The Institution of Engineering and Technology

Guidance on Teaching and Assessment of AHEP LOs 9 & 10 - Risk and Security

First issued: 23 May 2024
Last reviewed: 23 May 2024

theiet.org

Background

1. AHEP 4 has changed the emphasis on learning outcomes relating to risk and introduced a new learning outcome explicitly relating to security:

   Use a risk management **process** to **identify, evaluate,** and **mitigate** risks (the effects of uncertainty) associated with a particular project or activity.
   Adopt a holistic and proportionate approach to the mitigation of security risks.
   These must be delivered and assessed to have been achieved to at least a threshold level to level 4 for all students on programmes accredited for both Chartered and Incorporated Engineer.

2. It is recommended that technical and operational risk identification and mitigation be integrated across the curriculum so that the breadth of potential risks and approaches to mitigation are understood in context.

3. It is recommended that where a number of AHEP learning outcomes are being assessed in a single module (such as a project module) the contribution to the final mark for each LO should be significant and quantifiable.

4. UK Spec 4 provides the following expectation for registered engineers which may prove helpful in identifying aspects of risk which might be considered across the curriculum: "Identifying operational risks and evaluating possible engineering solutions, taking account of cost, quality, safety, reliability, accessibility, appearance, fitness for purpose, security (including cyber security), intellectual property constraints and opportunities, and environmental impact."

5. Risk analysis should include real world uncertainty and external factors including financial and political uncertainties and more holistic risks such as societal acceptability.

6. It is recommended that students should be given opportunities to demonstrate that they have applied risk mitigation strategies to meet objectives within deadlines and constraints with opportunities to learn from failure. Assessments should include a reflective element.

7. It is recommended that risk analysis should include consideration of functional risks attributable to individual failures within the context of holistic identification and analysis of the potential impact of such failures at a system level.

8. It is recommended that students should be able to apply a structured approach to manage risk throughout the project life cycle.

9. It is recommended that students should be taught the risks inherent with the use of disruptive technologies e.g. AI, big data, quantum computing etc.

10. It is recommended that security considerations should include but not be limited to cyber-security and should consider freedom from harm caused by any deliberate, unwanted, hostile or malicious acts.

11. Security considerations should include applying engineering thinking to problems that may have incomplete data and making design changes or developments to affect an improvement to resolve security problems that exist in legacy systems.

12. It is recommended that students gain an awareness of the importance of protecting data and know the legal frameworks exist. Sensitive data could come in the form of personal data, defence data or designs, or commercially sensitive information. They should have have an awareness of the ethics and legal implications of sharing sensitive information and can make informed decisions.

Background

13. We advise caution in teaching security to ensure that it is taught in an inclusive manner. This is particularly relevant to national security where international students could be alienated.

(a) Examples of Effective forms of delivery and assessment

1. Use of case studies and examples (e.g. from the RAE).

    1. A current example (in 2024) is the risks associated with the use of AI tools including reinforcement of biases (representational harms), privacy and security concerns, copyright infringement, lack of traceability of outputs and results, intentional poisoning of training data sets etc.
    2. Engineering Safety and Risk Management: A Structured Case Study Approach to Investigating Chemical Process Safety.
    3. Risk on complex projects - a case study
    4. Effective Risk Management in Innovative Projects: A Case Study of the Construction of Energy efficient, Sustainable Building of the Laboratory of Intelligent Building in Cracow

2. Project work where students should include risk assessments of operation, technical, and security risks with mitigation strategies.

3. Use of techniques such as the p-diagram for Failure Modes and Effects (FMEA) at a functional level and Fault-tree analysis (FTA) at a system level.

(b) Outside references/resources/reading lists.

1. EngC Guidance on Risk
2. EngC Guidance on Security for Engineers and Technicians
3. RAE Engineering X - Safer Complex Systems
4. ISO 16085 - Systems and Software engineering - Life cycle processes - Risk Management
5. ISO 27001 - Information security, cybersecurity and privacy protection
6. The UK National Cyber Strategy, 2022 Edition
7. Standards committee ISO/IEC JTC 1/SC 42 provides numerous documents relating to the risks associated with AI.

The Institution of Engineering and Technology

Contact information

London, UK
T +44 (0)20 7344 8460
E faradaycentre@ietvenues.co.uk

Stevenage, UK
T +44 (0)1438 313311
E postmaster@theiet.org

Beijing, China*
T +86 10 6566 4687
E china@theiet.org
W theiet.org.cn

Hong Kong SAR
T +852 2521 2140
E infoAP@theiet.org

Bengaluru, India
T +91 80 4089 2222
E india@theiet.in
W theiet.in

New Jersey, USA
T +1 (732) 321 5575
E ietusa@theiet.org
W americas.theiet.org

@TheIET theiet.org

E5B24006J/PDF/0722