Term Project

Our term project comprises three separate parts as detailed below and in another document, the Technical Roadmap (coming next). A project report is to be completed and submitted by **December 2, 2020**. Oral presentations of the essential project outcomes as presented in the project report follow on **December 4, 7,** and **8**.

OVERVIEW

Project Scope. Supervisory control is essential for the continuous operation of critical infrastructure and services. Automation enhances cost efficiency, quality of service delivery and safe operation of critical assets. Electric power grids, public water utilities and smart transportation networks routinely rely on supervisory control systems, with steadily increasing integration of computation, networking and physical processes. Contrary to the benefits, increasing reliance on automation also increases the attack surface for advanced persistent threats and amplifies the risk of cascading effects. In light of increasing cyber threats and existing vulnerabilities that expose critical infrastructure to a variety of adversarial scenarios, the project explores anomaly detection based intrusion detection methods used for cyber situational awareness in the analysis of automated control processes.

Challenges. A number of inescapable 'external factors' make anomaly detection in time series data streamed from the operation of a real-world supervisory control system challenging. Typical examples include: imperfections in the data, such as missing or corrupted values; lack of ground truth in historic data, unavailability of labels to differentiate normal observations from outliers; types of anomalies depending on the particular application context; striking a good balance between *precision* and *recall*, specifically also reducing the false alarm rate to make anomaly detection practical in any real application context with resource constraints.

Project Description. The project is logically organized in three separate parts:

> Part 1 - Data Analytics
> This part is about exploring and understanding the specific characteristics of the data and developing an analytic approach to anomaly detection for different types of simple and complex anomalies. Specifically, you need to find a suitable probabilistic model for the purpose of representing 'normal' system behaviour to the extend possible with no ground truth available. Think about common usage patterns one can identify and possible anomalies one may observe while continuously monitoring the system operation in a control centre. Generally, there may not be the one best solution but a number of reasonable alternatives how to address the problem. Highlight and explain your major design choices, providing a **proper rational** for each one.

Part 2 - Project Report
Each project team is supposed to describe their methodical approach, their experimental analysis, the key findings from their experiments, challenges encountered and lessons learned in the form of a **technical report**. Details about what is expected from a technical report in terms of overall structure, logical organization and writing style are described below. Generally, a technical report is a clearly written, well-structured document to communicate technical ideas and insights to an audience with a technical background.

Part 3 - Presentation
Each project team will present the outcome of their work in a 15 minutes **technical presentation** in class during the last week of classes. This means to properly summarize the findings of your solutions and your project report in a formal presentation using slides with intuitive textual and graphical illustrations. Normally, only two members of each team will actively present while the other members need to answer questions.

The marking of the term project will ultimately take into account all three parts: the breadth, the depth, and the quality of the technical solution, the project report and its presentation.

PROJECT REPORT

The report documents your team's work on the term project and the essential outcomes. Technical reports are routinely used in industry for communicating ideas, facts, problem descriptions and possible solutions for a technical subject matter. Common standards expected from a professionally written technical report are detailed below.

The term project report explains and illustrates at a technical level: (1) the **problem** being addressed; (2) the **methodology** used for solving the problem; (3) the **characteristics** of the solution and a **rational** for the underlying design choices; (4) major **problems** encountered in the course of the project; and (5) the **lessons learned**. It also serves as the primary resource for your project presentation, although the level of detail in the report typically exceeds what can be explained and discussed clearly and intelligibly in a 15 mins. presentation.

Technical writing is a type of writing where authors write about a particular technical subject that requires direction, instruction, or explanation. This style of writing serves a different purpose and has different characteristics than other writing styles such as creative writing, academic writing or business writing. It is a clear and efficient way of explaining something and how it works. A good technical writer can make a difficult task easy and can quickly explain a complex piece of information.

Tips for Good Technical Writing

Regardless of the type of document which is written, technical writing requires the writer to know their audience, writing in a clear, non-personal style and doing extensive research on the topic. By doing so, the writer can create clear instructions and explanations for the reader:

- **Know your audience**. An expert in the field will understand certain abbreviations, acronyms, and lingo that directly applies to such a field. A novice will not understand in the same manner and, therefore, specific details must be explained.

- **Use an impersonal style**. Write from a third person perspective, like a teacher instructing a student. Any opinions should be omitted.

- The writing should be straightforward, to the point, and as simple as possible to make sure the reader understands the process or instruction. This at times may appear as simple as a list of steps to take to achieve the desired goal or may be a short or lengthy explanation of a concept or abstract idea.

- **Know how to research.** Gather information from a number of sources, understand the information gathered so that it can be analyzed thoroughly, and then put the information into an easy to understand format to instruct those who read it. The more inexperienced your audience, the more information you will need to gather and explain.

- Be thorough in description and provide enough detail to make your points; but, you also have to consider that you need to use an economy of words so that you do not bore your reader with gratuitous details.

Project Report Structure

Proper logical organization and clear structuring of the project report demands for:

- a **title page** containing a title, name of all authors, student ID numbers, the course and semester, an abstract (i.e., a one paragraph outline of your report);
- some concise but meaningful **conclusions** (e.g., what you have accomplished, future work);
- page numbers and **numbered headings** of sections, subsections, etc.;
- a **table of contents** and a table of figures;
- a **list of references** (i.e., bibliographic items).

Note that online references are perfectly acceptable; you may want to give references to web pages or online documents or a reference to a specific web sub-page if referencing a particular point from that particular link.

Example of a bibliographic item:

> Zahra Zohrevand, Uwe Glässer, Mohammad A. Tayebi, Hamed Yaghoubi Shahir, Mehdi Shirmaleki, and Amir Yaghoubi Shahir. Deep-Learning Based Forecasting of Critical Infrastructure Data. *In Proceedings of the 26th ACM International Conference on Information and Knowledge Management*, Singapore (2017), pages 1129-1138.

The body of the report (excluding the title page, table of contents, list of references, etc.) should be about 20 pages double spaced. It should start by introducing the **problem scope** and **technical background**, and provide a basic rational for the concepts on which your solution builds. List the main contributions to the project and the report of **each team member**.

Getting Started. A clear breakdown of tasks and responsibilities among team members certainly helps in developing a clear roadmap allowing the team to work more productively. Please take into account though that the team as a whole is responsible for their project and all team members are expected to help each other in managing project tasks.

Please note: the technical tasks of the term project will be described in a separate document./

We hope that you will find this project a rewarding experience.

Thank you for your cooperation!