SAFety and secURity by design for interconnected mixed-critical cyber-physical systems

Ergebnisse in Kürze

Strategien, Methoden und Tools, die eingebettete Systeme sicherer machen

Eine Initiative der EU hat sich der Notwendigkeit angenommen, Schwachstellen und Angriffe auf Mixed-Criticality-Systeme besser zu erkennen sowie diese zu verhindern und diesen vorzubeugen.

DIGITALE WIRTSCHAFT

SICHERHEIT

© ESB Professional, Shutterstock

Eingebettete Systeme sind heutzutage sehr viel komplexer, als noch vor einigen Jahren. Daher wird es immer wichtiger schon während der Konzeptionsphase geeignete Strategien zu entwickeln, um sicherzustellen, dass sich Aspekte wie Datenintegrität, Timing und Temperatur weniger kritisch auf das System auswirken.

Darüber hinaus bemüht man sich heutzutage, die Untersysteme von sicherheitskritischen eingebetteten Systemen zu Sicherheitszwecken voneinander getrennt zu halten. Allerdings steht dieser Ansatz im Widerspruch zu technologischen Entwicklungen, die auf Offenheit, mehr Kommunikation und die Verwendung von Multicore-Architekturen setzen.

Das Ziel des EU-finanzierten Projekts SAFURE war es, „ein cyber-physisches System zu entwickeln, indem eine Methode implementiert wird, die Sicherheit und

Gefahrenabwehr schon durch den Aufbau garantiert“, so Projektkoordinator Klaus-Michael Koch. „Diese Methode wird durch einen Rahmen ermöglicht, der die Systemkapazitäten derart erweitert, dass die ständig bestehenden Auswirkungen von Sicherheitsrisiken auf das Systemverhalten unter Kontrolle gebracht werden können.“ In diesem Sinne nahm sich das Projekt vor, es europäischen Lieferanten von sicherheitskritischen eingebetteten Produkten zu ermöglichen, kosten- und energieeffizientere Lösungen zu entwickeln.

Die Projektpartner verfolgten einen ganzheitlichen Ansatz, um die Sicherheit und Gefahrenabwehr von eingebetteten zuverlässigen Systemen durch das Erkennen und Verhindern potenzieller Angriffe zu garantieren. Dadurch „geben sie Entwicklern und Designern Analysemethoden, Entwicklungswerkzeuge und Umsetzungsmöglichkeiten an die Hand, die ihnen alle helfen sollen, die Themen Sicherheit und Gefahrenabwehr anzugehen“, gibt Koch an. Die Partner schufen ebenfalls die Grundlage für die Entwicklung von SAFURE-konformen eingebetteten Mixed-Criticality-Systemen.

Ein Rahmen zur Erkennung, Verhinderung und zum Schutz gegen Sicherheitsrisiken

„Einer der wichtigsten Schritte in diese Richtung ist, kritische Untersysteme innerhalb ihrer eigenen Sicherheits- und Gefahrenabwehrgrenzen zu halten, ohne dabei die Leistung einzuschränken“, erklärt er. Das Team von SAFURE schuf einen Rahmen, der imstande ist, potenzielle Angriffe auf die Systemintegrität durch Zeit-, Energie-, Temperatur- und Datengefahren zu überwachen. Es erweitert die Systemkapazitäten, um die Systemintegrität zu bewahren. Dies wird erreicht, indem Sicherheitsanforderungen auf eine völlig neuartige Weise nahtlos in Sicherheitssysteme integriert werden. Diese Erweiterungen sind von den Design- und Entwicklungsphasen bis hin zur Anwendungsbereitstellung und der Ausführung auf mehrkernigen Chips und verteilten Hochleistungssystemen anwendbar.

Der Rahmen wird von einer Methode beziehungsweise einer Reihe von Richtlinien unterstützt, die Designern und Entwicklern bei Sicherheitsfragen helfen sollen. Die Teammitglieder erstellten diese Methode, um die gemeinsame Entwicklung von Sicherheit und Gefahrenabwehr in eingebetteten Systemen zu unterstützen. Wirksamkeitsnachweise wurden in drei industriellen Anwendungsfällen in den Bereichen Telekommunikation und Automobiln erreicht. Gleichzeitig legten sie Spezifikationen für die Entwicklung SAFURE-konformer Produkte fest.

Eine Vielzahl von Vorteilen

SAFURE wird europäische Lieferanten von sicherheitskritischen eingebetteten Produkten dabei unterstützen, kosteneffektivere und energieeffizientere Lösungen zu entwickeln. Das System reduziert die Gesamtbetriebskosten durch Senkung der hohen Entwicklungskosten, die mit komplexen Aufgaben wie der Prüfung,

Validierung und (Re-)Zertifizierung einhergehen. Das Projekt verbessert Mixed-Criticality-Systeme und Rekonfigurationsfunktionen (online und offline), wobei stets die Sicherheit bedacht wird. Darüber hinaus erhöht es die Leistung und Ressourcennutzung in komplexen Systemen mit Sicherheits- und Gefahrenabwehrauflagen.

Das Konsortium hat unermüdlich an der Verbesserung der Technologie gearbeitet, um deren tatsächliche Nutzung und Markteinfluss zu erreichen. „Einer der wichtigsten Erfolge von SAFURE ist dessen erheblicher Beitrag zu Standards und die Erweiterung bestehender Standards“, erklärt Koch weiter. „Die Anwendungsfälle in der Automobilbranche sind vielversprechend und sprechen eindeutig tatsächliche Bedürfnisse der Branche an.“ Um diese Ergebnisse zu erzielen, erweiterte das Projekt die Grenzen bestehender Ansätze zur Sicherheit und Gefahrenabwehr in Mixed-Criticality-Systemen.

Schlüsselbegriffe

SAFURE | Sicherheit | Gefahrenabwehr | eingebettete Systeme | Mixed-Criticality-Systeme | sicherheitskritische eingebettete Produkte | Sicherheitsrisiken | cyber-physisches System

Entdecken Sie Artikel in demselben Anwendungsbereich

3D-gedruckte Gebäude könnten schon bald Realität werden

30 März 2020

Neuartige Kryptografie beseitigt drohende Gefahr von Quantencomputern

28 Oktober 2022

Ein Online-Kochspiel im Kampf gegen lebensmittelbedingte Erkrankungen

17 Juni 2022

Grundausbildung im maschinellen Lernen für Feldroboter der nächsten Generation

16 Februar 2024

Projektinformationen

SAFURE

ID Finanzhilfevereinbarung: 644080

Projektwebsite

DOI
10.3030/644080

Projekt abgeschlossen

Finanziert unter
INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Gesamtkosten
€ 5 702 631,25

EU-Beitrag
€ 5 231 375,00

Koordiniert durch

EK-Unterschriftsdatum
8 Dezember 2014

Startdatum
1 Februar 2015

Enddatum
31 Mai 2018

TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH
Austria

Letzte Aktualisierung: 29 Oktober 2018

Permalink: https://cordis.europa.eu/article/id/240564-strategies-methodologies-and-tools-to-make-embedded-systems-safer/de