GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Functional safety and information security, PG_00062386		
Field of study	Automation, Robotics and Control Systems		
Date of commencement of studies	October 2023	Academic year of realisation of subject	2025/2026
Education level	first-cycle studies	Subject group	
Mode of study	Full-time studies	Mode of delivery	at the university
Year of study	3	Language of instruction	Polish
Semester of study	6	ECTS credits	3.0
Learning profile	general academic profile	Assessment form	assessment
Conducting unit	Department of Control Engineering -> Faculty of Electrical and Control Engineering -> Faculties of Gdańsk University of Technology		
Name and surname of lecturer (lecturers)	Subject supervisor	dr inż. Emilian Piesik	
	Teachers	dr inż. Emilian Piesik dr inż. Adam Kielak	

Lesson types

Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
Number of study hours	30.0	0.0	0.0	15.0	0.0	45

E-learning hours included: 0.0

Additional information:

Lecture, presentations and auxiliary materials. Project, instructions.

Learning activity and number of study hours

Learning activity	Participation in didactic classes included in study plan	Participation in consultation hours	Self-study	SUM
Number of study hours	45	3.0	27.0	75

Subject objectives

The aim of the course is to develop engineering knowledge related to hazard identification as well as risk analysis and assessment in technical systems, useful for designing control systems that take functional safety requirements into account.

Learning outcomes

Course outcome	Subject outcome	Method of verification
[K6_U07] can build and analyze models of systems and systems in the field related to control systems and automation	Identifies methodological foundations for assessing hazards associated with the operation of machinery, production lines, and industrial installations. Defines safety functions based on the results of risk analysis and assessment in order to rationally reduce the risk of accidents and human, environmental, and material losses. Performs analyses of layered protection systems and selects hardware architecture solutions that implement safety functions.	[SU5] Assessment of ability to present the results of task [SU3] Assessment of ability to use knowledge gained from the subject [SU4] Assessment of ability to use methods and tools
[K6_W07] has basic knowledge related to control and automation systems	Determines the required safety integrity level (PLr or SILr) of a safety function and verifies these levels based on a probabilistic model of an industrial automation and control system. Performs analyses involving interconnected operational, information, and cloud technologies (OT–IT–CT).	[SW1] Assessment of factual knowledge [SW3] Assessment of knowledge contained in written work and projects
K6_U06	ossesses the preparation necessary for safe work in an industrial environment, and is able to apply occupational health and safety principles as well as the requirements of functional safety standards. Identifies technical and information-related hazards in integrated OT–IT–CT systems, takes into account individual and societal risk, and applies the ALARP principle when making design decisions. Correctly interprets the requirements of standards PN-EN 13849, PN-EN 62061, PN-EN 61508 and PN-EN 61511, and selects appropriate protective measures and security layers (BPCS/AS/SIS/ESD). In practical project tasks, applies best practices in occupational safety, cybersecurity, and information protection, ensuring the safe operation of automation and control systems.	[SU5] Assessment of ability to present the results of task [SU4] Assessment of ability to use methods and tools

Subject contents

Course content – lecture
Lecture:

Safety and cybersecurity solutions in technical systems. Definitions of risk, including individual and societal risk. The ALARP principle, risk matrix, and required risk reduction. The concept of functional safety in control and protection systems. Design of electrical, electronic, and programmable electronic (E/E/PE) systems. Examples of functional safety solutions used in industry. Reliability and functional safety of machine control systems. Classification of control systems according to the standards PNEN 954, PNEN 13849 and PNEN 62061. Performance Levels (PL). Hazard analysis and the definition of safetyrelated functions. Determination of the required Safety Integrity Level (SIL) based on risk assessment in accordance with PNEN 61508. Verification of SIL using qualitative and quantitative methods. Protection layers according to PNEN 61511. The LOPA method. Design of Safety Instrumented Functions (SIF) within Safety Instrumented Systems (SIS) and alarm systems (AS). Information protection in computer systems. Criteria for risk assessment and determination of information protection levels

Course content – project
Project:

Analysis of hazards and risk identification. Determination of the required SIL for safetyrelated functions. Verification of the SIL level, design and implementation of the safety instrumented system (SIS) architecture. Safetyrelated devices. Layer of protection analysis (BPCS, human operator and alarm system, SIS/ESD).

Prerequisites and co-requisites

Knowledge concerning the probability calculus, the reliability analysis in technical systems, and the application of computer systems and programmable control systems in the industry.

Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	Project	60.0%	50.0%
	Two midterm colloquiums	60.0%	50.0%
Recommended reading	Basic literature	1. Kosmowski K.T. (red.): Podstawy bezpieczeństwa funkcjonalnego, Wydawnictwo Politechniki Gdańskiej, Gdańsk 2020. 2. Kosmowski K.T. (Ed.): Functional safety management in critical systems, Fundacja Rozwoju Uniwersytetu Gdańskiego Gdańsk 2007. 3. Liderman K.: Analiza ryzyka i ochrona informacji w systemach komputerowych. Wydawnictwo Naukowe PWN SA, Warszawa 2008.	
	Supplementary literature	1. Andersen R.: Inżynieria zabezpieczeń. WNT, Warszawa 2005. 2. Białas A.: Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, WNT, Warszawa 2006.	
	eResources addresses		
Example issues/ example questions/ tasks being completed	1. Risk graph for determining required safety integrity level (SIL). 2. Qualitative verification of the E/E/PE system's SIL. 3. Quantitative verification of the E/E/PE system's SIL.		
Practical activites within the subject	Not applicable		

Document generated electronically. Does not require a seal or signature.