Modulhandbuch

Certificate of Advanced Studies Hochschule Niederrhein „Embedded Systems Professional“

Eingebettete Systeme innovativ und sicher realisieren -
Bausteine für das Internet der Dinge

Titel des Zertifikatsstudiums	Eingebettete Systeme innovativ und sicher realisieren – Bausteine für das Internet der Dinge
Fachbereich(e)	03 Informatik und Elektrotechnik
Modulverantwortliche/r	Akademische Leitung des Zentrums für Weiterbildung
Modultyp	Zertifikatsstudium der WWB
Dauer	Die Zertifikatskurse laufen über einen Zeitraum von ca. 6 Monaten.
Häufigkeit des Angebots	Voraussichtlich jährlich und auf Nachfrage (Inhouse)
Zielgruppe(n)	Das CAS „Embedded Systems Professional“ richtet sich an berufserfahrene Fach- und Führungskräfte aller Branchen, die in Anwendungsgebieten eingebetteter Systeme tätig sind oder sein werden. Sie sollten einen Hintergrund in Elektrotechnik, Informatik, Mechatronik oder verwandten Disziplinen haben: • Entwicklerinnen und Entwickler • Ingenieurinnen und Ingenieure • Systemarchitektinnen und -architekten • Technische Projekt- oder Teamleitungen • Produkt- und Prozessverantwortliche
Angestrebte Lernergebnisse/ Learning outcomes	Mit erfolgreichem Abschluss des Zertifikatsstudiums sind Teilnehmende in der Lage: • Herausforderungen eingebetteter Systeme (wie limitierte Schreibzyklen, lange Standzeiten oder Sicherheit) einzuschätzen und zu adressieren. • Geeignete Entwicklungsmethoden auszuwählen und zugehörige Entwicklungsumgebungen aufzusetzen. • Sicherheitskonzepte für eingebettete Systeme zu erstellen und umzusetzen. • Selbständig vernetzte eingebettete Systeme zu konzipieren, zu realisieren, zu testen und zu deployen. • Hard- und Softwarekomponenten für digitale Netze auszuwählen. • IoT-Kommunikationsnetze zu planen, zu implementieren und zu konfigurieren. • Aktuelle softwaretechnische Werkzeuge für eingebettete Systeme einzusetzen.
Aufbau	• Deeply Embedded mit FreeRTOS (3 ECTS) • Open Embedded mit Linux (3 ECTS) • IoT-Kommunikation (3 ECTS) • Embedded Security (3 ECTS) Zu den Inhalten der Zertifikatskurse siehe die Modulbeschreibungen.
Wahlmöglichkeiten	keine
Lehrformen	Die originäre Wissensvermittlung erfolgt in Form klassischer Seminare. Durch rechnergestützte praktische Übungen wird das Erlernte sofort praktisch erprobt, mit der Möglichkeit individuelle

	Fragen und Problemstellungen der Teilnehmenden zu bearbeiten. Vielfältiger Medieneinsatz und die Begleitung durch eine Online-Lehrplattform unterstützen den Lernerfolg. Anhand eines kursübergreifenden Fallbeispiels realisiert jede Teilnehmerin und jeder Teilnehmer ein verteiltes, eingebettetes System auf Basis bereitgestellter Hardware-Komponenten.
Unterrichtssprache	Deutsch
Prüfungsleistung(en)	Über die in den Modulbeschreibungen beschriebenen Prüfungsleistungen der einzelnen Zertifikatskurse hinaus gibt es keine zusätzliche Abschlussprüfung.
Leistungspunkte	12 ECTS

Modulbeschreibung „Deeply Embedded mit FreeRTOS“

Modultitel	Deeply Embedded mit FreeRTOS
Kürzel/Modulnummer	---
Fachbereich	03 Elektrotechnik und Informatik
Modulverantwortliche/r	Prof. Dr. Jens Brandt, jens.brandt@hs-niederrhein.de
Dozent/in	Prof. Dr. Jens Brandt, jens.brandt@hs-niederrhein.de
Modultyp	Hochschulzertifikatskurs der WWB
Dauer	Ca. 3 Termine in 2 Monaten
Häufigkeit des Angebots	Voraussichtlich jährlich und auf Nachfrage (Inhouse)
Zielgruppe(n)	Berufserfahrene Fach- und Führungskräfte aller Branchen, die in Anwendungsgebieten eingebetteter Systeme tätig sind oder sein werden. Sie sollten einen Hintergrund in Elektrotechnik, Informatik, Mechatronik oder verwandten Disziplinen haben: • Entwicklerinnen und Entwickler • Ingenieurinnen und Ingenieure • Systemarchitektinnen und -architekten • Technische Projekt- oder Teamleitungen • Produkt- und Prozessverantwortliche
Angestrebte Lernergebnisse/ Learning outcomes	Mit erfolgreichem Abschluss des Kurses werden die Teilnehmenden in der Lage sein: • Software für einfache eingebettete Systeme überschaubarer Komplexität zu entwerfen, indem Sie aktuelle softwaretechnische Methoden und Modelle für eingebettete Systeme einsetzen. • Software basierend auf einem solchen Entwurf zu realisieren, indem Sie ein RTOS nutzen, um Nebenläufigkeit eingebetteter Systeme zu beherrschen • Effektive Tests für diese erstellte Software durchzuführen, indem systematisch Testfälle abgeleitet werden, um die Funktionalität abzusichern
Inhalte	**Entwurf eingebetteter Software** • Besondere Anforderungen eingebetteter Systeme • Modelle: Datenfluss, Zustandsautomaten etc. • Entwurfsprinzipien und -muster für eingebettete Software **Realisierung eingebetteter Systeme mit FreeRTOS** • Bare Metal vs. RTOS • Tasks, Scheduling, Races, Deadlocks **Testen eingebetteter Systeme** • Auswahl und Spezifikation von Testfällen • Testen von Echtzeiteigenschaften • Automatisierung der Tests
Lehrformen	Die originäre Wissensvermittlung erfolgt in Form eines klassischen Seminars. Durch rechnergestützte praktische Übungen wird das Erlernte sofort praktisch erprobt, mit der Möglichkeit individuelle Fragen und Problemstellungen der Teilnehmenden zu bearbeiten. Die als Prüfungsleistung durchzuführende Projektarbeit festigt die theoretischen und praktischen Inhalte.
Unterrichtssprache	Deutsch

Teilnahmevoraussetzungen	Hochschulabschluss mit mindestens einjähriger Berufserfahrung oder anderweitiger berufsqualifizierender Abschluss mit mindestens dreijähriger Berufstätigkeit. Programmierkenntnisse (C)
Abschluss	Hochschulzertifikat (Prüfungsteilnahme) oder Teilnahmebescheinigung (75% Anwesenheit)
Prüfungsleistung(en)	Kursbegleitendes Fallbeispiel: Anhand konkreter Fragestellungen werden die Inhalte des Zertifikatskurses am Beispiel einer SmartHome-Alarmanlage umgesetzt. Dieses Modul realisiert dabei deren Sensoren, Aktoren und Signalgeber. Umfang 40 h.
Leistungspunkte	3 ECTS
Workload/Arbeitsaufwand	75 h Gesamtstunden
Präsenzzeit	24 h Präsenz
Selbststudium	51 h (Vor- und Nachbereitung, Erstellung von Projektarbeit)
Geplante Gruppengröße	Max. 12 Teilnehmende
Verwendbarkeit des Moduls	Für CAS Embedded Systems Professional
Literatur	Wird in der Veranstaltung bekannt gegeben.

Modulbeschreibung „Open Embedded mit Linux“

Modultitel	Open Embedded mit Linux
Kürzel/Modulnummer	---
Fachbereich	03 Elektrotechnik / Informatik
Modulverantwortlicher/	Prof. Dr. Jürgen Quade, juergen.quade@hs-niederrhein.de
Dozent/in	Prof. Dr. Jürgen Quade, juergen.quade@hs-niederrhein.de
Modultyp	Hochschulzertifikatskurs der WWB
Dauer	Ca. 3 Termine in 2 Monaten
Häufigkeit des Angebots	Voraussichtlich jährlich und auf Nachfrage (Inhouse)
Zielgruppe(n)	Berufserfahrene Fach- und Führungskräfte aller Branchen, die in Anwendungsgebieten eingebetteter Systeme tätig sind oder sein werden. Sie sollten einen Hintergrund in Elektrotechnik, Informatik, Mechatronik oder verwandten Disziplinen haben: • Entwicklerinnen und Entwickler • Ingenieurinnen und Ingenieure • Systemarchitektinnen und -architekten • Technische Projekt- oder Teamleitungen • Produkt- und Prozessverantwortliche
Angestrebte Lernergebnisse/ Learning outcomes	Mit erfolgreichem Abschluss des Kurses werden die Teilnehmenden in der Lage sein: • Vernetzte und verteilte eingebettete Systeme zu entwerfen. • Geeignete Hard- und Softwarekomponenten auszuwählen. • Cross-Entwicklungsumgebungen aufzusetzen, mit der eigene Linux-Systeme gebaut und getestet werden können. • Ein eigenes Linux-System (Kernel und Userland) zu realisieren und zu betreiben. • Anwendungen als eigenständige Appliances zu implementieren.
Inhalte	**Einführung** Klassisch versus embedded; Systemarchitekturen; Arbeiten mit Linux **Theorie** Eingebettete Systeme; Linux; Entwicklungsumgebungen **Handmade Linux** Kernel konfigurieren, generieren, installieren; Systemaufbau (Partitionieren, Filesystem anlegen, Verzeichnisstruktur erstellen etc.); Basisprogramme; Userland konfektionieren (Netzwerk, Standardaufgaben) **Targetplattform Raspberry Pi** Bootloader; Systemsoftware **Host-/Target- und Cross-Entwicklung** **Systembuilder (Buildroot)** Installation, Konfiguration und Systemgenerierung; Systemkonfiguration **Test** **Applikationsentwicklung** Cross-Entwicklung; Anwendungsintegration **Systemmanagement** User-Management; Dienste-Management; Remote-Zugriff **Betrieb von eingebetteten Systemen**

Lehrformen	Die originäre Wissensvermittlung erfolgt in Form eines klassischen Seminars. Durch rechnergestützte praktische Übungen wird das Erlernte sofort mit praktischen Erfahrungen verknüpft. Vielfältiger Medieneinsatz und die Begleitung mit einer Online-Lehrplattform unterstützen den Lernerfolg. Die Prüfung findet in Form einer selbständigen Projektarbeit statt.
Unterrichtssprache	Deutsch
Teilnahmevoraussetzungen	Hochschulabschluss mit mindestens einjähriger Berufserfahrung oder anderweitiger berufsqualifizierender Abschluss mit mindestens dreijähriger Berufstätigkeit. Programmierkenntnisse (C)
Abschluss	Hochschulzertifikat (Prüfungsteilnahme) oder Teilnahmebescheinigung (75% Anwesenheit)
Prüfungsleistung(en)	Kursbegleitendes Fallbeispiel: Anhand konkreter Fragestellungen werden die Inhalte des Zertifikatskurses am Beispiel einer SmartHome-Alarmanlage umgesetzt. Dieses Modul realisiert dabei die Alarmzentrale. Umfang 40 h.
Leistungspunkte	3 ECTS
Workload/Arbeitsaufwand	75 h
Präsenzzeit	24 h
Selbststudium	51 h (Vor- und Nachbereitung, Erstellung von Projektarbeit)
Geplante Gruppengröße	Max. 12 TN
Verwendbarkeit des Moduls	Für CAS Embedded Systems Professional
Literatur	J. Quade: Embedded Linux lernen mit dem Raspberry Pi. Dpunkt-Verlag 2014 Quade/Kunst: Linux-Treiber entwickeln. 4. Auflage, Dpunkt-Verlag 2016.

Modulbeschreibung „IoT-Kommunikation“

Modultitel	IoT-Kommunikation
Kürzel/Modulnummer	---
Fachbereich	03 Elektrotechnik und Informatik
Modulverantwortliche/r	Prof. Dr. Jens Brandt, jens.brandt@hs-niederrhein.de
Dozent/in	Prof. Dr. Tobias Frauenrath, frauenrath@fh-aachen.de
Modultyp	Hochschulzertifikatskurs der WWB
Dauer	Ca. 3 Termine in 2 Monaten
Häufigkeit des Angebots	Voraussichtlich jährlich und auf Nachfrage (Inhouse)
Zielgruppe(n)	Berufserfahrene Fach- und Führungskräfte aller Branchen, die in Anwendungsgebieten eingebetteter Systeme tätig sind oder sein werden. Sie sollten einen Hintergrund in Elektrotechnik, Informatik, Mechatronik oder verwandten Disziplinen haben: • Entwicklerinnen und Entwickler • Ingenieurinnen und Ingenieure • Systemarchitektinnen und -architekten • Technische Projekt- oder Teamleitungen • Produkt- und Prozessverantwortliche
Angestrebte Lernergebnisse/ Learning outcomes	Mit erfolgreichem Abschluss des Kurses werden die Teilnehmenden in der Lage sein: • Kommunikationstechnische Terminologie zu verstehen und anzuwenden. • Aus den vielfältigen Möglichkeiten der Hard- und Softwaresysteme digitaler Netze sowie drahtloser und drahtbasierender Netzwerke die individuell passende Lösung für die jeweilige Problemstellung auszuwählen. • Zukünftige Kommunikationsnetze im Hinblick auf spezifische Anforderungen (z. B. Ressourcenverbrauch, Durchsatz, Effizienz) zu planen und zu realisieren. • Industrie 4.0 Konzepte zu implementieren und zu evaluieren. • Verschiedene Protokolle hinsichtlich ihrer Eignung für unterschiedliche Einsatzgebiete in der Industrie, sowie im Bereich des SmartHomes zu vergleichen und auszuwählen.
Inhalte	1. Elementare Grundlagen der industriellen Kommunikationsnetze a. Schichtenmodelle der technischen Kommunikation (OSI-Referenzmodell, TCP/IP-Modell) b. Kommunikationsprotokolle und Standards c. Adressierungskonzepte d. Vermittlungsprinzipien 2. Kommunikation verteilter Systeme a. Übertragungsmedien b. Medienzugriffsverfahren c. Ethernet-Technologien 3. Protokolle und Technologien a. TCP/UDP b. WLAN, Bluetooth, Thread, ZigBee, z-wave, DECT c. Modbus, EtherCat, Profibus, Profinet d. MQTT, REST, COAP, LoRaWAN e. lwM2M, SNMP 4. Anwendungen a. Router und Router-Konfiguration b. Switches und Switch-Konfiguration

	c. Gateways d. Sensoren/Aktoren 5. Dimensionierung a. Bestimmung von IoT Anforderungen b. Qualitätssicherung in industriellen Netzen c. Zukunftssichere Auslegung von Netzen
Lehrformen	Die Wissensvermittlung erfolgt überwiegend in Form eines klassischen Seminars. Mithilfe realitätsnaher Übungen wird das Erlernte sofort praktisch erprobt, so dass die Möglichkeit besteht individuelle Fragen und Problemstellungen der Teilnehmenden zu beantworten. Die als Prüfungsleistung durchzuführende Projektarbeit festigt die theoretischen und praktischen Inhalte.
Unterrichtssprache	Deutsch
Teilnahmevoraussetzungen	Hochschulabschluss mit mindestens einjähriger Berufserfahrung oder anderweitiger berufsqualifizierender Abschluss mit mindestens dreijähriger Berufstätigkeit.
Abschluss	Hochschulzertifikat (Prüfungsteilnahme) oder Teilnahmebescheinigung (75% Anwesenheit)
Prüfungsleistung(en)	Kursbegleitendes Fallbeispiel: Anhand konkreter Fragestellungen werden die Inhalte des Zertifikatskurses am Beispiel einer SmartHome-Alarmanlage umgesetzt. Dieses Modul realisiert dabei die Funkanbindung der Sensoren, Aktoren und Signalgeber an die Alarmzentrale. Umfang 40 h.
Leistungspunkte	3 ECTS
Workload/Arbeitsaufwand	75 h Gesamtstunden
Präsenzzeit	24 h Präsenz
Selbststudium	51 h (Vor- und Nachbereitung, Erstellung von Projektarbeit)
Geplante Gruppengröße	Max. 12 Teilnehmende
Verwendbarkeit des Moduls	Für CAS Embedded Systems Professional
Literatur	Kurose, Ross: Computer Networking: a Top—Down Approach. 7th Edition, Pearson Verlag 2016.

Modulbeschreibung „Embedded Security“

Modultitel	Embedded Security
Kürzel/Modulnummer	---
Fachbereich	03 Elektrotechnik und Informatik
Modulverantwortliche/r	Prof. Dr. Jens Brandt, jens.brandt@hs-niederrhein.de
Dozent/in	Prof. Dr. Jens Brandt, jens.brandt@hs-niederrhein.de Prof. Dr. Tobias Frauenrath, frauenrath@fh-aachen.de Prof. Dr. Jürgen Quade, juergen.quade@hs-niederrhein.de
Modultyp	Hochschulzertifikatskurs der WWB
Dauer	Ca. 3 Termine in 2 Monaten
Häufigkeit des Angebots	Voraussichtlich jährlich und auf Nachfrage (Inhouse)
Zielgruppe(n)	Berufserfahrene Fach- und Führungskräfte aller Branchen, die in Anwendungsgebieten eingebetteter Systeme tätig sind oder sein werden. Sie sollten einen Hintergrund in Elektrotechnik, Informatik, Mechatronik oder verwandten Disziplinen haben: • Entwicklerinnen und Entwickler • Ingenieurinnen und Ingenieure • Systemarchitektinnen und -architekten • Technische Projekt- oder Teamleitungen • Produkt- und Prozessverantwortliche
Angestrebte Lernergebnisse/ Learning outcomes	Mit erfolgreichem Abschluss des Kurses werden die Teilnehmenden in der Lage sein: • Sicherheitsziele zu berücksichtigen, indem sie systematisch auf Anforderungen abgebildet werden, um damit das Gesamtsystem insgesamt abzusichern. • Ein sicheres Systemdesign zu erstellen, indem dabei etablierte Angriffsvektoren berücksichtigt werden, damit klassische Angriffe auf die IT-Sicherheit nicht zum Problem werden. • Software sicher zu implementieren, indem etablierte Angriffsvektoren berücksichtigt werden, um kosten- und zeitintensive Ausbessermaßnahmen zu vermeiden. • Sicherheitsmechanismen wie beispielsweise Paket-Filter in die Systeme zu integrieren, um Angriffe wie Ports-Scans ins Leere laufen zu lassen. • Existierende Embedded Software in Bezug auf Sicherheitslücken zu untersuchen, indem etablierte Analysemethoden (Penetretion Tests) angewendet werden, um diese zu identifizieren. • Einen sicheren Betrieb der Systeme zu berücksichtigen, indem dieser bereits während der Entwicklung geplant wird, damit im Nachhinein bekannt gewordene Schwachstellen möglichst aufwandsarm geschlossen werden können.
Inhalte	**Grundlagen der IT-Sicherheit** • Allgemeines: Schutzziele, Gefährdungen, Besonderheiten eingebetteter Systeme • Kryptographie: Basics, Authentifizierung • Normen, Standards, Best Practice • Risikoanalyse am Beispiel der IEC62443 **IT-Sicherheit im Entwicklungsprozess** • Sicherheitsgerichtete Softwareentwicklung **Gruppenarbeit**

	• Schutzziele und Risikoanalyse für die SmartHome-Alarmanlage • Konzepterstellung „Alarmanlage - Jetzt aber sicher!" **Sichere Kommunikation** • Public-Key-Infrastructure • Sicherheitsrelevante Protokolle • Verschlüsselte MQTT-Kommunikation **Sichere Systeme** • Absicherung durch Firewall und IDS • Sichere Systemupdatesode Review / Static Source Code Analysis **Systemtest** • Code Review / Static Source Code Analysis • Fuzz Testing / Robustness Testing • Secure Configuration Testing • Penetration Testing • Hardware Integritäts-Checks • Vulnerability Scanner **Product Lifecycle** • Logistik / Umgang mit Zertifikaten • End-of-Life Scenario
Lehrformen	Die originäre Wissensvermittlung erfolgt in Form eines klassischen Seminars. Durch rechnergestützte praktische Übungen wird das Erlernte sofort praktisch erprobt, mit der Möglichkeit individuelle Fragen und Problemstellungen der Teilnehmenden zu bearbeiten. Die als Prüfungsleistung durchzuführende Projektarbeit festigt die theoretischen und praktischen Inhalte.
Unterrichtssprache	Deutsch
Teilnahmevoraussetzungen	Hochschulabschluss mit mindestens einjähriger Berufserfahrung oder anderweitiger berufsqualifizierender Abschluss mit mindestens dreijähriger Berufserfahrung. Programmierkenntnisse (C)
Abschluss	Hochschulzertifikat (Prüfungsteilnahme) oder Teilnahmebescheinigung (75% Anwesenheit)
Prüfungsleistung(en)	Kursbegleitendes Fallbeispiel: Anhand konkreter Fragestellungen werden die Inhalte des Zertifikatskurses am Beispiel einer SmartHome-Alarmanlage umgesetzt. In diesem Modulteil wird die Alarmanlage gegen Cyberangriffe geschützt. Die bisher realisierten Methoden werden kritisch hinterfragt und ggfs. auf eine sichere Art erneut implementiert. Umfang 40 h.
Leistungspunkte	3 ECTS
Workload/Arbeitsaufwand	75 h Gesamtstunden
Präsenzzeit	24 h Präsenz
Selbststudium	51 h (Vor- und Nachbereitung, Erstellung von Projektarbeit)
Geplante Gruppengröße	Max. 12 Teilnehmende
Verwendbarkeit des Moduls	Für CAS Embedded Systems Professional
Literatur	Wird in der Veranstaltung bekannt gegeben.