



Grundlagenseminar: Funktionale Sicherheit und Security in Embedded Systemen mit Prof. Dr. Peter Fromm, Hochschule Darmstadt

Embedded Systeme übernehmen immer mehr komplexe Steuerungs- und Regelungsaufgaben und damit Entscheidungen, die bislang im Verantwortungsbereich des Menschen lagen. Die spannenden Entwicklungen im Rahmen des autonomen Fahrens bilden hier nur eine Spitze zahlreicher Eisberge. Gleichzeitig werden immer mehr Systeme – Schlagwort IoT – als offene Systeme konzeptioniert und unterliegen dadurch der Gefahr von Cyberangriffen. Speziell an der Schnittstelle von funktionaler Sicherheit und Informationssicherheit ergeben sich spannende neue Herausforderungen – wer möchte schon, dass der Hacker bei Tempo 130 auf der Autobahn die Kontrolle über den fahrenden Untersatz übernimmt.

Im Rahmen des eintägigen Grundlagenseminars „Funktionale Sicherheit und Security in Embedded Systemen“ erläutert Prof. Fromm die Grundlagen funktionaler Sicherheit für die Hardware und Softwareentwicklung. Das Seminar richtet sich an Entwickler, Tester, technische Projektleiter und Qualitätssicherer, die sich mit dem Thema Funktionale Sicherheit und Informationssicherheit auseinandersetzen und einen ersten fundierten Einblick erhalten möchten.

Nach einer kurzen Exkursion in die Normenwelt werden anhand eines konkreten Anwendungsfalles Methoden zur systematischen Gefährdungsanalyse erläutert und dann gemeinsam mit den Kursteilnehmern eine beispielhafte Safety Architektur entwickelt. Ein Fokus liegt dabei auf der Vorstellung und Implementierung geeigneter Designmuster für fail-safe als auch fail-operational Systeme. Methoden zur Fehlererkennung und -behandlung sowie Fehler gemeinsamer Ursache werden ebenso beleuchtet wie die Forderung nach und Realisierung von Rückwirkungsfreiheit.

Nachdem eine erste Systemarchitektur entwickelt worden ist, wird der nächste Fokus auf das Thema Hardware gelegt. Ein Schwerpunkt ist hier die Auswahl geeigneter Microcontroller sowie die Erkundung wesentlicher Safety-Hardwarefeatures. Als Beispiel für einen aktuellen Safety-Controller wird der Aurix Multicore Controller der Firma Infineon vorgestellt und mit einem non-safety Controller verglichen.

Sind C/C++ als Programmiersprachen für Safety Systeme geeignet? Eine Frage, die unter Experten mit ähnlicher Leidenschaft diskutiert wird, wie die Frage, ob Windows oder Linux das bessere Betriebssystem ist. De-Facto gibt es trotz aller Schwächen dieser Sprachen keine wirkliche wirtschaftlich sinnvolle Alternative, so dass die Frage eher lautet: Wie kann ich diese Sprachen sicher nutzen? Standards wie MISRA-C/C++ sowie Werkzeuge zur Codegenerierung sowie zur statischen Codeanalyse können wichtige Hilfsmittel sein, wenn sie intelligent eingesetzt werden. Außerdem werden die Features eines Safety OS vorgestellt und die Implementierung einer Safety Architektur gezeigt. Das Thema Testmethoden rundet diesen Block ab.



Da immer mehr embedded Systeme als offene Systeme konzeptioniert werden, erhält das Thema Informationssicherheit einen immer höheren Stellenwert. Zum Abschluss des Seminars werden aktuelle Angriffsszenarien diskutiert und grundlegende Methoden zur Authentifizierung, Verschlüsselung und sicheren Kommunikation diskutiert.

Neben der Vermittlung der Grundlagen werden aktuelle Fragestellungen aufgegriffen, u.a.

- Nutzung von Open Source Software, Linux im Safety Kontext
- Sind Multicore Controller und Hypervisor Architekturen geeignete Lösungen
- Sind einfache bewährte Architekturmuster wie Redundanz bei komplexen Kanälen eine Option
- Wie können Fehler in einem KI-Algorithmus diagnostiziert werden
- Post-Quantum - Wie lange ist ein System secure

Ihr Referent:



Prof. Dr. Peter Fromm hat an der RWTH Aachen Elektrotechnik studiert und dort am Europäischen Zentrum für Mechatronik promoviert. In der Firma Continental, Division Fahrerinformationssysteme war er für den Bereich Software und System Engineering verantwortlich und hat dort erfolgreich systematische Entwicklungsprozesse nach CMMi L3 eingeführt. An der University for Applied Sciences in Darmstadt verantwortet er den Bereich Embedded Systems und ist seit 2017 Mitglied des Steering Board der embedded world Conference.

Er berät und unterstützt Firmen bei der Entwicklung komplexer und sicherer Embedded Architekturen. Gemeinsam mit dem FZI der Universität Karlsruhe und der Firma HighTec werden im Rahmen des ZIM Projektes „Zukunftstechnologie Multicore: Komplexe Applikationen mit Referenzarchitekturen und Werkzeugen sicher entwickeln“ innovative Lösungen für zukünftige Safetyarchitekturen entwickelt.

Termin: 21. September 2022

Ort: Hochschule Landshut

Anmeldung: www.safety-security-forum.de

Kontakt:

Alexandra Feuerstein

Event Manager

WEKA FACHMEDIEN GmbH

Tel.: 089.25556-1372

E-Mail: AFeuerstein@weka-fachmedien.de