INTERVIEW

# »Wann ist sicher sicher genug?«

Assistenzsysteme leisten einen wichtigen Beitrag zur Arbeitssicherheit, da sie den Maschinenführer gezielt vor Gefährdungen warnen oder sogar drohende Kollisionen verhindern können. Bei teil- oder vollautomatisierten Funktionen kommen heutige Assistenzsysteme an ihre Grenzen, da sie nicht als Sicherheitsfunktion im Sinne der ISO 12100 entwickelt wurden. Welche Anforderungen an solche Systeme gestellt werden und was abseits der funktionalen Sicherheit noch relevant ist, verrät Dr. Sebastian Jakobs, Lead Engineer für Funktionale Sicherheit bei der ITK Engineering GmbH.

***Assistenzsysteme im Maschinenumfeld leisten einen wichtigen Beitrag zur Arbeitssicherheit, da sie den Maschinenführer gezielt vor Gefährdungen warnen oder sogar drohende Kollisionen mit einem Bremseingriff verhindern können.*** © ITK Engineering

**Worin liegt der Unterschied zwischen assistierenden und teil-/vollautomatisierten Systemen?**
Assistenzsysteme, wie zum Beispiel ein Kollisionsvermeidungssystem, sollen den Operator einer Maschine in seiner Aufgabe unterstützen und entlasten. Dabei bleibt die Sicherheitslast jedoch beim Operator, da man sich den Schwächen der zugrundeliegenden Technologien bewusst ist. Somit dürfen Assistenzsysteme nicht zur Risikominderung der Maschine genutzt werden. Teil- oder vollautomatisierte Systeme hingegen übernehmen einen Teil der Maschinenfunktion bzw. erfordern keinen Eingriff mehr durch den Operator. Diese stellen Sicherheitsfunktionen dar, die entsprechend den Standards zur funktionalen Sicherheit entwickelt werden müssen.

**Müssen also Prinzipien der funktionalen Sicherheit bei Assistenzsystemen nicht angewandt werden?**
Da per Definition Assistenzsysteme im Maschinenumfeld keine Sicherheitsfunktion darstellen, fallen diese nicht direkt unter die Standards zur funktionalen Sicherheit. Da sich der Nutzer jedoch in aller Regel auf die Funktionalität verlässt, sind auch für solche Funktionen Basismechanismen nötig, um die korrekte Funktionalität zu überprüfen. Die ISO 21815 für Assistenzsysteme im Erbbaumaschinenumfeld fordert zum Beispiel eine Eigendiagnose während des Start-Ups und zyklische Diagnosen zum Test der Grundfunktionalität während des Betriebs. Der Standard legt jedoch nicht fest, welche Diagnosen nötig sind. Hier können Methoden aus der funktionalen Sicherheit helfen, um geeignete Maßnahmen zu definieren. An dieser Stelle sei erwähnt, dass sich durch die Nutzung eines Assistenzsystems neue Risiken ergeben könnten, die entsprechend der ISO 12100 bewertet und mitigiert werden müssen.

**Worin sehen Sie aktuell die größten Herausforderungen im Zusammenhang mit zunehmender Automatisierung?**
Unwegsames Gelände und externe Einflüsse, wie Staub, Regen oder Schnee stellen eine große Herausforderung für die Sensorik und Algorithmik dar, zuverlässig zwischen Hindernissen und befahrbarem Gelände unterscheiden zu können. Das gilt gleichermaßen für assistierende als auch für (teil-)automatisierte Systeme. Einerseits soll das System zuverlässig Kollisionen verhindern, andererseits aber eine hohe Verfügbarkeit garantieren und nur auf kritische Hindernisse reagieren. Das wird auch von den beiden Standards ISO 21815 und ISO 17757 aufgegriffen,

© ITK Engineering

**Dr. Sebastian Jakobs**

studierte und promomierte an der Technischen Universität Kaiserslautern im Bereich Physik. Er trat 2016 bei ITK Engineering zunächst als Functional Safety Engineer ein. Seit 2022 ist Dr. Jakobs Lead Engineer für Funktionale Sicherheit im Unternehmen.

die eine Minimierung von falschpositiven und -negativen Erkennungen fordern. Falsche Entscheidungen eines solchen Systems können ihren Ursprung in verschiedenen Ursachen haben. Hierbei reicht es nicht aus, nur E/E-Fehler zu betrachten, die ganz klassisch im Zusammenhang mit der funktionalen Sicherheit stehen. Auch funktionale Unzulänglichkeiten spielen dabei eine entscheidende Rolle.

**Können Sie näher auf das Thema funktionale Unzulänglichkeiten eingehen und die Abgrenzung zur funktionalen Sicherheit erläutern?**

In der Automobilbranche fällt das unter den Begriff Safety of the intended functionality, kurz SOTIF, die im kürzlich erschienenen Standard ISO 21448 behandelt wird. Abseits der in der funktionalen Sicherheit betrachteten zufälligen Hardware-Fehler und systematischen Fehler können auch funktionale Unzulänglichkeiten zu einem unsicheren Verhalten des Systems führen. Beispiel dafür ist ein LiDAR-Sensor, der einerseits Staub als Hindernis interpretiert und andererseits ein Objekt aufgrund einer zu geringen Reflektivität nicht als solches erkennt. Folglich muss identifiziert werden, welche funktionalen Unzulänglichkeiten ein System aufweist und welche sogenannten „Triggering Conditions" zu einem gefährlichen Verhalten führen können. Die beiden Standards ISO 21815 und ISO 17757 adressieren diese Themen anhand von Beispielen, definieren jedoch nicht, wie Fehler der Sollfunktion systematisch betrachtet und mitigiert werden können. Weiterhin können vom Operator falsch interpretierte Systeminformationen zu gefährlichen Situationen führen, sodass auch die Schnittstelle zwischen Mensch und Maschine ein gewisses Gefährdungspotential innehaben kann und in die Analysen einfließen sollte. Aufgrund der schier unendlichen Vielzahl an denkbaren Szenarien, die im Kontext SOTIF beleuchtet werden müssen, ist es notwendig, in einem systematischen Vorgehen die genauen Ziele und Strategien zu definieren, um eine Argumentation für die Sicherheit der Funktion aufbauen zu können.

**Welchen Beitrag kann ITK Engineering hier leisten?**

Neben unserer Expertise im Bereich funktionaler Sicherheit können wir auf unsere domänenübergreifende Erfahrung und Methodenexpertise zurückgreifen, um den Kunden ganzheitlich in seiner Entwicklung und Integration unterstützen zu können. Dabei hat es sich bewährt, Methoden und Herangehensweisen aus anderen Domänen wie Automotive oder Industry zu adaptieren und in geeigneter Form im Baumaschinenbereich anzuwenden – zum Beispiel SOTIF nach ISO 21448. Mittels dieser Systematik können wir schon frühzeitig in der Entwicklung funktionale Unzulänglichkeiten ermitteln, notwendige Anpassungen der Spezifikation und Architektur vornehmen und ein geeignetes V&V-Konzept entwickeln. Im Bereich Simulationen bietet ITK mit Individual Virtual Environment & Sensor Simulation (IVESS) ein Framework an, das die Entwicklung und den Einsatz von Assistenzsystemen und die Automatisierung an verschiedenen Punkten unterstützen kann. Beispielsweise können wir in einer frühen Designphase mittels Simulationen geeignete Sensorpositionen an der Maschine oder auch notwendige Veränderungen am Sensorset ermitteln. Während der Entwicklungsphase liefern Simulationen realitätsnahe synthetische Daten zum Test der Algorithmik und gegen Ende der Entwicklung können wir mit IVESS kritische Corner Cases ermitteln, auf die dann der Fokus für reale Tests gelegt werden kann. ■

**ITK Engineering**
**www.itk-engineering.de**

FIRMENPROFIL

## ITK Engineering: Partner für Zukunftstechnologie

Mit rund 1.300 Mitarbeitern ist ITK Engineering ein international anerkanntes Technologieunternehmen, das sich durch ausgeprägte Expertise in der Digitalisierung, Elektrifizierung, Automatisierung und Vernetzung von Systemen auszeichnet. Durch kundenspezifische System- und Softwareentwicklung, v.a. im Bereich Embedded Systems, trägt ITK dazu bei, die Mobilität von morgen mitzugestalten und setzt sich zum Ziel, sowohl menschlich als auch technologisch zu begeistern und Maßstäbe zu setzen.

Im Zentrum stehen langfristige und nachhaltige Partnerschaften – sowohl mit Kunden als auch mit Mitarbeitern – weshalb Vertrauen, Sicherheit und ein respektvoller Umgang großgeschrieben werden. Namhafte Unternehmen aus den Bereichen Automotive, Medizintechnik, Robotik, Motorsport, Bahntechnik, Industrie 4.0 sowie Gebäudetechnik setzen bei der Entwicklung maßgeschneiderter Systemlösungen auf die Flexibilität, das Engagement sowie die Professionalität von ITK Engineering. Safety und Cyber Security, modellbasierte Softwareentwicklung sowie virtuelle Absicherung (MiL, SiL, PiL, HiL) gehören zu den Kernkompetenzen. Darüber hinaus entwickelt ITK intelligente Algorithmen (Regelungstechnik, Bild- und Signalverarbeitung) sowie kundenspezifische und plattformunabhängige Lösungen für das Internet der Dinge.

itk ENGINEERING

**ITK Engineering GmbH**
**Im Speyerer Tal 6**
**76761 Rülzheim**
**Telefon: +49 (0) 7272/7703-0**
**Fax: +49 (0) 7272/7703-100**
**Web: www.itk-engineering.de**
**E-Mail: info@itk-engineering.de**