EITM130A Safety and Security in Automation

Studiengang	Elektro- und Informationstechnik Master
Modulname	EITM130A Safety and Security in Automation
Zugeordnete Lehrveranstaltungen	EITM131A Safety in Automation EITM132A Security in Automation
Studiensemester	1. Semester
Modulverantwortlicher	Prof. Dr. Jürgen Gentner
Dozenten	NN
Sprache	Deutsch
Lehrform, SWS und Gruppengröße	Vorlesungen, jeweils 2 SWS
Modus	Pflichtmodul
Turnus	Wintersemester
Arbeitsaufwand	Präsenzstudium 60 h, Eigenstudium 90 h
Kreditpunkte	5
Empfohlene Vorkenntnisse	Automatisierungstechnik, Digitale Signalverarbeitung
Voraussetzung nach Prüfungsordnung	keine
Lernziele / Kompetenzen	*Allgemein:* Ziel des Moduls ist es, das Verständnis für die "Funktionale Sicherheit" in Anlagen zu wecken und Schutz vor Gefährdung durch inkorrekte Funktionen erreichen sowie die Gefährdungslage in der globalen Datenkommunikation zu vermitteln und Strategien zur Vermeidung von Sicherheitslücken aufzeigen. *Zusammenhänge / Abgrenzung zu anderen Modulen:* Die elektrische Sicherheit, die Eigensicherheit (Schutz vor Explosionen) und die Feuersicherheit sind nicht Gegenstand des Moduls Safety. Ebenso sind die konkreten Implementierungen und Hardware-Komponenten nicht mit eingeschlossen. *Kenntnisse, Fertigkeiten, Kompetenzen:* Nach erfolgreichem Abschluss des Moduls: • kennen die Studierenden die heutigen Strategien der Sicherheitstechnik sowie die europäischen Maschinen- Niederspannungs- EMV- und ATEX-Richtlinien • haben sich die Studierenden auseinandergesetzt mit dem Regelwerk der EN954-1 und dem daraus resultierenden Risikograph • kennen die Studierenden die neue Norm IEC 61508 • können die Studierenden den Sicherheits-Integritätslevel (SIL) nach IEC 61508 bestimmen • sind die Studierenden in der Lage, für vorgegebene Anlagenstrukturen die Hardware-Fault-Tolerance (HFT) zu berechnen • können die Studierenden die analytischen Methoden der Failure Mode and Effect Analysis (FMEA) anwenden, um die Safe-Failure-Fraction (SFF) zu ermitteln und die Zuverlässigkeitsparameter zu berechnen • Kennen die Studierenden die Safety-Requirements-Specification für sichere Software-Entwicklung • kennen die Studierenden die heutigen Architekturen und verwendete Kommunikationsprotokolle in der Automatisierungstechnik • haben sich die Studierenden auseinandergesetzt mit der Problema-

	tik Sicherheit von Produktionsanlagen und den aktuellen umgesetzten Sicherheitsarchitekturen • 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 • lernen die Studierenden die verschiedenen Netzwerkprotokolle kennen und können deren Einfluss auf Sicherheit bewerten • haben sich die Studierenden mit verschieden Firewall- und Hardware-Technologien auseinandergesetzt • kennen die Studierenden verschiedene Methoden zur Absicherung der „Security-Qualität“ in der Entwicklung und im Test
Inhalt	*Vorlesung Safety:* • Begriffsbestimmungen zur Funktionalen Sicherheit • Gesetze und Normen • Sicherheitstechnik mit Relais • Sicherheitsbezogene Steuerungen • Regelwerk nach EN 954-1 • Aufgaben von Berufsgenossenschaften und TÜV • neue Normenlandschaft: IEC 61508 • Risiko und Risikominderung nach SIL • Hardware Fault Tolerance HFT • Fehler-Klassifizierung • Ausfallraten und Quantifizierung • Safe-Failure-Fraction und Diagnostic-Coverage • Sicherheits-Lebenszyklus für Hard- und Software • das Assessment-Prinzip *Vorlesung Security:* • 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 • Stand der Normung, Gremien
Studien- und 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.
Medienformen	• Skriptum, Tafelanschrieb • Folien
Literatur	Wratil, P. Kieviet, M.: *Sicherheitstechnik für Komponenten und Systeme*, VDE-Verlag 2010 Börcsök, J.: *Funktionale Sicherheit*, VDE-Verlag 2011

	Ross J. Anderson: *Security Engineering*, John Wiley&Sons 2011 N. Boudriga, M. Hamdi: *Security Engineering Techniques and Solutions for Information Systems,* Idea Group Reference 2013