



COURSE DESCRIPTION CARD - SYLLABUS

Course name

Functional Safety and Security of Supply Chains [S1Cybez1>BFiłD]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
24

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

Lecturers

Prerequisites

A student starting this course should have basic knowledge of computer networks and the Windows and Linux operating systems. They should also be familiar with at least one programming language (C, C++, Java, or C#). In addition, they should have the ability to gather information from the indicated sources and be willing to collaborate as part of a team.

Course objective

To provide students with in-depth theoretical and practical knowledge in the areas of functional safety, threat detection, risk analysis and assessment, as well as cost estimation for implementing secure computer control systems. The course will also cover standards, best practices, and mechanisms that ensure supply chain security.

Course-related learning outcomes

Knowledge:

- The student has structured and theoretically grounded general knowledge related to functional security, risk analysis, and risk assessment. [K1_W15]
- The student possesses advanced and detailed knowledge of selected topics in secure computer

control systems. [K1_W15]

- The student has in-depth and specialized knowledge of the processes occurring throughout the lifecycle of resilient computer systems. [K1_W09]
- The student is familiar with advanced methods, techniques, and tools used for threat identification, risk analysis, and risk assessment, as well as probabilistic modeling methods for E/E/EP systems. [K1_W15]

Skills:

- The student is able to acquire information from literature, databases, and other sources, such as recommendations and standards (in Polish and English) related to functional security, integrate them, interpret and critically evaluate them, draw conclusions, and formulate well-justified opinions. [K1_U01]
- The student is capable of planning and conducting experiments, including measurements and computer simulations, interpreting obtained results, drawing conclusions, and formulating and verifying hypotheses related to complex problems in functional security. [K1_U04]
- The student can apply analytical, simulation, and experimental methods to formulate and solve engineering tasks and simple research problems in risk analysis and assessment, as well as the cost evaluation of implementing security measures. They are also able to critically analyze existing risk assessment methods and propose improvements. [K1_U05]
- The student is able to collaborate effectively within a team, assuming various roles, and can determine directions for further learning and implement self-education processes in the field of functional security. [K1_U16]

Social competences:

The student understands that knowledge and skills in the field of functional security rapidly become outdated. [K1_K01]

The student recognizes the importance of utilizing the latest knowledge in functional security to solve research and practical problems. [K1_K02]

The student is aware of the necessity of a professional approach to solving functional security problems and taking responsibility for their proposed projects. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: Knowledge gained during the lecture is assessed through an exam, conducted either in a written or an oral form. In the written exam, students must answer 7-10 questions (a combination of multiple-choice and open-ended), each carrying different point values. There are three or four separate scoring groups. In the case of the oral exam, a student draws one question from each scoring group. During the oral exam, for each drawn question, the student may be asked an additional follow-up question related to the one drawn. The grade for each question (including both the main and the follow-up question) reflects the scope of the answer and the depth of understanding of the topic. A set of 50-60 questions is prepared for each exam. To pass, a student must earn at least 50% of the total possible points.

Laboratories: Skills gained in laboratory classes are assessed on an ongoing basis. In each lab session, the correctness of the completed exercises is graded on a scale of 0 to 10 points. To pass the lab component, a student must earn at least 50% of the total possible points.

Percentage of Points Grade

<=50% 2,0

51% - 60% 3,0

61% - 70% 3,5

71% - 80% 4,0

81% - 90% 4,5

91% - 100% 5,0

In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

The program covers basic elements of functional safety, including weaknesses, errors, faults, SIS, SIF, and SIL. It also discusses key standards in this area and presents methods for threat estimation. During the classes, students will learn essential concepts related to supply chains and the standards connected to their security.

Course topics

Lecture Topics

- The significance of safety integrity
- Basic design assumptions, hardware failures, and fault tolerance
- Guidelines for functional safety: IEC 61508, IEC 61511, and related standards
- Safety integrity objectives and functional safety management
- The human factor in functional safety
- Requirements for E/E/EP systems in relation to functional safety
- Functional safety in communication systems
- Functional safety in digital systems and PLC controllers
- Methods of hazard identification, risk analysis and assessment, including analysis of hazard layers and ring
- Probabilistic modeling of E/E/EP systems for the purpose of risk analysis and assessment
- Cost and benefit analysis of risk reduction
- Standards related to systems engineering, safety of computer control systems, and software
- Standards related to quality management, environmental management, and information security
- Resilient computer systems:
- General fault tolerance algorithms
- Testing, verification, and indications of hardware failures
- Recovery algorithms and data recovery preparation
- Programming languages for safety-critical systems
- Principles of writing C programs for safety-critical systems (MISRA-C)
- Basic definitions and standards for IT supply chains
- Methods of ensuring security in supply chains

Laboratory and Project Topics

Consistent with the lecture content.

Teaching methods

Lecture: Multimedia presentation supplemented with examples illustrated on the board.

Laboratory Exercises: Practical group work using network devices and virtualized environments.

Bibliography

Basic:

1. David J Smith, Kenneth G L Simpson: The Safety Critical Systems Handbook: A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2015 Edition) and Related Guidance, Butterworth-Heinemann, 2020, 2. Schagaev Igor., Kaegi-Trachsel Thomas: Software Design for Resilient Computer Systems, Springer International Publishing, 2016

Additional:

1. Josef Börcsök: Functional Safety: Basic Principles of Safety-related Systems, Vde Verlag GmbH, 2021.
2. Harvey T. Dearden: Functional Safety In Practice (3rd Edition), Independently Published, 2020.

Breakdown of average student's workload

	Hours	ECTS
Total workload	78	3,00
Classes requiring direct contact with the teacher	48	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00