

**Fachprüfungsordnung für den Masterstudiengang Functional Safety Engineering des Fachbereiches Elektrotechnik/Informatik der Universität Kassel vom 09. Mai 2018**

**Inhalt**

- § 1 Geltungsbereich
- § 2 Profiltyp, Akademischer Grad
- § 3 Studienbeginn, Regelstudienzeit, Umfang des Studiums
- § 4 Prüfungsausschuss
- § 5 Zulassungsvoraussetzungen
- § 6 Prüfungsleistungen, Modulprüfungen
- § 7 Prüfungsteile des Masterabschlusses
- § 8 Masterabschlussmodul
- § 9 Benotung der Module und Gesamtnote
- § 10 In-Kraft-Treten

**Anlage**

Studien- und Prüfungsplan

## **§ 1 Geltungsbereich**

Die Fachprüfungsordnung für den konsekutiven englischsprachigen Masterstudiengang Functional Safety Engineering des Fachbereichs Elektrotechnik/Informatik ergänzt die Allgemeinen Bestimmungen für Fachprüfungsordnungen mit den Abschlüssen Bachelor und Master (AB Bachelor/Master) an der Universität Kassel in der jeweils geltenden Fassung.

## **§ 2 Profiltyp, Akademischer Grad**

Der Masterstudiengang Functional Safety Engineering ist vom Profiltyp stärker forschungsorientiert. Aufgrund der bestandenen Prüfung wird der akademische Grad „Master of Science“ (M.Sc.) durch den Fachbereich Elektrotechnik/Informatik verliehen.

## **§ 3 Studienbeginn, Regelstudienzeit, Umfang des Studiums**

- (1) Das Masterstudium kann jeweils nur zum Wintersemester aufgenommen werden.
- (2) Die Regelstudienzeit für das Masterstudium beträgt drei Semester einschließlich der Masterarbeit und des Masterkolloquiums.
- (3) Im Masterstudium müssen 90 Credits erlangt werden.

## **§ 4 Prüfungsausschuss**

Die Entscheidungen in Prüfungsangelegenheiten trifft der Prüfungsausschuss für den Masterstudiengang Functional Safety Engineering. Dem Prüfungsausschuss gehören an:

- a) drei Professorinnen oder Professoren aus dem Fachbereich 16,
- b) eine wissenschaftliche Mitarbeiterin/ein wissenschaftlicher Mitarbeiter aus dem Fachbereich 16 sowie
- c) eine Studierende oder ein Studierender des Masterstudiengangs Functional Safety Engineering.

## **§ 5 Zulassungsvoraussetzungen**

- (1) Zum Masterstudium kann nur zugelassen werden, wer
  - a) die Bachelorprüfung oder die Diplom I-Prüfung im Studiengang Elektrotechnik, Informatik, Mathematik oder Mechatronik der Universität Kassel bestanden hat oder
  - b) einen fachlich mindestens gleichwertigen Abschluss einer anderen Hochschule in Deutschland oder einer gleichwertigen Hochschule im Ausland mit einer Regelstudienzeit von mindestens sieben Semestern und 210 Credits erworben hat. Oder
  - c) einen fachlich mindestens gleichwertigen Abschluss einer anderen Hochschule in Deutschland oder einer gleichwertigen Hochschule im Ausland mit einer Regelstudienzeit von mindestens sechs Semestern und 180 Credits erworben hat.
 Es gelten in diesem Fall die Qualifikationsauflagen nach § 5 Absatz 3.

(2) Des Weiteren sind hinreichende englische Sprachkenntnisse auf dem Niveau B 2 des Gemeinsamen Europäischen Referenzrahmens für Sprachen nachzuweisen. Der Nachweis ist nur erforderlich, wenn die Muttersprache der Bewerberin / des Bewerbers nicht Englisch ist oder die Unterrichtssprache des Programms, das zum ersten akademischen Grad führte, nicht Englisch ist.

(3) Fehlen der Bewerberin oder dem Bewerber Voraussetzungen für die Zulassung zum Masterstudium, kann der Prüfungsausschuss die Zulassung unter der Auflage aussprechen, dass bis zur Anmeldung der Masterarbeit die fehlenden Kenntnisse durch erfolgreiches Absolvieren von Modulen im Umfang von maximal 30 Credits aus der folgenden Liste nachgewiesen werden:

Modultitel	Credits
Project at the Department Computer Architecture and System Programming	8
Seminar at the Department Computer Architecture and System Programming	4
Computer Architecture	6
Microprocessor technology and Embedded Systems I	6
System Programming	6

Durch das Absolvieren der zusätzlichen Module kann sich die Studienzzeit um ein Semester verlängern.

### § 6 Prüfungsleistungen, Modulprüfungen

(1) Die studienbegleitenden Modulprüfungen werden im zeitlichen und sachlichen Zusammenhang mit einem Modul angeboten.

(2) Als Prüfungsleistung kommen in Frage:

- Schriftliche Prüfung/Klausur (60-180 Min.),
- mündliche Prüfung (20-40 Min.),
- Hausarbeit (15-20 Seiten),
- Vortrag (30-45 Min.),
- Projektarbeit (30-60 Seiten),
- Praktikumsbericht (ca. 20 Seiten).

Die Art der Prüfungsleistung eines Moduls oder Teilmoduls legt die Dozentin/der Dozent zu Beginn der Lehrveranstaltung, auf die sich die Modulprüfung bezieht, im Rahmen der Vorgaben des Studien- und Prüfungsplanes fest.

(3) Die studienbegleitenden Modulprüfungen können auch aus mehreren Teilprüfungen (Modulteilprüfungsleistungen) bestehen. Die Modulprüfung ist bestanden, wenn alle Modulteilprüfungsleistungen mit mindestens „ausreichend“ (4,0) bewertet wurden.

(4) Nicht bestandene Modulprüfungen können zweimal wiederholt werden. Eine Wiederholung bestandener Modulprüfungen ist nicht zulässig. Besteht eine Modulprüfung aus mehreren Modulteilprüfungsleistungen, so können die mit „nicht ausreichend“ (4,0) bewerteten Modulteilprüfungsleistungen zweimal wiederholt werden. Eine Wiederholung bestandener Modulteilprüfungsleistungen ist nicht zulässig.

(5) Modulprüfungsleistungen können im Einvernehmen mit den Prüfern bzw. den Prüferinnen in englischer oder in einer anderen Sprache erbracht werden.

(6) Gruppenarbeiten von maximal drei Kandidatinnen und/oder Kandidaten können zugelassen werden. Der Anteil des jeweiligen Bearbeiters muss individuell abgrenzbar und einzeln bewertbar sein.

### § 7 Prüfungsteile des Masterabschlusses

(1) Im Rahmen des Masterstudiums erfolgt eine Schwerpunktsetzung in einem der Schwerpunkte

- System and Control
- Mathematical models and Software technology
- Sensor and Communication
- Biomedical Engineering
- Safety structures for Vehicles

(2) Die Masterprüfung besteht aus den Modulprüfungen der Pflichtmodule gemäß Absatz 3, den Modulprüfungen der Schwerpunktmodule gemäß Absatz 4 und dem Masterabschlussmodul gemäß § 8.

(3) Pflichtmodule mit entsprechenden Credits:

Modultitel	Credits
Mathematical Models for Safety Systems	6
Selected topics on Programming languages and techniques according to IEC 61131-3	6
Theory of safety-related computer architectures	6
Introduction to information theory and coding	6
Safety standards and norms of electronic systems	6
Project	8
Seminar	4

(4) Die Schwerpunktmodule mit entsprechenden 18 Credits sind aus einem der gewählten Schwerpunkte zu erbringen:

a) im Schwerpunkt „System and Control“

- Advanced Digital Control (6 Credits)
- Computer based Design of microelectronic circuits (6 Credits)
- Functional Safety in computer architectures (6 Credits)
- Process computing (6 Credits)
- Reconfigurable Structures
- Risk determination of Computer architectures (6 Credits)
- Selected topics on microprocessor techniques (6 Credits)

b) im Schwerpunkt “Mathematical Models and Software technology”

- Functional Safety in computer architectures (6 Credits)
- Methods for Automation for safety related Systems (6 Credits)
- Methods for Software reliability and software quality (6 Credits)
- Pattern Recognition (6 Credits)
- Reliability Models and Software architecture for complex systems (6 Credits)
- Risk determination of Computer architectures (6 Credits)
- Verification of embedded systems (6 Credits)

c) im Schwerpunkt “Sensor and Communication”

- Functional Safety in computer architectures (6 Credits)
- Introduction to Signal Detection and Estimation (6 Credits)
- Semiconductor Lasers (6 Credits)
- Optical Communication Systems (6 Credits)
- RF Sensor Systems (6 Credits)
- Risk determination of Computer architectures (6 Credits)

d) im Schwerpunkt “Biomedical Engineering”

- Functional Safety of Biomedical Systems
- Biomedical engineering
- Biomedical Instrumentation
- Selected Topics of Biomedical Engineering

e) im Schwerpunkt “Safety structures for Vehicles”

- Safety Electronic Systems in Vehicles (6 Credits)
- Mathematical safety analysis of electronic systems in cars (6 Credits)
- Modeling of safety structure according to ISO 2626-2 (6 Credits)
- Modeling of safety architectures in automotive (6 Credits)

(5) Für die Bereiche Pflichtmodule (Abs. 3) und Schwerpunktmodule (Abs. 4) müssen insgesamt 60 Credits erfolgreich belegt werden. Darüber hinaus erbrachte Leistungen aus diesen Bereichen werden bis zu einer Anzahl von maximal 18 Credits dem Bereich Zusatzleistungen zugeordnet. Die Zuordnung der Module zu den Bereichen erfolgt spätestens mit der Anmeldung der Masterarbeit.

(6) Im Rahmen des Masterstudiums sind integrierte Schlüsselkompetenzen im Umfang von mindestens 9 Credits zu erwerben. Dazu zählen die Masterarbeit und das Masterkolloquium (6 Credits), Seminarvorträge bzw. Hausarbeiten (3 Credits).

### **§ 8 Masterabschlussmodul**

(1) Masterarbeit und Masterkolloquium bilden das Masterabschlussmodul. Für das Masterabschlussmodul werden 30 Credits vergeben.

(2) Zur Masterarbeit kann nur zugelassen werden, wer Module im Umfang von 48 Credits erfolgreich absolviert hat.

(3) Die Ausgabe des Themas der Masterarbeit erfolgt durch den Prüfungsausschuss. Mit der Ausgabe des Themas bestellt der Prüfungsausschuss den Erstgutachter oder die Erstgutachterin, der bzw. die die Arbeit betreuen soll, sowie den Zweitgutachter bzw. die Zweitgutachterin. Der Erstgutachter oder die Erstgutachterin muss Mitglied im Fachbereich Elektrotechnik/Informatik sein.

(4) Der Kandidat oder die Kandidatin kann für das Thema der Masterarbeit und für die Gutachter Vorschläge machen.

(5) Die Bearbeitungszeit der Masterarbeit beträgt 22 Wochen und beginnt mit der Bekanntgabe des Themas. Das Thema der Masterarbeit darf nur einmal und nur innerhalb des ersten vier Wochen zurückgegeben werden.

(6) Die Masterarbeit kann im Einvernehmen mit dem Erstgutachter oder der Erstgutachterin auch in einer anderen Sprache als Englisch erbracht werden.

(7) Kann der erste Abgabetermin aus Gründen, die der Kandidat oder die Kandidatin nicht zu vertreten hat, nicht eingehalten werden, so kann die Abgabefrist auf Antrag an den Prüfungsausschuss um die Zeit der Verhinderung, längstens jedoch um 11 Wochen verlängert werden.

(8) Die Masterarbeit ist fristgerecht in zwei gebundenen schriftlichen Exemplaren sowie in elektronischer Form auf Datenträger gespeichert beim Prüfungsausschuss abzugeben.

(9) Die Masterarbeit ist im Rahmen eines Masterkolloquiums vorzustellen. An dem Kolloquium nehmen außer der Kandidatin/dem Kandidaten zumindest die/der erste oder zweite Gutachter/in und ein/e Beisitzer/in teil. Das Masterkolloquium soll spätestens zehn Wochen nach Abgabe der Masterarbeit erfolgen. Die Zulassung zum Masterkolloquium setzt voraus, dass in der Masterarbeit mindestens die Note „ausreichend“ erzielt wurde. Die Dauer beträgt für das gesamte Kolloquium 30 bis maximal 60 Minuten.

(10) Um die Masterprüfung zu bestehen, müssen Masterarbeit und Masterkolloquium jeweils mindestens mit „ausreichend“ bewertet worden sein.

(11) Die Gesamtnote der Masterarbeit ergibt sich aus der Bewertung der schriftlichen Arbeit (Gewichtung: drei Viertel) und aus der Bewertung des Kolloquiums (Gewichtung: ein Viertel). Ein nicht mindestens mit „ausreichend“ bewertetes Kolloquium kann einmal wiederholt werden. Bei der Wiederholung des Kolloquiums müssen die/der erste und zweite Gutachter/in anwesend sein. Wird auch das Wiederholungskolloquium mit „nicht ausreichend“ bewertet, so ist das Mastermodul mit „nicht ausreichend“ zu bewerten und nicht bestanden.

(12) Die Masterarbeit kann im Einvernehmen mit dem ersten Gutachter bzw. der ersten Gutachterin, dem zweiten Gutachter bzw. der zweiten Gutachterin und der oder des Vorsitzenden des Prüfungsausschusses auch außerhalb der Hochschule angefertigt werden. In diesem Fall müssen der erste Gutachter bzw. die erste Gutachterin und der zweite Gutachter bzw. die zweite Gutachterin Mitglied im Fachbereich Elektrotechnik/Informatik sein. Die Regelungen der Absätze 1-11 gelten auch für externe Arbeiten.

### **§ 9 Benotung der Module und Gesamtnote**

(1) Die Gesamtnote eines Moduls ergibt sich aus dem mit den Credits gewichteten arithmetischen Mittel der Noten der ins Modul eingebrachten Lehrveranstaltungen. Jede eingebrachte Prüfungsleistung muss mit mindestens „ausreichend“ bewertet sein.

(2) Die Gesamtnote der Masterprüfung ergibt sich aus dem mit den Credits gewichteten arithmetischen Mittel der Noten der Module gemäß § 7 Abs. 2.

### **§ 10 In-Kraft-Treten**

Diese Prüfungsordnung tritt am Tag nach ihrer Veröffentlichung im Mitteilungsblatt der Universität Kassel in Kraft.

Kassel, den 21. Juni 2018

Der Dekan des Fachbereichs Elektrotechnik/Informatik  
Prof. Prof. Dr. -Ing. Axel Bangert

Beginn Wintersemester																														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	WS	Mathematical Models for Safety Systems					Selected topics on Programming languages and techniques according to IEC 61131-3						Theory of Safety-related computer architectures					Introduction to information theory and coding					Safety standards and norms of electronic systems							
2	SS	Projekt						Seminar				Schwerpunktmodule (18CP) (siehe Modulhandbuch Kapitel 2)																		
3	WS	Masterarbeit (22 Wochen)																												
Hellgraue Anteile zählen zu den integrierten Schlüsselkompetenzen																														

## Anhang. 1 Studien- und Prüfungsplan SPP

## 1. Pflichtmodule

<b>Modulname</b>	<b>Mathematical Models for Safety Systems</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Die/der Lernende kann</p> <ul style="list-style-type: none"> <li>• mathematische Verfahren, Modelle und Methoden für die Anwendung in der funktionalen Sicherheit und Zuverlässigkeit herleiten und anwenden</li> <li>• die Anwendbarkeit von mathematischen Modelle auf unterschiedliche Systemstrukturen der funktionalen Sicherheit erklären und beurteilen</li> <li>• unterschiedliche relevante Sicherheitsparameter für die Anwendung in der funktionalen Sicherheit und Zuverlässigkeitsbeurteilung finden, herleiten, interpretieren und analysieren</li> <li>• unterschiedliche Sicherheitsarchitekturen mathematisch modellieren, analysieren und bewerten</li> <li>• unterschiedliche Methodiken und Konzepte zur mathematischen Herleitung und Bestimmung von Sicherheitsparametern anwenden und interpretieren.</li> </ul> <p>Lernergebnisse in Bezug auf die Studiengangsziele:</p> <ul style="list-style-type: none"> <li>• Erwerben von vertieften Kenntnissen von diskreten und stetigen Verteilungen und deren Anwendung im Bereich der funktionalen Sicherheit und Zuverlässigkeit.</li> <li>• Erwerben von vertieften Kenntnissen von speziellen Verteilungen wie Weibull und deren Anwendung im Bereich der funktionalen Sicherheit und Zuverlässigkeit.</li> <li>• Erwerben von vertieften Kenntnissen von speziellen Schätzverfahren wie Maximum Likelihood Estimation und deren Anwendung im Bereich der funktionalen Sicherheit und Zuverlässigkeit</li> <li>• Erwerben von vertieften Kenntnissen von Markov-Ketten und Makrov-Modellen zur Bestimmung von Parametern (MTTF, etc.) der funktionalen Sicherheit und Zuverlässigkeit.</li> <li>• Erwerben von vertieftem Wissen wahrscheinlichkeitstheoretischer Analysemethoden zur Bestimmung von PFD- und PFH-Werten für Systeme der Funktionalen Sicherheit.</li> <li>• Sicheres Anwenden und Bewerten der oben beschriebenen analytischen Methoden bei der mathematischen Modellierung sicherheitsrelevanter Systeme</li> </ul>
<b>Lehrveranstaltungsarten</b>	4 SWS: 2 SWS Vorlesung 2 SWS Übung
<b>Voraussetzungen für Teilnahme am Modul</b>	Keine
<b>Studentischer Arbeitsaufwand</b>	180 h: 60 h Präsenzzeit 120 h Selbststudium
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	keine
<b>Prüfungsleistung</b>	Schriftliche Prüfung 120-180 Min. oder mündliche Prüfung 20-40 Min. je nach Teilnehmerzahl, wird in der ersten Vorlesung bekannt gegeben
<b>Anzahl Credits für das Modul</b>	6 Credits



<b>Modulname</b>	<b>Selected topics on Programming languages and techniques according to IEC 61131-3</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• Programme, Funktionsblöcke und Funktionen gemäß des internationalen Standards IEC 61131-3 entwickeln und testen,</li> <li>• die Funktionsweise der Sprachelemente erläutern</li> <li>• Programmabläufe mit Hilfe des Standards IEC 61131-3 organisieren, klassifizieren und analysieren,</li> <li>• Sicherheitsstrukturen und Überwachungsfunktionen, entwerfen, analysieren und bewerten</li> <li>• formal Ergebnisse dokumentieren und kritisch bewerten.</li> </ul> <p>Lernergebnisse in Bezug auf die Studiengangsziele:</p> <ul style="list-style-type: none"> <li>• Erwerben von vertieften Kenntnissen von zuverlässigen Programmierstrukturen</li> <li>• Erwerben von vertieften Kenntnissen zur systematischen Entwicklung und Verifizierung von Programmen</li> <li>• Erwerben von vertieften Kenntnissen in der Analyse und Bewertung von Überwachungsstrukturen und Diagnosemaßnahmen</li> </ul>
<b>Lehrveranstaltungsarten</b>	4 SWS: 2 SWS Vorlesung 2 SWS Übung
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h: 60 h Präsenzzeit 120 h Selbststudium
<b>Studienleistungen</b>	2 Dokumentationen/Berichte 6-10 Seiten nach vorgegebenem Format
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	keine
<b>Prüfungsleistung</b>	Elektronische Klausur (inkl. Programmieraufgabe) 120-180 Min.
<b>Anzahl Credits für das Modul</b>	6 Credits

<b>Modulname</b>	<b>Theory of safety related computer architectures</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• normative festgelegte Architekturmodelle unterschiedlichen Sicherheitsnormen (IEC61508, IEC62016, ISO26262, ISO13839) bewerten und beurteilen.</li> <li>• Modelleigenschaften von sicherheitsgerichteten Rechnerarchitekturen analysieren und bewerten.</li> <li>• Zuverlässigkeits- und Sicherheitsparameter für unterschiedliche Architekturmodelle ableiten und analysieren.</li> <li>• Diagnose- Prüf und Testverfahren für sicherheitsgerichteten Architekturen bewerten und beurteilen.</li> </ul> <p>Lernergebnisse in Bezug auf die Studiengangsziele:</p> <ul style="list-style-type: none"> <li>• Erwerben von vertieften Kenntnissen von sicherheitsgerichteten Architekturmodellen und Strukturen.</li> <li>• Erwerben von vertieften Kenntnissen zur Analyse von sicherheitsgerichteten Architekturmodellen zur Bestimmung von Ausfallwahrscheinlichkeiten.</li> <li>• Erwerben von vertieften Kenntnissen zur Bestimmung von Zuverlässigkeitsparametern unterschiedlicher sicherheitsgerichteter Architekturen.</li> <li>• Erwerben von vertieften Kenntnissen von speziellen M-von-N-Strukturen der Sicherheitstechnik.</li> <li>• Erwerben von vertieften Kenntnissen von Diagnose-, Prüf- und Teststrukturen für Architekturmodelle in sicherheitstechnischen Systemen.</li> </ul>
<b>Lehrveranstaltungsarten</b>	4 SWS: 2 SWS Vorlesung 2 SWS Übung
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h: 60 h Präsenzzeit 120 h Selbststudium
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	keine
<b>Prüfungsleistung</b>	Klausur (120 Min.) oder mündliche Prüfung (40 Min) oder Hausarbeit (15-20 Seiten), wird in der ersten Vorlesung bekannt gegeben.
<b>Anzahl Credits für das Modul</b>	6 Credits

<b>Modulname</b>	<b>Introduction to information theory and coding</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• grundlegende Zusammenhänge der Informationstheorie anwenden</li> <li>• optimale und suboptimale Verfahren zur Block- und Faltungscodierung und -decodierung entwickeln und anwenden</li> <li>• optimale und suboptimale Verfahren zur Quellencodierung und -decodierung entwickeln und anwenden</li> </ul> <p>Lernergebnisse in Bezug auf die Studiengangsziele:</p> <ul style="list-style-type: none"> <li>• Erwerben von vertieften Kenntnissen in den elektro-technischen Grundlagen</li> <li>• Erwerben von erweiterten und angewandten fachspezifischen Grundlagen</li> <li>• Erkennen und Einordnen von komplexen elektrotechnischen und interdisziplinären Aufgabenstellungen</li> <li>• Sicheres Anwenden und Bewerten analytischer Methoden</li> <li>• Selbständiges Entwickeln und Beurteilen von Lösungsmethoden</li> <li>• Tiefgehende und wichtige Erfahrungen in praktischen technischen und ingenieurwissenschaftlichen Tätigkeiten</li> <li>• Arbeiten und Forschen in nationalen und internationalen Kontexten</li> </ul>
<b>Lehrveranstaltungsarten</b>	4 SWS: 3 SWS Vorlesung und Übung 1 SWS Praktikum
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h: 70 h Präsenzzeit 110 h Selbststudium
<b>Studienleistungen</b>	Praktikum
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	Praktikum
<b>Prüfungsleistung</b>	mündliche Prüfung 30 Min.
<b>Anzahl Credits für das Modul</b>	6 Credits: Vorlesung/Übung: 5 Praktikum: 1

<b>Modulname</b>	<b>Safety standards and norms of electronic systems</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Die/der Lernende kann:</p> <ul style="list-style-type: none"> <li>• die Entstehung und den strukturellen Aufbau von Normen (Typ A, B, C) und Direktiven (Seveso) verstehen.</li> <li>• Basisnormen (IEC 61508) und sektorspezifische Normen der Funktionalen Sicherheit (z.B. IEC 615013) unterscheiden, zuordnen und anwenden.</li> <li>• internationale Normen in verschiedenen Industriebereichen (z.B. IEC61511 für Prozesstechnik, IOS 13849 für Maschinenbau) verstehen und anwenden.</li> <li>• den gesamten Sicherheitslebenszyklus für die Entwicklung von Sicherheitsrelevanter Systeme nach IEC 61508 und den gesamten Entwicklungszyklus in einzelne Phasen unterteilen und die notwendigen Entwicklungstätigkeiten definieren.</li> <li>• Verfahren und Methoden zur Zertifizierung von Sicherheitssystemen nach internationalen Normen (IEC61508) verstehen und anwenden.</li> <li>• Anforderungen und Spezifikationen von Sicherheitssystemen gemäß unterschiedlichen internationalen Normen herleiten und entwickeln.</li> </ul> <p>Lernergebnisse in Bezug auf die Studiengangsziele:</p> <ul style="list-style-type: none"> <li>• Verstehen von Normung, Organisationen, Normungsverfahren, Aufbau und Organisation von unterschiedlichen internationalen Standardisierungskomitees.</li> <li>• Erwerben von vertieftem Wissen der Grundlagen der Sicherheitstechnik (VDI 40022, IEC61508), und des strategischen Managements der Sicherheitstechnik.</li> <li>• Erwerben von vertieftem Wissen „Functional Safety Managements“.</li> <li>• Erwerben von vertieftem Wissen des Lebenszyklusmodpdlle IEC61508 und die SIL-Ebenen Einteilung.</li> <li>• Erwerben du Anwendung von vertieftem Wissen über die Planung der Erforderlichen Verifikations- und Validationstätigkeiten nach IEC 61508.</li> </ul>
<b>Lehrveranstaltungsarten</b>	4 SWS: 2 SWS Vorlesung 2 SWS Übung
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h: 60 h Präsenzzeit 120 h Selbststudium
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	keine
<b>Prüfungsleistung</b>	Schriftliche Prüfung 120-180 Min. oder mündliche Prüfung 20-40 Min. je nach Teilnehmerzahl, wird in der ersten Vorlesung bekannt gegeben
<b>Anzahl Credits für das Modul</b>	6 Credits

<b>Modulname</b>	<b>Seminar</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• sich ein Thema selbständig aus der Literatur, inklusive englischsprachiger Originalarbeiten erschließen</li> <li>• im Umgang mit Fachtexten wissenschaftliche Arbeitsmethoden anwenden, z.B. das Hinterfragen von Aussagen, das Bilden eigener Urteile, das Überprüfen von Aussagen, das Hinzuziehen von Sekundärliteratur und das Zusammenfügen von Informationen aus unterschiedlichen Quellen</li> <li>• wissenschaftliche Inhalte für Präsentationen verständlich und strukturiert aufbereiten</li> <li>• in wissenschaftlichen Präsentationen geeignete mündliche und schriftliche Ausdrucksformen einsetzen.</li> </ul>
<b>Lehrveranstaltungsarten</b>	4 SWS: Seminar
<b>Voraussetzungen für die Teilnahme am Modul</b>	Keine
<b>Studentischer Arbeitsaufwand</b>	180 h: 60 h Präsenzzeit 120 h Selbststudium
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	keine
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung (30-60 Seiten) und Vortrag (30–45 Minuten)
<b>Anzahl Credits für das Modul</b>	4 Credits

<b>Modulname</b>	<b>Projekt</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• neue Anwendungen konzipieren und realisieren</li> <li>• anspruchsvolle Probleme analysieren und selbständig sowie in Zusammenarbeit mit anderen Studierenden lösen</li> <li>• im Team Fragen der Arbeitsorganisation, aufgetretene Konflikte oder die Einordnung der eigenen Arbeit in wirtschaftliche und gesellschaftliche Zusammenhänge reflektieren und konstruktiv bearbeiten</li> <li>• sich bei Bedarf Informatik- bzw. Anwendungskennntnisse aus der Literatur oder durch Experimente erschließen</li> <li>• andere Studierende anleiten</li> </ul>
<b>Lehrveranstaltungsarten</b>	4 SWS: Projekt
<b>Voraussetzungen für die Teilnahme am Modul</b>	Keine
<b>Studentischer Arbeitsaufwand</b>	180 h: 60 h Präsenzzeit 120 h Selbststudium
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	keine
<b>Prüfungsleistung</b>	Schriftliche Ausarbeitung (30-60 Seiten) und Vortrag (30-45 Minuten)
<b>Anzahl Credits für das Modul</b>	8 Credits

<b>Modulname</b>	<b>Masterabschlussmodul</b>
<b>Art des Moduls</b>	Pflicht
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Die Abschlussarbeit soll zeigen, dass die Kandidatin oder der Kandidat in der Lage ist, in einem vorgegebenen Zeitraum eine wissenschaftliche und/oder praxisorientierte Problemstellung des Fachs mit wissenschaftlichen Methoden und Erkenntnissen des Fachs zu lösen.</p> <p>Lernergebnisse in Bezug auf die Studiengangsziele:</p> <ul style="list-style-type: none"> <li>• Erwerben von vertieftem Wissen in mathematisch-naturwissenschaftlichen Bereichen</li> <li>• Erwerben von vertieften Kenntnissen in den elektrotechnikspezifischen Grundlagen</li> <li>• Erwerben von erweiterten und angewandten fachspezifischen Grundlagen</li> <li>• Erkennen und Einordnen von komplexen elektrotechnischen und interdisziplinären Aufgabenstellungen</li> <li>• Sicheres Anwenden und Bewerten analytischer Methoden</li> <li>• Selbständiges Entwickeln und Beurteilen von Lösungsmethoden</li> <li>• Einarbeiten in neue Wissensgebiete, Durchführen von Recherchen und Beurteilen der Ergebnisse</li> <li>• Tiefgehende und wichtige Erfahrungen in praktischen technischen und ingenieurwissenschaftlichen Tätigkeiten</li> <li>• Bildung einer stabilen Persönlichkeit</li> <li>• Erwerben der Fähigkeit zur effektiven Führung interdisziplinärer Teams</li> <li>• Erwerben der Fähigkeit zu allein verantwortlicher Leitung und Führung</li> <li>• Arbeiten und Forschen in nationalen und internationalen Kontexten</li> </ul>
<b>Lehrveranstaltungsarten</b>	MA_A
<b>Voraussetzungen für Teilnahme am Modul</b>	siehe Prüfungsordnung § 8 Absatz 1
<b>Studentischer Arbeitsaufwand</b>	880 h
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	siehe Prüfungsordnung § 8 Absatz 1
<b>Prüfungsleistung</b>	Benotete Abschlussarbeit, Gewichtung drei Viertel und Präsentation der Forschungsarbeit in einem Kolloquium, Gewichtung ein Viertel
<b>Anzahl Credits für das Modul</b>	30 Credits, davon zählen 6 Cr zu den integrierten Schlüsselkompetenzen

## Schwerpunkt "System and Control"

<b>Modulname</b>	<b>System and Control</b>
<b>Art des Moduls</b>	<b>Schwerpunktmodule</b>
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• Systemstrukturen und Systemarchitekturen der funktionalen Sicherheit in verschiedenen Anwendungsbereichen anwenden und verstehen,</li> <li>• Verfahren und Methoden zur Modellierung und der funktionalen Sicherheit für Systemstrukturen herleiten und analysieren</li> <li>• Anforderungen und Spezifikationen für sicherheitsgerichtete Systemarchitekturen gemäß unterschiedlichen internationalen Standards herleiten und entwickeln</li> <li>• Unterschiedliche allgemeine und sektorspezifische Normen der funktionalen Sicherheit unterscheiden und gezielt anwenden</li> <li>• Kennt die unterschiedlichen Methoden, Modelle und Vorgehensweisen bei Analyse, Modellierung und Bewertung von Sicherheitsarchitekturen und Systemstrukturen und kann diese Verfahren anwenden</li> </ul>
<b>Lehrveranstaltungsarten</b>	VL+Ü, VL+P, P, S 4 SWS
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	Bearbeitung einer regelungs-theoretischen Aufgabe inklusive Implementierung, Halten eines Seminarvortrags; Verfassen einer Seminararbeit; Teilnahme an den Vorträgen aller Teilnehmer, Referat, Präsentation, Bericht, Übungsaufgaben, Testes, Ergebnisbericht, Testat, Abschlussgespräch, Laboraufgaben, Vorträge, Prüfungsgespräch, Hausarbeit
<b>Prüfungsleistung</b>	90 Minuten für Vortrag mit Diskussion, Mündliche Prüfung 20-40 Min., Schriftliche Prüfung 60-180 Min., Hausarbeit mit Präsentation, Benotete Hausarbeit
<b>Anzahl Credits für das Modul</b>	6 CP

## Schwerpunkt "Mathematical models and Software technology"

<b>Modulname</b>	<b>Mathematical models and Software technology</b>
<b>Art des Moduls</b>	Schwerpunktmodule
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• Mathematische Modellierungen und Softwarestrategien für sicherheitsgerichtete Systeme in verschiedenen sicherheitsrelevanten Applikationsbereichen anwenden und verstehen,</li> <li>• Mathematische Verfahren und Methoden für komplexe Sicherheitsstrukturen herleiten und analysieren</li> <li>• Anforderungen und Spezifikationen für mathematische Modelle und Softwarestrukturen in Sicherheitsrelevanten Systemstrukturen herleiten und entwickeln</li> <li>• Unterschiedliche allgemeine und sektorspezifische Berechnungsmodelle und Berechnungsmethoden sowie Softwaretechnologieansätze und Softwaremodelle unterscheiden und anwenden</li> <li>• Kennt die unterschiedlichen Methoden der mathematische Modellierung und Softwaretechnologie in der funktionalen Sicherheit und kann diese Verfahren anwenden</li> </ul>
<b>Lehrveranstaltungsarten</b>	VL+Ü, VL+P, P, S 4 SWS
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	Bearbeitung einer regelungs-theoretischen Aufgabe inklusive Implementierung, Halten eines Seminarvortrags; Verfassen einer Seminararbeit; Teilnahme an den Vorträgen aller Teilnehmer, Referat, Präsentation, Bericht, Übungsaufgaben, Testes, Ergebnisbericht, Testat, Abschlussgespräch, Laboraufgaben, Vorträge, Prüfungsgespräch, Hausarbeit
<b>Prüfungsleistung</b>	90 Minuten für Vortrag mit Diskussion, Mündliche Prüfung 20-40 Min., Schriftliche Prüfung 60-180 Min., Hausarbeit mit Präsentation, Benotete Hausarbeit
<b>Anzahl Credits für das Modul</b>	6 CP



## Schwerpunkt "Sensor and Communication"

<b>Modulname</b>	<b>Sensor and Communication</b>
<b>Art des Moduls</b>	Schwerpunktmodule
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• Sensorstrukturen und Aufbau in Verbindung mit unterschiedlichen Filter-Verfahren und Kommunikationsstrukturen im Zusammenhang der funktionalen Sicherheit und Zuverlässigkeit verstehen und anwenden</li> <li>• Unterschiedliche Strukturen, Modelle und Verfahren der Sensorik, Datenerfassung, Filterung und Kommunikation herleiten und analysieren.</li> <li>• Unterschiedliche Entwürfe, Verfahren und Techniken der Sensorik, Datenerfassung, Filterung und Datenübertragung unter dem Gesichtspunkt der funktionalen Sicherheit und Anforderungen von internationalen Normen herleiten, bewerten und analysieren.</li> <li>• unterschiedliche allgemeine und sektorspezifische Normen der funktionalen Sicherheit unterscheiden und gezielt anwenden.</li> <li>• unterschiedliche Methoden, Analysen, Modelle und Verfahren der Datenerfassung, Sensorik, Filterung und Datenübertragung (Kommunikation) analysieren und anwenden.</li> </ul>
<b>Lehrveranstaltungsarten</b>	VL+Ü, VL+P, P, S 4 SWS
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	Bearbeitung einer regelungs-theoretischen Aufgabe inklusive Implementierung, Halten eines Seminarvortrags; Verfassen einer Seminararbeit; Teilnahme an den Vorträgen aller Teilnehmer, Referat, Präsentation, Bericht, Übungsaufgaben, Testes, Ergebnisbericht, Testat, Abschlussgespräch, Laboraufgaben, Vorträge, Prüfungsgespräch, Hausarbeit
<b>Prüfungsleistung</b>	90 Minuten für Vortrag mit Diskussion, Mündliche Prüfung 20-40 Min., Schriftliche Prüfung 60-180 Min., Hausarbeit mit Präsentation, Benotete Hausarbeit
<b>Anzahl Credits für das Modul</b>	6 CP

## Schwerpunkt "Biomedical Engineering"

<b>Modulname</b>	<b>Biomedical Engineering</b>
<b>Art des Moduls</b>	Schwerpunktmodule
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/Die Lernende kann:</p> <ul style="list-style-type: none"> <li>• Vertiefte Kenntnisse der Biomedizintechnik erlernen</li> <li>• Unterschiedliche Mikrosysteme und Sensoren für den Einsatz in der Biomedizintechnik verstehen und anwenden</li> <li>• Unterschiedliche Normen und Standards für die Entwicklung biomedizinische Geräte verstehen und kann diese verwenden</li> <li>• Anforderungen und Spezifikationen für Modelle und Strukturen in der Biomedizintechnik erlernen und anwenden</li> </ul> <p>Lernergebnisse in Bezug auf die Studiengangsziele:</p> <ul style="list-style-type: none"> <li>• Erwerben von vertieften Kenntnissen in den biomedizinischen Grundlagen</li> <li>• Erwerben von erweiterten und angewandten Grundlagen zu Standards und Normen in der biomedizinischen Technik</li> <li>• Erwerben von vertieften Kenntnissen in biomedizinischen Geräten</li> <li>• Erkennen und Einordnen von komplexen biomedizinischen und interdisziplinären Aufgabenstellungen</li> <li>• Tiefgehende und wichtige Erfahrungen in praktischen biomedizinischen Tätigkeiten</li> <li>• Arbeiten und Forschen in nationalen und internationalen Kontexten</li> </ul>
<b>Lehrveranstaltungsarten</b>	VL+Ü, VL+P, P, S 4 SWS
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	Halten eines Seminarvortrags; Verfassen einer Seminararbeit; Teilnahme an den Vorträgen aller Teilnehmer, Referat, Präsentation, Bericht, Übungsaufgaben, Testes, Ergebnisbericht, Testat, Abschlussgespräch, Vorträge, Prüfungsgespräch, Hausarbeit
<b>Prüfungsleistung</b>	Je nach gewähltem Modul 90 Minuten für Vortrag mit Diskussion, Mündliche Prüfung 20-40 Min., Schriftliche Prüfung 60-180 Min., Hausarbeit mit Präsentation, Benotete Hausarbeit
<b>Anzahl Credits für das Modul</b>	6 CP

## Schwerpunkt "Safety structures for Vehicles"

<b>Modulname</b>	<b>Safety structures for Vehicles</b>
<b>Art des Moduls</b>	Schwerpunktmodule
<b>Lernergebnisse, Kompetenzen, Qualifikationsziele</b>	<p>Der/die Lernende kann:</p> <ul style="list-style-type: none"> <li>• Erwerben von vertieften Kenntnissen in verschiedenen elektrotechnikspezifischen Anwendungsbereichen anwenden und verstehen,</li> <li>• Erwerben von unterschiedliche, allgemeine und sektorspezifische Normen der funktionalen Sicherheit und gezielt in Praxisorientierte Problemstellungen anwenden.</li> <li>• Verfahren und Methoden von komplexen elektrotechnischen und interdisziplinären Aufgabenstellungen herleiten und analysieren.</li> <li>• Anforderungen und Spezifikationen für sicheres Anwenden und Bewerten analytischer Methoden gemäß unterschiedlichen internationalen Standards herleiten und entwickeln</li> <li>• kennt die unterschiedlichen Methoden zur Entwicklung von Lösungsmethoden für komplexe sicherheitsgerichtete Architekturen und kann diese Verfahren anwenden</li> <li>• Tiefgehende und wichtige Erfahrungen in praktischen, technischen und ingenieurwissenschaftlichen Vorgehensweisen und Methoden.</li> </ul>
<b>Lehrveranstaltungsarten</b>	VL+Ü, VL+P, P, S 4 SWS
<b>Voraussetzungen für Teilnahme am Modul</b>	keine
<b>Studentischer Arbeitsaufwand</b>	180 h
<b>Studienleistungen</b>	keine
<b>Voraussetzung für Zulassung zur Prüfungsleistung</b>	Bearbeitung einer regelungs-theoretischen Aufgabe inklusive Implementierung, Halten eines Seminarvortrags; Verfassen einer Seminararbeit; Teilnahme an den Vorträgen aller Teilnehmer, Referat, Präsentation, Bericht, Übungsaufgaben, Testes, Ergebnisbericht, Testat, Abschlussgespräch, Laboraufgaben, Vorträge, Prüfungsgespräch, Hausarbeit
<b>Prüfungsleistung</b>	90 Minuten für Vortrag mit Diskussion, Mündliche Prüfung 20-40 Min., Schriftliche Prüfung 60-180 Min., Hausarbeit mit Präsentation, Benotete Hausarbeit
<b>Anzahl Credits für das Modul</b>	6 CP