



## COURSE SYLLABUS

# Critical Infrastructure, 7.5 credits

*Kritisk infrastruktur, 7,5 högskolepoäng*

---

<b>Course Code:</b> TKIR24	<b>Education Cycle:</b> Second-cycle level
<b>Confirmed by:</b> Director of Education Mar 1, 2024	<b>Disciplinary domain:</b> Technology
<b>Revised by:</b> Director of Education May 1, 2024	<b>Subject group:</b> DT1
<b>Valid From:</b> Aug 1, 2024	<b>Specialised in:</b> A1N
<b>Version:</b> 2	<b>Main field of study:</b> Computer Science

---

### Intended Learning Outcomes (ILO)

After a successful course, the student shall:

Knowledge and understanding

- demonstrate comprehension of Operational Technology and Industrial Control Systems

Skills and abilities

- demonstrate skills in explaining and illustrating industrial network architectures
- demonstrate the ability to create a systematic analysis of a compromised critical infrastructure

Judgement and approach

- demonstrate the ability to suggest a design plan for industrial control system environments
- demonstrate the ability to suggest a solution for industrial control systems based on best practices

### Contents

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 essential topics such as cyberterrorism, cyberattack, cyber espionage that target industrial control systems and IoT devices, and the impact of these attacks on critical infrastructure.

Participants will learn about the diverse types of cyberthreats and the methods attackers use to gain unauthorised 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 infrastructures
- Industrial network, design, and architecture
- SCADA security

- Industrial environments
- Cyberattacks
- Cyberterrorism
- Failure of Defence in Depth
- Preventing intrusion
- Unidirectional gateways
- Security frameworks
- Secure remote access
- Encryption
- The Industrial Internet of Things

### **Type of instruction**

The course consists of lectures, active learning seminars, and individual and group project work.

The teaching is conducted in English.

### **Prerequisites**

The applicant must hold a minimum of a bachelor's degree (i.e., the equivalent of 180 ECTS credits at an accredited university) with at least 90 credits in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent. Proof of English proficiency is required.

### **Examination and grades**

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

Registration of examination:

Name of the Test	Value	Grading
Seminar <sup>1</sup>	5.5 credits	5/4/3/U
Assignment	2 credits	U/G

<sup>1</sup> Determines the final grade of the course, which is issued only when all course units have been passed.

### **Course literature**

The literature list for the course will be provided eight weeks before the course starts.

Title: Scada Security What's broken and how to fix it

Author: Andrew Ginter

Publisher: Abterra Technologies Inc

ISBN: 978-0-9952984-0-8

Title: ISC2 CISSP Certified Information Systems Security Professional Official Study Guide, 10th Edition

Author: Mike Chapple, James Michael Stewart, Darril Gibson

Publisher: Wiley

ISBN: 978-1-394-25469-9