



## 16. Internationales TÜV Rheinland Symposium

### **Funktionale Sicherheit und Cybersecurity in industriellen Anwendungen**

15. + 16. September 2026 in Köln

## CALL FOR PAPERS

**Veranstaltungsort:** **TÜV Rheinland – Köln**  
Hauptgebäude – Rheinland Saal

**Kontakt:** **Veronica Gras**  
☎ +49 221 – 806 2981  
[veronica.gras@de.tuv.com](mailto:veronica.gras@de.tuv.com)

**Florian Kiel**  
☎ +49 221 806 4355  
[florian.kiel@tuv.com](mailto:florian.kiel@tuv.com)



# CALL FOR PAPERS

## 16. Internationales TÜV Rheinland Symposium

Funktionale Sicherheit und Cybersecurity in industriellen Anwendungen

15. + 16. September 2026 in Köln.

TÜV Rheinland lädt Experten, Fachleute, Praktiker, Ausbilder, Forscher und Regulierungsexperten ein, neue Konzepte, Methoden und Erfahrungen zu Funktionaler Sicherheit, Cybersicherheit und KI vorzustellen und zu diskutieren.

Diese Fachveranstaltung soll eine Plattform für intensiven Erfahrungsaustausch für diejenigen sein, die im Themenbereich der Funktionalen Sicherheit und Cybersecurity unterschiedlicher industrieller Anwendungsbereiche tätig sind.

Der Fokus liegt auf persönlichem Kennenlernen aller Beteiligten und einem intensiven interaktiven – nicht virtuellen – Erfahrung- und Wissensaustausch.

Experten und Fachleute werden eingeladen, Vortragsvorschläge zu technischen Entwicklungen und Trends zum aktuellen Stand der Technik in der Funktionalen Sicherheit sowie in der Cybersecurity einzureichen. Dazu gehören auch Erfahrungsberichte, Projektbeispiele sowie Diskussionen zu technischen Problemstellungen.

Nach jedem Vortrag findet eine kurze Fragerunde mit Diskussion statt.

Die Veranstaltung wird von zwei Moderatoren begleitet.

Präsentationen zu Produkten oder werblichen Inhalten sowie solche, die vorwiegend auf Grundlagenwissen oder -kenntnissen basieren, sind nicht gewünscht.

Das Symposium wird zweisprachig (Deutsch und Englisch) gehalten und simultan übersetzt.

### Zielgruppe

System- und Softwarearchitekten, HW/SW und Entwicklungsingenieure, Produktmanager, Projektleiter, Safety-, Security- und Qualitäts-Manager, Anlagenbetreiber etc.

### Anwendungsbereiche:

Maschinenbau, Produktentwicklung und –herstellung, Prozessindustrie, etc.

### Vorträge

- Vortragende haben 30 Minuten Zeit für ihren Vortrag.
- Im Anschluss des Vortrages werden mit Unterstützung der Moderatoren Fragen gestellt.
- Vorträge sollen durch eine MS PowerPoint Präsentation unterstützt werden.
- Falls möglich, sollen alle Präsentationen auf der TÜV Rheinland Website nach der Veranstaltung zum Download zur Verfügung stehen.



# CALL FOR PAPERS

## 16. Internationales TÜV Rheinland Symposium

Funktionale Sicherheit und Cybersecurity in industriellen Anwendungen  
15. + 16. September 2026 in Köln.

Abgabe Abstract  
10. Februar 2026

### Vortragsvorschläge

Wenn Sie Interesse haben im Rahmen dieses Symposiums einen Vortrag zu halten, schicken Sie uns bitte Informationen zu Ihrem Vortrag zu.

Bitte nennen Sie uns:

1. Vortragstitel (in Englisch und in Deutsch)
2. Ihren Namen mit Email Adresse.
3. Genaue Firmenangabe.
4. Kurze Zusammenfassung des Vortragsthemas.

Bitte schicken Sie uns Ihren Vortragsvorschlag bis spätestens **10. Februar 2026** zu.

Vortragsvorschlag bitte per  
E-Mail an:

**veronica.gras@de.tuv.com**

### Programm

Im April/Mai 2026 wird das Programm feststehen und beworben.

Bis dahin erhalten alle, die einen Vortrag eingereicht haben, die Information, ob der Vortrag in das Programm aufgenommen worden ist und an welchem Tag und zu welcher Uhrzeit der Vortrag stattfindet.

### Präsentationen

- Präsentationen, die während des Vortrages verwendet werden, sollen in PowerPoint erstellt werden.
- Präsentationen sollten in Englischer Sprache verfasst sein (oder zweisprachig in D+ Eng).
- Für die ppt-Präsentation soll eine Formatvorlage, die von TÜV Rheinland zur Verfügung gestellt wird, verwendet werden.
- Ppt-Präsentationen sollen bis zum **1. September 2026** bei TÜV Rheinland eingereicht werden.

**Vortragsvorschlag:** bis **10. Februar 2026**

**Programm fertig:** **April/Mai 2026**

**Präsentation:** bis **1. September 2026**

### Kontakt

TÜV Rheinland Industrie Service GmbH  
Am Grauen Stein – 51105 Köln  
Veronica Gras  
☎ +49 221 806 2981  
veronica.gras@de.tuv.com



# CALL FOR PAPERS

## 16. Internationales TÜV Rheinland Symposium

Funktionale Sicherheit und Cybersecurity in industriellen Anwendungen

15. + 16. September 2026 in Köln.

### Themen

- **Internationale Normen – Inhalte/Status/Aktualisierung**  
IEC 61508 – aktueller Stand 3. Edition  
IEC 61511  
IEC 62061, ISO 13849  
ISO 26262, ISO 21434, ISO 21448  
IEC 62443  
VDE-AR-E 2842-61  
EN 50742  
EN 17955  
VDI/VDE 2180-5  
EN IEC 61800-5-3:2023
- **Relevanz der Normen zu Funktionale Sicherheit und Cybersecurity weltweit**
- **Neue europäische Richtlinien**  
Cyber Resilience Act (CRA)    EU 2024/2847  
EU-Maschinenverordnung    EU 2023/1230  
AI-Act    EU 2024/1689  
RED    2014/53/EU
- **Beispiele und Trends für Anwendungen in verschiedenen Branchen**  
Prozessindustrie, Maschinenbau, Produkt-Entwicklung und Herstellung; Energie etc.
  - Außergewöhnliche Beispiele aus der Praxis wie **Autonomous Guided Vehicles (AGV)** im Maschinenbau und in der Prozessindustrie
  - Funktionale Sicherheit / Cybersecurity bei **Batterie Management Systeme**
  - **Safety in der Wasserstoffherzeugung**
- **Penetrationstesting / Sicherheitsanalysen** in der Praxis: Tools, Frameworks, Fallstudien
- **Management Systeme** für Funktionale Sicherheit, Cybersecurity und KI
- **Field Instrumentation:** Networks (Communication/Safety/Security); Application Software; Verification/Validation.
- Relevanz der **Akkreditierung** von Cybersecurity (IEC 62443 series, ISASecure).
- **Künstliche Intelligenz** im Kontext zur Funktionalen Sicherheit/Cybersecurity  
**KI-Risiken:** Ausrichtung von KI-Systeme auf menschliche Werte, Präferenzen und ethische Prinzipien.  
**KI-Sicherheit:** Robustheit, Lernen unter Unsicherheit, Explainability, Vertrauenswürdige KI (Trustworthiness) in sicherheitskritischen Anwendungen (z. B. Automotive, Industrie, Medizin)
- **Datenschutz**, Privacy-Preserving Techniques in sicherheitsrelevanten Systemen
- **Cloud, OT- und IoT-Sicherheit** in sicherheitskritischen Umgebungen
- **Human Factor/Kompetenzen, Security Awareness**

.....sind willkommen.