# 34. SafeTRANS Industrial Day

In Kooperation mit

## Siemens AG

**Thema**

## Absicherung von Systemen mit KI-Komponenten

### Zielsetzung des Workshops

Der Workshop bringt führende Experten aus Industrie und Forschung zusammen, um den aktuellen Stand und die zukünftige Entwicklung zur Absicherung von Systemen mit KI Komponenten in den Domänen Automotive, Avionics, Maritime und Railway Systems zu diskutieren.

In den vergangenen Jahren haben sich Leistungsfähigkeit und Funktionsumfang von KI Algorithmen enorm gesteigert; viele Funktionen, die mit traditionellen Methoden nur schwer oder gar nicht realisiert werden konnten, rücken nun in den Bereich des Möglichen, ja sogar des effizient Realisierbaren. Der Einsatz solcher KI-basierten Funktionen stößt jedoch dort an seine Grenzen, wo ein hohes Maß an funktionaler Sicherheit für das Gesamtsystem erforderlich ist, da traditionelle Methoden und Verfahren zur Absicherung solcher Systeme das erforderliche Maß an funktionaler Sicherheit nicht nachweisen können. Die Absicherung von Systemen mit KI-Komponenten – d.h. Methoden und Verfahren zum Nachweis der funktionalen Sicherheit solcher Systeme – war und ist daher Gegenstand vieler Forschungsinitiativen.

Auf regulatorischer Seite wird durch den EU AI Act eine risiko-basierte Klassifikation solcher Systeme vorgegeben, mit unterschiedlichen Anforderungen an die notwendigen Sicherheitsanforderungen in jeder Klasse. Regularien, die die Zulassung solcher Systeme betreffen – wie etwa UN R157 im Automotive Bereich – definieren neue Anforderungen an die Absicherungsmethodik wie beispielsweise Szenarien-basiertes Testen, virtuelles Testen und kontinuierliches Monitoring und lassen damit prinzipiell auch die Absicherung von KI-basierten Systemen zu. Auf Seiten der Standards

sind domänenübergreifend mehr als 100 Initiativen zur Erstellung entsprechender Richtlinien oder Vorbereitung entsprechender Standards zu beobachten. Im Automotive Bereich ist hier insbesondere ISO 8800 „Road Vehicles – Safety and Artificial Intelligence“ zu nennen, in der domänenspezifische Richtlinien zur Verwendung von KI in sicherheitsrelevanten Funktionen aufgestellt werden und eine Methodik für den Sicherheitsnachweis von KI-Komponenten erstellt wird, die sich in den – typisch ISO 26262 und ISO 21448 SOTIF basierten – Sicherheitsnachweis des Gesamtsystems einfügt.

**Aufruf zur Einreichung von Beiträgen**

Beiträge – d.h. 30-minütige Präsentationen – zu den folgenden Themen sind hochwillkommen:

- Aktuelle Regularien und Standards für die Absicherung von Systemen mit KI-Komponenten in sicherheitskritischen Anwendungen
- Welche Klassen von KI-Systemen lassen den Nachweis der funktionalen Sicherheit des Gesamtsystems zu, welche nicht?
- Welche Prozesse müssen im Rahmen des Systems Engineering etabliert werden, um alle relevanten Umgebungscharakteristika zu identifizieren, die für eine sichere Anwendung einer KI-Komponente essentiell sind
- Wie sehen Prozesse und Methoden aus, um aus Incidents, Near Accidents und Accidents im Feld die Charakterisierung des notwendigen Wissens über den Umgebungskontext zu verfeinern
  Methoden und Werkzeuge zur Erstellung von Sicherheitsnachweisen („Assurance Cases“) von Systemen mit KI-Komponenten (z.B. als Forschungs- und Projektergebnisse) sowie deren Einpassung in aktuelle Regularien und Standards
- Einfluss von Absicherungsmaßnahmen auf Komponentenebene auf Systemsicherheit
- Zukünftige Entwicklungen
  - Sind aktuelle Regularien und Standards ausreichend bzw. welche „Lücken“ existieren noch? Welche Projekte und Initiativen existieren zum Schließen dieser „Lücken“?
  - Sind Werkzeuge zur Unterstützung der Methodik vorhanden? Sind diese ausreichend leistungsstark? Welche Projekte und Initiativen bestehen zur Verbesserung solcher Werkzeuge?

Bitte senden Sie eine Email mit Sprecher/in, Titel und Abstract (ca. ½ -1 Seite) des geplanten Beitrags bis zum 1. Oktober 2024 an katja.bonhagen@safetrans-de.org. Die Auswahl der Beiträge erfolgt bis Mitte Oktober.

**Workshop-Sprache**

Die Vortragssprachen des Workshops sind Deutsch und Englisch. Folien sind typisch – aber nicht verpflichtend – in Englisch abgefasst, die Vortrags- und Diskussionssprache ist typisch Deutsch (abhängig vom Teilnahmekreis ggf. auch Englisch).

**Datum und Veranstaltungsort**

Datum: 05.12.2024, 09:30 bis 17:00 Uhr

Veranstaltungsort: Siemens AG, München, Wittelsbacher Platz 2

Webseite: https://www.safetrans-de.org