



ASIIN-Akkreditierungsbericht

Bachelorstudiengänge

IT-Sicherheit

Robotik und Autonome Systeme

Masterstudiengänge

IT-Sicherheit

Robotics and Autonomous Systems

an der

Universität zu Lübeck

Inhaltsverzeichnis

A Zum Akkreditierungsverfahren	3
B Steckbrief der Studiengänge	5
C Bericht der Gutachter	9
D Nachlieferungen	45
E Nachtrag/Stellungnahme der Hochschule (17.05.2016)	46
F Zusammenfassung: Empfehlung der Gutachter (23.05.2016)	47
G Stellungnahme der Fachausschüsse	48
Fachausschuss 04 – Informatik (09.06.2016).....	48
Fachausschuss 02 – Elektro-/Informationstechnik (17.06.2016)	50
H Beschluss der Akkreditierungskommission (01.07.2016).....	51
I Erfüllung der Auflagen (30.06.2017).....	53
Anhang: Lernziele und Curricula	56

A Zum Akkreditierungsverfahren

Studiengang	Beantragte Qualitätssiegel	Vorhergehende Akkreditierung	Beteiligte FA ¹
Ba IT-Sicherheit	AR ²	-	FA 04
Ba Robotik und Autonome Systeme	AR	-	FA 04, FA 02
Ma IT-Sicherheit	AR	-	FA 04
Ma Robotics and Autonomous Systems	AR	-	FA 04, FA 02
<p>Vertragsschluss: 17.12.2015</p> <p>Antragsunterlagen wurden eingereicht am: 22.02.2016</p> <p>Auditdatum: 15.04.2016</p> <p>am Standort: Universität zu Lübeck, Marie-Curie-Straße, Gebäude 64, Raum Dijkstra (Raum 57/58)</p>			
<p>Gutachtergruppe:</p> <p>Prof. Dr. Dieter Gollmann, Technische Universität Hamburg-Harburg; Prof. Dr. Reinhard Möller, Universität Wuppertal; Prof. Dr. Ulrich Bühler, Hochschule Fulda; Detlef Wiese, Freiberuflicher IT-Berater; Jörn Tillmanns, Studentischer Gutachter Technische Universität Darmstadt</p>			
<p>Vertreterin der Geschäftsstelle: M.A. Madlen Schweiger</p>			
<p>Entscheidungsgremium: Akkreditierungskommission für Studiengänge</p>			
<p>Angewendete Kriterien:</p> <p>European Standards and Guidelines i.d.F. vom Mai 2015</p> <p>Kriterien für die Akkreditierung von Studiengängen des Akkreditierungsrates i.d.F. vom 20.02.2013</p>			

¹ FA 02 = Elektro-/Informationstechnik; FA 04 = Informatik

² AR: Siegel der Stiftung zur Akkreditierung von Studiengängen in Deutschland

A Zum Akkreditierungsverfahren

Zur besseren Lesbarkeit wird darauf verzichtet, weibliche und männliche Personenbezeichnungen im vorliegenden Bericht aufzuführen. In allen Fällen geschlechterspezifischer Bezeichnungen sind sowohl Frauen als auch Männer gemeint.

B Steckbrief der Studiengänge

a) Bezeichnung	Abschlussgrad (Originalsprache / englische Übersetzung)	b) Vertiefungsrichtungen	c) Angestrebtes Niveau nach EQF ³	d) Studiengangsform	e) Double/Joint Degree	f) Dauer	g) Gesamtkreditpunkte/Einheit	h) Aufnahme-rhythmus/erstmalige Einschreibung	i) konsekutive und weiterbildende Master	j) Studiengangsprofil nur bei Master, wenn von HS beantragt
B.Sc. IT-Sicherheit	Bachelor of Science (B.Sc.) IT-Security	-	EQF 6	Vollzeit	-	6 Semester	180 ECTS	WS/erstmalig WS 2016/2017	n.a.	n.a.
B.Sc. Robotik und Autonome Systeme	Bachelor of Science (B.Sc.) Robotics and Autonomous Systems	-	EQF 6	Vollzeit	-	6 Semester	180 ECTS	WS/erstmalig WS 2016/2017	n.a.	
M.Sc. IT-Sicherheit	Master of Science (M.Sc.) IT-Security	-	EQF 7	Vollzeit	-	4 Semester	120 ECTS	WS/SoSe/erstmalig WS 2019/2020	konsekutiv	forschungsorientiert
M.Sc. Robotics and Autonomous Systems	Master of Science (M.Sc.)	-	EQF 7	Vollzeit	-	4 Semester	120 ECTS	WS/SoSe/erstmalig WS 2019/2020	konsekutiv	forschungsorientiert

³ EQF = European Qualifications Framework

Für den **Bachelorstudiengang IT-Sicherheit** hat die Hochschule in der Studiengangsordnung folgendes Profil beschrieben:

„Die Ausbildung verfolgt das Ziel, die Studierenden durch Vermittlung von Kenntnissen und Einübung von Fertigkeiten in den Stand zu setzen, vielfältige Probleme der Sicherheit und Zuverlässigkeit informationstechnischer Systeme aufzugreifen und zu lösen. Die Fähigkeit, sich auf wechselnde Aufgabengebiete und Anwendungsgebiete einstellen zu können, ist dabei unerlässlich. Das Studium umfasst dazu eine breite, grundlagenorientierte Ausbildung in Informatik sowie eine fachbezogene Ausbildung in IT-Sicherheit und Zuverlässigkeit. Das zentrale Thema des Bachelorstudiengangs IT-Sicherheit ist die Konstruktion sicherer und zuverlässiger informationsverarbeitender Systeme für allgemeine und spezielle Anwendungen. Dies umfasst die Modellierung der Anwendungsanforderungen, den Entwurf und die Analyse von Verfahren zur Lösung der gestellten Aufgabe, die Entwicklung von Datenstrukturen und Algorithmen, deren Implementierung in Software und Hardware, sowie den Nachweis dafür, dass so konstruierte Systeme die gestellten Anforderungen erfüllen. Ebenfalls im Kern des Studiums steht der Erwerb von Fähigkeiten zur Analyse von Sicherheitsschwachstellen existierender informationstechnischer Systeme und zur Behebung dieser Schwachstellen. Für das Gespräch mit Anwenderinnen und Anwendern als deren Partnerin oder Partner bei der Lösung von sicherheitsrelevanten Fragestellungen bzw. grundsätzlich beim Entwurf und der Realisierung sicherer und zuverlässiger IT-Systeme müssen die Absolventinnen und Absolventen vor allem in der Lage sein, in der Fachsprache eines Anwendungsgebiets abgefasste Aufgabenstellungen sachgemäß so zu formulieren, dass diese mit Hilfe von IT-Systemen behandelt werden können.“

Für den **Masterstudiengang IT-Sicherheit** hat die Hochschule in der Studiengangsordnung folgendes Profil beschrieben:

„Das Ziel der Ausbildung im Masterstudiengang IT-Sicherheit besteht darin, die Studierenden durch Vermittlung von wissenschaftlichen Methoden und Modellen sowie Einübung von Fertigkeiten der IT-Sicherheit und Zuverlässigkeit in die Lage zu versetzen, vielfältige Probleme der sicheren und zuverlässigen Informationsverarbeitung zu verstehen und zu bearbeiten. Gegenstand des Studiengangs ist die Analyse, Beschreibung, Konstruktion und Validierung von informationsverarbeitenden Systemen, insbesondere unter dem Aspekt der Sicherheit und Zuverlässigkeit. Dabei liegt im Gegensatz zum Bachelorstudiengang die Betonung auf dem Erwerb von Fähigkeiten für wissenschaftliches Arbeiten. Die Ausbildung trägt dem durch ein grundlagenorientiertes, sowohl breites als auch vertiefendes Studium Rechnung und soll die Voraussetzung für ein lebenslanges Lernen im Bereich der Informatik und spezieller der sicheren und zuverlässigen IT-Systeme sowie für eine weitergehende akademische Qualifikation wie z.B. die Promotion schaffen. Weiter-

hin sollen die Studierenden aufgrund der von ihnen erworbenen Kompetenzen in der Lage sein, Leitungsfunktionen in der Wirtschaft zu übernehmen.“

Für den **Bachelorstudiengang Robotik und Autonome Systeme** hat die Hochschule in der Studiengangsordnung folgendes Profil beschrieben:

„Die Ausbildung verfolgt das Ziel, die Studierenden durch Vermittlung von fundierten und anwendungsorientierten Kenntnissen in den verschiedenen Teilgebieten der Robotik und autonomen Systeme in den Stand zu setzen, selbstständige Analyse-, Konzeptionierungs- und Entwicklungsfähigkeiten in den verschiedenen Bereichen der (teil-)autonomen Systeme und der Robotik zu erwerben. Die Fähigkeit, sich mit Hilfe eines hinreichend breiten mathematisch, technischen Grundlagenwissens auf wechselnde Aufgabengebiete einstellen zu können, ist dabei unerlässlich. Das Studium umfasst daher eine grundlagenorientierte Ausbildung in den Bereichen Technik, Informatik und Mathematik ergänzt durch praktische Umsetzungen sowie eine fachbezogene Ausbildung. Die zentralen Themen des Bachelorstudiums Robotik und Autonome Systeme sind die Analyse, der Entwurf und die Konstruktion von autonomen und teilautonomen Systemen aus den verschiedenen Bereichen der Robotik und Mechatronik. Dies umfasst die Modellierung der Anwendungsanforderungen, den Entwurf und die Analyse von Verfahren zur Lösung der gestellten Aufgaben, die Entwicklung von Algorithmen, Schaltungen und mechanischen Konstruktionen sowie deren Implementierung in Software und Hardware inklusive einer anschließenden Verifikation und Validierung. Die Vermittlung der zugrundeliegenden Konzepte steht dabei ebenso im Vordergrund, wie die Fähigkeit, im Gespräch mit Anwenderinnen und Anwendern als deren Partnerin oder Partner Anforderungen an das zu entwickelnde System herauszuarbeiten und auf dieser Basis eine geeignete Lösung des Problems zu erarbeiten und umzusetzen. Die Fähigkeit, sich auf wechselnde Aufgabengebiete und Anwendungsgebiete einstellen zu können, ist dabei unerlässlich. Der Bachelorstudiengang Robotik und Autonomen Systeme trägt dem durch die Kombination einer breiten Grundlagenausbildung mit konkreten, praktischen Projekten Rechnung, wobei sowohl analytische als auch holistische Konzepte und Kenntnisse vertieft werden.“

Für den **Masterstudiengang Robotics and Autonomous Systems** hat die Hochschule in der Studiengangsordnung folgendes Profil beschrieben:

„Das Ziel der Ausbildung im Masterstudiengang Robotics and Autonomous Systems besteht darin, die Studierenden durch Vermittlung von wissenschaftlichen Methoden und Modellen sowie Einübung von Fertigkeiten der Mathematik, Informatik und Technik in den Stand zu versetzen, (teil-) autonome Systeme, insbesondere aus dem Bereich der Robotik aber auch der Automation und Medizin zu konzipieren, zu entwickeln und zu er-

forschen. Dabei liegt im Gegensatz zum Bachelorstudiengang die Betonung auf dem Erwerb von Fähigkeiten für weiterführendes wissenschaftliches Arbeiten. Die Ausbildung trägt dem durch ein grundlagenorientiertes, sowohl breites als auch vertiefendes Studium Rechnung und soll die Voraussetzungen für ein lebenslanges Lernen im Bereich der autonomen und teilautonomen Systeme, insbesondere der Robotik sowie für eine weitergehende akademische Qualifikation wie z.B. die Promotion schaffen. Weiterhin sollen die Studierenden aufgrund der von ihnen erworbenen Kompetenzen in der Lage sein, Leitungsfunktionen in der Wirtschaft zu übernehmen.“

C Bericht der Gutachter

Vorbemerkung

Auf Anordnung des Ministeriums für Bildung und Wissenschaft des Landes Schleswig-Holstein hat die Universität zu Lübeck die Vertiefungsrichtungen „IT-Sicherheit“ und „Robotik und Autonome Systeme“ des Bachelor- und Masterstudiengangs Informatik herausgelöst und als eigenständige Studiengänge konzipiert. Die nun eigenständigen Bachelorstudiengänge „IT-Sicherheit“ und „Robotik und Autonome Systeme“ werden erstmals zum Wintersemester 2016/2017 angeboten. Die Masterstudiengänge „IT-Sicherheit“ und „Robotics and Autonomous Systems“ sollen erstmalig zum Wintersemester 2019/2020 angeboten werden.

Kriterium 2.1 Qualifikationsziele des Studiengangskonzeptes

Evidenzen:

- Selbstbericht der Hochschule, Kapitel 2
- Prüfungsverfahrensordnung (Satzung) der Universität zu Lübeck für Studierende der Bachelor und Master-Studiengänge in der Fassung vom 14. Dezember 2015
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs Robotik und Autonome Systeme an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs Robotics and Autonomous Systems an der Universität zu Lübeck
- § 4.2 der studiengangspezifischen Diploma Supplements

Vorläufige Analyse und Bewertung der Gutachter:

Die Gutachter analysieren die Studiengangsziele des Bachelor- und Masterstudiengangs IT Sicherheit und des Bachelor- und Masterstudiengangs Robotik und Autonome Systeme und begrüßen, dass für alle Studiengänge ein Studiengangskonzept vorgelegt wird, welches sich an Qualifikationszielen orientiert, die sowohl fachliche als auch überfachliche Aspekte umfassen. Für den Masterstudiengang Robotics and Autonomous Systems ist noch anzumerken, dass der Studiengang international ausgerichtet ist und insbesondere

auch internationale Studierende anspricht. Alle Module werden auf Englisch gehalten. Die fachlichen Aspekte werden im Folgenden separat betrachtet.

Im Bachelorstudiengang IT Sicherheit sollen die Studierenden fachliche Kompetenzen im Bereich der Informatik und insbesondere in der IT-Sicherheit erlangen, indem sie zentralen Konzepte und Methoden verstehen und präsentieren sowie passende mathematische, logische, algebraische und technische Hilfsmittel in theoretischen wie praktischen Kontexten auswählen und einsetzen können. Sie sollen die wichtigsten Algorithmen, Datenstrukturen und Muster zu Lösung von Problemen detailliert erläutern und konkret implementieren sowie besondere Probleme und Möglichkeiten, die bei komplexen Informatiksystemen entstehen, benennen und ihre Relevanz einschätzen können. Die Gutachter erkennen, dass besonderen Wert auf die Anwendungskompetenz der Studierenden gelegt wird, indem sie über Spezialkenntnisse in der IT-Sicherheit verfügen sollen, wodurch sie die theoretischen wie fachlichen Grundfragestellungen dieses Gebiets erläutern und die Methoden des Gebiets anwenden können. Durch die angestrebte Kompetenz, umfangreiche Programme in Industriestandard-Programmiersprachen schreiben zu können sowie über gute Kenntnisse in Softwaretechnik und Software-Engineering zu verfügen, sehen die Gutachter, dass die Studierenden dazu befähigt werden sollen, komplexe sichere und zuverlässige Hardware- und Software-Systeme entwerfen zu können. Anhand der Lernziele sehen die Gutachter auch, dass bei der Analyse, Modellierung und Realisierung sicherer und zuverlässiger Systeme die entsprechenden Aspekte in einem übergeordneten Zusammenhang betrachtet werden sollen. Des Weiteren wird angestrebt, dass die Studierenden Architektur, Konzepte und Funktionsweisen moderner Betriebssysteme ebenso wie das Zusammenspiel von Hard- und Software und die Wechselwirkung eingebetteter Rechnersysteme in ihrer Umgebung verstehen. Ferner sollen sie die Konzepte und Funktionsweisen von Kommunikationssystemen verstehen sowie Client-Server-Strukturen konzipieren können. Auch sollen sie im Bereich Datenbanken die theoretischen Grundlagen sowie die Techniken des Datenbankentwurfes unter dem Aspekt der IT-Sicherheit und Zuverlässigkeit erlernen. Die Gutachter kommen zu der Einschätzung, dass die angestrebten Lernergebnisse Level 6 für Bachelorabschlüsse des europäischen Qualifikationsrahmens für lebenslanges Lernen entsprechen. Auch können die Gutachter aus den formulierten Zielen erkennen, dass eine *wissenschaftliche Befähigung* angestrebt wird. In § 2 Absatz 4 der Studiengangsordnung wird festgelegt, dass im Rahmen des Bachelorstudiums die Studierenden auf eine künftige interdisziplinäre Arbeit in der Praxis vorbereitet werden. Hierin erkennen die Gutachter das Ziel angestrebt, die Absolventen zur *Berufsfähigkeit* zu führen. Durch das Ziel, wissenschaftliche Sachverhalte recherchieren und diese dann kritisch überdenken zu können, sehen die Gutachter, dass die *Befähigung zum ge-*

gesellschaftlichen Engagement angestrebt wird. Die *Persönlichkeitsentwicklung* soll insbesondere durch effizientes Arbeiten sowie das Arbeiten in Teams befördert werden.

Im Masterstudiengang IT Sicherheit sollen fachliche Kompetenzen dadurch hergestellt werden, indem die Studierenden über profundes Wissen und Verständnis über die Prinzipien der Informatik und speziell der IT-Sicherheit verfügen und lernen, komplexe Problemstellungen mithilfe formaler Methoden zu beschreiben sowie zu analysieren. Ferner sollen die Absolventen die Fähigkeit und das Urteilsvermögen besitzen, Probleme zu lösen, die unüblich oder unvollständig definiert sind sowie konkurrierende Spezifikationen aufweisen. Ebenso sollen sie dazu befähigt werden, Probleme aus einem neuen und in der Entwicklung begriffenen Bereich der IT-Sicherheit zu formulieren, zu strukturieren, zu formalisieren sowie Lösungsansätze dafür zu beurteilen, auszuwählen, zu erarbeiten und umzusetzen. Des Weiteren wird als Ziel formuliert, dass die Studierenden ein umfassendes Verständnis für anwendbare Techniken und Methoden sowie für deren Grenzen entwickeln. Ebenso sollen sie ein tiefgehendes Fachwissen auf dem Gebiet der sicheren und zuverlässigen IT-Systeme erwerben und die aktuellsten Technologien erfassen. Sie können sowohl wissenschaftliche als auch komplexere praxisnahe Themen und Ziele definieren, daraus Aufgabenstellungen ableiten und deren Lösungen organisieren und überwachen. Die Gutachter sehen, dass die angestrebten Lernergebnisse vollumfänglich Level 7 des europäischen Qualifikationsrahmens für lebenslanges Lernen entsprechen. In § 2 Absatz 1 der Studiengangsordnung ist verankert, dass die Absolventen des Masterstudiums auf Tätigkeiten im Bereich der IT-Sicherheit und Zuverlässigkeit in forschungs-, lehr-, entwicklungs- und anwendungsbezogenen Berufsfeldern vorbereitet. Hierin sehen die Gutachter die *wissenschaftliche Befähigung* auf Masterniveau angestrebt und erkennen ebenfalls, dass die Befähigung, eine *qualifizierte Erwerbstätigkeit* aufzunehmen, klar angestrebt wird. In dem Ziel, dass die Studierenden die Möglichkeiten der nicht-technischen Auswirkungen ihrer praktischen Tätigkeit als IT-Sicherheitsexperte kennen sollen, sehen die Gutachter, dass die Studierenden auch zum *gesellschaftlichen Engagement* angeregt werden sollen. Die Studierenden sind in der Lage, interdisziplinär zusammengesetzte Gruppen und Organisationen verantwortlich zu leiten und können Ideen, Konzepte, Methoden, Verfahren, Techniken und Technologien beurteilen und haben ein kritisches Bewusstsein über die neuen Erkenntnisse der IT-Sicherheit entwickelt, so dass den Gutachtern deutlich wird, dass hier auch die *Persönlichkeitsentwicklung* befördert werden soll.

Anhand der Studiengangszieleformulierung des Bachelorstudiengangs Robotik und Autonome Systeme können die Gutachter erkennen, dass die Studierenden formale, algorithmische und mathematischen Kenntnisse erlangen sollen, die die Grundlage für die Entwicklung von intelligenten Assistenzsystemen sowie autonome und teilautonome (Roboter-)Systeme bilden. Dazu zählen die Korrektheit und Effizienz von Verfahren mit Hilfe

mathematischer Methoden beurteilen zu können sowie mit den wesentlichen Elementen des Entwurfs von Software vertraut zu sein. Ebenso sollen die Studierenden, die wichtigsten konstruktiven, kinematischen und design-technischen Ansätze zur Lösung von Problemen in der Robotik beherrschen und in der Lage sein, Steuerungs- und Regelaufgaben zu identifizieren, Regelalgorithmen zu entwerfen und die technischen Anforderungen für Signalwege zu verstehen und zu schaffen. Ferner sollen sie die Grundlagen der elektrotechnischen Aspekte robotischer und autonomer Systeme sowie der kontinuierlichen und diskreten Mathematik kennen. Mit letzterer sehen die Gutachter die Studierenden in die Lage versetzt, Algorithmen zu entwerfen und zu analysieren. Komplementiert werden sollen diese Kenntnisse durch eine anspruchsvolle Ausbildung in der Digitaltechnik sowie grundlegendes Wissen über Verfahren der Künstlichen Intelligenz. Speziell im Bereich der Analyse, des Designs und der Realisierung von Informatik- und Techniksystemen sollen die Absolventen relevante Programmiersprachen sicher beherrschen und gute Kenntnisse im Software-Engineering besitzen. Ebenso sollen sie die grundlegenden Realisierungsformen kennen und den Umgang mit Konzeptionswerkzeugen für autonome Systeme beherrschen und darüber hinaus, in die Lage versetzt werden, anwendungsspezifische autonome Robotersysteme, insbesondere mobile Roboter, zu analysieren, zu entwerfen und zu realisieren. Anhand der Lernziele sehen die Gutachter auch, dass technologische Kompetenzen wie das Verstehen der Architektur, Konzepte und Funktionsweise moderner Betriebssysteme sowie Netzwerkstrukturen erlangt werden sollen. Des Weiteren wird angestrebt, dass die Studierenden umfangreiche Kenntnisse über die Komponenten der Medizintechnik und ein klares Verständnis davon besitzen, welche zukunftssträchtigen Technologien den verstärkten Einsatz interdisziplinären Handelns seitens der Elektrotechnik, Informatik und Regelungstechnik haben. Die Gutachter bestätigen, dass die Hochschule Qualifikationsziele formuliert hat, die der Stufe 6 des Europäischen Qualifikationsrahmens für lebenslanges Lernen entsprechen. Auch können die Gutachter aus den formulierten Zielen erkennen, dass eine *wissenschaftliche Befähigung* angestrebt wird. In § 2 Absatz 1 der Prüfungsverfahrensordnung wird festgelegt, dass durch die Bachelorprüfung festgestellt werden soll, ob die Studierenden die notwendigen grundlegenden Fachkenntnisse erworben haben, um in die Berufspraxis überzugehen. Hierin erkennen die Gutachter das Ziel angestrebt, die Absolventen zur *Berufsfähigkeit* zu führen. Durch das Ziel, neben den technologischen Aspekten auch gesellschaftliche und ökonomische Entwicklungen im Bereich der Robotik und Fertigungstechnik zu kennen, sehen die Gutachter, dass die *Befähigung zum gesellschaftlichen Engagement* angestrebt wird. Die *Persönlichkeitsentwicklung* soll insbesondere durch das Arbeiten in Teams befördert werden.

Im Masterstudiengang Robotics and Autonomous Systems sollen fachliche Kompetenzen dadurch hergestellt werden, indem Absolventen über profundes Wissen und Verständnis

über die Prinzipien der Robotik, künstlichen Intelligenz und der autonomen Systeme verfügen. Darüber hinaus sollen sie vertieftes informatisches Wissen im Bereich des Computer-Sehens und Maschinellen Lernens verfügen sowie ein kritisches Bewusstsein über die neueren Erkenntnisse entwickeln. Darüber hinaus sollen sie Probleme der Robotik aus industrieller und medizinischer Sicht bewerten, formalisieren und entsprechende Methoden darauf anwenden können. Die Gutachter erkennen darin, dass die Studierenden das Wissen aus verschiedenen Bereichen kombinieren und mit der Komplexität verteilter autonomer Systeme umgehen können. Ebenso sollen sie in der Lage sein, im Rahmen längerfristiger Projekt verschiedene technische Disziplinen sinnvoll zu kombinieren. Die Gutachter sehen, dass die angestrebten Lernergebnisse vollumfänglich Level 7 des europäischen Qualifikationsrahmens für lebenslanges Lernen entsprechen. In § 2 Absatz 1 der Studiengangsordnung ist verankert, dass die Absolventen des Masterstudiums auf ingenieurmäßige Tätigkeiten in anwendungs-, herstellungs-, lehr- und forschungsbezogenen Berufsfeldern sowie auf die Aufnahme eines weiterführenden Studiums vorbereitet. Hierin sehen die Gutachter die *wissenschaftliche Befähigung* auf Masterniveau angestrebt und erkennen ebenfalls, dass die Befähigung, eine *qualifizierte Erwerbstätigkeit* aufzunehmen, angestrebt wird. In dem Ziel, Studierenden ethisches Handeln bei wissenschaftlichen Arbeiten als auch bei Entwicklungsarbeiten beizubringen und ihre Projekte in einen gesellschaftlichen Kontext zu setzen, sehen die Gutachter, dass die Studierenden auch zum *gesellschaftlichen Engagement* angeregt werden sollen. Die Studierenden sind in der Lage, interdisziplinäre Teams und Projekte zu leiten sowie sich mit Kollegen anderer Disziplinen auszutauschen, so dass den Gutachtern deutlich wird, dass hier auch die *Persönlichkeitsentwicklung* befördert werden soll.

Die Gutachter können erkennen, dass sowohl fachliche als auch überfachliche Kompetenzen in den angestrebten Lernergebnissen für alle vier Studiengänge angemessen formuliert sind.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.1:

Die Gutachter bewerten das Kriterium als vollständig erfüllt.

Kriterium 2.2 (a) Konzeptionelle Einordnung des Studiengangs in das Studiensystem

Die Analyse und Bewertung zu den Anforderungen des Qualifikationsrahmens für deutsche Hochschulabschlüsse erfolgt im Rahmen des Kriteriums 2.1, in der folgenden detaillierten Analyse und Bewertung zur Einhaltung der Ländergemeinsamen Strukturvorgaben und im Zusammenhang des Kriteriums 2.3 (Studiengangkonzept).

Kriterium 2.2 (b) Konzeptionelle Einordnung des Studiengangs in das Studiensystem
--

Evidenzen:

- Selbstbericht der Hochschule
- Prüfungsverfahrensordnung (Satzung) der Universität zu Lübeck für Studierende der Bachelor und Master-Studiengänge in der Fassung vom 14. Dezember 2015
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs Robotik und Autonome Systeme an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs Robotics and Autonomous Systems an der Universität zu Lübeck
- exemplarisches Zeugnis je Studiengang
- Modulhandbücher
- § 4.2 der studiengangspezifischen Diploma Supplements
- Auditgespräche mit Hochschulleitung, Programmkoordinatoren, Lehrenden und Studierenden

Vorläufige Analyse und Bewertung der Gutachter:

Studienstruktur und Studiendauer

Grundsätzlich ist in der Prüfungsverfahrensordnung der Universität zu Lübeck in § 4 und 5 Absatz 1 festgelegt, dass die Regelstudienzeit einschließlich aller zu erbringenden Studien- und Prüfungsleistungen drei Jahre für die Bachelor- und zwei Jahre für die Masterstudiengänge beträgt. Ebenfalls wird im § 4 und 5 Absatz 2 festgelegt, dass die Bachelorstudiengänge mit 180 ECTS Punkten und Masterstudiengänge mit 120 ECTS Punkten angelegt sind. Entsprechend beträgt die Regelstudienzeit für die konsekutiv aufeinander aufbauenden Studiengänge fünf Jahre und 300 ECTS Punkte. Die Bachelorarbeit, begleitet durch ein Kolloquium im Umfang von 3 ECTS, umfasst 12 Leistungspunkte und entspricht somit der von der KMK vorgesehenen Bandbreite von 6-12 Kreditpunkten für Bachelorarbeiten. Das Abschlussmodul Masterarbeit wird mit 30 ECTS Punkten kreditiert. Somit erkennen die Gutachter, dass die Vorgaben der KMK zu Studienstruktur und Studiendauer von den Studiengängen eingehalten werden.

Zugangsvoraussetzungen und Übergänge

In § 2 Absatz 1 der Prüfungsverfahrensordnung wird für Bachelorstudiengänge und somit auch für die Bachelorstudiengänge IT-Sicherheit und Robotik und Autonome Systeme festgelegt, dass „die Kandidatin oder der Kandidat die für den Übergang in die Berufspraxis oder die Aufnahme eines weiterführenden Studiums notwendigen grundlegenden Fachkenntnisse erworben hat, die Zusammenhänge ihres oder seines Faches überblickt und die Fähigkeit besitzt, wissenschaftliche Methoden und Erkenntnisse anzuwenden.“ Die Gutachter erkennen, dass durch Laborpraktika, das Bachelor-Projekt sowie die Bachelorarbeit ein dem Qualifikationsprofil angemessener Anwendungs- bzw. Praxisbezug hergestellt wird und sehen, dass mit dem Bachelor ein erster berufsqualifizierender Abschluss erreicht werden soll. Das vorgelegte Konzept erscheint den Gutachtern plausibel. Die Gutachter stellen fest, dass für die Masterstudiengänge IT-Sicherheit und Robotics and Autonomous Systems ein erster berufsqualifizierender Abschluss (Bachelorstudium) vorausgesetzt wird, so dass die KMK Vorgaben diesbezüglich umgesetzt sind. Zur Qualitätssicherung hat die Hochschule für die Zulassung zum Masterstudium weitere Voraussetzungen definiert, die unter Kriterium 2.3 genauer behandelt werden.

Studiengangprofile

Die Hochschule macht in den Antragsunterlagen sowie im Rahmen des Vororttermins plausibel, dass in den Bachelorstudiengänge IT-Sicherheit und Robotik und Autonome Systeme wissenschaftliche Grundlagen, Methodenkompetenz und berufsfeldbezogene Qualifikationen gleichermaßen vermittelt werden.

Die Hochschule definiert die zu akkreditierenden Masterstudiengänge IT-Sicherheit und Robotics and Autonomous Systems als stärker *forschungsorientiert*. In den jeweiligen Studiengangsordnungen ist verankert, dass „[...] im Gegensatz zum Bachelorstudiengang die Betonung auf dem Erwerb von Fähigkeiten für wissenschaftliches Arbeiten [liegen]. Die Ausbildung trägt dem durch ein grundlagenorientiertes, sowohl breites als auch vertiefendes Studium Rechnung, soll die Voraussetzung für ein lebenslanges Lernen [...] sowie für eine weitergehende akademische Qualifikation wie z.B. die Promotion schaffen“. Darüber hinaus erkennen die Gutachter umfassende Forschungstätigkeiten der Lehrenden, die in die Lehre einfließen, so dass sie die Einordnung der Hochschule als forschungsorientierte Masterstudiengänge bestätigen.

Konsekutive und weiterbildende Masterstudiengänge

In § 2 Absatz 3 der jeweiligen Studiengangsordnungen wird festgelegt, dass die Masterstudiengänge IT-Sicherheit und Robotics and Autonomous Systems konsekutiv zu den Bachelorstudiengängen der IT-Sicherheit und Robotik und Autonome Systeme sind. Die Studienziele (§ 2 Absatz 2 der Studiengangsordnungen) sowie die in den Modulhand-

büchern verzeichneten Module sind auf den Erwerb vertiefender, verbreitender und fachübergreifende Kenntnisse und Fähigkeiten ausgelegt, daher können die Gutachter die Konsekutivität nachvollziehen.

Abschlüsse

Die Gutachter stellen fest, dass für alle zu akkreditierende Studiengänge nur ein Abschlussgrad vergeben wird und die Vorgaben der KMK somit eingehalten werden.

Bezeichnung der Abschlüsse

Die Gutachter erkennen, dass für die Bachelorstudiengänge der Abschlussgrad „B.Sc.“ und für die Masterstudiengänge „M.Sc.“ entsprechend der Ausrichtung der Programme verwendet werden und somit die Vorgaben der KMK erfüllt sind. In der Prüfungsverfahrensordnung für Bachelor- und Masterstudiengänge der Universität zu Lübeck ist zusätzlich zu der Abschlussnote die Vergabe einer relativen ECTS-Note vorgesehen, die im Zeugnis ausgewiesen wird.

Zusammen mit dem Zeugnis wird ein Diploma Supplement verliehen. Darin enthalten sind Angaben zur Person, zum Qualifikationsprofil des Studiengangs sowie der individuellen Leistungen. Statistische Daten gemäß ECTS Users Guide zur Einordnung des individuellen Abschlusses werden ausgewiesen. Die Gutachter weisen darauf hin, dass zukünftig die aktuelle Fassung des Diploma Supplements zu nutzen ist, die unter Ziffer 8 ebenso Bezug auf den Deutschen Qualifikationsrahmen für Lebenslanges Lernen (DQR) nimmt.

Modularisierung und Leistungspunktsystem

Für die erfolgreiche Absolvierung aller Module werden Leistungspunkte entsprechend dem ECTS vergeben. Ein Kreditpunkt entspricht 30 Stunden studentischer Arbeitslast. Laut Studienverlaufsplänen werden im Durchschnitt 30 Kreditpunkte pro Semester vergeben. Abweichungen von jeweils 10 % im fünften und sechsten Semester der Bachelorstudiengänge IT-Sicherheit und Robotik und Autonome Systeme erscheinen den Gutachtern für ein Vollzeitstudium unkritisch. In den Bachelorstudiengängen umfassen die Module 4-10 Leistungspunkte und in den Masterstudiengängen in der Regel 6-12 Kreditpunkte. Die Abweichung insbesondere in den Bachelorstudiengängen von den ländergemeinsamen Strukturvorgaben, die festlegen, dass die Mindestmodulgröße 5 ECTS betragen soll, begründet die Hochschule durch die Modulinhalt und mit dem Verwenden der Module in verschiedenen bereits akkreditierten Studiengängen der MINT-Sektion. Des Weiteren liegt eine Genehmigung des Ministeriums für Bildung und Wissenschaft des Bundeslandes Schleswig-Holsteins vor, die die Modulgrößen von 4 ECTS genehmigt, wenn die Anzahl der Prüfungen in den Bachelor- und Masterstudiengängen pro Semester auf maximal 6 beschränkt und die Mobilität der Studierenden nicht einschränkt wird. Die

Studierenden aus den verwandten Studiengängen der Informatik, Medieninformatik und Medizinischen Informatik äußerten sich im Allgemeinen nicht negativ über die Prüfungsbelastung, sodass die Gutachter annehmen, dass mit der oben genannten Regelung eine Kleinteiligkeit von Modulen und eine damit verbundene hohe Prüfungsbelastung auch in den neukonzipierten und zur Akkreditierung stehenden Studiengängen vermieden werden. In der Regel können in den Bachelorstudiengängen IT-Sicherheit und Robotik und Autonome sowie im Masterstudiengang IT-Sicherheit die Module innerhalb eines Semesters absolviert werden. Die zwei-semesterigen Module im Masterstudiengang Robotics and Autonomous Systems werden in den Abschnitten 2.3, 2.4 und 2.5 näher betrachtet.

Modulbeschreibungen

Die Gutachter können erkennen, dass in den Modulen thematisch und zeitlich abgerundete, in sich geschlossene und mit Leistungspunkten belegte Studieneinheiten zusammengefasst werden. Die Module setzen sich aus verschiedenen Lehr- und Lernformen zusammensetzen (z. B. Vorlesungen, Übungen, Praktika, Seminar etc.), die aus den Modulbeschreibungen eindeutig hervorgehen. Die Gutachter bestätigen, dass die Modulbeschreibungen detaillierte Auskunft geben über Titel, Lehrformen, Voraussetzungen für die Teilnahme, Verwendbarkeit des Moduls, Häufigkeit des Angebots und den Arbeitsaufwand geben. Allerdings ergeben sich für die Gutachter Fragen bezüglich der curricularen Abfolge von Modulen, die thematische und zeitlich aufeinander abgestimmt sein sollten (vgl. Kriterium 2.3). Teilweise konnten die Bedenken der Gutachter diesbezüglich durch die inhaltlichen Erläuterungen zu Modulen wie beispielsweise „Regelungstechnik“, „Signalverarbeitung“, „Kryptographische Protokolle“ und „Fallstudie“ der Programmverantwortlichen und Lehrenden während der Vor-Ort-Begehung ausgeräumt werden, sodass es sich hier um ein Darstellungsproblem handelt, da die im Gespräch erläuterten Inhalte und Qualifikationsziele nicht eindeutig aus den Modulbeschreibungen hervorgehen. Des Weiteren geben die Modulbeschreibungen zwar Auskunft über die Vergabe von Kreditpunkten sowie die Benotung spezifizieren aber nicht, ob die beschriebene Leistungsnachweise Voraussetzungen zur Teilnahme an der finalen Prüfungsleistung darstellen oder die finale Prüfungsleistung sind. Ebenso sind Dauer und Umfang der Prüfungen verbindlich festzulegen. Missverständlich erscheint den Gutachtern schließlich der Gebrauch des Terminus „Voraussetzungen“. Dass damit im Zusammenhang der vorliegenden Modulhandbücher lediglich Empfehlungen und keine verpflichtenden Vorbedingungen für den Besuch eines Moduls gemeint sind, erfahren sie erst auf Nachfrage. Die Gutachter halten daher eine Überarbeitung der Modulbeschreibungen hinsichtlich der oben genannten Monita für notwendig.

Die Gutachter begrüßen, dass die Modulhandbücher der zu akkreditierenden Studiengänge zum erstmaligen Studienbeginn auf den programmspezifischen Webseiten veröffentlicht werden sollen.

Mobilität

Als Mobilitätsfenster für einen Studienaufenthalt im Ausland, bietet sich laut Hochschule insbesondere das vierte und fünfte Semester an. Auf Nachfrage ob dies auch im Bachelorstudiengang IT-Sicherheit möglich ist, da das Modul „Sichere Netze und Computerforensik“ über zwei Semester unterrichtet wird, erläutert die Hochschule, dass sie eine wohlwollende Anerkennungspraxis pflegt und zuvor geprüft wird, ob die jeweilige Partnerhochschule ein adäquates Modul anbietet, um studienzeitverlängernde Effekte zu vermeiden. Die Studierenden der Bachelorstudiengänge Informatik, Medieninformatik und Medizinische Informatik bestätigen, dass das Akademische Auslandsamt potentielle Bewerber über die bestehenden Austauschprogramme und Finanzierungsmöglichkeiten berät. Allerdings erachten sie die Planung eines Auslandssemesters in der Praxis als sehr schwierig, da sich ein zweisemestriges Modul über das vierte und fünfte Semester erstreckt und der Koordinationsaufwand somit erhöht werde. Die Gutachter empfehlen daher zu prüfen, ob die Möglichkeiten zu einem Aufenthalt ohne Zeitverlust an einer anderen Hochschule oder in der Praxis verbessert werden können. Ebenso sollten die Studierenden aktiv über die Möglichkeiten eines Aufenthaltes informiert werden.

In den Masterstudiengängen IT-Sicherheit und Robotics and Autonomous Systems bietet sich laut Programmverantwortlichen eines der Blockpraktika oder die Masterarbeit für Auslandsaufenthalte an. Auch hier ist die Eigeninitiative der Studierenden die Basis, die durch den Prüfungsausschuss, das Studierenden Service-Center und das Auslandsamt gefördert und unterstützt wird.

Die Zugangsvoraussetzungen der Studiengänge (A 2 der Ländergemeinsamen Strukturvorgaben) werden im Rahmen des Kriteriums 2.3 behandelt.

Die Berücksichtigung der „Rahmenvorgaben für die Einführung von Leistungspunktsystemen und für die Modularisierung“ wird, von den vorgenannten Punkten abgesehen, im Zusammenhang mit den Kriterien 2.3 (Anerkennung), 2.4 (Kreditpunktsystem, studentische Arbeitslast, Prüfungsbelastung), 2.5 (Prüfungssystem: kompetenzorientiertes Prüfen) überprüft.

Kriterium 2.2 (c) Konzeptionelle Einordnung des Studiengangs in das Studiensystem
--

Das Land Schleswig-Holstein Hamburg hat keine landesspezifischen Strukturvorgaben für die Akkreditierung von Bachelor- und Masterstudiengängen verabschiedet.

Kriterium 2.2 (d) Konzeptionelle Einordnung des Studiengangs in das Studiensystem

Verbindliche Auslegungen des Akkreditierungsrates müssen an dieser Stelle nicht berücksichtigt werden.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.2:

Die Gutachter bedanken sich für die Stellungnahme der Hochschule bezüglich der Modulbeschreibungen. Aus den überarbeiteten Modulbeschreibungen zu „System Security“, „Kryptografische Protokolle“, „Fallstudien IT-Sicherheit“, „Regelungstechnik“ und „Signalverarbeitung“ gehen die während der Vor-Ort-Begehung erläuterten Inhalte und Qualifikationsziele nun hervor. Den Gutachtern wird anhand der Ausführungen der Hochschule deutlich, dass alle Module mit einer finalen Prüfungsleistung abschließen und die unter dem Punkt „Vergabe von Leistungspunkten und Benotung“ genannten Leistungsnachweise wie „Übungen“ oder „regelmäßige Teilnahme“ nicht Teil der finalen Prüfungsleistung sind und somit nicht in die Note eingehen. Diese Leistungsnachweise können zu Voraussetzungen für die Teilnahme an der Prüfung gemacht werden; dies legt der Dozent zu Beginn des Semesters verbindlich fest. Dennoch empfehlen die Gutachter, dies in den Modulbeschreibungen deutlicher hervorzuheben.

Die Hochschule nimmt den Hinweis der Gutachter auf, die Überschrift „Voraussetzungen“, die lediglich einen empfehlenden Charakter haben durch „Empfohlene Voraussetzungen“, „Empfohlene vorher zu besuchende Module“ oder „Module, auf denen dieses Modul inhaltlich aufbaut“ zu ersetzen.

Die Dauer der Prüfungen ist in den § 11 und 12 der PVO verbindlich festgelegt. Mündliche Prüfungen dauern zwischen 15 und 40 Minuten, Klausuren zwischen 60 bis 180 Minuten. Die Anmerkung der Gutachter bezog sich darauf, dass eine Angabe der Zeitspanne nicht detailliert genug ist, sondern die Dauer der Prüfungsleistungen eindeutig festgelegt werden muss. Die Hochschule macht glaubhaft, dass die Dauer der Prüfung zu Semesterbeginn oder bereits davor im UnivIS (Universitätsinformationssystem) durch die Studierenden eingesehen werden kann.

Die Gutachter begrüßen die Umstrukturierung des Bachelorstudiengangs IT-Sicherheit, Das bisher zweisemestrige Modul „Sichere Netze und Computerforensik“ (4. und 5. Semester) liegt nun im 6. Semester. Das Mobilitätshindernis ist ausgeräumt, sodass die Möglichkeiten zu einem Aufenthalt ohne Zeitverlust an einer anderen Hochschule oder in der Praxis verbessert wurden.

Die Gutachter bewerten das Kriterium als erfüllt.

Kriterium 2.3 Studiengangskonzept
--

Evidenzen:

- Selbstbericht der Hochschule
- Ziele-Module-Matrizen zu den jeweiligen Studiengängen
- Studienpläne
- Modulhandbücher
- Prüfungsverfahrensordnung (Satzung) der Universität zu Lübeck für Studierende der Bachelor und Master-Studiengänge in der Fassung vom 14. Dezember 2015
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs Robotik und Autonome Systeme an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs Robotics and Autonomous Systems an der Universität zu Lübeck
- Auditgespräche mit Hochschulleitung, Programmkoordinatoren, Lehrenden und Studierenden

Vorläufige Analyse und Bewertung der Gutachter:

Studiengangskonzept / Umsetzung der Qualifikationsziele

Die Gutachter untersuchen das Curriculum hinsichtlich der Umsetzung übergeordneter Qualifikationsziele. Die Gutachter können anhand der mit dem Selbstbericht vorgelegten Ziele-Matrizen nachvollziehen, dass das Studiengangskonzept der jeweiligen Studienprogramme die Vermittlung von Fachwissen und fachübergreifendem Wissen sowie von fachlichen, methodischen und generischen Kompetenzen umfasst.

Für den Bachelorstudiengang IT-Sicherheit können die Gutachter nachvollziehen, dass mathematische Grundlagen durch die im Curriculum verankerten Pflichtmodule „Lineare Algebra und Diskrete Strukturen 1 und 2“, „Analysis 1 und 2“ sowie „Stochastik 1“ erlangt werden, um diese zur Beschreibung dynamischer, mechanischer und elektrotechnischer Systeme zu verwenden sowie Algorithmen zu entwerfen und zu analysieren. Auch ist den Gutachtern plausibel, dass die Studierenden in den Pflichtmodulen des Bereichs Informatik „Einführung in die Programmierung“, „Algorithmen und Datenstrukturen“, „Techni-

sche Grundlagen der Informatik 1 und 2“, „Software Engineering“, „Praktikum Software-Engineering“, „Betriebssysteme und Netze“, „Datenbanken“, „Rechnerarchitektur“ mit Grundlagen der Informatik vertraut gemacht werden. In diesen eigenen sich die Studierenden u.a. Kenntnisse und Fertigkeiten zur Entwicklung von komplexen Hard- und Software-Systemen, die sichere Beherrschung von Programmiersprachen sowie gute Kenntnisse im Software-Engineering an. Des Weiteren erwerben sie durch diese Module ein breites Spektrum an technologischem Fachwissen aus dem Bereich der Systeminformatik. In die Thematik der IT-Sicherheit führen die Module „Cybersecurity“, „Kryptologie“, „Sichere Netzwerke und Computerforensik“, „Sichere Software“, „Zuverlässigkeit von Rechnersystemen“ ein und werden durch das Bachelorseminar, Bachelorprojekt und die Bachelorarbeit vertieft. Zu dem Modul „Sichere Software“ ergeben sich seitens der Gutachter folgende Fragen. Aus Sicht der Gutachter liest sich die vorgelegte Beschreibung als ein Modul zu „Softwareanalyse“. In der englischen Fassung heißt das Modul „Safe Software“, so dass nicht ersichtlich ist, ob bzw. welche Inhalte bezüglich der Entwicklung sicherer Software abgedeckt werden. Die angegebene Bibliographie enthält keine Literatur zu Software Security. Begriffe wie SQLi, XSS, Pufferüberlauf, OWASP, Fuzzing, Penetration Testing tauchen nicht auf. Die Gutachter bitten den Modulverantwortlichen zu erläutern, welche Inhalte für dieses Modul vorgesehen sind. Ebenso ist den Gutachtern nicht ersichtlich, in welchen Modulen Sicherheitsmanagement, die Fertigkeit „Sicheres Programmieren“, aber auch Software-Schwachstellen und die dazu benötigten Werkzeuge verankert sind. Dies sollte nach Ansicht der Gutachter aus den Modulbeschreibungen deutlich hervorgehen. Insgesamt stellen die Gutachter fest, dass der Bereich Netzwerk- und Kommunikationssicherheit sowie Kryptografie im Curriculum dominiert aber Bereiche wie Risikoanalyse, IT-Sicherheitsmanagement, Softwaresicherheit und IT-Recht weniger stark ausgeprägt sind. Die Gutachter sind der Ansicht, dass dies insbesondere daran liegt, dass in dem erstgenannten Bereich personelle Ressourcen bereits vorhanden sind und sich das Institut für IT-Sicherheit, welches die Studiengangsleitung übernehmen soll, noch im Aufbau befindet. Daher begrüßen die Gutachter, die zur Berufung ausgeschriebene W3-Professur für IT-Sicherheit und W2-Professur für zuverlässige Systeme. Dadurch können die im Curriculum noch weniger stark verankernden obengenannten Themenbereiche stärker integriert werden. Sie empfehlen dies ausdrücklich, um die angestrebte Berufsbefähigung der Studierenden zu gewährleisten.

In Bezug auf die sequenzielle Abfolge der Module im Bachelorstudiengang IT-Sicherheit stellen die Gutachter fest, dass es teilweise Dopplungen von Lehrinhalten zu geben scheint. Laut Modulbeschreibung werden Inhalte, die bereits im Modul „Kryptologie“ (3. Semester) vermittelt werden im Modul „Sichere Netze und Computerforensik“ (3. und 4. Semester) erneut gehört. Ebenso scheinen Inhalte zur Thematik der Computerforensik

sich in den Modulen „Cybersecurity“ (3. Semester) sowie „Sichere Netze und Computerforensik“ partiell zu doppeln. Die Programmverantwortlichen erläutern, dass manche Module in den verschiedenen Studienprogrammen der MINT-Sektion gehört und Grundlagen demnach für alle Studierenden erneut behandelt werden, um den Kenntnisstand zu vereinheitlichen. Ebenso werden diese Inhalte in unterschiedlicher Tiefe in den jeweiligen Modulen behandelt. Diese Argumentation können die Gutachter grundsätzlich nachvollziehen, allerdings trifft das laut Modulbeschreibungen für die oben genannten Beispiele nicht zu. Lediglich das Modul „Kryptologie“ wird in mehreren Studiengängen unterrichtet, die Module „Cybersecurity“ und „Sichere Netze und Computerforensik“ werden eigens für den Studiengang IT-Sicherheit konzipiert, sodass ein inhaltlicher Abgleich dieser Module hinsichtlich der Vermeidung von doppelten Lehrinhalten den Gutachtern für möglich erscheint. Bezüglich der thematisch und zeitlich aufeinander abgestimmten Module, stellen die Gutachter weiterhin fest, dass im Modul „Cybersecurity“ (3. Semester) Sicherheit von Betriebssystemen sowie die Sicherheit in Datenbanken vermittelt, die Grundlagen hierfür aber erst im vierten Semester in den Modulen „Betriebssysteme und Netze“ sowie „Datenbanken“ gelehrt werden. Als weiteres Beispiel seien hier noch die sich bedingenden Inhalte der Module „Sichere Netze und Computerforensik“ (4. und 5. Semester) und im gleichen Semester „Betriebssysteme und Netze“ (4. Semester) aufgeführt, aus denen nicht deutlich wird, wie die Inhalte aufeinander abgestimmt werden. Die Studierenden der verwandten Bachelorstudiengänge Informatik, Medieninformatik und Medizinische Informatik verweisen zudem darauf hin, dass aus studentischer Sicht beispielsweise das Modul „Einführung in die Logik“ (3. Semester) früher im Curriculum verankert werden sollte, um insbesondere die Inhalte des Moduls „Theoretische Informatik“ (3. Semester) besser verstehen zu können, um somit die Studierbarkeit des Moduls zu gewährleisten. Die Programmverantwortlichen erläutern, dass sie die sequenzielle Abfolge der Module als gewährleistet sehen und durch das parallele Unterrichten der Module „Einführung in die Logik“ und „Theoretische Informatik“, die Studierbarkeit gewährleistet wird. Die Gutachter können nicht abschließend bewerten, ob es sich in diesen Fällen um ein Darstellungsproblem handelt oder ob die sequenzielle Abfolge der Module im Bachelor IT-Sicherheit teilweise Unstimmigkeiten aufweist. Die Hochschule wird daher gebeten, Stellung zum Aufbau des Curriculums zu nehmen.

Das Konzept des konsekutiven Masterstudienprogramms IT-Sicherheit ist mit Blick auf die Umsetzung des übergeordneten Kompetenzprofils im Großen und Ganzen schlüssig strukturiert. In den Pflichtmodulen „Praktische Informatik“, „Technische Informatik“, „Algorithmik“, „Spezifikation und Modellierung“ sowie in den Wahlpflichtmodulen werden informatische Kenntnisse, Kompetenzen und Fertigkeiten angemessen vertieft. Sie bereiten die Studierenden auf komplexe anwendungs- und forschungsorientierte Frage-

stellungen vor. Der Bereich der IT-Sicherheit zeichnet sich durch ein angemessenes Wahlpflichtangebot zu den Themengebieten Security and Privacy, Software Safety und System Reliability aus. Ebenso werden aktuelle Themen der IT-Sicherheit in einem eigenständigen Modul behandelt, allerdings ist den Gutachtern nicht ersichtlich, ob auf dem Zeugnis ein konkretes Thema oder eine konkrete Anwendung ausgewiesen werden soll. Sie bitten hier um Nachtrag seitens der Hochschule. Im Zusammenhang mit den angestrebten Qualifikationszielen erschienen manche Inhalte des Moduls „System Security“ laut Modulbeschreibung eher Praxis-orientiert („Studierende sind in der Lage bekannte Systeme zur Gewährleistung von Systemsicherheit zu installieren und zur Anwendung zu bringen“). Es handelt sich dabei um ein neu zu entwerfendes Modul, so dass es sich hier um ein Darstellungsproblem handeln kann. Im Zusammenhang mit den angestrebten Qualifikationszielen erschienen die Inhalte des Moduls „Kryptographische Protokolle“ laut Modulbeschreibung als zu Grundlagen orientiert und dem Qualifikationsniveau nicht angemessen. Diese Bedenken konnten im Gespräch mit dem Modulverantwortlichen ausgeräumt werden, sodass es sich hier um ein Darstellungsproblem handelt. Des Weiteren begrüßen die Gutachter zwar die geplante Fallstudie zu Themen der IT-Sicherheit, allerdings wird ihnen nicht deutlich, welche Kompetenzziele im Sinne der IT Sicherheit angestrebt werden, da es sich laut Modulbeschreibungen wie ein Projektmanagementseminar liest. Sie erachten daher eine Überarbeitung der Modulbeschreibungen hinsichtlich der oben genannten Monita für notwendig (vgl. Kriterium 2.2). Sie regen ebenso an, das im Master Robotics and Autonomous Systems angebotene Wahlpflichtmodul „Legal foundations for IT“ auch im Masterstudienprogramm IT-Sicherheit anzubieten, da dies aus Sicht der Gutachter eine sinnvolle Ergänzung zum Studienangebot darstellen würde. Neben fachlichen werden auch überfachliche, soziale und gesellschaftliche Kompetenzen vermittelt. Beispielsweise im Rahmen des fachübergreifenden Wahlpflichtangebots, aber auch in der Abschlussarbeit und begleitend in den Fachmodulen, erwerben die Studierenden etwa Kommunikations- und Präsentationskompetenz sowie die Fähigkeit, die moralisch-ethischen Dimensionen eines späteren beruflichen Handelns zu reflektieren. Studierende sollen zur Übernahme von Leitungsfunktionen befähigt werden, wozu sie auch Kompetenzen im Sicherheitsmanagement und in der Risikoanalyse benötigen. Es wird den Gutachtern anhand der vorliegenden Modulbeschreibungen nicht ersichtlich, wie diese Kompetenzen vermittelt werden. Sie bitten die Hochschule um Nachtrag.

Die Gutachter halten zunächst fest, dass die an dem Bachelor- und Masterstudiengang Robotik und Autonome Systeme beteiligten Professoren und ihre jeweiligen Forschungs- und Lehrgebiete bereits bekannt sind und sich somit in die Konzeption der Studiengänge einbringen konnten. Infolgedessen ist die Kombination der einzelnen Module stimmig im

Hinblick auf die formulierten Qualifikationsziele aufgebaut und die curriculare Gestaltung erscheint den Gutachtern plausibel.

Für den Bachelorstudiengang Robotik und Autonome Systeme können die Gutachter nachvollziehen, dass mathematische Grundlagen durch die im Curriculum verankerten Pflichtmodule „Lineare Algebra und Diskrete Strukturen 1 und 2“, „Analysis 1 und 2“ sowie „Stochastik 1“ erlangt werden, um diese zur Beschreibung dynamischer, mechanischer und elektrotechnischer Systeme zu verwenden sowie Algorithmen zu entwerfen und zu analysieren. Auch ist den Gutachtern plausibel, dass die Studierenden in den Pflichtmodulen des Bereichs Informatik „Einführung in die Programmierung“, „Algorithmen und Datenstrukturen“, „Technische Grundlagen der Informatik 1 und 2“, „Software Engineering“, „Praktikum Software-Engineering“ sowie „Betriebssysteme und Netze“ mit Grundlagen der Informatik vertraut gemacht werden. In diesen eignen sich die Studierenden u.a. Kenntnisse und Fertigkeiten zur komplexen Entwicklung von Hard- und Software-Systemen, die sichere Beherrschung von Programmiersprachen sowie gute Kenntnisse im Software-Engineering an. Des Weiteren erwerben sie durch diese Module ein breites Spektrum an technologischem Fachwissen aus dem Bereich der Systeminformatik. Die technischen Grundlagen für den Entwurf autonomer Systeme und Roboter sowie das ingenieurmäßiges Entwickeln und Konstruieren sehen die Gutachter angemessen durch die Module „Einführung in die Robotik und Automation“, „Robotik“, „Technische Mechanik“, „Grundlagen der Elektrotechnik“, „Regelungstechnik und Mechatronik“ und „Signalverarbeitung“ realisiert. Anhand der Modulbeschreibungen erschien es den Gutachtern zunächst nicht plausibel, weshalb die Module „Regelungstechnik“ und „Signalverarbeitung“, die Grundlagen aus der Elektrotechnik sind und für Projekte im Bereich Robotik benötigt werden, erst im 5. bzw. 6. Semester gelehrt werden. Daraufhin erläutern die Programmverantwortlichen, dass die notwendigen Grundlagen der Regelungstechnik und Signalverarbeitung bereits in anderen Modulen wie beispielsweise „Einführung in die Robotik und Automation“ unterrichtet werden, sodass die Studierenden diese Kenntnisse für die Robotik-Module beherrschen. Die Studierenden haben diese Konzepte dann bereits verinnerlicht, sodass darauf aufbauend in den Modulen „Regelungstechnik“ und „Signalverarbeitung“ vertiefende theoretische/mathematische Inhalte vermittelt werden. Den Gutachtern erscheint diese didaktische Vorgehensweise plausibel, sie weisen aber darauf hin, dass dies aus den Modulbeschreibungen nicht ersichtlich wird. Dementsprechend sind die Modulbeschreibungen inhaltlich zu überarbeiten (vgl. Kriterium 2.2). Des Weiteren erläutert die Hochschule, dass die Thematik Mensch-Computer-Interaktion aufgrund von Abwägungen zugunsten der technischen Grundlagen im Wahlpflichtbereich und nicht im Pflichtcurriculum verankert ist. Auch diese Entscheidung können die Gutachter aufgrund der Ausrichtung des Studienprogramms nachvollziehen. In der Bachelorarbeit erarbeiten

die Studierenden ihre erste eigene wissenschaftliche Arbeit zu einem Themengebiet der Robotik und Autonomen Systeme. Im fachübergreifenden Wahlbereich sowie durch Teamarbeiten in den Modulen sollen auch überfachliche Kompetenzen entwickelt sowie Methoden des Projektmanagement eingeübt werden.

Im internationalen Masterstudiengang Robotics and Autonomous Systems werden aufbauend auf das Bachelorstudium Kenntnisse und Fertigkeiten in den Bereichen Robotik und Autonome Systeme durch die Pflichtmodule „Artificial Intelligence 2 and Medical Robotics“, „Autonomous Systems (Real-Time Systems, Control Engineering and System Dynamics“ und „Machine Learning and Computer Vision“ vertieft und erweitert. Die Gutachter verstehen, dass diese Module Wissen aus verschiedenen Bereichen kombinieren, ein umfassendes Verständnis für anwendbare Techniken und Methoden sowie deren Grenzen vermitteln, komplexe Problemstellungen aufzeigen und die Studierenden Lösungsansätze erarbeiten sollen. In den Vertiefungsmodulen sowie im Wahlpflichtkatalog können die Studierenden einen individuellen Schwerpunkt setzen. Insbesondere die im dritten Semester verankerten Praktika (Internship Robotics and Autonomous systems 1 und 2), die in Zusammenarbeit mit Unternehmen oder außeruniversitären Forschungseinrichtungen durchgeführt werden, führen zur vertiefenden praktischen/wissenschaftlichen Erarbeitung von Projekten im Bereich der Robotik und der autonomen Systeme und vermitteln ferner weiterführende Projektmanagement-Kompetenzen. Zudem präsentieren die Studierenden ihre Ergebnisse auf einer simulierten Konferenz (Modul „Student Conference“) und werden dadurch nach Auffassung der Gutachter auf eine berufspraktische Tätigkeit angemessen vorbereitet. Die Befähigung zu einer wissenschaftlichen Tätigkeit sehen die Gutachter durch die Anfertigung der Masterarbeit zu komplexen wissenschaftlichen Fragestellungen sowie die Auswahl und Anwendung adäquater Methoden als gewährleistet. Überfachliche Kompetenzen werden durch die oben beschriebenen Module und die Teamarbeiten ebenfalls weiterentwickelt.

Die Gutachter stellen fest, dass in allen zu akkreditierenden Studienprogrammen Möglichkeiten für die Studierenden zu einer individuellen Schwerpunktsetzung gegeben sind. In den Bachelorstudiengängen IT-Sicherheit und Robotik und Autonome Systeme können die Studierenden 2-3 fachspezifische Wahlpflichtmodule wählen und die Bachelorarbeit zu einem selbstgewählten Themengebiet anfertigen. In den Masterstudiengängen IT-Sicherheit und Robotics and Autonomous Systems können die Studierenden 4-6 fachspezifische Wahlpflichtmodule wählen sowie einen individuellen Schwerpunkt durch die Masterarbeit und die Praktika (nur im Masterstudiengang Robotics and Autonomous Systems) setzen. Der Wahlpflichtkatalog für die Bachelor- und Masterstudiengängen erscheint den Gutachtern insgesamt als umfassend.

Vor dem Hintergrund, dass der konsekutive Masterstudiengang Robotics and Autonomous Systems in englischer Sprache angeboten wird und die Absolventen in der Regel ein international vernetztes Arbeits- und Forschungsumfeld haben, problematisieren die Auditoren schließlich eine studienbegleitende Förderung englischer Sprachkompetenz. Die Gutachter erkennen, dass der Umgang mit englischer Fachliteratur im Pflichtbereich geübt und das Modul „Bachelor-Seminar“ in englischer Sprache angeboten wird. Einzelne Vorlesungen des Wahlpflichtbereichs werden darüber hinaus optional auf Englisch gehalten. Lernzielüberprüfungen werden dann sowohl auf Deutsch als auch auf Englisch angeboten. Auch Abschlussarbeiten können wahlweise auf Englisch geschrieben werden. Insgesamt erachten die Gutachter die Berücksichtigung der englischen Sprache zwar prinzipiell als ausreichend. Auch erkennen sie, dass das grundsätzlich zufriedenstellende Angebot von weniger Studierenden genutzt wird als dies wünschenswert wäre. Angesichts der hohen Bedeutung der englischen Sprache für das vorliegende Fachgebiet und das in englischer Sprache angebotene Masterprogramm raten sie den Verantwortlichen gleichwohl, eine entsprechende Sprachkompetenz der Studierenden konsequenter zu fördern.

Didaktisches Konzept / Praxisbezug

Die Gutachter begrüßen, dass sich die verschiedenen Lehr- und Lernformen aus denen jeweiligen Qualifikationszielen der einzelnen Module ableiten. An Lehrformen werden Vorlesungen, große und kleine Übungen, Seminare, Praktika und Projektarbeiten verwendet. Die dabei verwendeten Gruppengrößen sind so gewählt, dass die Studienleistungen auch tatsächlich als individuelle Leistung von jeweiligen Studierenden erbracht werden. Generell werden alle Module durch eine einheitliche E-Learning-Plattform (universitäres Moodle) unterstützt, die dazu genutzt wird, Videos, Dokumente, Prüfungsvorbereitungsaufgaben sowie podcasts zur Verfügung zu stellen. Des Weiteren soll sie den Studierenden als Diskussionsplattform dienen. Das didaktische Konzept scheint den Gutachtern geeignet, die angestrebten Studienziele umzusetzen.

In den Bachelorstudiengängen IT-Sicherheit und Robotik und Autonome Systeme wird durch Laborpraktika, das Bachelor-Projekt sowie die Bachelorarbeit ein dem Qualifikationsprofil angemessener Anwendungs- bzw. Praxisbezug hergestellt. Der Praxisbezug wird in den Masterstudiengängen IT-Sicherheit und Robotics and Autonomous Systems durch Fallstudien, Praktika sowie die Masterarbeit sicher gestellt. Bachelor- und Masterarbeiten können ebenso in Zusammenarbeit mit Unternehmen angefertigt werden, entsprechende Regelungen liegen vor. Insgesamt kommen die Gutachter für alle Studienprogramme zu dem Schluss, dass die Hochschule bereits während der Ausbildung angemessene Berührungspunkte zur beruflichen Praxis setzt.

Das Mobilitätsfenster wurde bereits unter Kriterium 2.2 behandelt.

Zugangsvoraussetzungen und Anerkennungsregeln

Gemäß den jeweiligen Studiengangsordnungen ist die formale Voraussetzung für die Immatrikulation in die Bachelorstudiengängen IT-Sicherheit und Robotik und Autonome Systeme die allgemeine Hochschulreife, eine einschlägige fachgebundene Hochschulreife oder eine durch Rechtsvorschrift oder von der zuständigen staatlichen Stelle als gleichwertig anerkannte Zugangsberechtigung. Bildungsausländer erbringen zusätzlich den Nachweis über ausreichende Deutschkenntnisse.

Gemäß den jeweiligen Studiengangsordnungen wird die Qualifikation für die Masterstudiengängen IT-Sicherheit und Robotics and Autonomous Systems durch einen Abschluss im Bachelor IT-Sicherheit bzw. für letzteren in Robotik und Autonome Systeme oder einen gleichwertigen Abschluss oder einen fachlich eng verwandten in- oder ausländischen Studienabschluss nachgewiesen. Bildungsausländer erbringen zusätzlich den Nachweis über ausreichende Deutschkenntnisse für den Masterstudiengang IT-Sicherheit. Angemessene Englischkenntnisse müssen Bewerber für das englischsprachige Masterstudium Robotics and Autonomous Systems nachweisen. Darüber hinaus muss das Erststudium mit einer Note von 2,7 oder besser abgeschlossen worden sein. Im Masterstudiengang Robotics and Autonomous Systems wird weiterhin vorausgesetzt, dass die Bewerber mathematische Anteile im Umfang von mindestens 32 ECTS sowie technische und informatorische Anteile von mindestens 28 ECTS (hierin müssen - neben weiteren - jedenfalls enthalten sein: Programmieren, Elektrotechnik, Mechanik, Technische Grundlagen der Informatik) im Bachelorstudium absolviert haben. Den Gutachtern erscheinen die Zugangsvoraussetzungen angemessen, sie weisen aber darauf hin, dass im Sinne der Lissabon Konvention die Zugangsvoraussetzungen kompetenzorientiert formuliert sein sollten.

Die Masterstudiengänge sind konsekutiv zu den Bachelorstudiengängen IT-Sicherheit und Robotik und Autonome Systeme der Universität zu Lübeck aufgebaut. Allerdings geben die Gutachter zu bedenken, dass es Deutschland- bzw. weltweit wenige spezialisierte Bachelorstudiengänge mit den Bezeichnungen IT-Sicherheit und Robotik und Autonome Systeme gibt. Externe Studieninteressierte könnten sich daher fragen, was die Hochschule unter einem gleichwertigen Abschluss bzw. fachlich eng verwandten Bachelorstudium versteht. Die Programmverantwortlichen erläutern, dass beispielsweise Informatikstudiengänge anerkannt werden, in denen die Studierenden Inhalte zur IT-Sicherheit oder Elektrotechnik, Mechanik und Technische Grundlagen der Informatik gehört haben. Die Gutachter empfehlen, im Sinne der Transparenz für die Studieninteressierten beispiele-

weise auf den programmspezifischen Webseiten näher zu erläutern, welche potenziellen Bachelorstudiengänge vom Prüfungsausschuss anerkannt werden.

An anderen Hochschulen erbrachte Studien- und Prüfungsleistungen werden gemäß § 20 der Prüfungsverfahrensordnung anerkannt, sofern „keine wesentlichen Unterschiede hinsichtlich der erworbenen Kompetenzen bestehen“. Die Anerkennung ist dabei auf maximal 50% des Zielstudiengangs beschränkt und schließt die Abschlussarbeit dezidiert aus. Der Grundsatz der Beweislastumkehr ist in den entsprechenden normativen Vorgaben (es besteht „ein *Rechtsanspruch* auf Anerkennung“, wenn von der Hochschule keine „substantziellen Unterschiede“ hinsichtlich der zu ersetzenden Kompetenzen „*nachgewiesen*“ werden) hinreichend transparent verankert. Außerhalb des Hochschulbereichs erworbene Kompetenzen können zu denselben Bedingungen (und damit ebenfalls bis maximal 50% des Zielstudiengangs) anerkannt werden.

Die Gutachter bewerten diese Regelung insofern kritisch, weil nach der derzeit verbindlichen Interpretation der Lissabon-Konvention durch Akkreditierungsrat und gemeinsame Kultusministerkonferenz (KMK) eine Begrenzung der Anerkennung von extern erbrachten Studienleistungen nicht zulässig ist. Allerdings sieht der Akkreditierungsrat selbst die bisherige Auslegung durch eine abweichende Regelungspraxis in einzelnen Ländern in Frage gestellt und hat deshalb die KMK um eine grundsätzliche Klärung des Sachverhaltes gebeten. Bis zu einer Neufassung der entsprechenden Vorgaben sind regelhafte Beschränkungen der Anerkennung weiterhin zu beanstanden, entsprechende Auflagen jedoch bis zu einer grundsätzlichen Klärung des Sachverhaltes auszusetzen. Eine Beschränkung der Anerkennung auf 50% oder weniger ist jedoch, dies haben die involvierten Akteure bereits deutlich gemacht, nicht mit dem Mobilitätsgedanken der Lissabon-Konvention vereinbar und deshalb in jedem Fall auch weiterhin unzulässig. Die Gutachter halten es dementsprechend für erforderlich, dass die Regelung zur Anerkennung von an anderen Hochschulen erbrachten Studien- und Prüfungsleistungen hinsichtlich der vorgesehenen Einschränkungen mit den Anforderungen der Lissabon-Konvention in Einklang gebracht wird.

Im § 19 der Prüfungsverfahrensordnung ist der Nachteilsausgleich für Studierende mit Behinderungen aus Sicht der Gutachter angemessen geregelt.

Studienorganisation

Bei den zur Akkreditierung beantragten Studienprogrammen handelt es sich um Präsenzstudiengänge, die in Vollzeit studiert werden. Die organisatorischen und infrastrukturellen Rahmenbedingungen erscheinen den Gutachtern dabei insgesamt zur Umsetzung der Studiengangskonzepte geeignet.

Zur Berücksichtigung der Belange der Studierenden sind die betreffenden Ausführungen zu Kriterium 2.4 zu vergleichen.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.3:

Die Gutachter bedanken sich für die ausführliche Stellungnahme der Hochschule. Die Hochschule führt aus, dass das Modul „Sichere Software“ des Bachelorprogramms IT-Sicherheit schwerpunktmäßig Themen der Sicherheit im Sinne von Safety behandelt. Security-Themen werden bewusst ausgelassen. Die angegebenen Begriffe wie SQL Injection, Cross Site Scripting etc. erscheinen der Hochschule zu detailliert für eine Angabe unter den Lehrinhalten eines Moduls. Die Punkte werden im Modul „Sichere Netze und Computerforensik“ unter der Thematik „Angriffe“ detailliert und in einer Übersicht im Modul „Cybersecurity“ abgehandelt. „Penetration Testing“ und „Intrusion Detection Systeme“ wurden als neue Punkte im Modul „Sichere Netze und Computerforensik“ aufgenommen.

Die Themenschwerpunkte Sicherheitsmanagement, Risikoanalyse, die Fertigkeit „Sicheres Programmieren“, Software-Schwachstellen und dazu benötigten Werkzeuge werden zukünftig in verschiedenen Modulen des Bachelorstudiengangs IT-Sicherheit behandelt. Das Modul „Einführung in die Programmierung“ wird um die Thematik „Techniken für sicheres Programmieren“ ergänzt. „IT-Sicherheitsmanagement“ wird durch „IT Grundschutz und ITIL“ im Modul „Sichere Netze und Computerforensik“ und durch „Internet Governance“ im Modul „Cybersecurity“ abgedeckt. Risikoanalyse wird in beiden Modulen implizit betrachtet (im Modul „Cybersecurity“ ist es explizit aufgenommen). IT-Recht wird als neues Wahlmodul im Master angeboten, ansonsten bietet das Modul „Cybersecurity“ eine grundlegende Einführung.

Die Gutachter sehen die Themenschwerpunkte Sicherheitsmanagement, Risikoanalyse, die Fertigkeit „Sicheres Programmieren“, Software-Schwachstellen und dazu benötigten Werkzeuge im Hinblick auf die Qualifikationsziele im Curriculum nach den Ausführungen der Hochschule besser verankert, allerdings empfehlen sie nach der Besetzung der Professur für IT-Sicherheit das Angebot im Bereich sichere Software noch einmal in Hinblick auf Aktualität zu überarbeiten.

In Bezug auf die sequenzielle Abfolge der Module im Bachelorstudiengang IT-Sicherheit erläutert die Hochschule folgendes:

Das Modul „Sichere Netze und Computerforensik“ besteht aus zwei Lehrveranstaltungen mit jeweils zwei Vorlesungen und einer Übung. Der Teil „Sichere Netze“ wird jedoch auch als eigenständiges Modul (zurzeit „Sicherheit in Netzen und verteilten Systemen“) mindestens als Wahlpflicht in allen anderen Bachelor-Studiengängen der Informatik angebo-

ten. Die hier sich teilweise doppelten Kryptographie-Inhalte lassen sich nicht vermeiden, wobei es weiterhin so ist, dass die Thematik in „Sichere Netze“ nur oberflächlich und in „Kryptologie“ stärker mathematisch behandelt wird.

In Bezug auf die Inhaltsdopplung wurde das Modul „Cybersecurity“ überarbeitet und inhaltlich mit dem Modul „Sichere Netze und Computerforensik“ abgestimmt haben, sodass es nun nur noch marginale Inhaltsdopplungen geben wird. Außerdem wird das Modul „Cybersecurity“ vom 3. in das 4. Semester verlegt: „Cybersecurity“ findet parallel zu den Modulen „Betriebssysteme und Netze“ und „Datenbanken“, in denen die zugehörigen Grundlagen vermittelt werden, statt. Damit können nun auch jeweils passend zu den Grundlagen gleich die dazugehörigen Sicherheitskonzepte erläutert werden bzw. mögliche Gefahren.

Das Modul „Sichere Netze und Computerforensik“, in dem Netzwerksicherheit sehr vertieft besprochen wird, findet nun erst im 6. Semester und damit nach der Grundlagenvorlesung „Betriebssysteme und Netze“ statt.

Bei dem Wunsch der Studierenden, das Modul „Einführung in die Logik“ aus dem 3. Semester früher im Curriculum zu verankern ist zunächst festzuhalten, dass das Modul Einführung in die Logik im Studiengang Medieninformatik nicht vorgesehen ist. Daher hört die Mehrzahl der Teilnehmer der Theoretischen Informatik die Veranstaltung Logik nicht und die Theoretische Informatik ist konzeptionell „darauf vorbereitet“. Weiterhin ist die Ausgestaltung der Logik im dritten Semester eine andere als im ersten Semester, da die Logik nun stärker in die Tiefe gehen kann. Gerade für den Studiengang IT-Sicherheit ist ein tieferes Verständnis von logischen Formalismen sehr sinnvoll.

Die Gutachter können die Erläuterungen nachvollziehen und begrüßen die konzeptionellen Anpassungen des Curriculums. Die sequenzielle Abfolge der Module erachten sie nun als stimmig, um die angestrebten Qualifikationsziele zu erreichen und die Studierbarkeit zu gewährleisten.

Im Masterprogramm IT-Sicherheit werden „Aktuelle Themen der IT-Sicherheit“ in einem eigenständigen Modul behandelt. Die Hochschule erläutert, dass eine Ausweisung des jeweiligen konkreten aktuellen Themas auf dem Zeugnis zukünftig im Rahmen der Einführung eines neuen Campus-Managementsystems angestrebt wird. Die Gutachter begrüßen dies und können nachvollziehen, dass es derzeit jedoch mit den HIS-Systemen in der Prüfungsverwaltung nicht möglich ist.

Des Weiteren begrüßen die Gutachter, dass das Modul „Rechtliche Grundlagen für die IT“ (CS5820-KP04) auch von den Master-Studierenden der IT-Sicherheit aus der Liste der fächerübergreifenden Wahlmodule gewählt werden kann.

Die Gutachter nehmen zur Kenntnis, dass kostenlose Englisch-Sprachkurse vom Sprachzentrum der Hochschule angeboten werden und sehen die Verwendung von englischsprachigen Lehrmaterialien oder Lehrvideos als richtigen Schritt an. Dennoch halten sie an ihrer Empfehlung fest, fachbezogene englische Sprachkompetenzen der Studierenden systematischer zu fördern, um auf den englischsprachigen Masterstudiengang sowie das spätere Arbeitsumfeld vorzubereiten.

Die Gutachter erachten die vorgelegten kompetenzorientierteren Formulierungen der Zugangsvoraussetzungen für den Masterstudiengang Robotics and Autonomous Systems als angemessen und empfehlen weiterhin, die für das jeweilige Masterstudienprogramm vorausgesetzten Kenntnisse, Kompetenzen und Fertigkeiten (anerkannte Bachelorabschlüsse) für Studieninteressierte transparent zu gestalten.

Die Gutachter nehmen zur Kenntnis, dass die Universität bis zu einer endgültigen Klärung des Sachverhalts durch die gemeinsame Kultusministerkonferenz an einer Beschränkung der Anerkennung von an anderen Hochschulen erworbenen Kompetenzen auf maximal 50% des Zielstudiengangs festhalten wird. Die Gutachter weisen in diesem Zusammenhang erneut darauf hin, dass die Frage, ob Hochschulen berechtigt sind, die Anerkennung von extern erworbenen Studienleistungen zu begrenzen, innerhalb der gemeinsamen Kultusministerkonferenz derzeit kontrovers diskutiert und wahrscheinlich mittelfristig neu gefasst werden wird. Der Akkreditierungsrat hat in diesem Zusammenhang jedoch festgelegt, dass regelhafte Beschränkungen der Anerkennung bis zu einer Neufassung weiterhin zu beanstanden sind. Entsprechende Auflagen sind bis zu einer grundsätzlichen Klärung des Sachverhalts dann außer Vollzug zu setzen, wenn eine Anerkennung von mehr als der Hälfte der für den Studiengang vorgesehenen Kreditpunkte ermöglicht wird. Gerade dies ist im vorliegenden Fall jedoch nicht gegeben. Die Gutachter sehen hier dementsprechend nach wie vor kurzfristigen Änderungsbedarf und halten an einer diesbezüglichen Auflage fest.

Die Gutachter bewerten das Kriterium mit Ausnahme der nicht Lissabon-konformen Anerkennungsregelungen als erfüllt. Allerdings fehlt hier noch eine Klärung des Sachverhalts durch die KMK.

Kriterium 2.4 Studierbarkeit

Evidenzen:

- Selbstbericht der Hochschule
- Curriculare Übersichten und Studienpläne
- Modulhandbücher

- Prüfungsverfahrensordnung (Satzung) der Universität zu Lübeck für Studierende der Bachelor und Master-Studiengänge in der Fassung vom 14. Dezember 2015
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs Robotik und Autonome Systeme an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs Robotics and Autonomous Systems an der Universität zu Lübeck
- Abschlussbericht „Sicherung der Studierbarkeit durch Qualitätsmanagement in Studium und Lehre“ 2013
- Auswertung der Absolvent_innenbefragung 2014
- Bericht zur Lehrevaluation WS 2014/2015 (Auszug Informatik)
- Bericht zur Lehrevaluation SoSe 2015 (Auszug Informatik)
- Publikation „Sicherung der Studierbarkeit durch Qualitätsmanagement in Studium und Lehre“ – Ein Projekt des Nordverbunds“ 2014
- Beratungsangebote auf der Homepage (Zugriff 18.04.2016): <https://www.uni-luebeck.de/studium/studierenden-service-center/studienberatung.html>

Vorläufige Analyse und Bewertung der Gutachter:

Eingangsqualifikationen / Studienplangestaltung

Die Eingangsqualifikationen wurden bereits unter Kriterium 2.3 behandelt und sind aus Sicht der Gutachter angemessen, um die Studierbarkeit der Studiengänge zu gewährleisten. Die Studienplangestaltung in den Bachelorstudiengängen ist so aufgebaut, dass es einige Hürden für Studierende gibt, um von einem Studienabschnitt in den nächsten überzugehen. Grundsätzlich halten die Gutachter es für plausibel, dass von der Hochschule gefordert wird, dass bestimmte Leistungen innerhalb eines bestimmten Zeitraums erbracht werden müssen, damit Studierende selbst einschätzen können, ob sie für einen Studiengang geeignet sind.

Studentische Arbeitslast

Für die zur Akkreditierung beantragten Studiengänge liegen noch keine statistischen Daten vor, da die erste Kohorte erst zum Wintersemester 2016/2017 ihr Bachelorstudium aufnehmen wird und die ersten Masterstudierenden für das WS 2019/2020 erwartet

werden. Allerdings werden die studentische Arbeitsbelastung als Ganzes sowie die Zuordnung von ECTS zu einzelnen Modulen im Rahmen der Lehrevaluation regelmäßig auf Plausibilität überprüft. Die Studierenden der Informatik, Medieninformatik und Medizinischen Informatik erläutern, dass es zwar arbeitsintensivere Module gibt, sie die studentische Arbeitsbelastung insgesamt und in den jeweiligen Modulen jedoch für angemessen halten. Die Programmverantwortlichen betonen in diesem Zusammenhang, dass die Ergebnisse der Lehrevaluation kritisch reflektiert und in der Vergangenheit wiederholt zur Adaption von Modulen geführt haben. Beispielsweise sei hier das Modul „Algorithmendesign“ aufgeführt, welches ebenso nach Aussagen der Studierenden „studierbarer“ geworden ist. Die Gutachter halten die die Kreditpunktekalkulation auf Grundlage der vorgelegten Studiengangskonzepte insgesamt für plausible.

Prüfungsbelastung und –organisation

Anhand der vorgelegten curricularen Übersichten inklusive Angabe der zu absolvierenden Prüfungen untersuchen die Gutachter die Prüfungsdichte. Die Prüfungsbelastung in den Bachelorstudiengängen und dem Masterstudiengang IT-Sicherheit erscheint den Gutachtern prinzipiell angemessen. Im Durchschnitt werden 4-5 Prüfungen am Ende des Semesters absolviert. In den Bachelorstudiengängen IT-Sicherheit und Robotik und Autonome Systeme sowie im Masterstudiengang IT-Sicherheit erstreckt sich jeweils ein Modul über zwei Semester, sodass die finale Prüfungsleistung am Ende des zweiten Semesters erfolgt. Die Studierenden bemängeln, dass die finalen Modulprüfungen der zweisemestrigen Module in der Praxis nicht immer miteinander verzahnt werden, sodass sie für zwei separate Prüfungen lernen und diese aufeinanderfolgend am selben Tag geschrieben werden. Die Gutachter nehmen dies zur Kenntnis, können dies für die zur Akkreditierung beantragten Studiengänge jedoch nicht verifizieren. Dennoch sollte die Hochschule darauf achten, dass in allen zweisemestrigen Modulen jeweils eine in sich kohärente Prüfungsleistung absolviert wird.

Im Masterstudiengang Robotics and Autonomous Systems erstrecken sich insgesamt drei Pflicht- und ein Vertiefungsmodul im Umfang von 8 oder 12 ECTS über die ersten beiden Fachsemester. Zusätzlich sind Wahlpflichtmodule im Umfang von insgesamt 16 ECTS über zwei Semester zu belegen. Die Anzahl der ECTS variiert bei den Wahlpflichtmodulen zwischen 4, 6 und 8 ECTS. Ein weiteres fachübergreifendes Modul im Umfang von 4 ECTS wird ebenfalls über zwei Semester unterrichtet. Die Studierenden der anderen Masterstudiengänge, in denen es eine ähnliche Studienplangestaltung gibt, erläutern, dass sehr genau abgewogen werden muss, welche Vertiefungs- und Wahlpflichtmodule man belegt, damit zum Ende des zweiten Fachsemesters die Anzahl der Prüfungen angemessen bleibt. Anhand der vorgelegten curricularen Übersicht können die Gutachter nicht abschließend bewerten, ob die Studienplangestaltung in Form der zweisemestrigen Module sowie die

daraus resultierende Prüfungsdichte die Studierbarkeit des Studiengangs gewährleistet. Sie bitten die Hochschule, Musterstudienpläne inkl. der Anzahl der Prüfungen pro Semester jeweils für Studierende die im SoSe und WS beginnen, nachzureichen.

Das Prüfungssystem wird im Übrigen eingehend unter Kriterium 2.5 behandelt.

Beratung / Betreuung

Das Verhältnis zwischen Studierenden und Lehrenden wird von allen Beteiligten als sehr gut beschrieben. Eine familiäre Lernatmosphäre und eine enge persönliche Betreuung werden vor allem von den Studierenden als wesentlicher Standortvorteil der Universität zu Lübeck hervorgehoben. Die Dozenten verfolgen dabei eine „Politik der offenen Tür“ und sind ohne feste Sprechzeiten fast jederzeit für studienbezogene Probleme ihrer Klientel aufgeschlossen. Als feste Ansprechpartner für fachliche und studienorganisatorische Fragestellungen stehen den Studierenden zudem der Vorsitzende des Prüfungsausschusses, der Studiengangskoordinator sowie Mentoren zur Verfügung. Für die Beratung von Studienanfängern und Studieninteressierten ist das Studierenden-Service-Center zuständig. Bei überfachlichen Problemen können die Studierenden schließlich auf das Angebot des Studentenwerks Lübecks zurückgreifen. Neben einer psychosozialen Beratungsstelle finden Betroffene hier beispielsweise Hilfe bei der Wohnungssuche oder der Studienfinanzierung. Insgesamt bewerten die Gutachter das Beratungsangebot als angemessen.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.4:

Die vorgelegten Prüfungspläne für den Masterstudiengang Robotics and Autonomous Systems verdeutlichen, dass die Prüfungsdichte 6 Prüfungen am Ende des zweiten Semesters nicht überschreiten. Allerdings weist die Prüfungsdichte starke Unterschiede auf. So sind es am Ende des ersten Semesters 1-2 Prüfungen je nachdem, ob man im Sommer- oder Wintersemester beginnt und am Ende des zweiten Semesters 5-6 Prüfungen, wobei 3 der finalen Prüfungsleistungen Inhalte aus zwei Fachsemestern beinhalten. Die Ungleichverteilung der Prüfungsdichte erachten die Gutachter als nicht förderlich, wenngleich sie die Studierbarkeit nicht gänzlich in Frage stellen. Sie empfehlen daher, die studentische Prüfungsbelastung gleichmäßiger auf die ersten beiden Fachsemester zu verteilen und greifen den Vorschlag der Studierenden auf, die Teilmodule so zu kombinieren, dass sie innerhalb eines Semesters gehört und abgeschlossen werden können.

Kriterium 2.5 Prüfungssystem

Evidenzen:

- Selbstbericht der Hochschule
- Curriculare Übersichten und Studienpläne
- Modulhandbücher
- Prüfungsverfahrensordnung (Satzung) der Universität zu Lübeck für Studierende der Bachelor und Master-Studiengänge in der Fassung vom 14. Dezember 2015
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs Robotik und Autonome Systeme an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs Robotics and Autonomous Systems an der Universität zu Lübeck

Vorläufige Analyse und Bewertung der Gutachter:

Kompetenzorientierung der Prüfungen

Aus den Modulbeschreibungen geht hervor, dass die meisten Prüfungen in den Bachelorstudiengängen Klausuren sind. Auf Nachfrage inwiefern mündliche Prüfungen sowie Prüfungen in Form von Vorträgen, Hausarbeiten, Projekten oder Gruppenarbeiten stattfinden, erläutert die Hochschule, dass diese Prüfungsformen beispielsweise in den Modulen „Codierung und Sicherheit“, „Kryptologie“, „Computergestützter Schaltungsentwurf“, „Graphentheorie“ oder auch im Bachelorprojekt- und Bachelorseminar Anwendung finden. In den Masterstudiengängen finden häufig Prüfungsformen wie Projekt- und Seminararbeiten sowie Präsentationen Anwendung.

Jedes Modul schließt in der Regel mit einer das gesamte Modul umfassenden Prüfung am Ende des Semesters ab. In einigen Modulen ist die erfolgreiche Teilnahme an Laborpraktika oder die Lösung von Übungsaufgaben Zulassungsvoraussetzung für die abschließende Modulprüfung. Die Gutachter halten dies für didaktisch sinnvoll und erwarten keine negativen Auswirkungen auf den Studienverlauf. In diesem Zusammenhang heben die Studierenden positiv hervor, dass in jedem Semester am Ende der vorlesungsfreien Zeit ein zweiter Prüfungszeitraum angeboten wird. Dieser Termin biete dabei nicht nur die Möglichkeit, eventuelle strukturelle Spitzen in der Prüfungsbelastung durch eine individuelle

Planung auszugleichen, sondern führe insbesondere dazu, dass eventuell notwendige Wiederholungsprüfungen einen regelhaften Studienverlauf nicht behindern.

Für die Studiengänge liegen noch keine Klausuren, Hausarbeiten und Abschlussarbeiten vor. Allerdings konnten die Gutachter Prüfungsleistungen sowie Abschlussarbeiten der Studierenden der Informatik mit den derzeitigen Vertiefungsschwerpunkten IT-Sicherheit sowie Robotik und Autonome Systeme einsehen. Sie kommen zu der Einschätzung, dass die Prüfungsleistungen in der vorgelegten Form, Wissen und Kompetenzen auf dem angestrebten Niveau angemessen abzu prüfen. Eine Einschätzung für die zur Akkreditierung beantragten Studiengänge ist naturgemäß nicht möglich. Allerdings erwarten die Gutachter keine Probleme.

Die Gutachter erachten insgesamt das vorgelegte Prüfungskonzept- und system für plausibel.

Zum Nachteilsausgleich sind die betreffenden Ausführungen unter Kriterium 2.3, zum Verbindlichkeitsstatus der vorgelegten Ordnungen die Ausführungen unter Kriterium 2.8 zu vergleichen.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.5:

Die Gutachter bewerten das Kriterium als erfüllt.

Kriterium 2.6 Studiengangsbezogene Kooperationen

Evidenzen:

- Selbstbericht der Hochschule, Kapitel 5
- Letter of Support, IHK Lübeck
- Webseite des Akademisches Auslandsamt: <https://www.uni-luebeck.de/studium/international-office.html> (Zugriff am 17.04.2016)
- Auditgespräche mit Hochschulleitung, Programmkoordinatoren, Lehrenden und Studierenden

Vorläufige Analyse und Bewertung der Gutachter:

Die Bachelor- und Masterstudiengänge IT-Sicherheit und Robotik und Autonome Systeme werden zu weiten Teilen aus den Angeboten der Lehrereinheit Informatik/Technik getragen. Vor allem in den Wahlfächern werden zum Teil Leistungen der übrigen Lehrereinheiten importiert. Die Lehrimporte sind zwischen den beteiligten Sektionen (die Universität Lü-

beck gelidert sich in Sektionen und nicht in Fachbereiche/Fakultäten) vereinbart. Die Gutachter sehen die für die Studiengänge benötigten Lehrimporte als gesichert an.

Insbesondere begrüßen die Gutachter, die Kooperationen der universitären Institute (u.a. Institut für Robotik und Kognitive Systeme (ROB), Institut für Softwaretechnik und Programmiersprachen (ISP) etc.) mit zahlreichen regionalen und internationalen Unternehmen sowie außeruniversitären Forschungseinrichtungen. Auf Grundlage dieser Kooperationen können Praktikumsplätze generiert werden und die Studierenden können in Zusammenarbeit mit diesen Einrichtungen ihre Abschlussarbeiten schreiben. Darüber hinaus sehen die Gutachter gewährleistet, dass durch diese Kooperationen aktuelle Entwicklungen ebenfalls in Forschung und Lehre einfließen.

Zur Förderung der Studierendenmobilität unterhält die Universität zu Lübeck bzw. die MINT-Sektion eine Reihe von Kooperationsvereinbarungen mit europäischen Universitäten im Rahmen des Erasmus Programms sowie mit weiteren internationalen Hochschulen. Wie bereits im Kapitel 2.2 angemerkt werden die Möglichkeiten für einen Auslandsaufenthalt allerdings selten von den Studierenden genutzt.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.6:

Die Gutachter bewerten das Kriterium als vollumfänglich erfüllt.

Kriterium 2.7 Ausstattung

Evidenzen:

- Selbstbericht der Hochschule, Kapitel 5
- Personalhandbuch
- Weiterbildungsangebot: <https://www.uni-luebeck.de/universitaet/einrichtungen/dozierenden-service-center.html> (Zugriff am 18.04.2016)
- Curricularnormwertberechnung für die Bachelor- und Masterstudiengänge IT-Sicherheit und Robotik und Autonome Systeme
- Auditgespräche mit Hochschulleitung, Programmkoordinatoren, Lehrenden und Studierenden
- Im Rahmen der Vor-Ort-Begehung: Besichtigung studiengangsrelevanter Einrichtungen

Vorläufige Analyse und Bewertung der Gutachter:

Personelle Ausstattung

Die verfügbaren Personalressourcen für die Studiengänge IT-Sicherheit und Robotik und Autonome Systeme werden von der Lehrereinheit Informatik der MINT-Sektion bereitgestellt. Das Deputat des Personals steht den Studiengängen fast voll zur Verfügung, da praktisch alle Lehrveranstaltungen immer in mehreren Studiengängen genutzt werden. Die Universität zu Lübeck greift mit ein bis zwei Lehrbeauftragten im Wahlangebot kaum auf externe Lehrbeauftragte zurück. Im Wahlangebot des Bachelor-/Master IT-Sicherheit wird sich dies noch ändern, da hier der Einsatz von juristischen bzw. betriebswirtschaftlichen externen Experten für bestimmte Module geplant ist, allerdings derzeit noch nicht feststeht. Das neugegründete Institut für IT-Sicherheit wird für die Durchführung der Studiengänge IT-Sicherheit verantwortlich sein und die Studiengangsleitung übernehmen. Die Gutachter begrüßen, dass dieses mit einer W3-Professur für IT-Sicherheit und einer W2-Professur für zuverlässige Systeme ausgestattet werden wird. Die aus Sicht der Gutachter noch weniger stark im Curriculum verankernden Themenbereiche Risikoanalyse, IT-Sicherheitsmanagement, sichere Software und IT-Recht (vgl. Kapitel 3) könnten durch die neuen Stelleinhaber abgedeckt werden. Die Gutachter sehen in den ausgeschriebenen Professuren eine angemessene Erweiterung des fachlichen Lehrpersonals, die die curricularen Inhalte, den Qualifikationszielen entsprechend, abdecken können. Den Gutachtern erscheint die personelle Ausstattung für die Durchführung der Studiengänge insbesondere für die Studiengänge der IT-Sicherheit als ausreichend aber knapp bemessen. Sie weisen aber darauf hin, dass bei steigenden Studierendenzahlen, ebenso die Mitarbeiterzahlen signifikant mitwachsen müssen, um ein angemessenes Betreuungsverhältnis zu gewährleisten.

Personalentwicklung

Das Dozierenden-Service-Center der Universität zu Lübeck stellt ein umfangreiches Angebot zur hochschuldidaktischen Weiterbildung bereit, welches die Dozenten auch wahrnehmen. Zur fachlichen Weiterbildung können von Professoren außerdem turnusmäßig Forschungsfreisemester beantragt werden. Als positiv bewerten die Gutachter zudem, dass studentische Tutoren didaktische Schulungen erhalten und damit optimal auf ihre Tätigkeit vorbereitet werden.

Finanzielle und sächliche Ausstattung

Die finanzielle Ausstattung wird nach Aussagen der Hochschulleitung in den kommenden Jahren auf einem guten Niveau konsolidiert. Auf Basis der zusätzlichen Länderfinanzmittel sei die Finanzierung der neukonzipierten Studiengänge für die Dauer von 10 Jahren gesichert; hinzukommen projektbezogene Drittmittel, die den Studiengängen damit ebenfalls

mittelbar zu Gute kommen. Zudem wird die neue Finanzierung der Hochschule im Rahmen des Hochschulpakts III ab WS 2016 dazu führen, dass neue Mittel in erheblichem Umfang für die Lehre bereitstehen werden. Die Gutachter bewerten die finanzielle Ausstattung mit Blick auf die Umsetzung der Studiengangskonzepte als angemessen.

Die Gutachter gelangen bei der Vor-Ort-Begehung zu einem sehr positiven Eindruck der räumlichen Ausstattung, sodass die diese den Gutachtern zur Durchführung der Studiengänge als gesichert erscheint. Laborarbeitsplätze stehen nach Aussagen der Studierenden derzeit noch ausreichend zur Verfügung. Allerdings bemängeln sie, dass insbesondere das Labor für technische Informatik bereits sehr stark ausgelastet sei und bei zukünftig größeren Studierendenzahlen ein Kapazitätsproblem entstehen könnte. Die Programmverantwortlichen erläutern, dass praktische Übungen bei höheren Studierendenzahlen zukünftig bis nach 18:00 Uhr ausgedehnt werden könnten, sodass mittelfristig die räumlichen Kapazitäten ausreichen würden. Die Studierenden bemängeln insbesondere die limitierten studentischen Arbeitsplätze. Die Gutachter begrüßen, dass die Hochschule darauf durch eine geplante Erweiterung der Infrastruktur reagiert und empfehlen diese, insbesondere in Hinblick auf die räumlichen Kapazitäten für Übungen/Praktika und Studierendenarbeitsplätze zu erweitern.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.7:

Die Gutachter halten an ihrer Empfehlung fest, die räumlichen Kapazitäten für Übungen/Laborpraktika sowie im Hinblick auf die Studierendenarbeitsplätze zu erweitern.

Kriterium 2.8 Transparenz

Evidenzen:

- Selbstbericht der Hochschule
- Prüfungsverfahrensordnung (Satzung) der Universität zu Lübeck für Studierende der Bachelor und Master-Studiengänge in der Fassung vom 14. Dezember 2015
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs IT-Sicherheit an der Universität zu Lübeck
- Studiengangsordnung (Satzung) für Studierende des Bachelorstudiengangs Robotik und Autonome Systeme an der Universität zu Lübeck

- Studiengangsordnung (Satzung) für Studierende des Masterstudiengangs Robotics and Autonomous Systems an der Universität zu Lübeck
- exemplarisches Zeugnis je Studiengang
- exemplarisches Diploma Supplement je Studiengang
- exemplarisches Transcript of Records je Studiengang

Vorläufige Analyse und Bewertung der Gutachter:

Studiengänge, Zulassungsbedingungen, Studienverläufe, Prüfungsanforderungen sowie Nachteilsausgleichsregelungen für Studierende mit Behinderung sind im Rahmen der Prüfungsverfahrensordnung und der jeweiligen Studiengangsordnungen verbindlich geregelt. Die vorliegenden Ordnungen haben die hochschulüblichen Genehmigungsverfahren durchlaufen. Die jeweiligen Studiengangsordnungen liegen derzeit im Entwurf vor, die in Kraft gesetzten Ordnungen für die Studiengänge sind noch vorzulegen.

Für alle zur Akkreditierung beantragten Studiengänge sind programmspezifische Zeugnisse und Diploma Supplements dokumentiert. Dass das Diploma Supplement nicht dem aktuellen Muster von HRK und KMK entspricht, wurde bereits im Kriterium 2.2 angemerkt.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.8:

Die Hochschule erläutert, dass die Bachelor-Studiengangsordnungen voraussichtlich Mitte Juli 2016 in Kraft gesetzt werden. Die Master-Studiengangsordnungen werden nach Eingang der abschließenden Hinweise aus der Sitzung der Akkreditierungskommission voraussichtlich im Dezember 2016 in Kraft gesetzt.

Die Gutachter halten fest, dass die in Kraft gesetzten Ordnungen für die Studiengänge noch vorzulegen sind.

Kriterium 2.9 Qualitätssicherung und Weiterentwicklung

Evidenzen:

- Selbstbericht der Hochschule
- Universität zu Lübeck: Webseite Dezernat für Qualitätsmanagement und Organisationsentwicklung (<https://www.uni-luebeck.de/universitaet/verwaltungsstruktur/dezernate/dezernat-iii-qualitaetsmanagement-und-organisationsentwicklung.html>) (17.04.2016))

- Rahmenqualitätssatzung der Universität zu Lübeck
- Evaluationssatzung für Studium und Lehre der Universität zu Lübeck
- Abschlussbericht „Sicherung der Studierbarkeit durch Qualitätsmanagement in Studium und Lehre“ 2013
- Auswertung der Absolvent_innenbefragung 2014
- Bericht zur Lehrevaluation WS 2014/2015 (Auszug Informatik)
- Bericht zur Lehrevaluation SoSe 2015 (Auszug Informatik)
- Publikation „Sicherung der Studierbarkeit durch Qualitätsmanagement in Studium und Lehre“ – Ein Projekt des Nordverbunds“ 2014

Vorläufige Analyse und Bewertung der Gutachter:

Im Kontext einer immer stärkeren sektionsübergreifenden Verzahnung der Lehre, aber auch mit Blick auf eine mittelfristig angestrebte Systemakkreditierung, hat sich das Qualitätsmanagementsystem der Universität zu Lübeck in den vergangenen Jahren zunehmend von studiengangindividuellen Ansätzen gelöst. Die stattdessen angestrebte Implementierung von studiengangsübergreifenden Prozessen wird vom Dezernat Qualitätsmanagement und Organisationsentwicklung zentral gesteuert. Eine zuletzt 2015 umfassend überarbeitete Qualitäts- sowie eine Evaluationssatzung setzen dabei einen hochschulweit verbindlichen normativen Rahmen, der von den Sektionen weitgehend eigenverantwortlich ausgefüllt wird.

Die Gutachter stellen fest, dass einer auch für die zur Akkreditierung beantragten konsekutive Masterstudiengänge charakteristischen Vernetzung des Lehrangebots verschiedener Organisationseinheiten, durch institutionalisierte Abstimmungsprozesse entsprochen wird. Monatliche Treffen des „Ausschusses Lehre“ (Studiengangsleiter, Qualitätsmanagement, Justizariat, Verwaltung) und der Studiengangskoordinatoren erscheinen den Auditoren als geeignet, eine sachgerechte Koordination des Studienangebots zwischen den verschiedenen Organisationseinheiten zu unterstützen.

Sämtliche Lehrveranstaltungen werden jedes Semester mit einem standardisierten Fragebogen evaluiert. Koordiniert werden die Befragungen seit Januar 2016 auf zentraler Ebene vom Dezernat für Qualitätsmanagement und Organisationsentwicklung. In allen MINT-Studiengängen findet die Evaluation nach zwei Dritteln des Semesters statt. Die Dozenten erhalten die Auswertung für ihre jeweilige Lehrveranstaltung bis anderthalb Wochen vor Ende der Vorlesungszeit, eine anschließende Rückkopplung mit den Studierenden ist standardmäßig vorgesehen. Die Ergebnisse der Erhebungen werden in Evaluationsberichten gebündelt und im Senatsausschuss Lehre vorgestellt. Verbesserungsmaß-

nahmen auf der Ebene einzelner Lehrveranstaltungen, werden zudem zwischen Vertretern der Fachschaft, dem Studiendekan und dem Sektionsvorsitzenden diskutiert und notwendigenfalls zusammen mit dem betroffenen Dozenten implementiert. Die befragten Studierenden bezeichnen dieses System als funktional; in der Regel nehmen sich die Dozenten hier geäußerte Kritik zu Herzen. Verbesserungen der Lehre aufgrund von Evaluationsergebnissen werden bestätigt.

Zusätzlich zur Lehrevaluationen finden regelmäßig Erstsemesterbefragungen statt. Auch die Absolventen werden standardmäßig zu ihrem Verbleib nach Studienabschlussbefragt und um eine retrospektive Einschätzung des abgeschlossenen Studiengangs gebeten.

Studienverlaufsanalysen werden durchgeführt und dem Eindruck nach interpretiert und für eine kontinuierliche Verbesserung der Studierbarkeit genutzt.

Die Gutachter bewerten das Qualitätsmanagementkonzept zusammenfassend überwiegend positiv. Die vorgefundenen Strukturen und Prozesse sind ihrer Meinung nach dazu geeignet, strukturelle Probleme frühzeitig zu erkennen. Die erhobenen Daten werden dem Anschein nach in der Regel dann auch sinnvoll für eine beständige Verbesserung der Qualität von Studium und Lehre genutzt.

Insgesamt begrüßen die Studierenden die Einführung der neukonzipierten Studiengänge IT-Sicherheit und Robotik und Autonome Systeme. In Bezug auf die studentische Beteiligung an der Entwicklung neuer Studiengänge bemerken sie allerdings, dass sie erst eingebunden wurden, als das Konzept und insbesondere die Modulabfolge bereits feststanden. Die Programmverantwortlichen erläutern, dass die Studierenden viel stärker als zuvor an der Entwicklung der neuen Studiengänge beteiligt wurden und können diese Kritik nicht nachvollziehen. Die Gutachter nehmen dies zur Kenntnis und weisen daraufhin, dass die Studierenden zukünftig an der kontinuierlichen Weiterentwicklung der Studiengänge zu beteiligen sind.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.9:

Die Gutachter bewerten das Kriterium als erfüllt, empfehlen dennoch die Studierenden kontinuierlich an der (Weiter)-Entwicklung der Studiengänge zu beteiligen.

Kriterium 2.10 Studiengänge mit besonderem Profilspruch

Nicht relevant.

Kriterium 2.11 Geschlechtergerechtigkeit und Chancengleichheit

Evidenzen:

- Selbstbericht der Hochschule
- Portal Chancengleichheit und Familie: <https://www.uni-luebeck.de/universitaet/chancengleichheit-und-familie.html> (Zugriff am 17.04.2016)

Vorläufige Analyse und Bewertung der Gutachter:

Die Hochschule führt aus, dass sie die Strategie der Verankerung von Gleichstellung als einer Querschnittsaufgabe der gesamten Organisation verfolgt und dies auch entsprechend umsetzt. Dafür erhielt sie 2011 und 2014 das Prädikat TOTAL E-QUALITY (TEQ) der Initiative TOTAL E-QUALITY Deutschland e. V. und wird sich 2017 erneut dafür bewerben. Die Hochschule verfügt über eine hauptamtliche Gleichstellungsbeauftragte, den zentralen Gleichstellungsausschuss und die Frauenbeauftragte, welche für eine angemessene Umsetzung der Gleichstellung von Frauen und Männern sorgen.

Des Weiteren bietet die Universität zu Lübeck ein umfangreiches Angebot für Studierende in besonderen Lebenslagen. Die Hochschule nimmt 2016 am Diversity-Audit „Vielfalt gestalten“ teil. Im Rahmen des Audits soll in den nächsten Jahren ein umfangreiches, auf die Universität zu Lübeck zugeschnittenes Diversity-Management-Konzept aufgebaut werden, damit die Studierenden ihre individuellen Potentiale noch besser entfalten können. Des Weiteren wurde 2009 das Netzwerktreffen InformatiXX für Informatikstudentinnen der Universität initiiert. Im Zentrum stehen die gezielte Kontaktförderung zwischen den Studentinnen und Weiterbildungsmöglichkeiten durch fachspezifische Workshops oder Workshops zur Förderung sogenannter Soft Skills. Die Universität zu Lübeck versucht ebenso die Rahmenbedingungen zur besseren Vereinbarkeit von Studium/Beruf mit Familie für alle Studierenden beziehungsweise Beschäftigten zu verbessern und erhielt bereits mehrfach das Zertifikat „Familiengerechte Hochschule“. Für ausländische Studierende und Studierende mit Migrationshintergrund bzw. Flüchtlinge gibt es auf den Webseiten der Hochschule Beratungs- und Betreuungsangebote.

Die Gutachter können erkennen, dass die Hochschule angemessene Maßnahmen im Bereich des Diversity Managements zur Verfügung stellt.

Zur Berücksichtigung der Belange der Studierenden sind die betreffenden Ausführungen zu Kriterium 2.4 zu vergleichen.

Abschließende Bewertung der Gutachter nach Stellungnahme der Hochschule zum Kriterium 2.11:

Die Gutachter bewerten das Kriterium als vollständig erfüllt.

D Nachlieferungen

Um im weiteren Verlauf des Verfahrens eine abschließende Bewertung vornehmen zu können, bitten die Gutachter um die Ergänzung bislang fehlender oder unklarer Informationen im Rahmen von Nachlieferungen gemeinsam mit der Stellungnahme der Hochschule zu den vorangehenden Abschnitten des Akkreditierungsberichtes:

1. Ma Robotics and Autonome Systeme: Musterstudienpläne inkl. der Anzahl der Prüfungen pro Semester jeweils für Studierende die im SoSe und WS beginnen

E Nachtrag/Stellungnahme der Hochschule (17.05.2016)

Die Hochschule legt eine ausführliche Stellungnahme sowie folgende Dokumente vor:

- Ma Robotics and Autonome Systeme: Musterstudienpläne inkl. der Anzahl der Prüfungen pro Semester jeweils für Studierende die im SoSe und WS beginnen
- Überarbeitete Modulbeschreibungen
- Ba IT-Sicherheit: Überarbeitetes Curriculum

F Zusammenfassung: Empfehlung der Gutachter (23.05.2016)

Die Gutachter geben folgende Beschlussempfehlung zur Vergabe des beantragten Siegels:

Studiengang	Siegel Akkreditierungs- rat (AR)	Akkreditierung bis max.
Ba IT-Sicherheit	Mit Auflagen	30.09.2021
Ma IT-Sicherheit	Mit Auflagen	30.09.2021
Ba Robotik und Auto- nome Systeme	Mit Auflagen	30.09.2021
Ma Robotik und Auto- nome Systeme	Mit Auflagen	30.09.2021

Auflagen

Für alle Studiengänge

- A 1. (AR 2.3) Die Regelung zur Anerkennung von an anderen Hochschulen erbrachten Studienleistungen muss hinsichtlich der vorgesehenen Einschränkung mit den Anforderungen der Lissabon-Konvention in Einklang gebracht werden.
- A 2. (AR 2.8) Die in Kraft gesetzten Ordnungen für die Studiengänge sind vorzulegen.

Empfehlungen

Für alle Studiengänge

- E 1. (AR 2.7) Es wird empfohlen, die räumlichen Kapazitäten für Übungen/Laborpraktika sowie im Hinblick auf die Studierendenarbeitsplätze zu erweitern.
- E 2. (AR 2.9) Es wird empfohlen, die Studierenden kontinuierlich an der (Weiter-)Entwicklung der Studiengänge zu beteiligen.

Für Ba IT-Sicherheit

- E 3. (AR 2.3) Es wird empfohlen, nach der Besetzung der Professur für IT-Sicherheit das Angebot im Bereich sichere Software noch einmal zu überarbeiten.

Für die Bachelorstudiengänge IT-Sicherheit und Robotik und Autonome Systeme

E 4. (AR 2.3) Es wird empfohlen, fachbezogene englische Sprachkompetenz der Studierenden systematischer zu fördern.

Für die Masterstudiengänge

E 5. (AR 2.3) Es wird empfohlen, die für das jeweilige Masterstudienprogramm vorausgesetzten Kenntnisse, Kompetenzen und Fertigkeiten (anerkannte Bachelorabschlüsse) für Studieninteressierte transparent zu gestalten.

Für den Masterstudiengang Robotics und Autonome Systeme

E 6. (AR 2.4) Es wird empfohlen, die studentische Prüfungsbelastung gleichmäßiger auf die ersten beiden Fachsemester zu verteilen.

G Stellungnahme der Fachausschüsse

Fachausschuss 04 – Informatik (09.06.2016)

Analyse und Bewertung

Der Fachausschuss diskutiert das Verfahren. Er empfiehlt die Empfehlung 4 zu streichen, da es in der Eigenverantwortung der Studierenden liegt, Defizite während des Bachelorstudiums auszugleichen, wenn sie ein englischsprachiges Masterstudienprogramm anschließen möchten. Das Sprachzentrum der Hochschule bietet diese Möglichkeit.

Bezüglich der Auflagen und anderen Empfehlungen schließt sich der Fachausschuss den Gutachtern an.

Der Fachausschuss 04 – Informatik empfiehlt die Siegelvergabe für die Studiengänge wie folgt:

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba IT-Sicherheit	Mit Auflagen	30.09.2021
Ma IT-Sicherheit	Mit Auflagen	30.09.2021

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba Robotik und Autonome Systeme	Mit Auflagen	30.09.2021
Ma Robotik und Autonome Systeme	Mit Auflagen	30.09.2021

Auflagen

Für alle Studiengänge

- A 1. (AR 2.3) Die Regelungen zur Anerkennung von an anderen Hochschulen erbrachten Leistungen müssen der Lissabon-Konvention entsprechen.
- A 2. (AR 2.8) Die in Kraft gesetzten Ordnungen für die Studiengänge sind vorzulegen.

Empfehlungen

Für alle Studiengänge

- E 1. (AR 2.7) Es wird empfohlen, die räumlichen Kapazitäten für Übungen/Laborpraktika sowie im Hinblick auf die Studierendenarbeitsplätze zu erweitern.
- E 2. (AR 2.9) Es wird empfohlen, die Studierenden kontinuierlich an der (Weiter-)Entwicklung der Studiengänge zu beteiligen.

Für Ba IT-Sicherheit

- E 3. (AR 2.3) Es wird empfohlen, nach der Besetzung der Professur für IT-Sicherheit das Angebot im Bereich sichere Software noch einmal zu überarbeiten.

Für die Masterstudiengänge

- E 4. (AR 2.3) Es wird empfohlen, die für das jeweilige Masterstudienprogramm vorausgesetzten Kenntnisse, Kompetenzen und Fertigkeiten (anerkannte Bachelorabschlüsse) für Studieninteressierte transparent zu gestalten.

Für den Masterstudiengang Robotics und Autonome Systeme

- E 5. (AR 2.4) Es wird empfohlen, die studentische Prüfungsbelastung gleichmäßiger auf die ersten beiden Fachsemester zu verteilen.

Fachausschuss 02 – Elektro-/Informationstechnik (17.06.2016)

Analyse und Bewertung

Der Fachausschuss diskutiert das Verfahren. Er schlägt eine Ergänzung der Empfehlung 4 (IT-Sicherheit) vor, um zu verdeutlichen, dass mit dem Sicherheitsthema hier speziell die Manipulationssicherheit der Software im Unterschied zu ihrer funktionalen Sicherheit gemeint ist.

Im Übrigen folgt der Fachausschuss der Beschlussempfehlung der Gutachter.

Der Fachausschuss FA 02 - Elektro-/Informationstechnik empfiehlt die Siegelvergabe für die Studiengänge wie folgt:

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba Robotik und Autonome Systeme	Mit Auflagen	30.09.2021
Ma Robotik und Autonome Systeme	Mit Auflagen	30.09.2021

Auflagen

Für alle Studiengänge

- A 1. (AR 2.3) Die Regelung zur Anerkennung von an anderen Hochschulen erbrachten Studienleistungen muss hinsichtlich der vorgesehenen Einschränkung mit den Anforderungen der Lissabon-Konvention in Einklang gebracht werden.
- A 2. (AR 2.8) Die in Kraft gesetzten Ordnungen für die Studiengänge sind vorzulegen.

Empfehlungen

Für alle Studiengänge

- E 1. (AR 2.7) Es wird empfohlen, die räumlichen Kapazitäten für Übungen/Laborpraktika sowie im Hinblick auf die Studierendenarbeitsplätze zu erweitern.
- E 2. (AR 2.9) Es wird empfohlen, die Studierenden kontinuierlich an der (Weiter-)Entwicklung der Studiengänge zu beteiligen.

Für Ba IT-Sicherheit

- E 3. (AR 2.3) Es wird empfohlen, nach der Besetzung der Professur für IT-Sicherheit das Angebot im Bereich Sichere Software mit Blick auf die Themen Risikoanalyse, IT-Sicherheitsmanagement, Softwaresicherheit und IT-Recht noch einmal zu überprüfen und ggf. zu verbessern.

Für die Bachelorstudiengänge IT-Sicherheit und Robotik und Autonome Systeme

- E 4. (AR 2.3) Es wird empfohlen, die fachbezogene englische Sprachkompetenz der Studierenden systematischer zu fördern.

Für die Masterstudiengänge

- E 5. (AR 2.3) Es wird empfohlen, die für das jeweilige Masterstudienprogramm vorausgesetzten Kenntnisse, Kompetenzen und Fertigkeiten (anerkannte Bachelorabschlüsse) für Studieninteressierte transparent zu gestalten.

Für den Masterstudiengang Robotics und Autonome Systeme

- E 6. (AR 2.4) Es wird empfohlen, die studentische Prüfungsbelastung gleichmäßiger auf die ersten beiden Fachsemester zu verteilen.

H Beschluss der Akkreditierungskommission (01.07.2016)

Analyse und Bewertung

Die Akkreditierungskommission für Studiengänge diskutiert das Verfahren.

Da die nach wie vor gültige Interpretation der Lissabon-Konvention eine Beschränkung der Anerkennung von an anderen Hochschulen erbrachten Studien- und Prüfungsleistungen untersagt, bekräftigt das Gremium weiterhin ausdrücklich die diesbezügliche Auflage 1. Da im Fall der Universität zu Lübeck die Anerkennung auf 50% begrenzt wird, ist diese Auflage im Einklang mit dem Beschluss der 85. Sitzung des Akkreditierungsrats nicht auszusetzen.

In Übereinstimmung mit Gutachtern und dem Fachausschuss 02 – Elektro-/Informationstechnik empfiehlt die Akkreditierungskommission für Studiengänge, die

fachbezogene englische Sprachkompetenz der Studierenden in den Bachelorstudiengänge IT-Sicherheit und Robotik und Autonome Systeme systematischer zu fördern, da die Universität ein englischsprachiges konsekutives Masterprogramm anbietet. Durch die fachbezogene Sprachförderung gewährleistet die Hochschule eine angemessene Vorbereitung der zukünftigen Studierenden auf das konsekutive Masterprogramm.

Unter Berücksichtigung der vom Fachausschuss 02 – Elektro-/Informationstechnik vorgeschlagenen redaktionellen Änderung stimmt die Akkreditierungskommission für Studiengänge der Beschlussempfehlung der Gutachter in allen Punkten zu.

Die Akkreditierungskommission für Studiengänge beschließt folgende Siegelvergabe:

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba IT-Sicherheit	Mit Auflagen	30.09.2021
Ma IT-Sicherheit	Mit Auflagen	30.09.2021
Ba Robotik und Autonome Systeme	Mit Auflagen	30.09.2021
Ma Robotik und Autonome Systeme	Mit Auflagen	30.09.2021

Auflagen

Für alle Studiengänge

- A 1. (AR 2.3) Die Regelung zur Anerkennung von an anderen Hochschulen erbrachten Studienleistungen muss hinsichtlich der vorgesehenen Einschränkung mit den Anforderungen der Lissabon-Konvention in Einklang gebracht werden.
- A 2. (AR 2.8) Die in Kraft gesetzten Ordnungen für die Studiengänge sind vorzulegen.

Empfehlungen

Für alle Studiengänge

- E 1. (AR 2.7) Es wird empfohlen, die räumlichen Kapazitäten für Übungen/Laborpraktika sowie im Hinblick auf die Studierendenarbeitsplätze zu erweitern.
- E 2. (AR 2.9) Es wird empfohlen, die Studierenden kontinuierlich an der (Weiter-)Entwicklung der Studiengänge zu beteiligen.

Für Ba IT-Sicherheit

- E 3. (AR 2.3) Es wird empfohlen, nach der Besetzung der Professur für IT-Sicherheit das Angebot im Bereich Sichere Software mit Blick auf die Themen Risikoanalyse, IT-Sicherheitsmanagement, Softwaresicherheit und IT-Recht noch einmal zu überprüfen und ggf. zu verbessern.

Für die Bachelorstudiengänge IT-Sicherheit und Robotik und Autonome Systeme

- E 4. (AR 2.3) Es wird empfohlen, die fachbezogene englische Sprachkompetenz der Studierenden systematischer zu fördern.

Für die Masterstudiengänge

- E 5. (AR 2.3) Es wird empfohlen, die für das jeweilige Masterstudienprogramm vorausgesetzten Kenntnisse, Kompetenzen und Fertigkeiten (anerkannte Bachelorabschlüsse) für Studieninteressierte transparent zu machen.

Für den Masterstudiengang Robotics und Autonome Systeme

- E 6. (AR 2.4) Es wird empfohlen, die studentische Prüfungsbelastung gleichmäßiger auf die ersten beiden Fachsemester zu verteilen.

I Erfüllung der Auflagen (30.06.2017)

Bewertung der Gutachter

Die Gutachter kommen zu folgender Einschätzung der Auflagenerfüllung:

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba Robotik und Autonome Systeme	Alle Auflagen erfüllt	30.09.2021
Ma IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021
Ma Robotics and Autonomous Systems	Alle Auflagen erfüllt	30.09.2021

Bewertung des Fachausschusses 04 (21.06.2017)

Der Fachausschuss kommt zu folgender Einschätzung der Auflagenerfüllung:

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021
Ba Robotik und Autonome Systeme	Alle Auflagen erfüllt	30.09.2021
Ma IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021
Ma Robotics and Autonomous Systems	Alle Auflagen erfüllt	30.09.2021

Bewertung des Fachausschusses 02 (21.06.2017)

Der Fachausschuss kommt zu folgender Einschätzung der Auflagenerfüllung:

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021
Ba Robotik und Autonome Systeme	Alle Auflagen erfüllt	30.09.2021
Ma IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021
Ma Robotics and Autonomous Systems	Alle Auflagen erfüllt	30.09.2021

Beschluss der Akkreditierungskommission (30.06.2017)

Die Akkreditierungskommission für Studiengänge beschließt, die Siegelvergabe wie folgt zu verlängern:

Studiengang	Siegel Akkreditierungsrat (AR)	Akkreditierung bis max.
Ba IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021
Ba Robotik und Autonome Systeme	Alle Auflagen erfüllt	30.09.2021
Ma IT-Sicherheit	Alle Auflagen erfüllt	30.09.2021
Ma Robotics and Autonomous Systems	Alle Auflagen erfüllt	30.09.2021

Anhang: Lernziele und Curricula

Gem. Studiengangsordnung sollen mit dem Bachelorstudiengang IT-Sicherheit folgende **Lernergebnisse** erreicht werden:

(1) Die Ausbildung im Bachelorstudium IT-Sicherheit bereitet die Absolventinnen und Absolventen auf Tätigkeiten in anwendungs-, entwicklungs-, lehr- und forschungsbezogenen Berufsfeldern der IT-Sicherheit und Zuverlässigkeit von IT-Systemen sowie auf die Aufnahme eines weiterführenden Studiums vor.

(2) Die Ausbildung verfolgt das Ziel, die Studierenden durch Vermittlung von Kenntnissen und Einübung von Fertigkeiten in den Stand zu setzen, vielfältige Probleme der Sicherheit und Zuverlässigkeit informationstechnischer Systeme aufzugreifen und zu lösen.

(3) Die Fähigkeit, sich auf wechselnde Aufgabengebiete und Anwendungsgebiete einstellen zu können, ist dabei unerlässlich. Das Studium umfasst dazu eine breite, grundlagenorientierte Ausbildung in Informatik sowie eine fachbezogene Ausbildung in IT-Sicherheit und Zuverlässigkeit. Das zentrale Thema des Bachelorstudiengangs IT-Sicherheit ist die Konstruktion sicherer und zuverlässiger informationsverarbeitender Systeme für allgemeine und spezielle Anwendungen. Dies umfasst die Modellierung der Anwendungsanforderungen, den Entwurf und die Analyse von Verfahren zur Lösung der gestellten Aufgabe, die Entwicklung von Datenstrukturen und Algorithmen, deren Implementierung in Software und Hardware, sowie den Nachweis dafür, dass so konstruierte Systeme die gestellten Anforderungen erfüllen. Ebenfalls im Kern des Studiums steht der Erwerb von Fähigkeiten zur Analyse von Sicherheitsschwachstellen existierender informationstechnischer Systeme und zur Behebung dieser Schwachstellen. Für das Gespräch mit Anwenderinnen und Anwendern als deren Partnerin oder Partner bei der Lösung von sicherheitsrelevanten Fragestellungen bzw. grundsätzlich beim Entwurf und der Realisierung sicherer und zuverlässiger IT-Systeme müssen die Absolventinnen und Absolventen vor allem in der Lage sein, in der Fachsprache eines Anwendungsgebiets abgefasste Aufgabenstellungen sachgemäß so zu formulieren, dass diese mit Hilfe von IT-Systemen behandelt werden können.

(4) Die Ausbildung erfolgt in Vorbereitung auf eine künftige interdisziplinäre Arbeit in der Praxis sowie in Vorbereitung eines weiterführenden Studiums.

(5) Durch die Ausprägung der Lehrmodule wird während des gesamten Curriculums die Vermittlung von Fachwissen eng mit der Vermittlung von Querschnittskompetenzen verknüpft.

Hierzu legt die Hochschule folgendes **Curriculum** vor:

1. Semester (30 KP)	2. Semester (30 KP)	3. Semester (30 KP)	4. Semester (30 KP)	5. Semester (29 KP)	6. Semester (31 KP)
CS1700-KP04 Einführung in IT-Sicherheit und Zuverlässigkeit 4 KP (2V+1Ü)	CS3050-KP04 Codierung und Sicherheit 4 KP (2V+1Ü)	CS2250-KP08 Cybersecurity 8 KP (2V+1Ü+2P)	CS2550-KP08 Sichere Netze und Computerforensik 8 KP (4V+2Ü)		CS4172-KP04 Zuverlässigkeit von Rechensystemen 4 KP (2V+1Ü)
CS1000-KP10 Einführung in die Programmierung 10 KP (3V+3Ü+2P)	CS1001-KP08 Algorithmen und Datenstrukturen 8 KP (4V+2Ü)	CS2300-KP06 Software Engineering 6 KP (3V+1Ü)	CS3420-KP04 Kryptologie 4 KP (2V+1Ü)	CS3250-KP08 Sichere Software 8 KP (4V+2Ü)	CS3993-KP15 Bachelorarbeit IT-Sicherheit 15 KP
	CS1200-KP06 Technische Grundlagen der Informatik 1 6 KP (2V+2Ü)		CS2100-KP04 Rechnerarchitektur 4 KP (2V+1Ü)		
MA1000-KP08 Lineare Algebra und Diskrete Strukturen 1 8 KP (4V+2Ü)	MA1500-KP08 Lineare Algebra und Diskrete Strukturen 2 8 KP (4V+2Ü)	CS1002-KP04 Einführung in die Logik 4 KP (2V+1Ü)	CS2150-KP08 Betriebssysteme und Netze 8 KP (4V+2Ü)	CS3000-KP04 Algorithmendesign 4 KP (2V+1Ü)	
MA2000-KP08 Analysis 1 8 KP (4V+2Ü)		CS2000-KP08 Theoretische Informatik 8 KP (4V+2Ü)		CS3702-KP04 Bachelor-Seminar IT-Sicherheit 4 KP (2S)	
	MA2510-KP04 Stochastik 1 4 KP (2V+1Ü)	Allg. Wahl 4 KP	CS2700-KP04 Datenbanken 4 KP (2V+1Ü)	CS3701-KP05 Bachelor-Projekt IT-Sicherheit 5 KP (3P)	
					Wahlmodul 2 4 KP
					Wahlmodul 3 4 KP
4 Prüfungen	5 Prüfungen	4 Prüfungen	4 Prüfungen	4 Prüfungen	5 Prüfungen
Semesterwochenstunden: Vorlesung / Übung / Praktikum / Seminar					
Pflichtmodul Bereich IT-Sicherheit		Pflichtmodul Bereich Informatik	Pflichtmodul Bereich Mathematik	Wahlpflicht (fachspezifisch)	Wahlbereich (disziplinübergreifend)

Gem. Studiengangsordnung sollen mit dem **Masterstudiengang IT-Sicherheit** folgende **Lernergebnisse** erreicht werden:

(1) Das Masterstudium bereitet die Absolventinnen und Absolventen auf Tätigkeiten im Bereich der IT-Sicherheit und Zuverlässigkeit in forschungs-, lehr-, entwicklungs- und anwendungsbezogenen Berufsfeldern vor.

(2) Das Ziel der Ausbildung im Masterstudiengang IT-Sicherheit besteht darin, die Studierenden durch Vermittlung von wissenschaftlichen Methoden und Modellen sowie Einübung von Fertigkeiten der IT-Sicherheit und Zuverlässigkeit in die Lage zu versetzen, vielfältige Probleme der sicheren und zuverlässigen Informationsverarbeitung zu verstehen

und zu bearbeiten. Gegenstand des Studiengangs ist die Analyse, Beschreibung, Konstruktion und Validierung von informationsverarbeitenden Systemen, insbesondere unter dem Aspekt der Sicherheit und Zuverlässigkeit. Dabei liegt im Gegensatz zum Bachelorstudiengang die Betonung auf dem Erwerb von Fähigkeiten für wissenschaftliches Arbeiten. Die Ausbildung trägt dem durch ein grundlagenorientiertes, sowohl breites als auch vertiefendes Studium Rechnung und soll die Voraussetzung für ein lebenslanges Lernen im Bereich der Informatik und spezieller der sicheren und zuverlässigen IT-Systeme sowie für eine weitergehende akademische Qualifikation wie z.B. die Promotion schaffen. Weiterhin sollen die Studierenden aufgrund der von ihnen erworbenen Kompetenzen in der Lage sein, Leitungsfunktionen in der Wirtschaft zu übernehmen.

(3) Der Masterstudiengang IT-Sicherheit ist forschungsorientiert und konsekutiv zum Bachelorstudiengang IT-Sicherheit der Universität zu Lübeck aufgebaut. Von den Studierenden wird als Voraussetzung erwartet, dass sie bereits Wissen, Fertigkeiten und Kompetenzen im Bereich der IT-Sicherheit und Zuverlässigkeit in Umfang und Tiefe besitzen, wie es im Bachelorstudiengang vermittelt wird.

Hierzu legt die Hochschule folgendes **Curriculum** vor:

1. Semester (30 KP)	2. Semester (30 KP)	3. Semester (30 KP)	4. Semester (30 KP)
Wahlpflichtbereich Security und Privacy 6 KP	Wahlpflichtbereich Security und Privacy 6 KP	Wahlpflichtbereich Security und Privacy 6 KP	CS5993-KP30 Masterarbeit IT-Sicherheit 30 KP
Basismodul Praktische Informatik 6 KP	Wahlpflichtbereich Software Safety oder System Reliability 6 KP	Wahlpflichtbereich Software Safety oder System Reliability 6 KP	
Basismodul Technische Informatik 6 KP	Vertiefungsmodul 12 KP		
CS4000-KP06 Algorithmik (WS) oder CS4020-KP06 Spezifikation und Modellierung (SS) 6 KP (2V+2Ü)	CS4000-KP06 Algorithmik (WS) oder CS4020-KP06 Spezifikation und Modellierung (SS) 6 KP (2V+2Ü)	CS5195-KP08 Aktuelle Themen IT-Sicherheit 8 KP (4P+3S)	
CS4421-KP12 Fallstudie IT-Sicherheit 12 KP (2S+6P)		Wahlmodul 4 KP	
4 Prüfungen	3 Prüfungen	4 Prüfungen	
Semesterwochenstunden: Vorlesung / Übung / Praktikum / Seminar			KP: Kreditpunkte / ECTS-Punkte
Pflichtmodul Bereich IT-Sicherheit		Pflichtmodul Bereich Informatik	Wahlbereich (fächerübergreifend)

Gem. Studiengangsordnung sollen mit dem **Bachelorstudiengang Robotik und Autonome Systeme** folgende **Lernergebnisse** erreicht werden:

(1) Die Ausbildung im Bachelorstudium Robotik und Autonome Systeme bereitet die Absolventinnen und Absolventen auf ingenieurmäßige Tätigkeiten in anwendungs-, herstellungs-, lehr- und forschungsbezogenen Berufsfeldern sowie auf die Aufnahme eines weiterführenden Studiums vor.

(2) Die Ausbildung verfolgt das Ziel, die Studierenden durch Vermittlung von fundierten und anwendungsorientierten Kenntnissen in den verschiedenen Teilgebieten der Robotik und autonomen Systeme in den Stand zu setzen, selbstständige Analyse-, Konzeptionierungs- und Entwicklungsfähigkeiten in den verschiedenen Bereichen der (teil-)autonomen Systeme und der Robotik zu erwerben. Die Fähigkeit, sich mit Hilfe eines hinreichend breiten mathematisch, technischen Grundlagenwissens auf wechselnde Aufgabengebiete einstellen zu können, ist dabei unerlässlich. Das Studium umfasst daher eine grundlagenorientierte Ausbildung in den Bereichen Technik, Informatik und Mathematik ergänzt durch praktische Umsetzungen sowie eine fachbezogene Ausbildung. Die zentralen Themen des Bachelorstudiums Robotik und Autonome Systeme sind die Analyse, der Entwurf und die Konstruktion von autonomen und teilautonomen Systemen aus den verschiedenen Bereichen der Robotik und Mechatronik. Dies umfasst die Modellierung der Anwendungsanforderungen, den Entwurf und die Analyse von Verfahren zur Lösung der gestellten Aufgaben, die Entwicklung von Algorithmen, Schaltungen und mechanischen Konstruktionen sowie deren Implementierung in Software und Hardware inklusive einer anschließenden Verifikation und Validierung. Die Vermittlung der zugrundeliegenden Konzepte steht dabei ebenso im Vordergrund, wie die Fähigkeit, im Gespräch mit Anwenderinnen und Anwendern als deren Partnerin oder Partner Anforderungen an das zu entwickelnde System herauszuarbeiten und auf dieser Basis eine geeignete Lösung des Problems zu erarbeiten und umzusetzen.

(3) Die Fähigkeit, sich auf wechselnde Aufgabengebiete und Anwendungsgebiete einstellen zu können, ist dabei unerlässlich. Der Bachelorstudiengang Robotik und Autonomen Systeme trägt dem durch die Kombination einer breiten Grundlagenausbildung mit konkreten, praktischen Projekten Rechnung, wobei sowohl analytische als auch holistische Konzepte und Kenntnisse vertieft werden.

(4) Die Ausbildung erfolgt in Vorbereitung auf eine künftige interdisziplinäre Arbeit in der Praxis. Dazu müssen die Absolventinnen und Absolventen vor allem in die Lage versetzt werden, in den verschiedenen Fachsprachen der Einzeldisziplinen kommunizieren zu können, um auf diese Weise in fächerübergreifenden Teams zu arbeiten.

I Erfüllung der Auflagen (30.06.2017)

(5) Durch die Ausprägung der Lehrmodule wird während des gesamten Curriculums die Vermittlung von Fachwissen eng mit der Vermittlung von Querschnittskompetenzen verknüpft. In einem derart interdisziplinären Feld wie der Robotik kommt der Kommunikationsfähigkeit eine besondere Rolle zu. Diese wird, ebenso wie Eigenverantwortung, Lernbereitschaft und ergebnisorientiertes Handeln in Übungen, Seminaren und Praktika vertieft.

Hierzu legt die Hochschule folgendes **Curriculum** vor:

1. Semester (30 KP)	2. Semester (30 KP)	3. Semester (32 KP)	4. Semester (30 KP)	5. Semester (27 KP)	6. Semester (31 KP)
CS1500-KP04 Einführung in die Robotik u. Automation 4 KP (2V+1Ü)	RO1500-KP08 Technische Mechanik 8 KP (4V + 2Ü)		CS2110-KP04 Mobile Roboter 4 KP (2V+1Ü)	ME2151-KP04 Einführung in die Medizintechnik 4 KP (2V + 1Ü)	CS3204-KP04 Künstliche Intelligenz 1 4 KP (2V + 1Ü)
CS1000-KP10 Einführung in die Programmierung 10 KP (3V + 3Ü + 2P)	CS1001-KP08 Algorithmen und Datenstrukturen 8 KP (4V + 2Ü)	CS2500-KP04 Robotik 4 KP (2V + 1Ü)	ME2700-KP08 Grundlagen der Elektrotechnik 2 8 KP (4V + 2Ü)	CS3501-KP04 Praktikum Robotik & Automation 4 KP (3P)	ME2450-KP08 Regelungstechnik und Mechatronik 8 KP (4V + 2Ü)
	CS1200-KP06 Technische Grundlagen der Informatik 1 6 KP (2V + 2Ü)	CS1202-KP06 Technische Grundlagen der Informatik 2 6 KP (2V + 2Ü)		CS3100-KP08 Signalverarbeitung 8 KP (4V + 2Ü)	Wahlpflicht 2 4 KP
MA1000-KP08 Lin. Algebra u. Disk. Strukturen 1 8 KP (4V + 2Ü)	MA1500-KP08 Lin. Algebra u. Disk. Strukturen 2 8 KP (4V + 2Ü)	ME2400-KP08 Grundlagen der Elektrotechnik 1 8 KP (4V + 2Ü)	CS2301-KP06 Praktikum SW-Engineering 6 KP (4P)	Wahlpflicht 1 4 KP	CS3990-KP15 Bachelorarbeit Robotik mit Kolloquium 15 KP
MA2000-KP08 Analysis 1 8 KP (4V + 2Ü)	MA2500-KP04 Analysis 2 4 KP (2V + 1Ü)	CS2300-KP06 SW-Engineering 6 KP (3V + 1Ü)	CS2150-KP08 Betriebssysteme und Netze 8 KP (4V+2Ü)		
MA2510-KP04 Stochastik 1 4 KP (2V + 1Ü)	Wahlbereich 4 KP				
4 Prüfungen	4 Prüfungen	6 Prüfungen	5 Prüfungen	3 Prüfungen	4 Prüfungen
Semesterwochenstunden: Vorlesung / Übung / Praktikum / Seminar					
Pflichtmodul Robotik und Autonome Systeme		Pflichtmodul Informatik	Pflichtmodul Mathematik	Wahlbereich (fächerübergreifend)	Wahlpflicht (fachspezifisch)

Gem. Studiengangsordnung sollen mit dem **Masterstudiengang Robotics and Autonomous Systems** folgende **Lernergebnisse** erreicht werden:

(1) Das Masterstudium bereitet die Absolventinnen und Absolventen auf Tätigkeiten in forschungs-, lehr-, entwicklungs- und anwendungsbezogenen Berufsfeldern im Bereich der Robotik und Autonomen Systeme vor.

(2) Das Ziel der Ausbildung im Masterstudiengang Robotics and Autonomous Systems besteht darin, die Studierenden durch Vermittlung von wissenschaftlichen Methoden und Modellen sowie Einübung von Fertigkeiten der Mathematik, Informatik und Technik in den Stand zu versetzen, (teil-) autonome Systeme, insbesondere aus dem Bereich der Robotik aber auch der Automation und Medizin zu konzipieren, zu entwickeln und zu erforschen. Dabei liegt im Gegensatz zum Bachelorstudiengang die Betonung auf dem Erwerb von Fähigkeiten für weiterführendes wissenschaftliches Arbeiten. Die Ausbildung trägt dem durch ein grundlagenorientiertes, sowohl breites als auch vertiefendes Studium Rechnung und soll die Voraussetzungen für ein lebenslanges Lernen im Bereich der autonomen und teilautonomen Systeme, insbesondere der Robotik sowie für eine weitergehende akademische Qualifikation wie z.B. die Promotion schaffen. Weiterhin sollen die Studierenden aufgrund der von ihnen erworbenen Kompetenzen in der Lage sein, Leitungsfunktionen in der Wirtschaft zu übernehmen.

(3) Der Masterstudiengang Robotics and Autonomous Systems ist forschungsorientiert und konsekutiv zum Bachelorstudiengang Robotik und Autonome Systeme der Universität zu Lübeck aufgebaut. Von den Studierenden wird als Voraussetzung erwartet, dass sie bereits Wissen, Fertigkeiten und Kompetenzen im Bereich der Robotik und Autonomen Systeme in Umfang und Tiefe besitzen, wie es im Bachelorstudiengang vermittelt wird.

Hierzu legt die Hochschule folgendes **Curriculum** vor:

1. Semester (30 KP)	2. Semester (30 KP)	3. Semester (30 KP)	4. Semester (30 KP)
CS4271-KP08 Artificial Intelligence 2 and Medical Robotics 8 KP (4V+2Ü)			
RO4000-KP12 Autonomous Systems (Real-Time Systems, Control Engineering and System Dynamics) 12 KP (4V+4Ü)		RO5000-KP12 Internship Robotics and Autonomous Systems 1 12 KP (12P)	
CS4251-KP08 Machine Learning and Computer Vision 8 KP (4V + 2Ü)			
Advanced Course 12 KP		RO5001-KP12 Internship Robotics and Autonomous Systems 2 12 KP (12P)	RO5990-KP30 Master Thesis Robotics and Autonomous Systems 30 KP
Elective Courses 16 KP		PS5000-KP06 Student Conference 6 KP (4S)	
Interdisciplinary Field 4 KP			
10 Prüfungen*		3 Prüfungen	1 Prüfung
Semesterwochenstunden: Vorlesung / Übung / Praktikum / Seminar			KP: Kreditpunkte / ECTS-Punkte
Pflichtmodul Robotics und Autonomous Systems	Vertiefung	Wahlpflicht (fachspezifisch)	Wahlbereich (fächerübergreifend)