Modulbezeichnung	**Grundlagen der Sicherheitsanalyse und des Designs**
Modulverantwortliche(r)	Prof. Dr. D. Hutter
Modulart	Pflicht/Wahl ☐ Wahlpflicht ☒
Spezialisierungsbereich	Automatisierung und Robotik, Mechatronik, Systemsoftware / Eingebettete Systeme, Produktionstechnik, Raumfahrt-Systemtechnik
Dauer des Moduls	1 Semester
Kreditpunkte	6 CP
Arbeitsaufwand	Berechnung des Workloads Präsenz 56 h Übungsbetrieb/Prüfungsvorbereitung 124 h Summe 180 h
Turnus des Moduls	i. d. R. jedes Jahr
Voraussetzung für die Teilnahme	Keine ☐ Folgende: Inhaltliche Voraussetzungen: Kenntnisse in formalen Methoden bzw. Informationssicherheit sind nützlich aber nicht zwingend erforderlich
Lehr- und Lernformen	Seminar ☐ Vorlesung ☒ Tutorium ☒ Praktikum ☐ Projekt ☐
Lernziele	• Verfahren der (formalen) Modellierung von (Informations)Sicherheitsanforderungen und Sicherheitsmechanismen kennen • Verschiedene Sicherheitsanalysetechniken einschätzen und bewerten können • Die Modellierungstiefe und deren Auswirkungen auf die Analyse einschätzen und bewerten können • Das Zusammenspiel von verschiedenen Sicherheitsanforderungen und -garantien verstehen
Lerninhalte	Grundlagen der Modellierung im Bereich der Informationssicherheit Design und Analyse von Sicherheitsprotokollen • Modellierung eines Angreifers • Prinzipien des Designs von Sicherheitsprotokollen • Analyse und Verifikation von Sicherheitsprotokollen Design und Analyse von Sicherheitspolitiken • Modellierung (formaler) Sicherheitspolitiken • Grundlagen der Informationsflusskontrolle, Vertraulichkeit und Integrität als Informationsflusseigenschaften • Zustandsbasierte Informationsflusskontrolle • sprachbasierte Informationsflusskontrolle und Programmanalyse • Realisierung von Informationsflusskontrolle durch Zugriffskontrolle Komposition verschiedener Sicherheitsmechanismen am Beispiel des Semantic Web
Prüfungsformen	Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung

Literatur	Skript bzw. Folien Dieter Gollmann: Computer Security, Wiley&Sons, 2006 Matt Bishop: Computer Security, Art und Science, Addison Wesley, 2003 Diverse Fachartikel