**Abstract**

Industrial Control Systems (ICS) are commonly used in various domains, where it consists of many devices to automate industrial process. One of the most used control systems for ICS is Supervisory Control and Data Acquisition (SCADA) systems, where in this work the measurements data from SCADA is going to be used to build the model.

In recent years, ICS security is hot topic that concern many companies. One example is the recent attack on ARAMCO which was later called Shamoon. Obtaining such sensitive data is quite difficult due to many constraints. In this project the model helps us classify if something is an cyberattack or a normal fault on the facility.

**Design**

This project originates can be seen as first import the data needed then start cleaning the data to make it easy to manipulate and visualize.

**Data**

The dataset contains than 10,000 rows, Oak Ridge National Laboratories (ORNL) have created 3 datasets which include measurements related to electric transmission system normal, disturbance, control, cyber attack behaviors. Measurements in the dataset include synchrophasor measurements and data logs from Snort, a simulated control panel, and relays.

([Tommy Morris - Industrial Control System (ICS) Cyber Attack Datasets (google.com)](https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets))

**Algorithms**

For this project classification algorithms such as KNN, LogisticRegression and Stacking a long others were used.

**Tools**

* Numpy and Pandas for data manipulation
* Scikit-learn for classification modeling
* Matplotlib and Seaborn for plotting

**Communication**

slides and two-word files