**PROJECT PROPOSAL**

|  |  |  |  |
| --- | --- | --- | --- |
| **PROJECT TOPIC** | Industrial Control System (ICS) Cyber Attack Classification | | |
| **NAME** | Ahmed Almuaybid | **DATE** | 29/9/2021 |

|  |
| --- |
| 1. **Introduction** |
| 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. |
| 1. **Motivation & Benefits** |
| This model could help different infrastructures such as smart grids, power distribution, transportation systems, water treatment plants, and manufacturing. Some of recent attacks on SCADA systems for example, Stuxnet and Maroochy in Australia |
| 1. **Datasets**  **& Tools** |
| The use of the following datasets:  - Industrial Control System (ICS) Cyber Attack Datasets : Power System Datasets  The modeling target of this to classify based on SCADA data if this instance is cyber-attack or normal fault. This work will be done using mainly python and might involve others.  Tools   * Matplotlip * SKLEARN * GoogleColab * Pandas and Numpy |