**Attack Scenarios**

**Four Aspects of an Attack:**

1. Obtaining OT Credentials
2. Attack on SCADA system
3. Attack on on-field devices
4. Outcome of the attack

In this document, the aspects 2, 3 and 4 are discussed w.r.t. implementation on the platform.

**Attack 1**: *False Data Injection (FDI) attack*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Real Load** | **Real Frequency** | **False Load** | **False Frequency** | **Pump state** | **Outcome** |
| 7 | 49.4 Hz | 4 | 50 Hz | Remains at low | No change when there was supposed to be a change |
| 7 | 49.4 Hz | 1 | 51.2 Hz | High to Low | **Black out** as frequency goes below tripping levels |
| 4 | 50 Hz | 7 | 49.4 Hz | Low to High | **Black out** as frequency goes above tripping levels |

**Attack 2**: *False Command Injection (FCI) attack*

|  |  |  |  |
| --- | --- | --- | --- |
| **Present Load\*** | **Present Frequency\*** | **Pump input** | **Outcome** |
| 6 | 50 Hz | High to Low | Fall of frequency that leads to **black out** |
| 4 | 50 Hz | Switch off | Complete **shutdown of the facility** |

\*- The injection of false data to match these states creates a stealthy attack