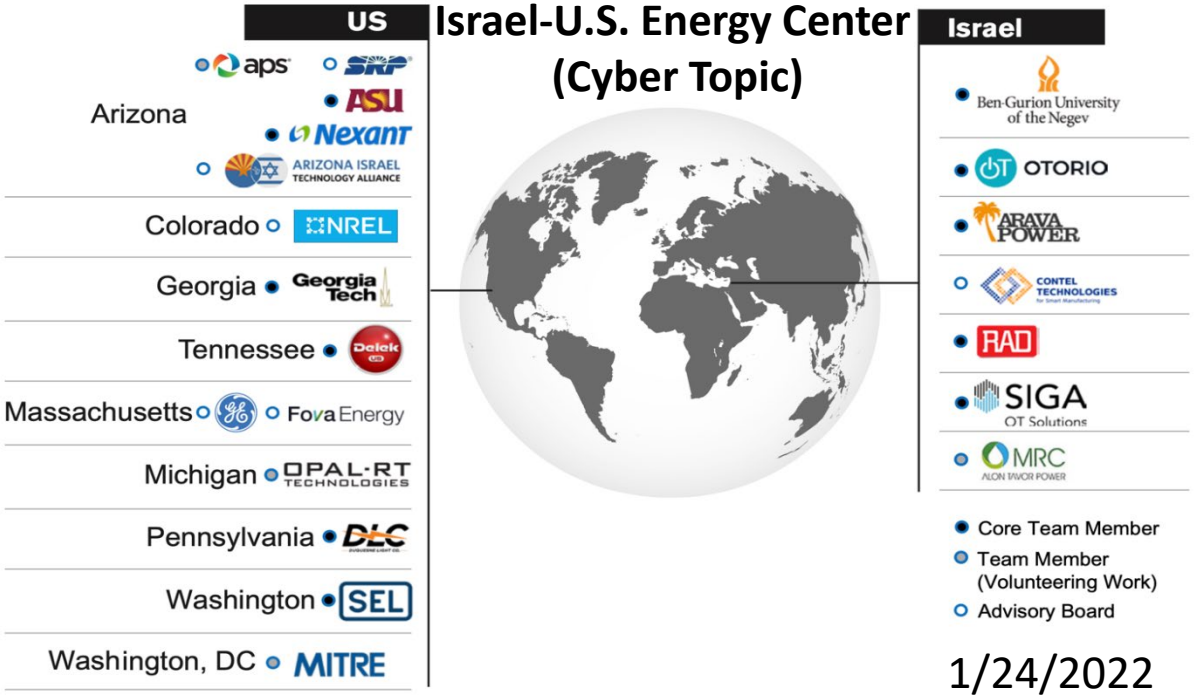
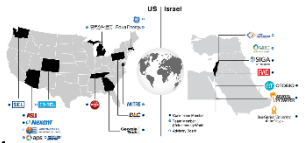
# BIRD ICRDE: Task 17 - ICS Security by Design




1/24/2022

# Introduction



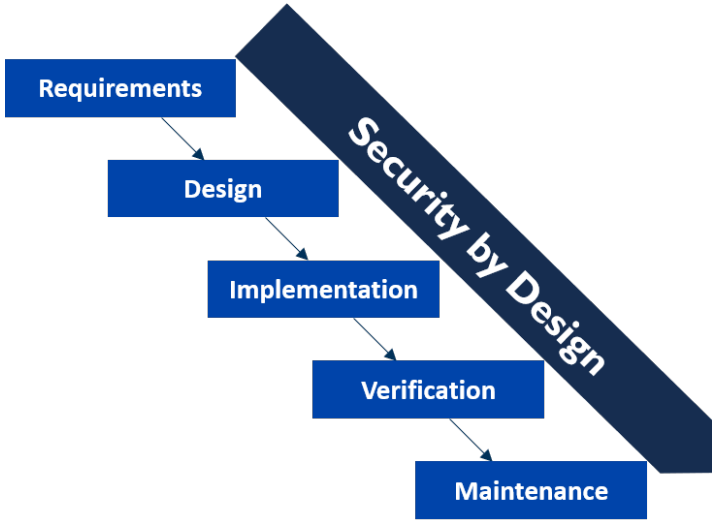
Yuval Elovici

- Today, there are mechanisms for protecting the industrial control system infrastructure.

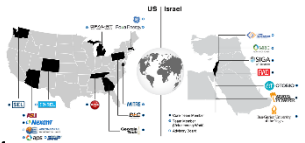
- The common approach is to develop/deploy security solutions to address the security requirements under the constraints of the current ICS environments

- The deployed solutions cannot provide optimized security (IDS, honeypots, encryption, Blockchain, etc.) since they were not designed as part of the ICS.

- There is a need to adopt the concept for security-by-design in the development of new ICS systems.



# Goal



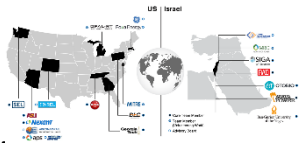
Yuval Elovici

- Designing and developing a blueprint for a future ICS environment, that considers security by design.

- The design will cover the various aspects and components of the ICS environment including the endpoints, internal network communication, monitoring, and interfaces with external networks.

- The secure ICS architecture will be used as a future reference for vendors, energy facilities, engineering and integration companies, as well as governments and regulators.

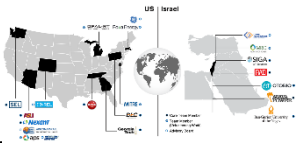
# Proposed Method



Yuval Elovici

- The design will take into account the availability of state-of-the-art technologies, such as IIoT, SDN, cloud and edge computing, Blockchain, deep learning, 5G/O-Ran
- Focus on providing the following main capabilities:
  - Automated network visibility, asset management and modeling of operational processes;
  - Trusted monitoring
  - Automated attack detection and auto-remediation
  - Authentication of elements and encryption of data
  - Ability to integrate third-party “untrusted” elements;
  - Seamless and secure delegation of analytical tasks to edge/cloud environments;
  - Continuous attack graph-based risk assessment;
  - Integration of OT and IT data;
  - Redundancy

# Proposed Method



Yuval Elovici

- To achieve the objectives of this activity we will:
  - Map new and future technologies that can be integrated into the future ICS (energy) environment
  - Collect the security requirements
  - Review related work, including future technologies design (e.g., future Internet, G5/O-RAN), as well as novel security solutions; conduct deep analysis of strengths and weaknesses for relevant identified works.
  - Map a set of solutions for every attack vector and technique, as identified by MITRE ATT&CK ICS, within the context of:
    - (1) ICS equipment (Hardware, software, firmware);
    - (2) ICS communication protocols;
    - (3) Inter-operability and integration between different equipment sets and vendors
  - Rendering consolidated architecture