the new GIAC certification, the GICSP certification. Tim is a Full member of the Institute of Information Security Professionals (IISP), a Fellow of the Chartered Management Institute (FCMI) and is the holder of the GIAC Security Leadership (GSLC) and GIAC Security Essentials (GSEC) Certifications. Tim is an elected member of the Board of Directors for the Institute of Information Security Professionals with the Board portfolio of IS skills and competencies.

Christina Kubecka, Former Group Leader, Aramco Overseas, Consultant and Founder HypaSec ^infinity.

Chris formerly led the Security Operations Centre for Aramco Overseas Company. She holds degrees in Aeronautical Engineering, Computer Science and Information Technology. Chris holds an alphabet soup of certifications such as MCSE, MCDBA, CISSP, etc… and GCIA,GCIH, GPEN trained. Her hobbies include research of smartphone/Android OS exploitation, cyber warfare, process and automated control systems, DNS and IPv6 protocols, cryptography, SIEM's/correlation engines and cyber-intelligence. Chris has over 20 years of extensive experience in the field of information security. Her career has spanned from the US Air Force, Space Command, private and public sector.

Harwood Security and Training Consultancy

09:10-09:40 Key Note Presentation: **International priorities, information sharing and strategic objectives**
Chris Blask, Chair at Industrial Control System Information Sharing and Analysis Center, **ICS ISAC**
International priorities, information sharing and strategic objectives

09:40-10:10 **Cyber Security within critical elements of the energy sector**

Regulation
Collaboration
Risk Management
Compliance
IT and OT Convergence
Enterprise facing architecture
Legacy systems
BYOD
Graham Wright, CISO & Global Head of Digital Risk and Security, **National Grid**

10:10-10:50 **Regulating Cyber Security & Information Assurance in the UK Civil Nuclear Sector: Maturity, Agility and Transformation in the digital era**

20 minute discussion includes:

Objectives, requirements, model standards and regulatory expectations for transformation of cyber security in the UK civil nuclear sector
Views on leadership, maturity and agility of information assurance
The need for cyber risk aware culture; continuous improvement planning; and the critical requirement to ensure and test robust resilience plans.
20 minute Q&A

Robert Orr, Head of Information & Cyber Security Regulation, **Office for Nuclear Regulation**

10:50-11:20 **Coffee Break**

11:20-11:50 **ENISA: ICS-SCADA security**. ENISA will discuss their vision for ICS cyber security, findings and proposed recommendations so far and a vision for future improvements.

Dr. Evangelos Ouzounis, Head of Secure Infrastructure and Services Unit, **European Network Information Security Agency**

11:50-12:20 **Cyber-security efforts among NRAs**

Efforts undertaken from European NRAs in the electricity and gas sector to promote cyber-security
Examples for best practices
An outlook on what is expected to come in the future in regard to cyber-security legislation and regulatory actions
Philipp Irschik, Executive Assistant to the Board of Directors, **Austrian National Regulatory Authority E-Control**

12:20-12:50 **SGIS Report update** from the CEN-CENELEC-ETSI Smart Grid Coordination Group – Smart Grid Information Security Working Group (SG-CG/SGIS)
Jean-Pierre Mennella, Co Chair for SG-CG/SGIS

12:50-13:20 **Panel 1: Regulation and Compliance, expectation and transformation**
Clarity on compliance and regulation
Will the processes solutions we are implementing deliver compliance at a later date?
Examples and a US Perspective

13:20-14:20 **Networking Lunch**

14:20-14:50 **Panel 2: How are Government and Industry promoting and helping to create culture of awareness? What examples of Public and Private information have been implemented, what works and how can we overcome current challenges?**

Panel 1 & 2 Participants include:

Chris Blask, Chair at Industrial Control System Information Sharing and Analysis Center, **ICS ISAC**
Graham Wright, CISO & Global Head of Digital Risk and Security, **National Grid**
Philipp Irschik, Executive Assistant to the Board of Directors, **Austrian National Regulatory Authority E-Control**
Robert Orr, Head of Information & Cyber Security Regulation, **Office for Nuclear Regulation**
Dr. Evangelos OUZOUNIS, Head of Secure Infrastructure and Services Unit, **European Network Information Security Agency**
Jean-Pierre Mennella, Co Chair, **SG-CG/SGIS**

14:50-15:20 **Ground Truths: The true state of ICS attack and defense**

This presentation will focus on lessons learned through active defense and incident response in ICS systems across the world. Topics covered will include: ICS security myths, ICS threat landscape, ICS defensive techniques, and more
Eric Cornelius, Director of Critical Infrastructure and Industrial Control Systems (ICS), **Cylance**

CYLANCE

15:20-15:50 **Coffee break and Networking**

15:50-16:20 **Privacy & Security is part of the Alliander Enterprise Risk Management**

Introduction
Privacy & Security ecosystem
Alliander Privacy & Security Maturity Model
Roadmap 2015-2020
Lessons learned
Next steps
Questions
Johan Rambi, Privacy & Security advisor GRC, **Alliander**

16:20-16:50 **Case Study: The 2012 cyber-attacks against Saudi Aramco** and the Aramco family of affiliates was a major game changer in IT & ICS Security. The energy sector, relevant markets and governments worldwide shuddered. Although oil production wasn't directly affected, business operations were greatly interrupted and remain so. This presentation is the story how I implemented the first IT Security unit for Aramco Overseas Company, a Saudi Aramco affiliate which provides all IT services for Saudi Aramco in South America and the EMEA region outside of Saudi Arabia.

1.Cybergeddon 2012
•Description of Shamoon and attack effects on the Aramco family
2.Starting from Zero to Hero
•An offer I couldn't refuse after "The Incident"
•Implementation of basic IT security
•Recruitment of skilled in-house IT security staff
3.Maturization -IT Security to the next level
•Development of staff: hackers, lock pickers, geniuses and Harlem Shakers
•Exercises and independent operational audits
•Building the framework for a functional incident response team and CERT
4.Lessons Learned
•Twitter setbacks
•Dealing with panic
•What I would do different if I had a time machine
Chris Kubecka, Former Head of Operations Centre, Aramco Overseas,
Researcher Security Evangelist EU

16:50-17:20 **Panel: Maturation, Incident Response and Recovery**
-Developing a maturity model
-Understanding your incident response capability and how to fortify it
-How to improve
-Framework and response centers
Chris Blask, Chair at Industrial Control System Information Sharing and Analysis Center, **ICS ISAC**
Eric Cornelius, Director of Critical Infrastructure and Industrial Control Systems (ICS), **Cylance**
Chris Kubecka, Former Head of Operations Centre, Aramco Overseas, **Researcher Security EvangelistEU**
Johan Rambi, Privacy & Security advisor GRC, **Alliander**

17:20-18:20 **Concurrent Roundtable demonstrations and discussion**
Table 1: Justin Harris, Systems Engineer, SCADA & Industrial Control Systems. **Palo Alto Networks**

17:20-18:20 **Table 2**
Data Exfiltration: Detecting and Preventing
Dr. Sylvain Frey, Senior Research Associate, **Lancaster University**

DAY - 2

09:10-09:40 **Designing and implementing a holistic Industrial Security network**

Physical, procedural and electronic defence in depth strategy
Ensuring security by design, security should not be bolted on
Action plan: policies, procedures and awareness
Network security designed to block unauthorised communications
Patch management
Application monitoring and change management
Remote access and device hardening
Mark McCormick, Industrial IT Security Engineering Consultant, **Siemens**

09:40-10:10 **Advanced Control Network design and deployment for visible operations and cyber security assurance with software defined networks.**
Control system networks have moved from traditional time division technologies such as SONET rings to Ethernet edges with Multi Protocol Labeling and Switching cores. The next evolution is Software Defined Networking that can make the network dance with isolated virtual circuits while also providing full wire-speed fire walling, load balancing, packet manipulation and intrusion detection capabilities. CWP has developed a monitoring network based upon SDN that will allow us to see all interactions on the network for both operations reliability and cyber detection capability.
Steve Brunasso, Cyber Security Manager, **California Water and Power Utility**

10:10-10:50 Software, Vulnerabilites and Remedies — the good, the bad and the ugly
Lauri Piikivi, Senior Manager, Security Testing Tools, **Codenomicon**

10:50-11:20 **Coffee and Networking**

11:20-11:50 **Implementing Security by Design in IT and OT practice – by bringing the roles of IT/OT architecture and security together into one**

Introduction (of myself, the company and agenda)
Threats of the outer world – some examples of probably already read/heard news highlights
ICS security is not just about servers – keep focus on PLC also (firmware, board design)
Physical security as part of the whole – there's no "cyber" without physical assets, that need to be protected as well
Risk is a driver – know your environment and track potential risks constantly, plan actions accordingly
Maksim Gluhhovtsenko, Information Security Officer, **Elektrilevi**

11:50-12:20 **Managing Cybersecurity in a control systems environment**

– Governance & Awareness
– Threats & Countermeasures
– Incident response & recovery
– Addressing security in the supply chain
Paul Jenkinson, Cyber Security Manager, **UK Power Networks**

12:20-12:50 **Cyber Security for Level 1 Devices**

- Understanding and optimizing security of field devices
- Meaningful techniques to strike the balance between security and ease of use
- Lesson Learned from the field

Jalal Bouhdada, Founder, Principal Security Consultant, **Applied Risk**

12:50-13:20 **Panel: IT and OT Collaboration**

- How can work together to better manage risk?
- What barriers exist and how are we meeting the challenge?
- Sharing best practices

Jalal Bouhdada, Founder, Principal Security Consultant, **Applied Risk**
Paul Jenkinson, Cyber Security Manager, **UK Power Networks**
Maksim Gluhhovtsenko, Information Security Officer, **Elektrilevi**
Steve Brunasso, Cyber Security Manager, **California Water and Power Utility**
Chris Blask, Chair at Industrial Control System Information Sharing and Analysis Center, **ICS ISAC**

13:20-14:20 **Networking Lunch**

14:20-14:50 **Panel: ICS Security Lifecycle – Best practice and Q&A**

Assess, implement, maintain
Understanding the lifecycle and overcoming implementation challenges
Chris Blask, Chair at Industrial Control System Information Sharing and Analysis Center, ICS ISAC
Jalal Bouhdada, Founder, Principal Security Consultant, Applied Risk

14:50-15:20 **Cloud Computing, an opportunity or risk to far for critical infrastructure environments?**
Why is the adoption of cloud computing inevitable for critical environments? What measures are necessary for the cloud in order to support critical infrastructure?
Raj Samani, CTO, **McAfee**

15:20-15:50 **Coffee and Networking**

15:50-16:20 **Emerging Markets Threat and Dialogue: Internet of Things the extended attack surface**

16:20-16:50 **Smart Cities and Critical National Infrastructure:**
OT/IT integration in Smart Cities, opportunities and risks of connected applications, can Cities be secure by design or are we already playing catch up?
Dr Theo Tryfonas, MBCS CITP, MINCOSE, CISA, Senior Lecturer in Systems Engineering, Dept. of Civil Engineering, **University of Bristol**

16:50-17:15 **Wash Up.** What have you learned, why has this opportunity been important and how can we as a community convey and communicate more effectively to ensure a more resilient future?

OUR SPEAKERS

Dr. Evangelos Ouzounis

Head of Secure Infrastructure and Services Unit, European Network Information Security Agency (ENISA)
Dr. Evangelos OUZOUNIS is the head of ENISA's Secure Infrastructure and Services Unit. His unit implements EU Commission's CIIP action plan, facilitates Member States efforts towards a harmonised implementation of incident reporting scheme (article 13 a & article 4 of new Telecom Package), contributes to the development of the NIS Platform and develops good practices for national cyber security strategies.

Graham Wright

CISO and Global Head of Digital Risk, National Grid
"Graham joined National Grid as CISO and Global Head of Digital Risk in April 2014 after holding senior positions in cybersecurity with organisations in Ministry of Defence, Central Government and in the private sector. He joined National Grid from Northrop Grumman where he led their UK Cyber and Intelligence interests.; and prior to that was Deputy Director of the Office of Cyber Security in the Cabinet Office where he was responsible for leading the planning and resourcing of the National Cyber Security Strategy. Graham has also acted as the Special Advisor on Cyber Security for the House of Commons Defence Committee; and currently chairs the UK pan-sector Emergency Executive Committee for Cyber Security"

Philipp Irschik

Executive Assistant to the Board of Directors at the Austrian National Regulatory Authority E-Control, E Control
Philip Irschik is leading cyber-security efforts in the Austrian electricity and natural gas sector on behalf of the Austrian energy regulatory authority E-Control. In the past years we as the regulator together with the electricity and natural gas sector carried out several projects to augment cyber-resilience through several private-public partnerships and projects focusing on ICT-risk assessments and dedicated cyber-exercises. In addition we are currently – together with other stakeholders – as one of the first countries worldwide in the process of setting up a dedicated Computer Emergency Response Team (CERT) for the energy sector.

Robert Orr

Head of Information- & Cyber Security Regulation, Office for Nuclear Regulation
Rob leads information and cyber security regulation of the UK civil nuclear sector, in order to ensure the safety of the public, the protection and safeguarding of nuclear material, the non-proliferation of enrichment technologies, and the control of sensitive nuclear information. He is responsible for enabling, influencing, assuring and ensuring the transformation of cyber security and information assurance across the UK civil nuclear sector, through effective and efficient regulation.

Johan Rambi

Privacy & Security advisor GRC, Alliander
Johan Rambi is Alliance manager Privacy & Security at Alliander and supports the organization with the development of Smart Meter Privacy & Security and Smart Grid/SCADA Cyber Security in the role of subject matter expert.

Chris Kubecka

Private Researcher Former Group Leader, Aramco Overseas
Christina Kubecka, Chris leads the Security Operations Centre for Aramco Overseas Company.

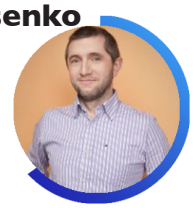
Raj Samani

VP, EMEA Chief Technology Officer, Member of Advisory Group on Internet Security
EUROPOL CyberCrime Centre, McAfee, EUROPOL CyberCrime Centre. He is currently working as the VP, Chief Technical Officer for McAfee EMEA, volunteers as the Cloud Security Alliance Chief Innovation Officer, and Special Advisor for the European CyberCrime Centre

Jean Pierre Mannella

Co Chair for SG-CG/SGIS, CEN-CENELEC-ETSI Smart Grid Coordination Group – Smart Grid Information Security Working Group (SG-CG/SGIS)
Jean-Pierre is also co-chairman of the European working group CEN-CENELEC-ETSI Smart Grid Coordination Group – Smart Grid Information Security (SG-CG/SGIS) and a member of the European Commission Smart Grids Task Force Expert Group 2 (EG2).

Maksim Gluhhovtsenko



Information Security Officer, Elektrilevi OÜ
Over ten years of working experience in Utility area from Software Engineer to Architect. Deep understanding of Power Distribution business and related Information Systems.

Lauri Piikivi

Lauri Piikivi is the Senior Manager of Security Testing Tools and platform development for Codenomicon. Lauri has worked on SW development for 17 years, in internet communications and security area. During that time his work has span from testing and implementation to requirements and product management. At Codenomicon Lauri has worked in implementing and deploying a solution for the ISASecure certification program.

Lauri's interests are security in SW and system

Jalal Bouhdada

Founder, Principal ICS Security Consultant, Applied Risk

Founder and Principal ICS Security Consultant , Applied Risk
Jalal Bouhdada, Founder and Principal ICS Security Consultant for Applied Risk, the Netherlands. With over 15 years of experience in security assessment, design and deployment with focus on Process Control Domain and Industrial IT Security.

Steven Brunasso

Manager Cyber Security, California Water and Power Utility
He has focused on utility systems security for the past decade as the information security manager at Southern California Edison for the initial NERC CIP rollouts and is currently managing security in the operations technology group at one of the most innovative California Water and Power Utilities. He has an MBA from the University of California at Los Angeles specializing in technology strategy.

OUR SPEAKERS

Paul Jenkinson

Paul Jenkinson has over 15 years' experience in cyber security within the energy sector covering both operational technology and enterprise systems, overseeing security improvements plans and leading teams in the areas of infrastructure and application strategy and design, information governance, incident response and stakeholder engagement.

In Paul's current role at UKPN, he's spearheads and develops the company's cyber security approach in close liaison with senior business leaders, industry partners and government agencies. Notably, in preparation for the London 2012 Olympics, Paul and his team implemented industry acclaimed cyber security resilience and lockdown measures into the Electricity Distribution networks feeding the Olympic venues. This activity included managing, testing and activating defensive cyber security measures in response to high profile cyber threats and incidents across the Olympic calendar. These measures have been further developed to underpin the company's operational security arrangements.

Justin Harris

Systems Engineer,
Palo Alto Networks
Mr Harris will be leading a Roundtable discussion end of

Justin Harris is currently a systems engineer with Paloaltonetworks specialising in industrial control systems security. He has previously worked in a number of roles as a control systems engineer designing and commissioning control systems in the Petrochemicals, Industrial gases and Electronics manufacturing industries. He holds a BEng in Mechanical Engineering from the University of Surrey, BEng in Chemical Engineering from the University of Strathclyde and an MSC in Control Systems Engineering from the University of Sheffield.

Chris Blask

Executive Director of Webster University's Knowledge Sharing Directorate, Chair ICS-ISAC,
Industrial Control System Information Sharing and Analysis Center
Chris Blask has been involved in the industrial control system and information security industries for more than twenty years. Mr. Blask's career spans the breadth of the cybersecurity spectrum. He invented one of the first commercial firewall products, built a multi-billion dollar firewall business at Cisco System, co-founded an early SIEM vendor and authored the first book on SIEM. Today he is Executive Director of Webster University's Knowledge Sharing Directorate where he oversees the operation of the Industrial Control System Information Sharing and Analysis Center (ICS-ISAC), Insurance Industry Information Sharing and Analysis Organization (INS-ISAO) and Senior Partner at Fearless Security.

Dr Theo Tryfonas

Theo Tryfonas is an academic with the University of Bristol. He is a computer scientist and systems engineer working in the fields of Smart Cities, Internet of Things and Cybersecurity. He is interested in secure, energy-efficient and resilient urban applications of IoT, data driven models of civic innovation, privacy and technology policy. He teaches one of the first courses on smart cities in the UK and is currently involved with nationally and European funded research on smart buildings and resilient networks of smart connected objects.

Eric Cornelius

Director of Critical Infrastructure and Industrial Control Systems ,
Cylance
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.

Mark McCormick

Mark joined Siemens in 1998 and has worked on many Siemens Industrial Control Factory and Process Automation systems across many industries, encompassing both wired and wireless networks using various communication protocols.

Mark has been a regular presenter on network communication in this field.
With the growth of Ethernet connectivity in Industrial Control Systems, security has become a regular discussion topic involving many applications across Wide Area and Local Area networks.