Part II: Term Project Report and Presentation

The term project report presents, explains and illustrates your **experimental analysis** and your **interpretation of the results** for the electric energy consumption datasets. Beyond plain text, this requires DIAGRAMS, GRAPHS and TABLES describing in detail the experiments performed and a comparison of the outcomes. Specifically, this includes:

1) Comparing each response variable with the others based on the results of performing PCA and illustrating the rationale for your final choice of variables;

2) Explaining the selection of response variables and providing a proper rationale for the observation time window chosen for the analysis;

3) Explaining your choice for partitioning the data into training and test sets;

4) Providing an overview of both the log-likelihood and BIC values for different numbers of HMM states to justify your final model selection;

5) Comparing the normalized training log-likelihood and test log-likelihood to assess how well your model fits the data;

6) Comparing the normalized log-likelihood of each of the 10 data subsets to the trained model to determine the normal behaviour threshold of your data.

The project report is due by 30 March 2025. Oral presentations of your project outcomes (experiments, results, lessons learned, etc) follow on **April 1-4**. Each group has 18 mins. to present their key findings. We also need a **PDF copy** of your presentation slides by 31 March 2025.

OVERVIEW

Project Scope. 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. Increasing reliance on automation also increases the attack surface for advanced persistent threats and amplifies the risk of cascading effects. Existing vulnerabilities expose critical infrastructure to a range 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 mission-critical 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 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 technical subject matters. 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) any major **problems** encountered over the course of the project; and (5) what are the **lessons learned?**

Technical writing is 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.

Project Report Organization

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

- a **title page** containing: title, group number, name of all authors, student ID numbers, the course and semester, an abstract, i.e., a one paragraph outline of your report;
- concise but meaningful **conclusions** (e.g., what you have accomplished, lessens learned);
- 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 acceptable; you need to add references to web pages or online documents or a sub-page if referencing a particular point from that particular link.

Example of a bibliographic item:

> Z. Zohrevand, U. Glässer, M. A. Tayebi, H. Yaghoubi Shahir, M. Shirmaleki, and A. 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 your report—excluding the title page, abstract, table of contents, list of references, and any extra pages—should be about **12-15 pages, double spaced**, including figures, graphs and tables. It should start by introducing the **problem scope** and **technical background**, and provide a basic rational for the concepts on which your solutions build. Add an extra page to list for **each group member** the approx. percentage of their main contributions to the project and the report; otherwise, all group members will receive the same marks for the term project.