Module Description, available in: EN

Engineering of safety critical systems

General Information

Number of ECTS Credits

3

Module code

TSM_SafeSys

Valid for academic year

2026-27

Last modification

2019-08-31

Coordinator of the module

Pierluigi Capone (ZHAW, capo@zhaw.ch)

Explanations regarding the language definitions for each location:

- Instruction is given in the language specified for each location and module execution.
- Documentation is available in the language(s) listed for each location and module execution. If the documentation is in multiple languages, the percentage distributed is indicated (100% = all documentation provided).
- The examination, including both questions and answers, is provided entirely (100%) in the language(s) specified for each location and module execution. The exams are on-site.

	Winterthur			
Instruction	**X** E 100%			
Documentation	**X** E 100%			
Examination	**X** E 100%			

Module Category

TSM Technical scientific module

Lessons

2 lecture periods and 1 tutorial period per week

Entry level competences

Prerequisites, previous knowledge

The students are expcted to have basic knowledge of aircraft engineering such as:

- Aerodynamics
- Aircaft Structures
- Understanding of Aircraft Systems
- Understanding of Aircraft Propulsion
- Basic concepts of Maintenance
- Safety:
    - System Safety
    - Safety Process

Brief course description of module objectives and content

Safety-critical systems are those systems whose failure could result in loss of life. An aircraft such as an airliner has more than one safety critical systems.

The engineering activities required to design and manage these complex systems over their life cycles require a deep understanding of several disciplines and a systematic approach to problems such as:

- Requirements engineering
- Requirement based testing
- Validation and verification of complex function
- Managing human factors and teams

In this module the students will have an overview of Safety Critical Systems and related engineering activities and how these actitivties must be planned and executed in order to lead to successful certification and continued airworthiness.

Aims, content, methods

Learning objectives and competencies to be acquired

Understand core engineering and human-centered disciplines necessary to successful design, development and continued airworthiness of Safety Critical Systems (SCS).

The student are expected to acquire the following competencies:

- Understanding of safety critical system
- Be able to apply system engineering principles
- Understanding of system components qualification
- Understanding of aircraft certification process
- Logic of human behaviour

Module content with weighting of different components

Syllabus:

1. Introduction to Safety Critical Systems (SCS): General Concepts, Examples of SCS
2. Review of System Engineering Principles
3. Requirements: Writing, Verification and Validation, Testing
4. Safety Process: SAE-ARP-4761
5. Development Assurance Level: SAE-ARP-4754A
6. Unmanned Aircraft: Concept of Operations, Holistic Approach/SORA, Integration with Manned Aviation
7. Robustness, Redundancy, Dissimilarity and Integrity
8. Modeling and Simulation: Introduction
9. Modeling and Simulation of SCS
10. Testing of SCS
11. Human Reliability
12. Personality Motivation / Interpersonal Skills
13. Stress & Resilience
14. Safety Culture & Team Performance

Teaching and learning methods

- All lectures are strictly connected to current aviation practice and, where feasible, practical examples will be provided
- Real world examples with lessons learned will be provided for self study

Literature

- SAE-ARP-4754B - *Guidelines For Development Of Civil Aircraft and Systems*
- Aircraft Design - A Systems Engineering Approach M. H. Sadraey, Wiley Aerospace Engineering
- SAE-ARP4761A - Guidelines And Methods For Conducting The Safety Assessment Process On Civil Airborne Systems And Equipment
- DO-178C, Software Considerations in Airborne Systems and Equipment Certification

Assessment

Additional performance assessment during the semester

The module does not contain an additional performance assessment during the semester

Basic principle for exams

As a rule, all standard final exams are conducted in written form. For resit exams, lecturers will communicate the exam format (written/oral) together with the exam schedule.

Standard final exam for a module and written resit exam

Kind of exam

Written exam

Duration of exam

120 minutes

Permissible aids

Aids permitted as specified below:

Permissible electronic aids

- A non programmable calculator

Other permissible aids

- Closed Book
- Formulary will be distributed

Exception: In case of an electronic Moodle exam, adjustments to the permissible aids may occur. Lecturers will announce the final permissible aids prior to the exam session.

Special case: Resit exam as oral exam

Kind of exam

Oral exam

Duration of exam

30 minutes

Permissible aids

No aids permitted