GDAŃSK UNIVERSITY OF TECHNOLOGY

Subject card

Subject name and code	Safety-Critical Systems , PG_00048278						
Field of study	Informatics						
Date of commencement of studies	February 2026		Academic year of realisation of subject		2025/2026		
Education level	second-cycle studies		Subject group		Optional subject group Specialty subject group Subject group related to scientific research in the field of study		
Mode of study	Full-time studies		Mode of delivery		at the university		
Year of study	1		Language of instruction		Polish		
Semester of study	1		ECTS credits		2.0		
Learning profile	general academic profile		Assessment form		assessment		
Conducting unit	Department Of Software Engineering -> Faculty Of Electronics Telecommunications And Informatics -> Wydziały Politechniki Gdańskiej						
Name and surname of lecturer (lecturers)	Subject supervisor		dr inż. Andrzej Wardziński				
	Teachers		dr inż. Andrzej Wardziński				
Lesson types and methods of instruction	Lesson type	Lecture	Tutorial	Laboratory	Project	Seminar	SUM
	Number of study hours	15.0	0.0	0.0	15.0	0.0	30
	E-learning hours included: 0.0						
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	30		4.0		16.0	50
Subject objectives	To develop understanding of the role and scope of the requirements and the related assurance related to critical systems To acquire knowledge on the methods and techniques of designing and analyzing such systems. Practicing risk anaysis techniques with respect to a selected critical system						

Learning outcomes	Course outcome	Subject outcome	Method of verification
	[K7_U04] can apply knowledge of programming methods and techniques as well as select and apply appropriate programming methods and tools in computer software development or programming devices or controllers using microprocessors or programmable elements or systems specific to the field of study, making assessment and critical analysis of the prepared software as well as a synthesis and creative interpretation of information presented with it	Student knows mechanisms leading to failures of computer systems. Student is able to design system architecture to satisfy specific safety requirements.	[SU4] Assessment of ability to use methods and tools [SU1] Assessment of task fulfilment
	[K7_W03] knows and understands, to an increased extent, the construction and operating principles of components and systems related to the field of study, including theories, methods and complex relationships between them and selected specific issues - appropriate for the curriculum	Student knows mechanisms leading to failures and accidents of technical systems containing software. Student is able to perform safety analysis of a technical system.	[SW3] Assessment of knowledge contained in written work and projects
	[K7_W11] knows and understands, to an increased extent, the general principles of creation and development of forms of individual entrepreneurship and the economic, legal and other conditions of various types of activities related to the awarded qualification, including the principles of protection of industrial property and copyright law	The student knows the basics of the process of technical systems qualification in terms of safety of their use.	[SW1] Assessment of factual knowledge
	[K7_U12] is able, to an increased extent, to analyze the operation of components and systems related to the field of study, as well as to measure their parameters and study their technical characteristics, and to plan and carry out experiments related to the field of study, including computer simulations, interpret the obtained results and draw conclusions	The student knows the mechanisms of failures in technical systems containing software. The student is able to perform a safety analysis of the technical system and plan work to achieve the required safety level.	[SU4] Assessment of ability to use methods and tools

Subject contents	1. High integrity systems definitions, examples 2. Design principles: diversity, hazards management, risk reduction 3. Case study of Arian 5 4. Reliability theory; redundancy and its impact on reliability and safety 5. Diversity principle and its application to software 6. Impact of diversity on reliability and safety 7. Standard IEC 61508 definitions and scope 8. Standard IEC 61508 the ALARP principle 9. The concept of Safety Integrity Level (SIL) 10. IEC61508 requirements for software development 11. Human error 12. Trust case and safety case: objectives and scope 13. Risk analysis methods: Hazard Analysis, HAZOP, ETA 14. Risk analysis methods: FTA, FMEA, FMECA, CCA 15. Risk analysis methods: FMECA, CCA
Prerequisites and co-requisites	No requirements

Assessment methods and criteria	Subject passing criteria	Passing threshold	Percentage of the final grade
	Theory	50.0%	50.0%
	Project	50.0%	50.0%

Recommended reading	Basic literature	J Gorski, High Integrity Systems, Lecture notes,2010 E. Hollnagel, D. D Woods, N. Leveson, Resilience Engineering, Concepts and Precepts, TJ International, 2008 Nancy Leveson, SAFEWARE: System Safety and Computers, published by Addison Wesley, 1994 Peter Neumann, Computer Related Risks, published by ACM Press, New York, 1995 Tom Anderson and Peter Lee, Fault Tolerance: Principles and Practice, published by Springer-Verlag, New York, 1990 Trust-IT Framework, http://kio.eti.pg.gda.pl/trust_case/
	Supplementary literature	No requirements
	eResources addresses	Adresy na platformie eNauczanie:

Example issues/ example questions/ tasks being completed	- hazard analysis methods
	- risk assessment, ALARP
	- risk mitigation methods
Work placement	Not applicable

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