Hear first about SASIG events and industry news
Follow us on:

Interconnected by design

The convergence of IT, OT and CPS

Organisationally the cybersecurity team usually has a limited view of the operational technology that's vital to business operations. For many businesses, Enterprise IT, operational technology (OT) and cyber-physical systems (CPS) are managed by teams that work to different leaders. The frictions, and gaps created, are often not addressed in a way that helps secure the business. Gaining a view of the minimum viable company is essential for maintenance of business operations should there be a breach. Understanding how the enabling technologies, OT and CPS systems are connected, either directly or indirectly, is key to business continuity.

This expanded connectivity introduces pathways for adversaries to move between IT and OT/CPS environments. The issue we face now is how well that integration is controlled and secured.

Join us as we consider the impact of moving from air-gapped systems to those that are interconnected by design to satisfy emerging business needs and expectations of real-time data-driven operations and predictive analytics.

Thursday 12 November 2026

9am to 3pm

London

Chair

Prof. Andrew Clark, Content Advisor, The SASIG

9.00am **Registration, coffee, and networking**

9.30am **Welcome and introductions**
Prof. Andrew Clark Content Advisor, The SASIG

9.45am **Keynote presentation: Why should I be bothered?**
Peter Wood Lead Consultant, Naturally Cyber

Building on his many years of ethical hacking, pen testing and red teaming Peter will highlight how networks that regularly fit on the periphery of a CISO's remit can provide vectors for penetration of organisations' information systems. Today, with increasing convergence of IT, OT and Cyber Physical Systems, the nature of this change should be on CISO's radar. Even if OT and CPS are not currently and explicitly within their terms of reference the impact of their being breached may be as great as, if not more than, those identified within the current enterprise risk model.

10.15am **Panel discussion: The landscape**
Facilitated by Liz Murray Chief of Staff, The SASIG
Tim Harwood CEO, Siker Cyber
Abel Archundia-Pineda VP Global Operational Technology, Kudelski Security
Peter Wood Lead Consultant, Naturally Cyber
Tim Nursall Sales Director, Cymulate

In his 6th Century BCE treatise "The Art of War", Sun Tzu allocated a whole chapter to 'Terrain' and its importance to both the attacker and defender. Today the breadth of our business terrain is greater than ever, particularly with IT/OT/CPS convergence and encompassing services and systems provided by third parties.
How realistic is it for us to understand it completely? How much do we need to know?

11.00am **Tea, coffee, and networking break**

11.15pm **Securing the factory that builds the factory**
Matt Campbell Senior Security Solutions Architect, Qualys

Continuous software delivery is rapidly coming to operational technology, but a Continuous Integration/Continuous Delivery/Deployment (CI/CD) pipeline for OT is itself an OT system, full of real hardware, unpatchable instruments and custom test rigs you can't just tear down and rebuild in the cloud. This session asks what that means for the security of the physical product at the end of the line, and what can be done to minimise the risks introduced by your Industrial DevOps platform.

11.45am **How Do You Know Your Security Works Across IT, OT and AI?**
Tim Nursall Sales Director, Cymulate

Security now spans IT, OT and AI, but having controls in place does not mean they will work when attacked. Continuous security validation provides evidence that defences are effective, exposes gaps before attackers do, and helps teams prioritise what matters most. This session explores why validation must become a core part of security across every environment and asks: if you are not continuously validating your defences, how do you know they will work when it matters?

12.15pm **Networking lunch**

1.00pm **From Air Gaps to Identity: Who Can We Trust in Connected Factories?**
Florian Pouchet Head of Cybersecurity and Operational Resilience UK, Wavestone
Emeline Legrand Manager – Product & Industrial Cybersecurity, Wavestone

For decades, industrial cybersecurity was built around isolation, segmentation and trusted networks. As factories become increasingly connected, these traditional assumptions are being challenged.

Drawing on real-world industrial cybersecurity engagements and market observations, this session explores why identity is emerging as a strategic foundation for OT security. Through practical lessons learned, benchmark insights and operating model examples, we will discuss what works, what does not, and why the future of industrial cybersecurity may depend less on networks and more on identities.

1.30pm **The threat lives in behaviour: From IT identity to OT impact**
Jake Anthony Principal Solutions Engineer, Exabeam

In a converged IT, OT, and Cyber-Physical Systems (CPS) environment, the initial point of compromise, whether a stolen human credential, a compromised machine identity, or a rogue AI agent, is simply the entry point. The real challenge is not managing these various identities but detecting them once they are inside.

Traditional access controls fail to spot the subtle indicators of a threat moving laterally from corporate IT toward critical physical infrastructure. This session explores why the true threat lives in behaviour and how shifting from static identity checks to continuous behavioural intelligence provides the vital visibility needed across interconnected systems. By baselining normal activity for humans, machines, and AI alike, security teams can expose malicious intent and stop a compromise before it leads to OT impact.

2.00pm **Panel discussion: A broadened perspective**

Facilitated by Liz Murray Chief of Staff, The SASIG
Tim Harwood CEO, Siker Cyber
Stephen French Principal Security Consultant, Bridewell
Stuart Codack Principal OT Consultant, PA Consulting
Cathy McCann Founder, Invistra AI
Ian McGowan Managing Director, Barrier Networks

With a new understanding of IT/OT/CPS the pressure to monitor and securely manage the increased estate doesn't only fall to the CISO. Once an organisation identifies the problem and frictions how can they gain assurance that the liminal spaces are understood? How can gaps in responsibility be identified and addressed to enable organisations to deliver a complete protective strategy across technology, people and processes?

What needs to be in place to manage a complex environment well. Where are businesses succeeding and where are the pinch points? Does individual role ego have a part to play in preventing organisations from truly effectively securing their estates? This interactive discussion will explore what's working, what's not and how organisations might succeed in securing their interconnected environments.

2.45pm **Closing Remarks**

3.00pm **End of meeting**

About

The Security Awareness Special Interest Group (SASIG)

SASIG is a subscription-free networking forum, membership now represents thousands of organisations of all sizes from across the world and from all sectors, public and private. Its 11,200+ membership is drawn from CIOs, CISOs and their staff with responsibility for cybersecurity within their organisations. Professionals from other disciplines (risk, HR, legal, supply, etc.) and representatives from government, law enforcement and academia are also being increasingly welcomed at events. The Chatham House Rule is strictly enforced and universally respected at all meetings, and vendors and the Press are routinely excluded. Thus, the level of debate is extraordinarily revealing and rewarding.

SASIG has a members' website at www.thesasig.com. Please register here for membership.

With thanks to our Supporters and Contributors…

Redflags · WAVESTONE · exabeam · Qualys · ncc group · CoreView · BREACHRX · Symantec by Broadcom · Carbon Black by Broadcom · Arrow · MIMOTO · f5

CYBSAFE · censys · Bridewell · KUDELSKI SECURITY · Vanta · COFENSE · Patrowl · PENTERA · Talanos cybersecurity · cymulate · Qevlar AI · KYOCERA · Astran · SECURITY JOURNEY

020 4583 5030
info@thesasig.com
www.thesasig.com