Call for Papers

In diesem Jahr findet das disziplinübergreifende »Forum Safety & Security« vom 08. - 10. Juli 2019 (Basisseminar & Workshops am 08.07.) in der Stadthalle Sindelfingen statt.

Während des Forums werden die Einzelthemen Safety und Security sowie das Zusammenspiel beider Aspekte diskutiert und zwar aus Sicht der Anwendungsbranchen Industrie, Automotive und Medizintechnik. Das Vortragsprogramm spannt den Bogen von den verfügbaren Hard- und Softwarekomponenten, den Tools, Hilfsmitteln und der Zertifizierung bis zum praktischen Einsatz sicherer Systeme in der Fertigung, im Automobil und in der Medizintechnik.

Beteiligen Sie sich mit technischen Vorträgen, Praxisbeispielen und Erfahrungsberichten aus entsprechenden Projekten und senden Sie uns Ihre Themenvorschläge zum Beispiel zu folgenden Themen:

Grundlagen

- Die verschiedenen Normen/Richtlinien und Initiativen zur Funktionalen Sicherheit und/oder Security und ihre Unterschiede
- SIL- und ASIL-Klassifizierung
- Weiterentwicklung der Normen – was ändert sich?
- Umsetzung der Funktionalen Sicherheit – Erfahrungen mit Safety-Prozessen, veränderte Entwicklungsprozesse
- Cyber Security
- Best Practice aus anderen Industrien
- Safety- bzw. Security-Mechanismen
- Zertifizierung & Prüfung
- Rechtliche Aspekte, Produkthaftung, Zertifizierung

Hard- und Software, Tools

- Confidence in Use of Software Tools
- Software-Entwicklungsmethoden, agile Methoden
- Qualifizierung von Softwarewerkzeugen
- HIPS (Host Intrusion Prevention Systems), BOPS (Pufferüberläufe)
- Angriffssichere Software und deren Entwicklung
- (Tool-gestützte) Sichere Softwareentwicklung
- ISO-Standard 27034
- Verifikation funktionaler Anforderungen – Strategien & Tools
- Gefährdungs- und Risikoanalysen
- Applikations-Software, Codegeneratoren, Betriebssysteme, Compiler
- Simulations- und Visualisierungswerkzeuge
- „SOUP“ und funktionale Sicherheit
- Modellbasierte Entwicklung & Test
- Tool-Qualifizierung, SW-Test, -Verifikation und –Dokumentation, Code Coverage

- Diagnosemaßnahmen in Hardware & Software
- HW-Sicherheitskonzepte, -mechanismen & -Berechnungsmethoden
- Sicherheitsmechanismen in Hardware

Automotive

- Robustness Validation
- ISO26262 – Praxisbeispiele & realisierte Projekte
- AUTOSAR und ISO26262
- Automotive SPICE und ISO26262
- Zertifizieren und Testen nach ISO26262
- Sicherheitsanalytik, Analysemethoden
- Lösungskonzepte (HW/SW) für FuSi-Anwendungen im Auto
- Automotive Security – Status quo: Wie weit ist die Standardisierung?
- Safety & Security im gesamtheitlichen Kontext
- Safety & Automotive Ethernet: Auf dem Weg zum autonomen Fahren
- Blockchain unter Safety- und Security-Aspekten

Medizin

- Was ist funktionale Sicherheit von Medizinprodukten?
- Anwendbare Normen (IEC 60601, DIN VDE 0801, IEC 61508)
- Unterscheidung: systematische und zufällige Fehler, Fehler in Hardware und Software
- „Bedingung des ersten Fehlers" aus der IEC 60601-1
- Die Rolle der Software bei der funktionalen Sicherheit
- Methoden für den Selbsttest von CPU, RAM, EPROM, Sensoren (analog und digital), Abschaltweg, Alarmabgabe, Zeitbasis, Watchdog
- Programmlaufüberwachung
- Überwachung der Versorgungsspannung
- Besondere Probleme bei Fernsteuerung und Telemedizin
- Zugekaufte Software (Betriebssysteme, Bibliotheken)
- Sicherheitsaspekte objektorientierter Programmierung
- Software-Update und Code-Download
- Sicherheitsanalytik, Analysemethoden
- Risikomanagement und Risikoanalyse für Medizinprodukte nach ISO 14971
- CE-Zertifizierung von Medizin-Software
- Implementierung der Norm IEC 62304 für die Hersteller von Medizinprodukten
- Cyber-Security in der Medizintechnik
- Infiltration mit Malware und deren Abwehr
- Security als Teil der Risikoanalyse
- Information Security Management Systeme (ISMS)
- Industrie 4.0. in der Medizintechnikindustrie – aber sicher
- Schutz vertraulicher Patientendaten
- Safety & Security im gesamtheitlichen Kontext
- Software als Medizinprodukt

Industrie

Security

- Typische Angriffsvektoren in der Industrie
- Infrastrukturkomponenten für die sichere Datenkommunikation
- IT-Sicherheitskonzepte
- Mobile Endgeräte in der Industrie
- Verschlüsselungsverfahren
- Wie lassen sich Cyber-Angriffe erkennen?
- Security-Schwachstellen identifizieren
- Cyber-Security-Managementsysteme
- Industrielle IT-Sicherheit vs. klassische IT-Sicherheit
- Fernwartung: Was gilt es zu beachten?

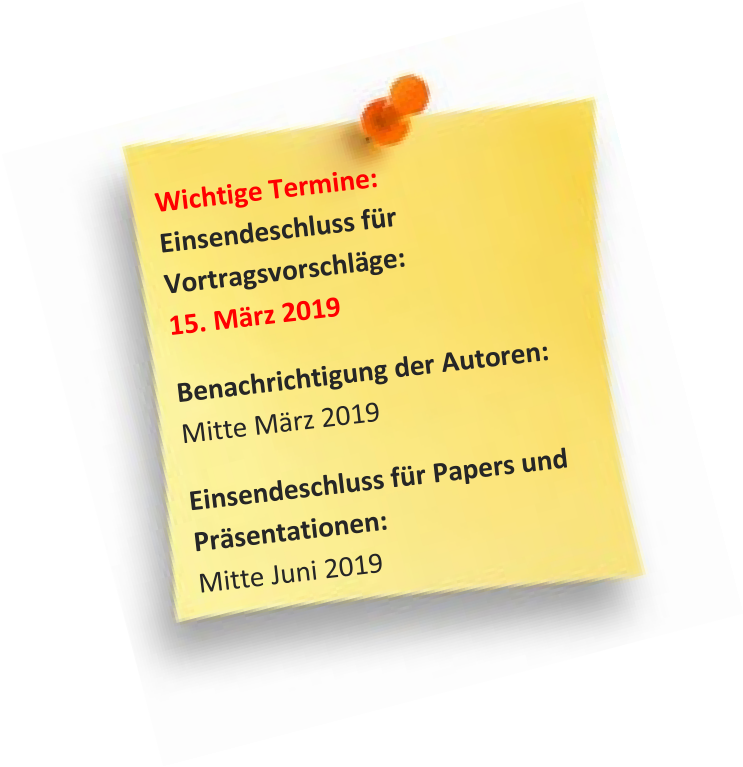
Safety

- Safety in „dynamischen“ Produktionsumgebungen
- Entwicklungs- und Programmiersysteme für sichere Automatisierungskomponenten
- Was bei der Verkettung mehrerer Sicherheitssteuerungen bzw. –sensoren zu beachten ist
- Sichere Kommunikation über Ethernet-basierte Protokolle
- Safety über drahtlose (wireless) Übertragungsmedien
- Safety im internationalen Vergleich
- Sichere Mensch-Roboter-Interaktion
- Praxisbeispiele: Realisierte Functional-Safety-Projekte in der Industrie
- Umbau und wesentliche Veränderungen an Maschinen und Anlagen
- Sicherheit und Standard-Automation im Mix
- SIL-Nachweis in der Praxis
- Risikobeurteilung für Konstruktion und Bau von sicheren Maschinen
- Safety auf PC-Plattformen – geht das?

Bitte reichen Sie eine aussagekräftige Kurzfassung Ihres Vortrags bis zum **15. März 2019** ein!

Eine rein technische Abhandlung des Themas ist zwingend erforderlich. Marketingorientierte Vorträge werden nicht akzeptiert.

Wir freuen uns auf Ihre interessanten Beiträge!



Kontakt:
WEKA FACHMEDIEN GmbH
Renate Ester, Event Manager
Tel. +49 (0)89 25556 - 1349
E-Mail: REster@weka-fachmedien.de
www.safety-security-forum.de

Eine gemeinsame Veranstaltung der Redaktionen: