Module Description, available in: EN

Security of Industrial Operational Technology

General Information

Number of ECTS Credits

3

Module code

TSM_SecIndOpT

Valid for academic year

2025-26

Last modification

2023-07-25

Coordinator of the module

Luca Haab (HES-SO, luca.haab@hefr.ch)

Explanations regarding the language definitions for each location:

- Instruction is given in the language defined below for each location/each time the module is held.
- Documentation is available in the languages defined below. Where documents are in several languages, the percentage distribution is shown (100% = all the documentation).
- The examination is available 100% in the languages shown for each location/each time it is held.

	Lausanne			Lugano	Zurich		
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

Students should have a basic understanding of computer networks and security concepts. It is recommended that students have completed introductory courses in computer networking and security before taking this module.

Pre-reading material required for specific labs may be provided.

Brief course description of module objectives and content

This module provides an understanding of the fundamental principles of the security of Operational Technology (OT) in an industrial context. The module will cover the standards, key concepts and methodologies involved in securing OT systems commonly used in industrial environments, such as factories, power plants, and other critical infrastructure.

The module will begin by exploring particularities of OT systems and the unique security challenges associated with OT environments. Different aspects of OT systems and their implication for security are studied, such as network technology and network architecture. Challenges related to product lifecycle and key management as well as existing solutions to those problems are explored. A specific focus is put on the implementation of standard IEC 62443.

Aims, content, methods

Learning objectives and competencies to be acquired

Upon completion of the module, students should be able to

- Understand the unique security challenges associated with OT environments
- Comprehend the main cybersecurity standards related to OT environments
- Identify and assess the risks and threats associated with OT systems
- Understand which security measures are suitable to protect OT systems and how to respond to incidents

Module content with weighting of different components

The module will address the following topics:

- An introduction to the particularities of OT systems in comparison to IT systems and Sensor Technology
- Securing OT-relevant aspects of SCADA, DCS & ICS
- Communication technology relevant to OT environment as well as the implications of air-gapped and connected systems
- Threat models for OT systems
- Product lifecycle, in particular issues related to key generation and key management
- Incident Response in an OT context
- The application of Standard IEC 62443, in particular weakness analysis, post-incidence analysis and auditing

Teaching and learning methods

In addition to lectures, the module is completed by exercises on simulated OT environments corresponding to industry standards. The exercises will apply the content from the lectures to specific situations inspired by the challenges of real world environments.

Literature

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

None

Other permissible aids

A written summary, up to 4 double-sided A4 pages long, can be utilized during the exam. It can be handwritten or digital, though the font used must be size 9 or larger. The summary is to be handed in at the end of the exam.

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