JÖNKÖPING UNIVERSITY
School of Engineering

COURSE SYLLABUS

Critical Infrastructure and Industrial Cybersecurity, 7.5 credits

Kritisk infrastruktur och industriell cybersäkerhet, 7.5 högskolepoäng

Course Code:	T2KIOI	Education Cycle:	Second-cycle level
Confirmed:	Sep 01, 2025	Disciplinary domain:	Technology
Valid From:	Jan 18, 2027	Subject group:	Computer Technology
		Specialised in:	A1F Second cycle, has second-cycle course/s as entry requirements
		Main field of study:	Computer Science

Intended Learning Outcomes (ILO)

On completion of the course the student shall:

Knowledge and understanding

- demonstrate comprehension of operational technology and industrial control systems.
- demonstrate knowledge of communication protocols for emerging technologies such as industrial internet of things (IIoT) and industrial robotics.
- demonstrate knowledge of cybersecurity risks within emerging technologies such as IIoT, industrial automation, and robotic systems.

Skills and abilities

- demonstrate the ability to identify and assess vulnerabilities within operational technology environments.

Judgement and approach

- demonstrate the ability to critically evaluate industrial system architectures from a security perspective.

Content

The course is designed to provide an in-depth understanding of the potential risks and vulnerabilities associated with critical infrastructures using interconnected systems. The course covers topics such as cyberterrorism, cyberattacks that target industrial control systems and IoT devices, and the impact of these attacks on critical infrastructure.

Participants will explore topics such as PLC and SCADA systems, industrial robotics, and the various types of cyber threats, including the techniques attackers use to gain unauthorized access to these systems. They will also learn about the best practices and security measures necessary to secure industrial control systems and IoT devices, security architecture, and threat intelligence.

The course includes the following elements:

- Critical Infrastructure Cyber Security
- Cyberterrorism
- Industrial Internet of Things
- Communication Protocols
- PLC, SCADA and Robotics
- Robotics Security Incidents

Type of instruction

The course consists of lectures, seminars and project work.

Language of instruction is in English.

Entry requirements

Passed courses at least 90 credits within the major subject in Computer Science, Informatics, Information Systems, Computer Engineering, Mechanical Engineering, Civil Engineering, Industrial Engineering and Management, or the equivalent, and taken course Cybersecurity Overview, or Automation and Production Technology, 7,5 credits or the equivalent. Proof of English proficiency is required.

Examination and grades

The course is graded 5, 4, 3 or U.

Registration of examination:

Name of the Test	Value	Grading
Project [1]	4.5 credits	5/4/3/U
Seminar	3 credits	G/U

[1]Determines the final grade of the course, which is issued only when all course units have been passed.

Course literature

Please note that changes may be made to the reading list up until eight weeks before the start of the course.

Relevant scientific conference or journal publications in the field of industrial automation.