Fraunhofer IESE

SICK Sensor Intelligence.

WIEDERVERWENDUNG MODULARER FUNKTIONSBLÖCKE IM SICHERHEITS-KRITISCHEN KONTEXT

UNSERE KOMPETENZEN UND LÖSUNGEN

- Entwicklung modularer Sicherheitskonzepte
- Explizite Safety-Argumentation zur Zertifizierung innovativer Sicherheitskonzepte
- safeTbox – Werkzeugrahmenwerk des Fraunhofer IESE für die Entwicklung und Zertifizierung sicherheitskritischer Systeme

DER KUNDENNUTZEN

- Wiederverwendung von Funktionalität auf verschiedenen Plattformen und in unterschiedlichen Anwendungskontexten
- Transfer der Ergebnisse aktueller Diskussionen in Wissenschaft und Industrie sowie künftiger Sicherheitsnormen in den Prozess des Kunden

UM WAS ES GEHT

Industrie 4.0 eröffnet eine neue Ära der industriellen Automation. Während in der Vergangenheit die Massenproduktion im großen Stil die treibende Kraft war, sorgen neue technologische Möglichkeiten heute für flexible und adaptive, dabei jedoch hochautomatisierte Fertigungsanlagen, bis hin zu kleinen Losgrößen oder kundenindividuellen Produkten. Flexibilität und Modularität sind zwei der wichtigsten Enabler für diesen Wandel. Als Innovationsführer an der Spitze der Entwicklung modernster Sensorik bietet SICK Lösungen, die für diese Herausforderung bereit sind – mit intelligenten Sensoren, die Daten erfassen, in Echtzeit auswerten, sich an ihre Umgebung anpassen und im Netzwerk miteinander kommunizieren. Vor allem, wenn es sich um sicherheitsrelevante Daten handelt, kommt der Absicherung der Systeme eine besondere Bedeutung zu. Ein Grund, warum SICK hier auf die Safety-Expertise und Unterstützung des Fraunhofer IESE vertraute.

DIE HERAUSFORDERUNG

Flexibilität und Anpassungsfähigkeit erhöhen jedoch auch immer die Komplexität. Dies gilt insbesondere an den Schnittstellen zwischen der digitalen Welt und der physikalischen Welt der Fertigungsanlagen – den Sensoren: Die Informationen zur Überwachung und Kontrolle der Qualität, Effizienz und Sicherheit von Produktionsprozessen müssen mit einem sehr hohen Maß an Zuverlässigkeit bereitgestellt werden. Diese Sensoren so intelligent wie möglich zu machen, erfordert den umfangreichen Einsatz von Software bereits auf der Ebene einzelner Sensoren und noch mehr innerhalb von Sensorsystemen und in der Steuerung.

Die Entwicklung von Funktionsblöcken für sicherheitsbezogene Anwendungen modular und transparent zu machen war das Ziel unseres gemeinsamen Projekts mit dem Fraunhofer IESE. Der vom Fraunhofer IESE vorgeschlagene modellbasierte Ansatz bot dafür die ideale Basis: Alle Schnittstellen sind gut beschrieben, sowohl mit den erbrachten und erforderlichen Services als auch mit den sicherheitsrelevanten Eigenschaften. Dies ermöglicht die Ausführung des Funktionsblocks auf verschiedenen Plattformen und die Wiederverwendung in verschiedenen Sensorsystemen. Unsere Kollegen vom Fraunhofer IESE haben hervorragende Arbeit geleistet, um unsere Herausforderungen zu verstehen und ihren Ansatz an unsere Anforderungen anzupassen.

Dr. Magnus Albert
Expert Safety Methods
Corporate Unit Functional Safety
SICK AG

Besonders wenn die von den Sensoren bereitgestellten Daten sicherheitsrelevant sind, wird die Absicherung solcher Systeme zu einer herausfordernden Aufgabe. Ziel des Projekts mit dem Fraunhofer IESE war die Erstellung und Etablierung einer Methodik, die die Entwicklung von modularen, flexiblen und dennoch »sicheren« Funktionsblöcken erlaubt. Damit können sicherheitsrelevante Funktionalitäten aus zahlreichen unabhängigen Funktionsblöcken zusammengesetzt, auf unterschiedlichen Plattformen ausgeführt und in verschiedenen Anwendungen wiederverwendet werden.

SICK wandte sich aus mehreren Gründen an das Fraunhofer-Institut für Experimentelles Software Engineering IESE: Das Institut verfügt über umfangreiche Kompetenzen im Bereich Safety Engineering und modellbasierte Ansätze. Die Verbindung des Wissens des Fraunhofer IESE im Bereich Safety Engineering mit der Erfahrung von SICK im Bereich Sensorik ermöglichte eine maßgeschneiderte Lösung für die Entwicklung sicherheitsrelevanter Funktionsblöcke in Sensorsystemen.

DIE UNTERSTÜTZUNG

Die Zusammenarbeit zwischen SICK und dem Fraunhofer IESE konzentrierte sich auf die Entwicklung eines spezifischen Funktionsblocks für kollaborative Anwendungen, bei denen Mensch und Maschine sich den gleichen Arbeitsbereich teilen. Während die Einbettung des Funktionsblocks in eine reale Anwendung dazu beitrug, Annahmen über den relevanten Kontext zu identifizieren, wurde der Funktionsblock selbst so generisch wie möglich entwickelt, um maximale Flexibilität und Wiederverwendbarkeit zu gewährleisten.

Mittels eines serviceorientierten Ansatzes wurde im ersten Schritt des modellbasierten Entwicklungsansatzes ein Blockmodell der Gesamtarchitektur der Anwendung erstellt. Auf der Basis dieser Servicearchitektur wurden die horizontalen Schnittstellen zu anderen Services und die vertikalen Schnittstellen zu den Plattformservices identifiziert. Anhand umfassender und servicespezifischer Leitwortlisten wurde jede einzelne Schnittstelle analysiert und alle relevanten Fehlermodi wurden identifiziert. Die entsprechenden Fehlerlogiken wurden dann mithilfe von Komponentenfehlerbäumen erstellt. Während der Fokus bei der Analyse auf den modularen Services lag, sorgte die Kombination der einzelnen Komponentenfehlerbäume für das Gesamtsystem für Vollständigkeit auf Systemebene. Im dritten und letzten Schritt wurde mithilfe der Analyse ein Sicherheitsnachweis erstellt, der eine umfassende und unverzichtbare Argumentation für die Gesamtsicherheit liefert.

Der modellbasierte Ansatz stellt sicher, dass jedes der drei Artefakte – Service-Blockdiagramm, Komponentenfehlerbaum und Sicherheitsnachweis – in anderen Projekten wiederverwendet werden kann, zusammen mit dem entsprechenden Funktionsblock.

DAS ERGEBNIS

Der vom Fraunhofer IESE vorgeschlagene modellbasierte Entwicklungsansatz konnte erfolgreich in das Entwicklungsprojekt bei SICK integriert werden und wurde bereits erfolgreich auf andere Entwicklungsprojekte übertragen. Das vom Fraunhofer IESE entwickelte Tool safeTbox verbindet alle erforderlichen modellbasierten Techniken in einer Toolbox und erleichtert den Einsatz der Methodik.

Name: SICK AG

Website: sick.com

Branche: Sensorherstellung

Zentrale: Waldkirch, Deutschland

Anzahl Mitarbeiter: 9.700 (2018)

Kontakt

Dr. Daniel Schneider
Department Head Embedded Systems
Quality Assurance (ESQ)
Telefon +49 631 6800-2187
daniel.schneider@iese.fraunhofer.de

Jan Reich
Expert „Dynamic Assurances of
Connected Autonomous Systems"
Telefon +49 631 6800-2254
jan.reich@iese.fraunhofer.de

www.iese.fraunhofer.de