Exercise 1

Questions – Answers
Task 1: Think of the Universities OIS system [https://ois2.ut.ee/](https://ois2.ut.ee/). Describe the four facets of this system context:

• **Usage facet:**
  • OIS is a platform to provide an administration of academic-related details. OIS would have three different kinds of users i.e. students, teachers and administrative staff. The OIS system would contain students course registration, students grades records, timetable, students status, curriculum and other details

• **Subject facet:**
  • OIS uses by students to perform course registration, to keep track of their grades, to check course timetable and students status. It also allows seeing student information and other details
  • Another interaction with the OIS system is from teachers. OIS allows teachers to check student progress, course timetable and other relevant details
  • Third interaction is from administrative staff to add course information, to update course timetable, to add students grades and other relevant details
  • The OIS system will interact with other University of Tartu systems which hold the student relevant information or require student information
Task 1: Think of the Universities OIS system [https://ois2.ut.ee/]. Describe the four facets of this system context:

- **IT system facet:**
  - The OIS system would have a URL and deploy on a web server. The web server would be managed by the University of Tartu IT department. Due to a large number of users, the OIS system should be deployed on the dedicated server. The server will take timely backups as well.

- **Development facet:**
  - The OIS system will be accessible only after student authentication. The security of user personal data should be analysed. The OIS system would not disclose or share information to the third party without the consent of the University or Student. The OIS system should be GDPR compliance or compliance with European privacy policy laws.
Task 2
These requirements are extracted from solutions of your colleagues. Do they correspond to the “criteria of good requirements”? If not, please refine them so that they would correspond to the “criteria of good requirements”.
Do not write like this

- **Ambiguity – or**
  - The ERIS system shall also be able to generate visible or audible caution or warning signal for the attention of security or business analyst

- **Multiple requirements – and, or, with, also**
  - The warning indicator shall light up when an ERIS intrusion is detected and the current Football Federation Employees workspace or Game report data shall be saved

[Alexander and Stevens, 2002]
Do not write like this

• Let-out clauses
  * if, when, except, unless, although, always
  • The fire alarm shall always be sounded *when* the smoke in Football Federation building is detected, *unless* the alarm is being tested
  * when* the antivirus is deployed

• Long rumpling sentences
  • Provided that the designated Game report input signals from the specified mobile devices are received in the correct order by the way which the ERIS is able to differentiate the designators, the security solution should comply with the required framework to indicate the desired security states

[Alexander and Stevens, 2002]
Do not write like this

- Speculation
  *usually, generally, often normally, typically*
  - Umpires and Team Representatives normally require early indication of intrusion into ERIS

- Vague, undefinable terms
  *user-friendly, versatile, approximately, as possible, efficient, improved, high-performance, modern*
  - Security-related messages should be versatile and user-friendly
  - The OK status indicator shall be illuminated as soon as possible after ERIS security self-check is completed

[Alexander and Stevens, 2002]
Do not write like this

• Wishful thinking

 100% reliable/ safe/ secure. Handle all unexpected failures. Please all users. Run on all platforms. Never fail. Upgrade to all future situations.

  • The gearbox shall be 100% secure in normal operation
  • The network shall handle all unexpected errors without crashing

[Alexander and Stevens, 2002]
Do not write like this

• System design:
  no names of components, materials, software objects/procedures, database fields
  • The antenna shall be capable of receiving FM signals, using a copper core with nylon armoring and a waterproof hardened rubber shield

• Mix of requirements and design:
  no references to system, design, testing, or installation
  • The user shall be able to view the current selected channel number which shall be displayed in 14pt Swiss type on an LCD panel tested to standard 657-89 and mounted with shockproof rubber washers

[Alexander and Stevens, 2002]
Good requirements

- Use simple direct sentences
  - Security analyst should be able to view ERIS status.

- Use a limited vocabulary
  - Security analyst should be able to change the infected ERIS component in less than 12 h; or
  - Security analyst should be able to reconfigure the infected ERIS component in less than 12 h

[Alexander and Stevens, 2002]
Good requirements

- Identify the type of user who wants each requirements
  - *The Football Federation Employee shall be able to …*

- Focus on stating result
  - … view game reports …

- Define verifiable criteria
  - … after 2 h after the game.

[Alexander and Stevens, 2002]
Criteria for writing good requirements

• **What**, not how (external observability)
  • Avoid premature design or implementation decisions
• **Understandability, clarity** (not ambiguous)
• **Cohesiveness** (one thing per requirement)
• **Testability**
  • Somehow possible to test or validate whether the requirement has been met, clear acceptance criteria
  • Often requires quantification, this is more difficult for security than e.g. for performance
    • *The response time of button press should be max 2 s.*
    • *The security of function F should be at least 99.9%*
T2: These requirements are extracted from solutions of your colleagues. Do they correspond to the “criteria of good requirements”? If not, please refine them so that they would correspond to the “criteria of good requirements”.

**SecReq.1**: The football federation employee, Bob, may remove the league secretary at any time and it should be available.

**SecReq.1**: The football federation employee should remove the league secretary.

**SecReq.2**: After match team representatives sign the report and optionally provide comments.

**SecReq.2.1**: Team representatives should sign the report of the finished match.  
**SecReq.2.2**: Team representatives should provide comments.

**SecReq.3**: Confirmation of game results by the team shall be allowed only for team representative which represents team under action

**SecReq.3**: Only team representative should access the confirmation of game results.
**SecReq.4:** Football Federation Employee should be identified before having access to use the functions related to the creation of the game report to prevent unauthorized people to create fake game reports.

**SecReq.4.1:** System should identify Football Federation Employee.

**SecReq.4.2:** Football Federation Employee should create the game report.

**SecReq.5:** ERIS shall allow all Users to view all Data in the Game Report.

**SecReq.5:** User should view *Data* in the *Game Report*.

---

**T2:** These requirements are extracted from solutions of your colleagues. Do they correspond to the “criteria of good requirements”? If not, please refine them so that they would correspond to the “criteria of good requirements”.