Task 9
SIGA

Focus:

Addressing grid attack scenarios which are utilizing operational grid's stabilization tools for destabilization purposes by using ML tools on high sampled raw data.

- Malicious Voltage Collapse
- Malicious loss of grid's Inertia

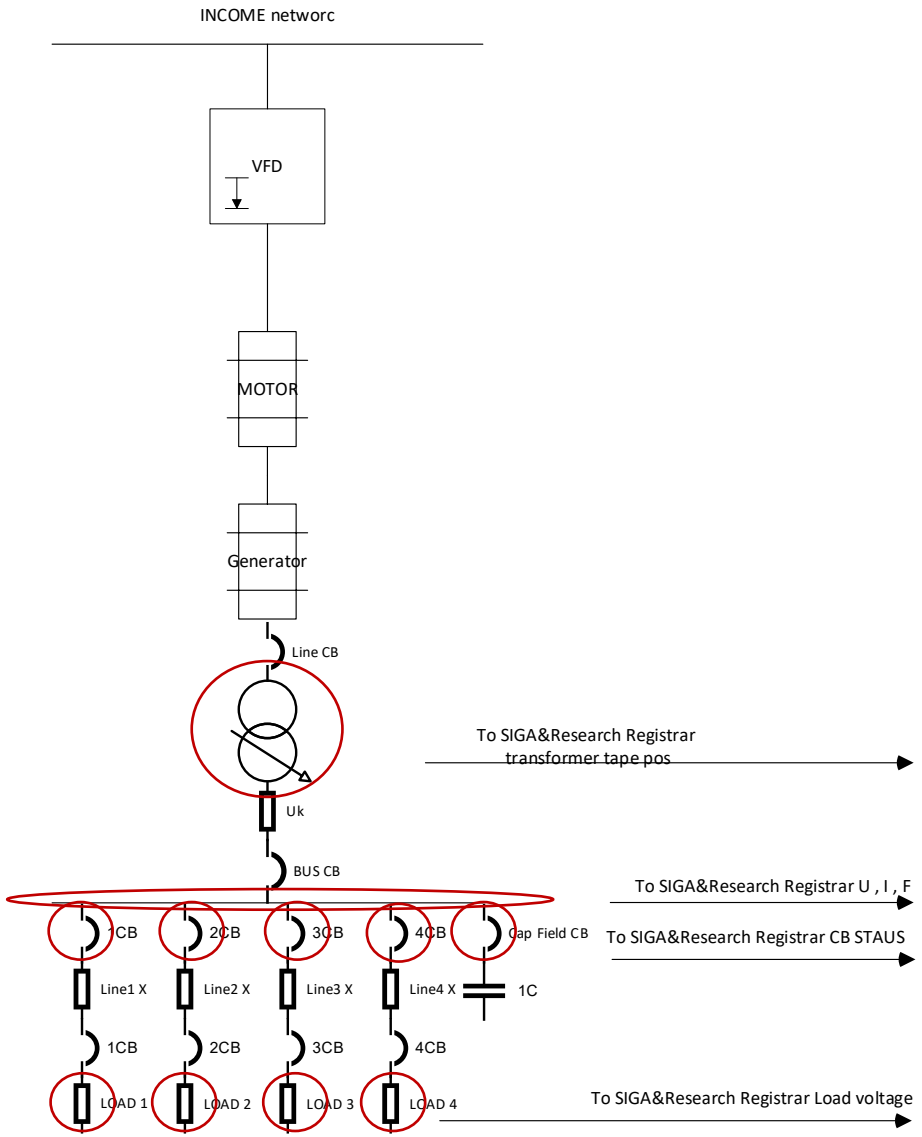
Malicious Voltage Collapse

Attack:

Utilizing digital AVR to trigger voltage collapse at a given sub-station

Tool's goal:

Early detection of malicious manipulation based on learning period of 1KHz sampling of the substation's monitored components



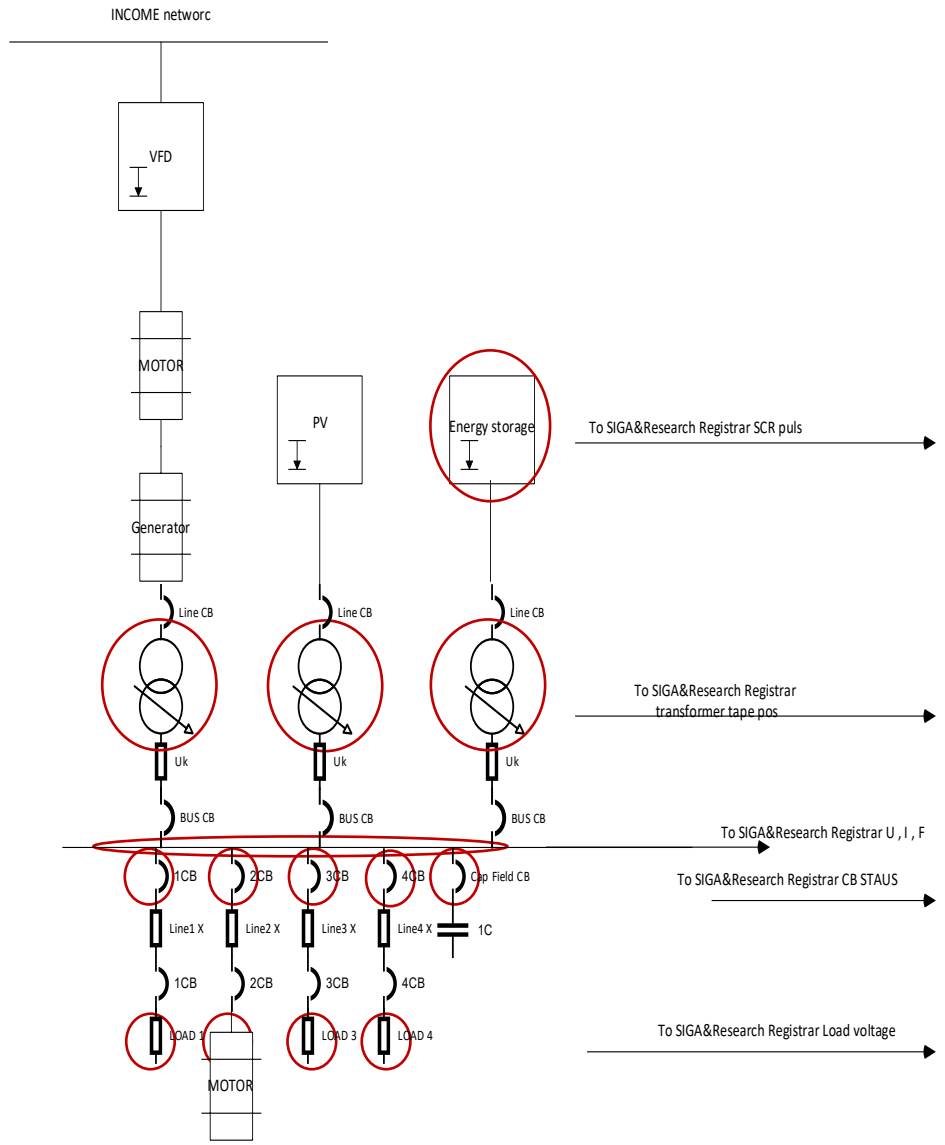
Malicious loss of grid's Inertia

Attack:

Using energy storage SCR's control to invert the grid's inertia's stabilization to divergence.

Tool's goal:

Learning the given storage's SCR's control's normal behavior combined with the input's measured with the grid and storage to identify abnormal control or reaction patterns which can lead to grid's divergence.



Upcoming research tasks

- Setting up lab testbeds for each of the attacks (in collaboration with the partner's lab)
- High sampling hardware – integrating feasible monitoring options
- Adjust framework and algorithmic models to real-time high sampling rate of the data collected
- Validating tool's effectiveness on the given testbeds and attack scenarios
- Strengthening tools' effectiveness when incorporating multi-sites monitoring information