3.2.3 Safety and Security in Automation

Modulname: Safety and Security in Automation

Modulübersicht
EDV-Bezeichnung: EITM 130A
Modulverantwortliche(r): Prof. Dr.-Ing. Dirk Feßler
Modulumfang (ECTS): 5 CP Arbeitsaufwand: Präsenzzeit 60 h, Selbststudium 90 h
Einordnung (Semester): 1. oder 2. Semester
Inhaltliche Voraussetzungen: Automatisierungstechnik, Wahrscheinlichkeitstheorie, Digitale Signalverarbeitung
Voraussetzungen nach SPO: keine
Kompetenzen: Nach erfolgreichem Abschluss des Moduls: • sind die Studierenden vertraut mit den Begriffen Sicherheit, Safety sowie Security, können diese unterscheiden und auftretende Fragestellungen den verschiedenen Themengebieten zuordnen • sind den Studierenden die relevanten Vorschriften und europäischen Sicherheits-Richtlinien sowie die heutigen Strategien der Sicherheitstechnik bekannt • kennen die Studierenden die Norm IEC 61508 • haben sich die Studierenden mit den Methoden der Gefahrenanalyse, wie beispielsweise der FEMA oder FTA, auseinandergesetzt • können die Studierenden die Methoden der Risikoanalyse anwenden • sind die Studierenden in der Lage den Sicherheits-Integritätslevel (SIL) nach IEC 61508 zu bestimmen • lernen die Studierenden die verschiedenen Sicherheitssystemarchitekturen bzw. -strukturen und -diversitäten aufgrund eventueller Common Cause Failures (CCF) kennen • können die Studierenden für vorgegebene Anlagenstrukturen die Hardware-Fault-Tolerance (HFT) ermitteln • sind die Studierenden in der Lage, Sicherheitskenngrößen, wie beispielsweise Ausfallrate λ, Safe Failure Fraction (SFF), Diagnostic Coverage (DC), Probability of dangerous Failure on Demand (PFD) sowie Probability of dangerous Failure per Hour (PFH), zu berechnen • kennen die Studierenden die Safety-Requirements-Specification für sichere Software-Entwicklung • sind die Studierenden mit den heutigen Architekturen und verwendeten Kommunikationsprotokollen in der Automatisierungstechnik vertraut • haben sich die Studierenden mit der Problematik Sicherheit von Produktionsanlagen und den aktuell umgesetzten Sicherheitsarchitekturen auseinandergesetzt • sind die Studierenden in der Lage, Schwachstellen in einer Automatisierungsanlage zu bewerten und Maßnahmen für zusätzliche Security zu erarbeiten • lernen die Studierenden verschiedene Verschlüsselungsmethoden kennen und beurteilen • sind die Studierenden mit verschiedenen Netzwerkprotokollen vertraut und können deren Einfluss auf Sicherheit bewerten • haben sich die Studierenden mit verschieden Firewall- und Hardware-Technologien beschäftigt

• kennen die Studierenden unterschiedliche Methoden zur Absicherung der „Security-Qualität“ in der Entwicklung und im Test.
Prüfungsleistungen: Die theoretischen Kenntnisse der Studierenden werden in einer schriftlichen Klausur (Dauer 120 min) oder in einer mündlichen Prüfung (Dauer 20 min) bewertet. Die Prüfungsart wird rechtzeitig zu Semesterbeginn bekannt gegeben.
Verwendbarkeit: *Allgemein:* Ziel des Moduls ist es, das Verständnis für die "Funktionale Sicherheit (FuSi)" zu wecken und Schutz vor Gefährdung durch inkorrekte Funktionen zu erreichen. Die Gefährdungslage in der globalen Datenkommunikation zu vermitteln und Strategien zur Vermeidung von Sicherheitslücken aufzuzeigen. *Zusammenhänge / Abgrenzung zu anderen Modulen:* Die elektrische Sicherheit, die Eigensicherheit (Schutz vor Explosionen) und die Feuer- sowie Strahlensicherheit sind nicht Lehrgegenstand dieses Moduls. Ebenso sind die konkreten Implementierungen und Hardware-Komponenten nicht mit eingeschlossen.

Lehrveranstaltung: Safety in Automation
EDV-Bezeichnung: EITM 131A
Dozent/in: Prof. Dr.-Ing. Dirk Feßler
Umfang (SWS): 2
Turnus: jährlich, Wintersemester
Art und Modus: Vorlesung; Pflichtmodul für die Studienrichtung Automatisierungstechnik, Wahlmodul für die anderen Studienrichtungen des Masterstudiengangs
Lehrsprache: Deutsch
Inhalte: • Begriffsbestimmungen zur Funktionalen Sicherheit (FuSi) • Aufgaben von Berufsgenossenschaften und TÜV • Gesetze, Richtlinien und Normen • neue Normenlandschaft: IEC 61508 • Sicherheits-Lebenszyklus für Hard- und Software • Gefahren- bzw. Risikoanalyse und Risikominderung nach SIL • Sicherheitsbezogene Steuerungen • Strukturen und Hardware Fault Tolerance (HFT) • Fehler-Klassifizierung • Ausfallraten und Quantifizierung • Safe Failure Fraction (SFF) und Diagnostic Coverage (DC) • Probability of dangerous Failure on Demand (PFD) und Probability of dangerous Failure per Hour (PFH)
Empfohlene Literatur: Wratil, P.; Kieviet, M.: *„Sicherheitstechnik für Komponenten und Systeme”*, VDE-Verlag, 2010 Börcsök, J.: *„Funktionale Sicherheit”*, VDE-Verlag, 2015
Anmerkungen: -

Lehrveranstaltung: Security in Automation
EDV-Bezeichnung: EITM 132A
Dozent/in: Dipl.-Ing. Jürgen Bieber
Umfang (SWS): 2
Turnus: jährlich, Wintersemester

Art und Modus: Vorlesung; Pflichtmodul für die Studienrichtung Automatisierungstechnik, Wahlmodul für die anderen Studienrichtungen des Masterstudiengangs
Lehrsprache: Deutsch
Inhalte: • Stand der Normung, Gremien • Netzwerk-Grundlagen in der Automatisierungstechnik • Client/Server-Konzepte • Sicherheitsarchitektur in der Automatisierung • Defense in Depth-Strategie • Physikalische / Organisatorische Security • Netzwerkprotokolle und Firewalls • Sichere Kommunikation über ein unsicheres Netzwerk • Verschlüsselungsmethoden / Cypher Techniken • Qualitäts- und Testkonzepte für Security in der Software-Entwicklung
Empfohlene Literatur: Anderson, Ross J.: *„Security Engineering"*, John Wiley&Sons, 2011 Boudriga, N.; Hamdi, M.: *„Security Engineering Techniques and Solutions for Information Systems"*, Idea Group Reference, 2013
Anmerkungen: -