Ruhr Master School
of Applied Sciences

Dieses Wahlpflichtmodul ist ein Angebot der:

Fachhochschule Dortmund
University of Applied Sciences and Arts

Master Digital Transformation

Digital Systems 1

daniel.vonfalkenhayn@fh-dortmund.de

Prof. Dr. Ingo Kunold
kunold@fh-dortmund.de

Hochschule Bochum
Bochum University
of Applied Sciences

Fachhochschule Dortmund
University of Applied Sciences and Arts

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

STIFTUNG MERCATOR

Digital Systems 1 (MOD1-03)

Code Number	Workload	Credits	Semester	Frequency	Duration
48030/31	180 h	6	1	winter semester	1 Semester

1	Course Title	Contact hours	Self-Study	Planned Group Size
	Digital Systems 1	4 SWS / 60 h	120 h	25 students

2 Course Description

The module is intended to give students to competence to understand, analyze, develop, set up and evaluate digital systems based on the latest scientific state of the art. This involves the basic layers of the Internet-of-Things (IoT) stack including M2M devices and gateways, the relevant protocol stacks for IoT and the relevant communication network technologies (both wireless and wireline). During the module, students will set up a complete IoT device with all relevant functionality to be connected to the cloud. Recent topics from research projects (e.g. connected car, smart home) complement the course with the aim to stimulate discussion of scientific results.

3 Course Structure

1. Introduction to M2M and IoT devices and gateways
2. Processor architecture for embedded devices and gateways
3. IP based communication
4. IoT and M2M protocols
5. Communication gateway architectures
6. Wireline communication networks and standards
7. Wireless communication networks and standards
8. Case study of a state-of-the-art application, e.g. connected car or industry 4.0

4 Application Focus

Project IoT System: students will set up and implement a IoT system with an M2M device, a gateway with wireless and wireline transmission and a IoT cloud connection. The respective case study will be taken from a recent R&D project or an industry case. The result will be a demonstrator system.

Trainings: students attend a training for the Siemens Embedded Software Developer tool chain

5 Scientific Focus

Students will do a scientific evaluation of the potential of IoT usage in a specific domain (e.g. eMobility charging systems) based on recent scientific literature.

6 Parameters

- ECTS: 6
- Hours of study in total: 180
- Weekly hours per semester: 4
  - Contact hours: 60
  - Self-Study hours: 120

	• Course characteristics: compulsory • Course frequency: every year – winter semester • Maximal capacity: 25 students • Course admittance prerequisites: none • Skills trained in this course: theoretical knowledge, practical skills and scientific competencies • Assessment of the course: Theoretical knowledge: Written Exam at the end of the course (50%) and Practical Skills: Individual programming task (50%): implementation of an IoT device, gateway and protocol stack system => demonstration of the result • Teaching staff: Prof. Dr. Ingo Kunold, staff from IKT institute, guest lecturers from joint research projects
7	**Learning outcomes** 7.1 Knowledge • Knows relevant theoretical foundations of M2M and IoT • Knows relevant gateway and processor architectures • Knows relevant protocol stacks and communication systems • Know methodical background of IoT system design • Is aware of critical limitations of IP based protocols, esp. in real time tasks 7.2 Skills • Can model IoT and M2M systems • Can implement embedded systems into IoT systems • Can apply state of the art tools for SW for embedded systems • Can select IoT and M2M platforms according to system requirements 7.3 Competence – attitude • Can discuss IoT device and gateway systems with experts • Can lead cross domain design for IoT systems • Understands SW and HW experts and translates between different domains
8	**Teaching and training methods** • Theoretical knowledge: e-learning modules on IoT devices and protocols, tool tutorials • Practical Skills: Projects, Labs & Exercises, small project with an IoT device and protocol stack • Scientific Competences: own research on IoT in e-mobility
9	**Course mapping** Input for: MOD2-03 – Digital Systems 2 Input from: none
10	**References** <u>Basics & Practitioner</u> Andrew S. Tanenbaum, David J. Wetherall: Computer networks, 2014 Peter Prinz, Tony Crawford, C in a Nutshell, 2nd Edition, 2015 Herbert Schildt, Java: The Complete Reference, Eleventh Edition

K.C. Wang, Embedded and Real-Time Operating Systems, 2017

OWASP Foundation, „Open Web Application Security Project,“, [Online] Available: https://www.owasp.org/index.php/Main_Page

BSI - Federal Office for Information Security, “Protection profile for the gateway of a smart metering system,” 2014, [Online] Available: https://www.bsi.bund.de

BSI - Federal Office for Information Security, “BSI TR-03116-4,” 2012, [Online] Available: https://www.bsi.bund.de

„RFC 4253: The Secure Shell (SSH) Transport Layer Protocol“, [Online] Available: https://tools.ietf.org/html/rfc4253

„RFC 7252: The Constrained Application Protocol (CoAP)“, [Online] Available: *https://tools.ietf.org/html/rfc7252*

W3C, „Web of Things (WoT) Thing Description,“ 16 May 2019. [Online]. Available: https://www.w3.org/TR/wot-thing-description/.

OpenAPI Specification (Version 2.0), [Online] Available: https://swagger.io/specification/v2/

Research (Examples for selected papers)

M. Niemeyer und I. Kunold, „Security Aspects of Cyber Physical Systems and Services,“ in *Smart Energy 2016 Digitalisierung der Energieversorgung — Treiber und Getriebene*, Dortmund, vwh, 2016.

B. M. H. Alhafidh, W. H. Allen, “High Level Design of a Home Autonomous System Based on Cyber Physical System Modeling”, IEEE 017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW), July 2017

Hoeller and R. Toegl, “Trusted Platform Modules in Cyber-Physical Systems: On the Interference Between Security and Dependability “, 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, 2018, pp. 136-144.