



**WEDNESDAY**  
**JUN 05, 2024**  
 13:00 – 20:30 Uhr

**THURSDAY**  
**JUN 06, 2024**  
 09:00 – 17:00 Uhr

**LOCATION:**  
 Microsoft Munich  
 Walter-Gropius-Straße 5  
 80807 München  
 Germany

© stock.adobe.com – Zilnetron

**Organizer**



**Hosting Company**



**Presenting Partners**



**FBI**

**BECKHOFF**



**SIEMENS**





**Stefan Hoppe, OPC Foundation**  
President and Executive Director  
stefan.hoppe@opcfoundation.org

Welcome to the newest event of the OPC Foundation – The OPC UA Security Summit – where we address the pressing need within our community to openly discuss and exchange insights on critical cybersecurity requirements. This summit provides updates on top security topics like the Cyber Resilience Act (CRA), with its components such as SBOM (Software Bill of Materials) and CVE (Common Vulnerabilities and Exposures), all taking center stage alongside discussions on Certificate Management, Security in Cloud and OT Systems, and adherence to IEC62443 standards.

My special thanks to our esteemed speakers, starting with the keynote from the EU Commission, providing firsthand information about the latest timeline and content updates of the CRA. Additional appreciation goes to all speakers from national agencies such as BSI and ANSSI, alongside international players like the FBI, all converging to share invaluable perspectives on the CRA and its contents.

The insights into views and approaches to address the CRA from industry giants and sponsors of the event such as Siemens, Schneider Electric, and Beckhoff will further provide input during coffee-break discussions as well as in moderated Q&A sessions.

Legal experts will dissect the complex legal aspects of the act, while library providers will shed light on their contributions to OPC UA security. Last but not least, I extend my sincere thanks to OPC Foundation Board member, Microsoft, for hosting this event in Munich.

Regards,  
**Stefan Hoppe**  
President and Executive Director  
OPC Foundation  
stefan.hoppe@opcfoundation.org  
www.opcfoundation.org



Europäische Union

**Benjamin Bögel**, European Commission



Bundesamt für Sicherheit in der Informationstechnik

**N.N.**, ANSSI

**Lena Schnepfer**, BSI

**Anna Schwendicke**, BSI

FBI

**SA Brian Kaiser**, FBI

**BECKHOFF**

**Torsten Förder**, Beckhoff Automation GmbH

**Sven Goldstein**, Beckhoff Automation GmbH



equinor

**Trond Kvamme**, Equinor

**Jan Munkejord**, Equinor



Schneider Electric

**David Smith**, Schneider Electric

**Erich Barnstedt**, Microsoft



Microsoft

**Dr. Holger Kenn**, Microsoft

**Frank Laurig**, Siemens

**SIEMENS**

**Anna Palmin**, Siemens

**Dr. Thomas Pröll**, Siemens

**Dr. Kai Wollenweber**, Siemens



systemrel

**Vincent Lacroix**, Systemrel



Unified Automation

**Matthias Damm**, Unified Automation



VOELKER

**Dr. Gerrit Hötzel**, Voelker Gruppe



OPC FOUNDATION

**Stefan Hoppe**, OPC Foundation

**Alexander Allmendinger**, OPC Foundation

**Randy Armstrong**, OPC Foundation



VDMA

**Alexey Markert**, VDMA

**WEDNESDAY, JUN 05, 2024**

13:00 – 20:30 Uhr

- 13:00 – 14:30** Welcome & OPC UA Overview
- 14:30 – 15:00** Coffee break
- 15:00 – 16:30** CRA Overview and Expectation
- 16:30 – 17:00** Coffee break
- 17:00 – 18:00** Customer View
- 18:00 – 18:30** Q&A
- 18:30 – 20:30** Come together

**THURSDAY, JUN 06, 2024**

09:00 – 17:00 Uhr

- 09:00 – 10:15** Keynotes with Focus CRA
- 10:15 – 10:45** Coffee break
- 10:45 – 13:00** Focus CRA
- 13:00 – 14:00** Lunch
- 14:00 – 15:00** Focus OPC UA
- 15:00 – 15:30** Coffee break
- 15:30 – 16:00** Focus OPC UA
- 16:00 – 17:00** Q&A & Farewell



**LOCATION**

Microsoft Munich  
Walter-Gropius-Straße 5  
80807 München  
Germany

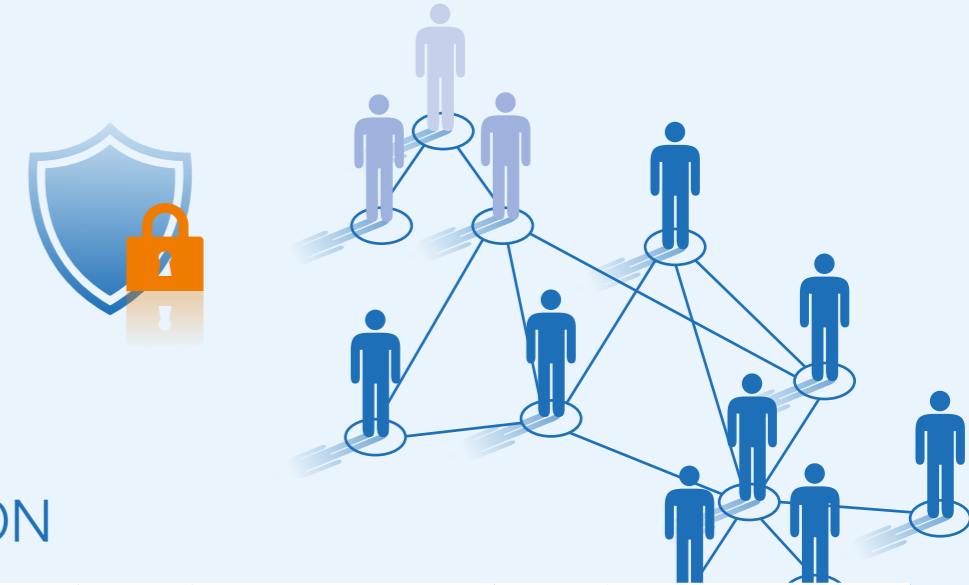
**DAY 1**

|              |               |  |
|--------------|---------------|--|
| Session 1 1  | 13:00 – 13:15 | <b>Greetings from Host</b><br>Dr. Holger Kenn, Microsoft   |
| Session 1 2  | 13:15 – 14:00 | <b>Welcome &amp; Introduction to OPC UA</b><br>Stefan Hoppe, OPC Foundation  |
| Session 1 3  | 14:00 – 14:30 | <b>OPC UA Security Architecture</b><br>Matthias Damm, Unified Automation   |
|              | 14:30 – 15:00 | <b>Coffee break</b>  |
| Session 1 4  | 15:00 – 15:30 | <b>The CRA is coming – the CE Mark is extended to include security</b><br>Lena Schnepfer, BSI<br>Anna Schwendicke, BSI |
| Session 1 5  | 15:30 – 16:00 | <b>A component manufacturer's considerations regarding security</b><br>Torsten Förder, Beckhoff                        |
| Session 1 6  | 16:00 – 16:30 | <b>Machinery manufacturers commitment to the CRA</b><br>Alexey Markert, VDMA   |
|              | 16:30 – 17:00 | <b>Coffee break</b>  |
| Session 1 7  | 17:00 – 17:30 | <b>Security, a foundation for the Digital Factory</b><br>Trond Kvamme, Jan Munkejord, Equinor                          |
| Session 1 8  | 17:30 – 18:00 | <b>OPC UA Cloud Solutions &amp; Security</b><br>Erich Barnstedt, Microsoft   |
| Session 1 9  | 18:00 – 18:30 | <b>Q&amp;A Day 1</b>   |
| Session 1 10 | 18:30 – 20:30 | <b>Come together</b>   |



### DAY 2 MORNING

|                     |               |   |                      |  |
|---------------------|---------------|---|----------------------|--|
|                     | 08:45 – 09:00 | <b>Coffee start</b>   |                      |  |
| <b>Session 2 1</b>  | 09:00 – 09:15 | <b>Welcome Day 2</b><br>Stefan Hoppe, OPC Foundation  |                      |  |
| <b>Session 2 2</b>  | 09:15 – 09:45 | <b>Keynote</b><br>Benjamin Bögel, Head of Sector for Product Security and Certification Policy at the European Commission |                      |  |
| <b>Session 2 3</b>  | 09:45 – 10:15 | <b>For effective Vulnerability Management – SBOM in the CRA</b><br>Lena Schnepfer, BSI<br>Anna Schwendicke, BSI           |                      |  |
|                     | 10:15 – 10:45 | <b>Coffee break</b>   |                      |  |
| <b>Session 2 4</b>  | 10:45 – 11:15 | <b>Vulnerability Management – CVE</b><br>N.N., ANSSI  |                      |  |
| <b>Session 2 5</b>  | 11:15 – 11:45 | <b>CRA and EN IEC 62443</b><br>Dr. Kai Wollenweber, Siemens   |                      |  |
|                     | 11:45 – 12:00 | <b>Room adjustments</b>   |                      |  |
| <b>Session 2 6a</b> | 12:00 – 12:30 | <b>CVE from experience</b><br>Dr. Thomas Pröll, Siemens   | <b>Session 2 6 b</b> | <b>The OPC Foundation CVE Management Process</b><br>Randy Armstrong, OPC Foundation  |
| <b>Session 2 7a</b> | 12:30 – 13:00 | <b>CVE in context of supply chain</b><br>Dr. Thomas Pröll, Siemens  | <b>Session 2 7 b</b> | <b>Secure device registration &amp; certificate management for heterogeneous OT environments incl. OPC UA</b><br>Anna Palmin, Siemens<br>Frank Laurig, Siemens |
|                     | 13:00 – 14:00 | <b>Lunch break</b>  |                      |  |



### DAY 2 AFTERNOON

|                     |               |   |                     |  |                     |  |
|---------------------|---------------|---|---------------------|--|---------------------|--|
| <b>Session 2 8a</b> | 14:00 – 14:30 | <b>Secure OPC UA Software Development – Good practices</b><br>Vincent Lacroix, Systemel                         | <b>Session 2 8b</b> | <b>Central Security Management with OPC UA GDS</b><br>Matthias Damm, Unified Automation              | <b>Session 2 8c</b> | <b>Part 21: Integrating the supply chain into the OT security process</b><br>Randy Armstrong, OPC Foundation |
| <b>Session 2 9a</b> | 14:30 – 15:00 | <b>Integrating PubSub Security in UAFX</b><br>David Smith, Schneider Electric                                   | <b>Session 2 9b</b> | <b>OPC Compliance Testing of Security Features and GDS</b><br>Alexander Allmendinger, OPC Foundation | <b>Session 2 9c</b> | <b>A real-world look at industrial OPC UA setups</b><br>Sven Goldstein, Beckhoff Automation                  |
|                     | 15:00 – 15:30 | <b>Coffee break</b>   |                     |  |                     |  |
| <b>Session 2 10</b> | 15:30 – 16:00 | <b>Operational Technology (OT) Threats and the Need for Cybersecurity Collaboration</b><br>SA Brian Kaiser, FBI |                     |  |                     |  |
| <b>Session 2 11</b> | 16:00 – 17:00 | <b>Q&amp;A Day 2 Farewell</b><br>Stefan Hoppe, OPC Foundation   |                     |  |                     |  |

| DAY | SESSION |
|-----|---------|
| 1   | 1       |

### Greetings from the Host

| DAY | SESSION |
|-----|---------|
| 1   | 2       |

### Welcome & Introduction to OPC UA: The Industrial Interoperability Standard

OPC UA is the IEC62541 standard for semantic interoperability for the secure exchange of information, scalable from sensor to all levels to IT/cloud solutions such as DataSpaces, DigitalTwins and Metaverse.

#### This presentation will give you an overview introduction:

1. OPC Foundation: the non-profit organization with > 980 international members
2. OPC UA technology: The rich modeling language with various transport options (such as TCP, UDP, MQTT, but also field transfer and REST interface) and integrated security-by-design.
3. Companion Specifications: >151 area-specific semantic information models for factory, process, energy and other industries
4. Acceptance in the industry
5. Offerings such as: Certification, Open Source, Academic Program

| DAY | SESSION |
|-----|---------|
| 1   | 3       |

### OPC UA Security Architecture

The OPC Unified Architecture includes security as one of its core features. This presentation provides an overview of the OPC UA security architecture, the scalable features available for OPC UA applications, and the centralized security management options defined by OPC UA.

| DAY | SESSION |
|-----|---------|
| 1   | 4       |

### The CRA is coming – the CE Mark is extended to include security

With the Cyber Resilience Act (CRA) security will be prerequisite for market access additionally to safety. This comes with new obligation for manufacturers, not only regarding conformity assessments before bringing on the market but also for the lifetime of the product. What does that imply? A short overview over motivation for the new law and essential changes for manufacturers and consumers.

| DAY | SESSION |
|-----|---------|
| 1   | 5       |

### A component manufacturer's considerations regarding security

Based on experience, good practice and considering the requirements of the European Union's Cyber Resilience Act, this presentation describes the perspective of a resourceful component manufacturer who cares about system integrators. The perspective focuses on the economy and efficiency of applied cyber security in technology and processes. It includes not only the components, but also the systems built with them and the applicability during operation.

With a pinch of humor, positive and negative examples of technical and formal applications of cyber security are presented. The description of alternatives raises the question of how we want to "live" the cyber security required by regulations and standards in the automation sector. The lecture puts forward the thesis that we still have room to design the solution.

| DAY | SESSION |
|-----|---------|
| 1   | 6       |

### Machinery manufacturers commitment to the CRA

The CRA was developed on the initiative of the VDMA, among others. It will have a significant impact on the quality of digital products, including software and hardware. The presentation outlines the resulting opportunities and risks for mechanical engineering in Germany.

| DAY | SESSION |
|-----|---------|
| 1   | 7       |

### Security, a foundation for the Digital Factory

Navigating within new automation initiatives to move into the digital factory in an interoperable way, is challenging. Cybersecurity is one important building block to succeed with the digital transformation within the OT domain. An energy company journey into the secure interoperable digital twins, will be presented.

- Digital Factory, interoperability and standards
- Cybersecurity, IEC 62443, Zones & Conduits

| DAY | SESSION |
|-----|---------|
| 1   | 8       |

### OPC UA Cloud Solutions & Security

Cloud technology comes with its own set of security features and this talk will highlight how these security features can be combined with existing OPC UA security features, including Public Key Infrastructure (PKI).

| DAY | SESSION |
|-----|---------|
| 2   | 1       |

### Welcome Day 2

| DAY | SESSION |
|-----|---------|
| 2   | 2       |

### Keynote

| DAY | SESSION |
|-----|---------|
| 2   | 3       |

### For effective Vulnerability Management – SBOM in the CRA

In the US the EO 14028 requires vendors of software for the US government to list all components they have used in creating their software in a software bill of materials (SBOM). This is supposed to increase transparency and security in the software by providing clear information on components and dependencies of software applications. With the CRA the legal obligation to maintain an SBOM comes to the EU, too, and not just for software, but for all products with digital elements. What does the CRA demand, why, and for what?

| DAY | SESSION |
|-----|---------|
| 2   | 4       |

### Vulnerability Management – CVE

| DAY | SESSION |
|-----|---------|
| 2   | 5       |

### CRA and EN IEC 62443

The presentation provides an overview and status of the CRA related standardization activities. It focusses on the interplay with the relevant standards of the EN IEC 62443 cybersecurity framework and the challenges on the way to get harmonized and listed standards to provide presumption of conformity.

| DAY | SESSION |
|-----|---------|
| 2   | 6a      |

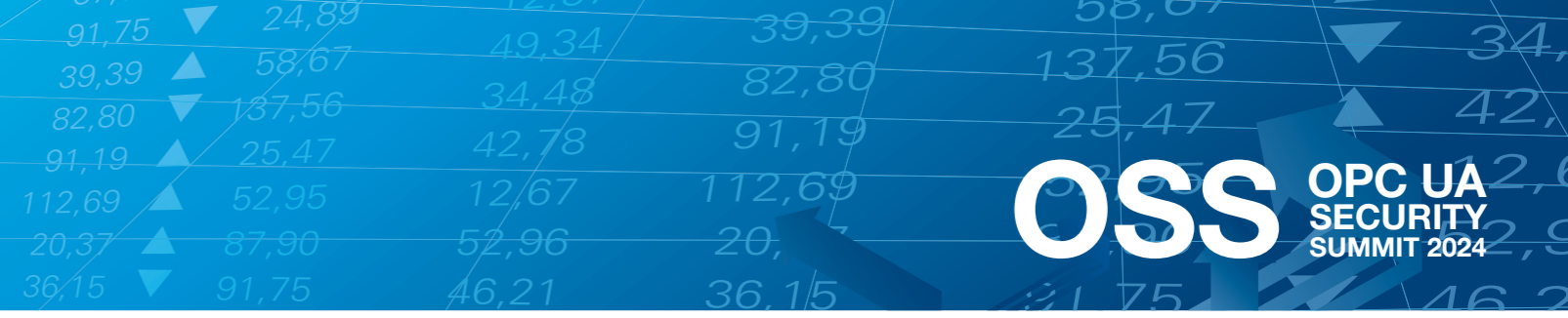
### CVE from experience

Vulnerabilities are inherited along the supply chain. With every integration into a new product and every adaption into a new branch, they likely change their characteristics and the resulting risk. This presentation is looking into industrial software supply chains and the effects that vulnerabilities cause.

| DAY | SESSION |
|-----|---------|
| 2   | 6b      |

### The OPC Foundation CVE Management Process

This presentation will discuss how the OPC Foundation handles reports of security vulnerabilities. It will explain the differences between handling vulnerabilities that affect OPC specifications and vulnerabilities that affect specific products or SDKs. It will also discuss the efforts work with security researchers.



DAY 2 SESSION 6c

**Liability for Open-Source-Software under the Cyber Resilience Act**  
 The first draft of the Cyber Resilience Act (CRA) led to an outcry from the Open Source community given that it looked like the average Open Source contributor would have to fully adhere to the CRA. A change to the CRA draft introducing the criteria of a commercial activity raised even more questions regarding paid contributors and non-profit-organizations. The current CRA draft includes a whole section on Open-Source-Software which may have resolved the issue for the Open Source community. But one question remains: What does a commercial enterprise need to do if they use Open-Source-Software in their commercial products – do they have to declare conformity under the CRA for the Open Source Software?

DAY 2 SESSION 7c

**Contract Design along the Supply Chain under the Cyber Resilience Act**  
 One key element of the Cyber Resilience Act (CRA) is the focus on the supply chain. Many obligations of a commercial enterprise can only be observed if suppliers are contractually obligated to collaborate in the conformity assessment (e.g. regarding the software included in their products). But not only the contractual situation towards the supplier is important. The contractual situation regarding the customer is at least equally important. Besides stipulations for providing security updates and information to customers, the CRA introduces one big change: an extended liability of up to five years. Do all warranty and liability clauses in all terms and conditions and sales contracts have to be changed to reflect this?

DAY 2 SESSION 8c

**Part 21: Integrating the supply chain into the OT security process.**  
 This presentation discusses the life cycle of devices and how a secure system requires a secure supply chain. It will elaborate on the necessity of cryptographically identifying and verifying all devices upon their integration into an OT network and discuss the onboarding process using APIs defined in Part 21. Additionally, it will explain the relation between OPC UA and other device identification and onboarding standards, such as the IEC's „Identification Link“ (IL) strings (IEC 61406).

DAY 2 SESSION 9c

**A real-world look at industrial OPC UA setups**  
 As one of the early adaptors of OPC UA, Beckhoff Automation has been offering OPC UA Client/Server implementations for its automation software TwinCAT since 2007. Based on this long-term experience, Beckhoff has seen thousands of OPC UA devices in multiple different scenarios and has given customers advise on how to securely install and set up their client/server applications. This presentation will give an overview of the status of common automation scenarios and provide some best practice tips to create a better awareness for the security of an industrial OPC UA setup.

DAY 2 SESSION 7a

**CVE in context of supply chain**  
 Vulnerabilities are inherited along the supply chain. With every integration into a new product and every adaption into a new branch, they likely change their characteristics and the resulting risk. This presentation is looking into industrial software supply chains and the effects that vulnerabilities cause.

DAY 2 SESSION 8a

**Secure OPC UA Software Development – Good practices**  
 The emergence of new security regulations has affected development practices. This presentation aims to introduce some of these contemporary techniques and approaches, now considered good practices regardless of the normative framework in use (BSZ/CSPN, Common Criteria, IEC62443, ...) These include Software Bills Of Materials (SBOMs), Continuous Integration, Secure Coding Rules, Pentesting, and User Security Guidelines.

DAY 2 SESSION 9a

**Integrating PubSub Security in UAFX**  
 “Integrating PubSub Security in UAFX – Adapting OPC UA PubSub to work with dynamic connections has required adapting PubSub security. We take a look at adaptations required to ensure a secure PubSub connection including the addition of a Push Model for the Security Key Service in Part 14, UAFX architecture choices to ensure interoperability and robustness, and the workflow of the Security Key Service to provide keys to the PubSub Connections.”

DAY 2 SESSION 10

**Operational Technology (OT) Threats and the Need for Cybersecurity Collaboration**  
 This presentation explores threats to Operational Technology (OT) systems. It emphasizes breach consequences, using real-world examples to stress the need for robust cybersecurity. The multifaceted threats require comprehensive defense strategies, advocating collaboration to counter cyber threats and create resilient OT environments. Emphasizing the consequences raises awareness, empowering decision-makers to implement measures for a secure technological future. Advocating for collaboration between government agencies, private sectors, and international entities is deemed crucial for fortifying defenses and responding effectively to emerging threats.

DAY 2 SESSION 7b

**Secure device registration and certificate management for heterogeneous OT environments incl. OPC UA**  
 When OT components communicate in a secure way using standard protocols like OPC UA they use their secure identities for authentication. A secure identity according to IEEE 802.1AR consists of a private key, the X.509 certificate and the corresponding certificate chain. Managing certificates manually is very time consuming and prone to error. We will show how to manage certificates and register OT components in heterogeneous OT environments in a secure, user friendly and automated way using OPC UA and further standard protocols. Thereby, the SINEC Registration Authority that enables the IT and OT convergence by connection the OT environments to a legacy PKI hosted in IT will be introduced.

DAY 2 SESSION 8b

**Central Security Management with OPC UA GDS**  
 A Global Discovery Server (GDS) enables the registration of OPC UA-enabled devices and applications for centralized discovery services and certificate management. It enables the management and deployment of application certificates and trust relationships between OPC UA applications. This presentation introduces the central security management services defined in OPC UA and shows how Unified Automation's UaGDS manages certificates for different OPC UA applications and devices.

DAY 2 SESSION 9b

**OPC Compliance Testing of Security Features and GDS**  
 Security has always been an important part of OPC UA. As such it was covered by certification implicitly and explicitly from the beginning of the certification program. Learn which security aspects are covered by the OPC Foundation Certification program and why you can trust the security of certified products. We will also share information about tests which are covered by the automated test tool (CTT) of the OPC Foundation for verifying your products OPC UA Security integration.

| DAY | SESSION | TOPIC  | BIOGRAPHY  |
|-----|---------|--|--|
| 2   | 9b      | <b>OPC Compliance Testing of Security Features and GDS</b> | <p><b>Alexander Allmendinger</b> is the Test Lab Manager of the OPC Foundation European Certification Lab, overseeing its operations since its establishment in 2016. In this role, he actively interacts with a diverse range of OPC products and solutions on a daily basis. With extensive experience in working with various communication protocols, he has long been aligned with the vision of the OPC Foundation. He started his journey with OPC UA during its early stages, validating the initial implementations of the Unified Architecture stacks. Furthermore, he is an active member of several working groups, including the Security Working Group, OPC UA over MQTT and REST, and a group dedicated to harmonizing domain-specific information models. This involvement has provided him with valuable insights across these different groups, contributing to his comprehensive understanding of various aspects within the field.</p> |



**Alexander Allmendinger, OPC Foundation**  
alexander.allmendinger@opcfoundation.org

| DAY | SESSION | TOPIC   | BIOGRAPHY  |
|-----|---------|---|--|
| 2   | 6b      | <b>The OPC Foundation CVE Management Process</b>                          | <p><b>Randy Armstrong</b> serves as the Chair of the OPC UA Security Working Group and is also a co-author of the OPC UA specification. With three decades of experience in the OT industry, he has consistently championed secure OT software development with a focus on simplifying security management through adherence to standards and robust software design principles.</p> |
| 2   | 8c      | <b>Part 21: Integrating the supply chain into the OT security process</b> | <p><b>Randy Armstrong</b> serves as the Chair of the OPC UA Security Working Group and is also a co-author of the OPC UA specification. With three decades of experience in the OT industry, he has consistently championed secure OT software development with a focus on simplifying security management through adherence to standards and robust software design principles.</p> |



**Randy Armstrong, OPC Foundation**  
randy.armstrong@opcfoundation.org

| DAY | SESSION | TOPIC  | BIOGRAPHY  |
|-----|---------|--|--|
| 1   | 8       | <b>OPC UA Cloud Solutions &amp; Security</b> | <p><b>Erich Barnstedt</b> has worked in various engineering roles at Microsoft for over 20 years, initially in the Windows team and later in the Azure team. Throughout his career, he worked in the automotive and manufacturing verticals and is the founder of both the Windows and the Azure Industrial IoT teams and is the inventor of many Industrial IoT products. More recently, he shifted his work to the support of open standards in Microsoft products as well as commitments to open-source and consortia work in the Azure Edge &amp; Platform team at Microsoft as Chief Architect. He is the holder of various IoT-related patents and has a bachelor and two master's degrees in computer science from Trinity College, Dublin.</p> |



**Erich Barnstedt, Chief Architect Standards, Consortia & Industrial IoT, Azure Edge + Platform**  
erichb@microsoft.com

| DAY | SESSION | TOPIC          | BIOGRAPHY  |
|-----|---------|----------------|--|
| 2   | 2       | <b>Keynote</b> | <p><b>Benjamin Bögel</b> is Head of Sector for Product Security and Certification Policy at the European Commission. Benjamin has studied economics and political science in Germany, France and Belgium. Thereafter, he has worked for seven years as personal advisor to a Member of the European Parliament. Since 2019 he is developing and overseeing the implementation of cybersecurity policy in the Unit for Cybersecurity Policy in the European Commission, where he is mostly dealing with the cybersecurity of critical infrastructures as well as with the security of hardware and software products.</p> |



**Benjamin Bögel, Head of Sector for Product Security and Certification Policy at the European Commission**  
benjamin.BOEGEL@ec.europa.eu

| DAY | SESSION | TOPIC  | BIOGRAPHY   |
|-----|---------|--|---|
| 1   | 3       | <b>OPC UA Security Architecture</b>                | <p><b>Matthias Damm</b> is the founder and CEO of Unified Automation, a provider of software products, software development kits and services for industrial automation and the Industrial Internet of Things. The company's main focus is on OPC UA, a communication standard for industrial automation. Matthias has more than 25 years of experience in this field and has been involved in the development and implementation of OPC UA from the beginning. He is an active member of the OPC Foundation, where he serves on the Board of Directors and as editor and chair of several OPC UA working groups.</p> |
| 2   | 8b      | <b>Central Security Management with OPC UA GDS</b> | <p><b>Matthias Damm</b> is the founder and CEO of Unified Automation, a provider of software products, software development kits and services for industrial automation and the Industrial Internet of Things. The company's main focus is on OPC UA, a communication standard for industrial automation. Matthias has more than 25 years of experience in this field and has been involved in the development and implementation of OPC UA from the beginning. He is an active member of the OPC Foundation, where he serves on the Board of Directors and as editor and chair of several OPC UA working groups.</p> |




**Matthias Damm, Unified Automation**  
matthias.damm@ascolab.com

| DAY | SESSION | TOPIC   | BIOGRAPHY   |
|-----|---------|---|---|
| 1   | 5       | <b>A component manufacturer's considerations regarding security</b> | <p><b>Torsten Förder</b> joined Beckhoff Automation in 2020. He works in the TwinCAT Product Management Department, where he is responsible for the security features of the products and uses his 30 years of experience in software and product development, including more than 20 years with a focus on security.</p> |



**Torsten Förder, Beckhoff Automation GmbH**  
t.foerder@beckhoff.com


| DAY | SESSION | TOPIC   | DESCRIPTION  |
|-----|---------|---|--|
| 2   | 9c      | A real-world look at industrial OPC UA setups | <b>Sven Goldstein</b> joined Beckhoff Automation in 2005. He works in the TwinCAT Product Management Department, where he is responsible for connectivity-related matters. |



**BECKHOFF**

**Sven Goldstein,**  
Beckhoff Automation GmbH  
s.goldstein@beckhoff.com


| DAY | SESSION | TOPIC                            | DESCRIPTION   |
|-----|---------|----------------------------------|---|
| 1   | 2       | Welcome & Introduction to OPC UA | <b>Stefan Hoppe</b> is the OPC Foundation President since end 2018 coordinating the OPC expansion into the Internet of Things & Industrie4.0. Stefan has been the Global Vice President since 2014 and the President of the OPC Europe organization since 2010 being the catalyst for initiating liaisons with other industrial consortiums that has resulted in OPC working groups developing companion specifications for the organizations respective information models. Stefan Hoppe studied electrical engineering at the Technical University of Dortmund, Germany. Since 1995 he has worked for BECKHOFF Automation, starting as a software developer later as a lead Product Manager with focus on PC based Automation, connectivity and embedded software products. |



**OPC FOUNDATION**

**Stefan Hoppe, President and Executive Director OPC Foundation**  
stefan.hoppe@opcfoundation.org

| DAY | SESSION | TOPIC                   | DESCRIPTION   |
|-----|---------|-------------------------|---|
| 1   | 1       | Greetings from the Host | <b>Dr. Holger Kenn</b> is responsible for the technology strategy in the AI and MR business development team at Microsoft, working with a cross-functional team building out the ecosystem of technology partners, standards bodies, and other innovation catalysts in the domains of IoT and AI. Previous roles within Microsoft include Architect, working with industrial OEMs to build a wide variety of AI- and IOT-powered industrial and consumer solutions across a range of industries and Applied Researcher in Microsoft Research, working on distributed systems technology and system-level innovations such as real-time hypervisors and security systems. Outside of Microsoft, Dr. Kenn has led international research teams in the domains of robotics, wearable computing and AI at several international research organizations. Dr. Kenn earned a Ph.D. degree from Vrije Universiteit Brussels in Belgium, designing operating systems for autonomous systems. |



**Microsoft**

**Dr. Holger Kenn, Microsoft**  
holger.kenn@microsoft.com

| DAY | SESSION | TOPIC   | DESCRIPTION  |
|-----|---------|---|--|
| 2   | 8a      | Secure OPC UA Software Development – Good practices | <b>Vincent Lacroix</b><br><ul style="list-style-type: none"> <li>20 years of experience in critical software development (functional safety, then cybersecurity)</li> <li>S2OPC product owner</li> </ul> |



**systemel**

**Vincent Lacroix, Systemel**  
vincent.lacroix@systemel.fr

| DAY | SESSION | TOPIC  | DESCRIPTION  |
|-----|---------|--|--|
| 2   | 7b      | Secure device registration and certificate management for heterogeneous OT environments incl. OPC UA | <b>Frank Laurig</b><br>Product Owner for Cybersecurity Infrastructure like Certificate Management and for Zero Trust in the OT<br><ul style="list-style-type: none"> <li>Developing and delivering cybersecurity infrastructure products as a product owner for almost 5 years</li> <li>Defining Zero Trust OT requirements</li> <li>Creating solutions and talking to Siemens Digital Industry customers</li> </ul> |



**SIEMENS**

**Frank Laurig, Siemens**  
frank.laurig@siemens.com

| DAY | SESSION | TOPIC   | DESCRIPTION   |
|-----|---------|---|---|
| 1   | 6       | Machinery manufacturers commitment to the CRA | <b>Alexey Markert</b> has been working for the VDMA in the Department of Technical Affairs and Standardization since 2022. Since 2023, he is responsible for the regulatory aspects of the CRA and is the contact person for the more than 3,000 VDMA member companies. |



**VDMA**

**Alexey Markert, VDMA**  
alexey.markert@vdma.org



DAY 1 SESSION 4

**The CRA is coming – the CE Mark is extended to include security**



**Lena Schnepfer** is policy officer in the Division for Expert Committee Work and Quality Management for Evaluation and Certification Processes. The division supported the Federal Ministry of the Interior and Community in the Cyber Resilience Act negotiations.the CRA demand, why, and for what?



**Lena Schnepfer, BSI**  
lena.schnepfer@bsi.bund.de

DAY 2 SESSION 3

**For effective Vulnerability Management – SBOM in the CRA**



**Anna Schwendicke** is Head of Division for Market Surveillance in the Federal Office for Information Security, BSI. Since 2021 the market surveillance of BSI watches certified and labelled products and services. To this end products can be sampled or chosen incident-related and tested for conformity with the underlying standards..



**Anna Schwendicke, BSI**  
anna.schwendicke@bsi.bund.de

DAY 2 SESSION 7b

**Secure device registration and certificate management for heterogeneous OT environments incl. OPC UA**



**Anna Palmin**, Head of the “Cybersecurity & Trust” group, Principle Key Expert, Digital Industries, Process Automation For almost 20 years has been driving, coordinating and shaping the development of holistic, innovative, system-wide concepts and solutions which enable optimal protection for OT products and heterogeneous OT environments. Current focus in particular on cybersecurity by design and cybersecurity architecture in alignment with relevant standards and regulations incl. trust management (e.g. secure device registration, automated certificate management), security events/logging



**Anna Palmin, Siemens**  
anna.palmin@siemens.com

DAY 2 SESSION 6a

**CVE from experience**



**SIEMENS**

**Dr. Thomas Pröll, Siemens**  
thomas.proell@siemens.com


DAY 2 SESSION 4

**Vulnerability Management – CVE**

N.N.

DAY 2 SESSION 10

**Operational Technology (OT) Threats and the Need for Cybersecurity Collaboration**



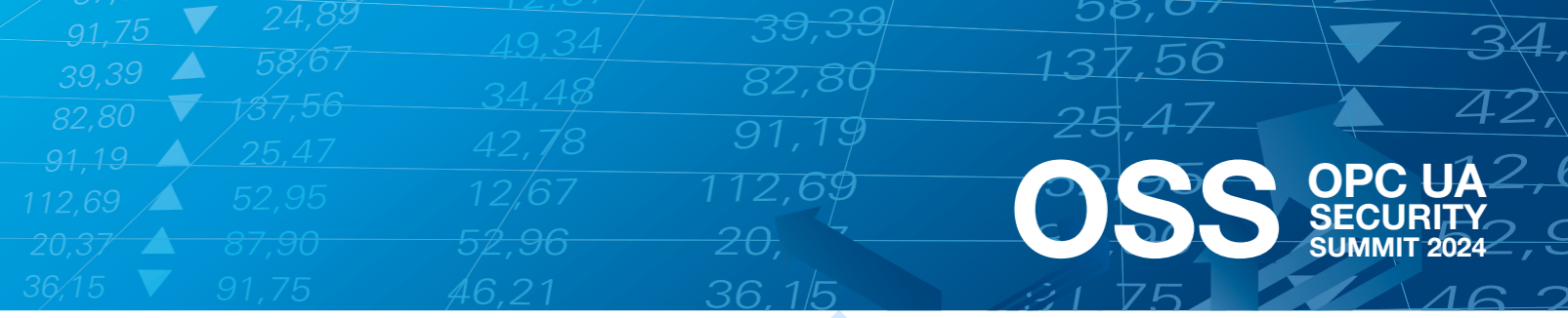
**Special Agent Brian Kaiser, FBI**


DAY 2 SESSION 7a

**CVE in context of supply chain**

**Dr. Thomas Pröll**

- Started in Siemens since 2006 with product Penetration Tests
- Founding member of the Siemens ProductCERT in 2011 and doing vulnerability handling on Siemens products since then
- Currently investigating the life of vulnerabilities along the supply chain



| DAY | SESSION | TOPIC                | SPEAKER   |
|-----|---------|----------------------|---|
| 2   | 5       | CRA and EN IEC 62443 |  <p><b>Dr. Kai Wollenweber</b></p> <ul style="list-style-type: none"> <li>At Siemens Digital Industries responsible for the governance in the areas of cybersecurity standardization, regulation and conformity assessment.</li> <li>Since more than 20 years he held various positions in the field of security &amp; safety in the industrial and aerospace &amp; defense domains and has doctorate in embedded security</li> <li>Active participation at e.g. IEC, CEN/CENELEC, DKE and in the CRA related standardization activities as a convenor and editor of the IEC 62443 cybersecurity framework.</li> </ul> <p><b>SIEMENS</b></p> <p>Dr. Kai Wollenweber, Siemens, kai.wollenweber@siemens.com</p> |

| DAY | SESSION | TOPIC   | SPEAKER  |
|-----|---------|---|--|
| 2   | 6c      | Liability for Open-Source-Software under the Cyber Resilience Act     |  <p><b>Dr. Gerrit Hötzel</b></p> <ul style="list-style-type: none"> <li>Certified Expert Attorney for Information Technology Law and Certified Expert Attorney for Copyright and Media Law</li> <li>Partner at VOELKER law firm leading the IP / IT team of the Stuttgart office</li> <li>legal compliance, contract design and litigation within digitalization projects since 15 years</li> </ul> <p><b>VOELKER</b><br/>Rechtsanwälte · Wirtschaftsprüfer · Steuerberater</p> |
| 2   | 7c      | Contract Design along the Supply Chain under the Cyber Resilience Act | <p><b>Dr. Gerrit Hötzel</b></p> <ul style="list-style-type: none"> <li>Certified Expert Attorney for Information Technology Law and Certified Expert Attorney for Copyright and Media Law</li> <li>Partner at VOELKER law firm leading the IP / IT team of the Stuttgart office</li> <li>legal compliance, contract design and litigation within digitalization projects since 15 years</li> </ul>   |

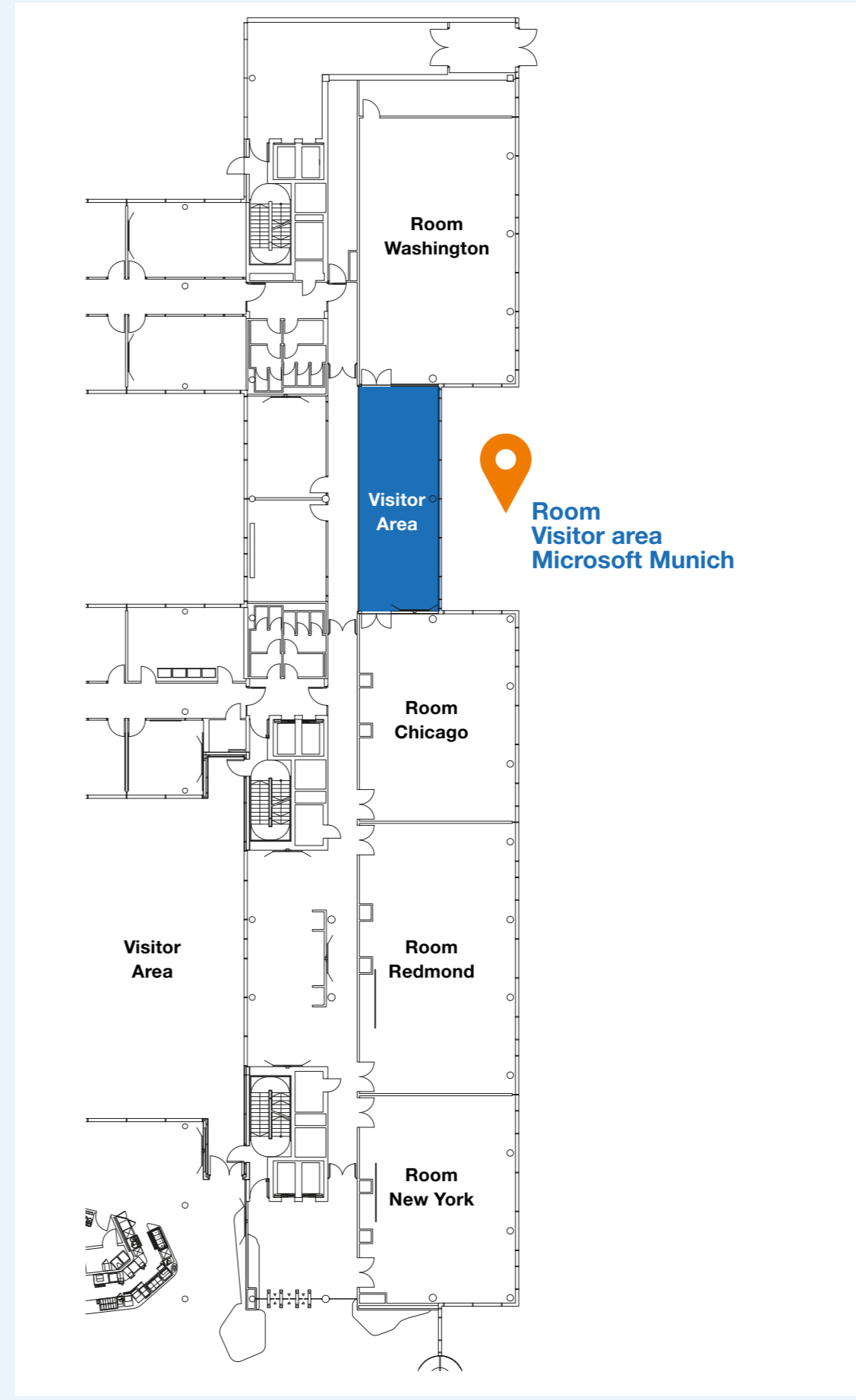
| DAY | SESSION | TOPIC  | SPEAKERS  |
|-----|---------|--|---|
| 1   | 7       | Security, a foundation for the Digital Factory |   <p><b>Trond Kvamme, Equinor</b></p> <p><b>Jan Munkejord, Equinor</b></p> |

| DAY | SESSION | TOPIC                               | SPEAKER  |
|-----|---------|-------------------------------------|--|
| 2   | 9a      | Integrating PubSub Security in UAFX |  <p><b>David Smith</b> is a Cyber Security Architect as Schneider Electric. He has 15 years of experience as a developer working on industrial controls systems focusing on network redundancy, high availability, and machine to machine communications. Focusing on security for the past few years, he has been involved with implementation of security features, preparing devices for IEC-62443 certification, and the development and prototyping of secure OT protocols like OPC UA.</p> <p><b>Schneider Electric</b></p> <p>David Smith, Schneider David_Andover.Smith@se.com</p> |

# EXHIBITING COMPANIES

# MAP OF LOCATION

|  |  |  |
|--|--|--|
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |



# OSS OPC UA SECURITY SUMMIT 2024



## HEADQUARTERS / USA

OPC Foundation  
16101 N. 82nd Street  
Suite 3B  
Scottsdale, AZ 85260-1868  
Phone: (1) 480 483-6644  
office@opcfoundation.org

## OPC EUROPE

Huelshorstweg 30  
33415 Verl  
Germany  
opceurope@opcfoundation.org

## OPC JAPAN

c/o Microsoft Japan Co., Ltd  
2-16-3 Konan Minato-ku, Tokyo  
1080075 Japan  
opcjapan@opcfoundation.org

## OPC KOREA

c/o KETI  
22, Daewangpangyo-ro 712,  
Bundang-gu, Seongnam-si, Gyeonggi-do  
13488 South Korea  
opckorea@opcfoundation.org

## OPC CHINA

B-8, Zizhuyuan Road 116,  
Jiahao International Center, Haidian District,  
Beijing, P.R.C  
P.R.China  
opcchina@opcfoundation.org

[www.opcfoundation.org](http://www.opcfoundation.org)