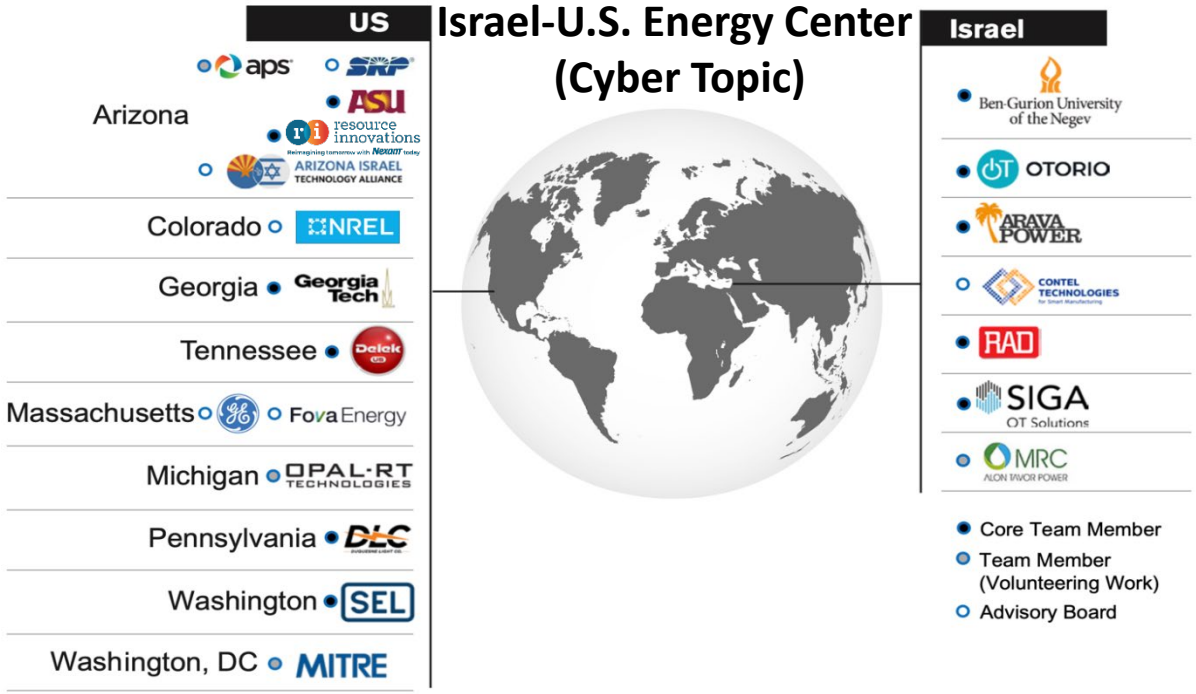
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



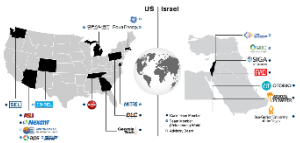
Prepared for

Eitan Yudilevich, Eynan Lichterman, and **Tal Fischelovitch**

BIRD

May 9, 2022

Task 9 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 grid Voltage Collapse
- Malicious loss of grid's Inertia

Attack Scenario NO. 1

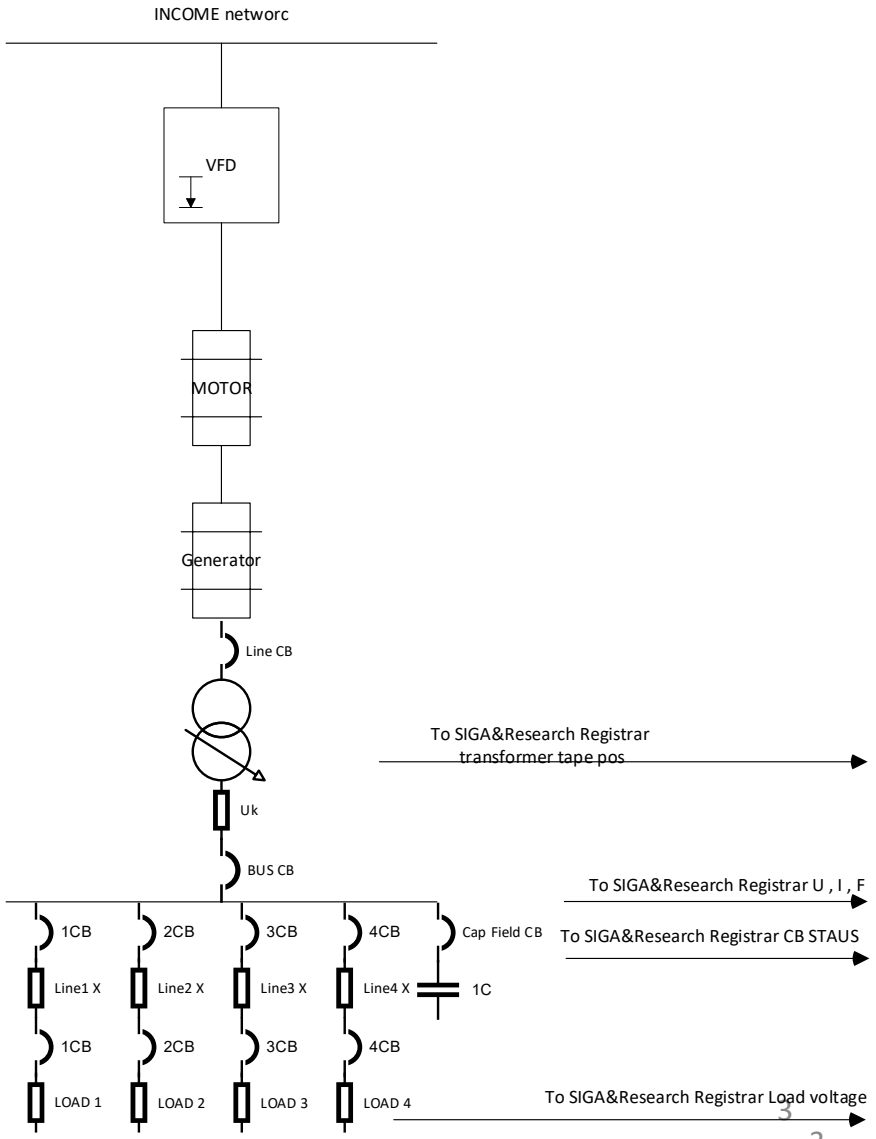
Malicious Voltage Collapse

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 high sampling of the substation's monitored components



Attack Scenario NO. 2

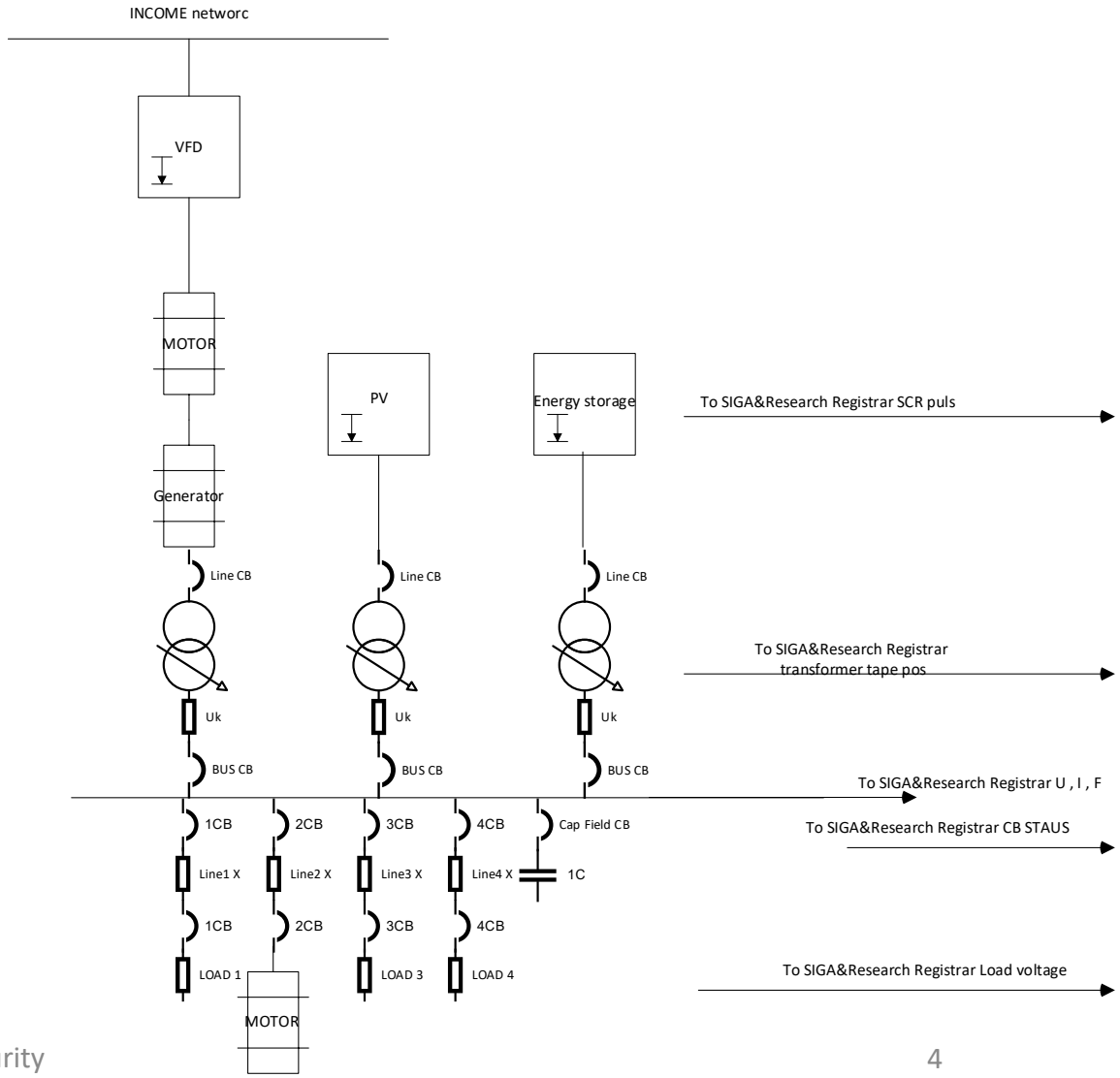
Malicious Loss of Grid's Inertia

Attack:

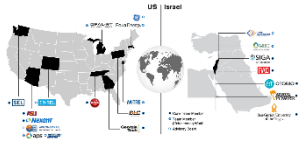
Using energy storage SCR's control to invert the grid's inertia's stabilization to divergence.

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.



Task Research Roadmap



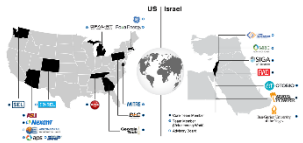
Specifying the addressed attack scenarios and the related grid set-up and conditions → Initial design of a testbed, simulating the grid set-up suitable for the addressed attack scenarios → Specification and detailed design with a partner for the testbed lab → High sampling hardware – locating feasible monitoring devices options

Setting up lab testbeds for each of the attacks (in collaboration with the partner's lab) → High sampling hardware – integrating into the testbed with other SigaGuard components → Run the testbed in the lab and create operational process data for SIGA R&D → Adjust framework and algorithmic models to real-time high sampling rate of the data collected

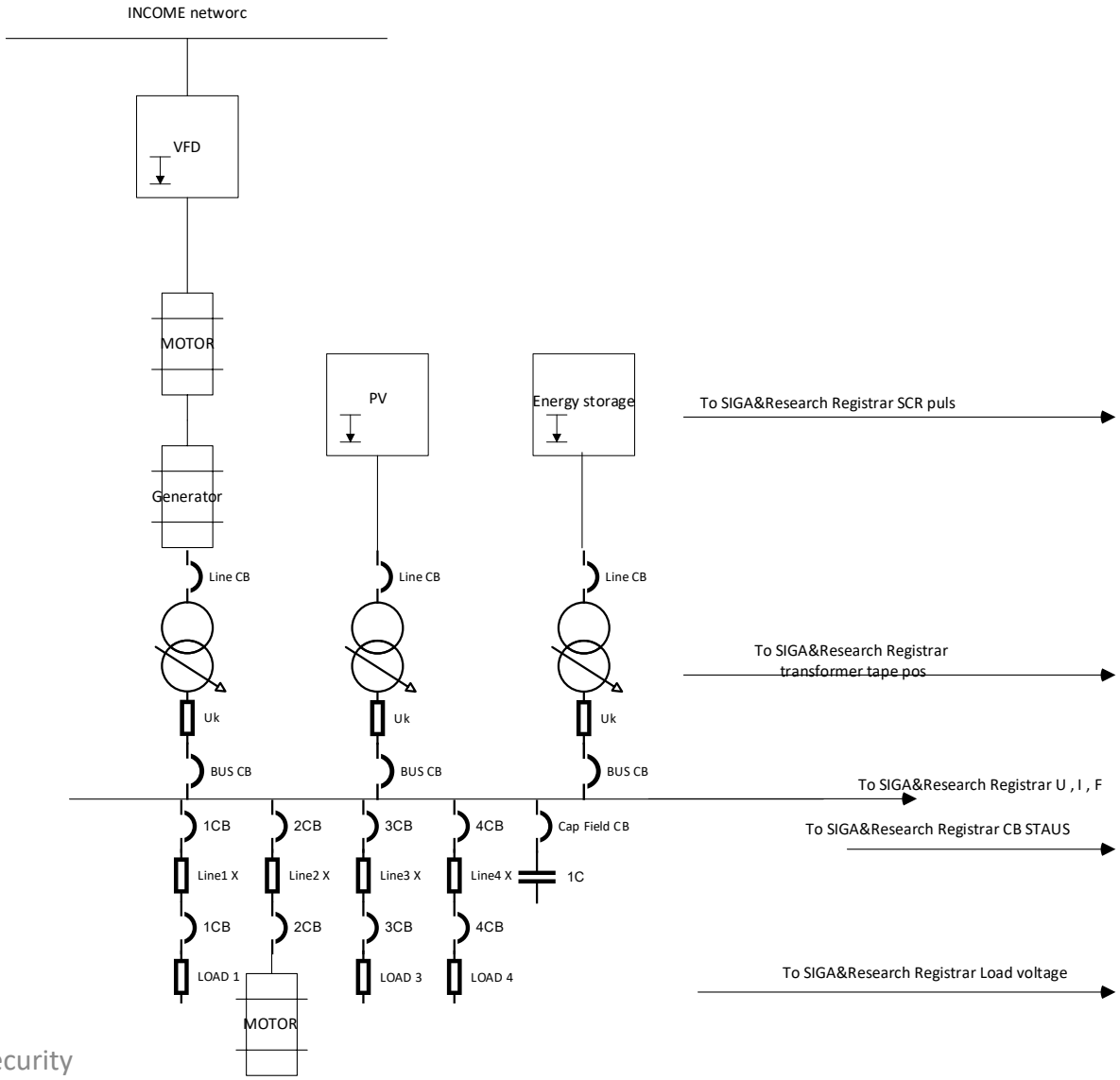
Validating tool's effectiveness on the given testbeds and attack scenarios → Strengthening tools' effectiveness when incorporating multi-sites monitoring information

- Done
- Planned

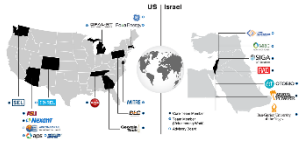
Lab Testbed Design



- Testbed environment is designed to enable the attack scenarios use cases and create data accordingly for research
- Specification of all components has been performed
- Testbed can be established as a physical or a virtual lab (or a combination of the two)
- The set-up of the testbed requires a partner/3rd party with relevant capabilities
- Project budget will be allocated for the lab construction (physically or virtually affect the cost)



Lab Testbed Current Options



1. Physical Lab

All components in the testbed will be physical (according to the design) and it will be built and integrated by one of the consortium partners (Meptagon).

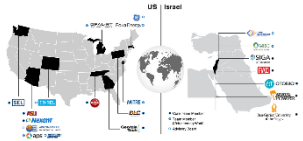
Advantage:

- Close to the real world, mechanical and electrical real-time process data

Disadvantage:

- Complex construction and requires higher funds, comparing to the second option
- Not flexible and limited in capabilities for fine tuning (restricted by equipment installed)

Lab Testbed Current Options



2. Semi-Virtual Lab

Consists of two parts, combined together for testing:

- Hardware rack - is an actual machine which produces the simulated IO's and is connected to a real physical controller
- Level-0 Simulator – creating, managing and activating pre-defined use cases and test scenarios

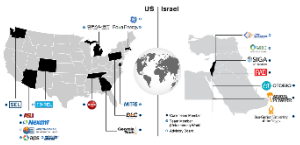
Advantage:

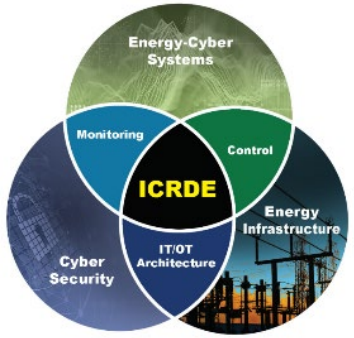
- Flexible, can be adjusted and fine tuned by requirement
- Significantly lower cost than the first option and can be set-up in less time

Disadvantage:

- Doesn't consist of physical real-world electrical equipment

Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-based Centralized Defence and Edge Resilience





Theme 1: Cyber-Physical System (CPS) Data Preparation

- **Project 1**: Physical Processes as Cybersecurity Assets
  - **T1: Realization of advanced energy management applications**
  - **T2**: Digital representation of physical processes and operational process modelling
    - **T3**: Data collection and aggregation
- **Project 2**: Knowledge Base Establishment and Representation Learning of Threats
  - **T4**: Multi-level threat intelligence knowledge base (MITRE)
    - **T5**: Adversarial mimicking (Theoretic)
    - **T6**: Threat hunting (Actively learning)

Theme 2: Data Analytics for Monitoring

- **Project 3**: Cyber Attacks Detection of IT/OT Architecture
  - **T7**: Malware threats mitigation (Smart enemy? Reduce probing and plan)
  - **T8**: Detect event mimicking attacks
    - **T10**: Multilayer anomaly detection (Uncertainty)
    - **T9**: False Data Injection (Physical Embedding)
  - **T11**: AI-based intrusion detection (Engage operator)
  - **T12**: Explainable cyber-AI analytics (Metric + Temporal)

Theme 3: Control and Validation

- **Project 4**: Cyber Resilience and Robustness for Control Actions
  - **T13**: Firmware verification (Edge)
  - **T14**: Attack tolerance (Insensitive to the attack)
  - **T15**: Self healing and auto-remediation (Optimization)
    - **T16**: RL control for CPS (Advise Sys Operator)
- **Project 5**: Future-Proof Architectures
  - **T17**: ICS security by design
  - **T18**: Hardware in the loop