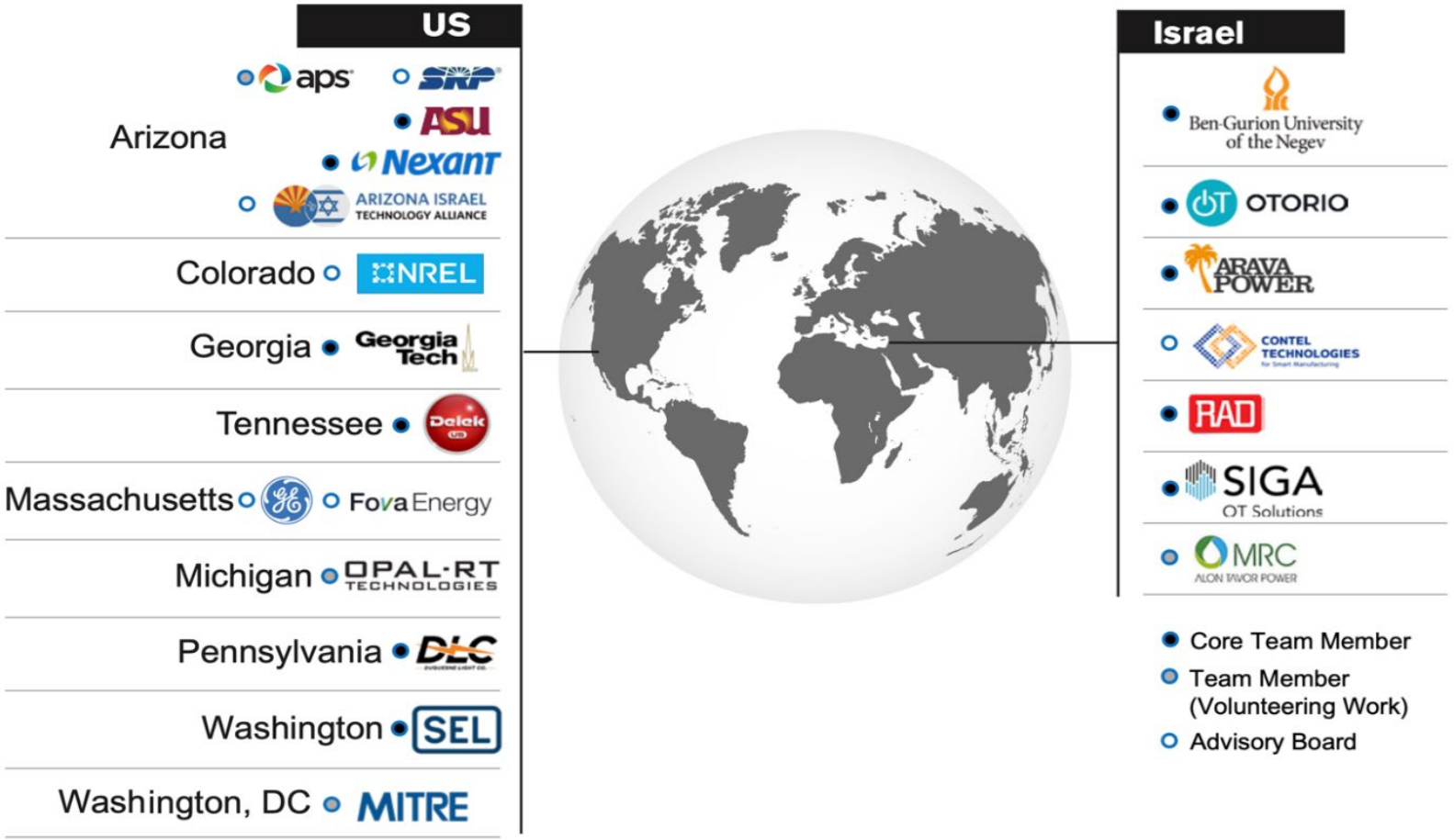
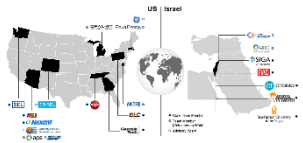
BIRD ICRDE: Task 17 - **ICS Security by Design**



Israel-U.S. Energy Center
(Cyber Topic)

05/09/2022

Work Package 1

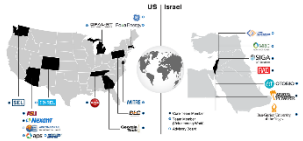


Dov Shirtz

WP1 - Requirements

- Identify **current cybersecurity issues** which are **relevant now** and may be **relevant for future energy cybersecurity**.
- **Gather requirements** for desired attributes of **secure ICS architecture**.
- **Define relevant criteria** against which architecture proposals will be evaluated, as well as on the method of evaluation.

Activities



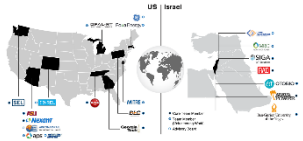
Dov Shirtz

- We have just started survey:
  - Academic papers;
  - International standards (e.g., IEC/TS 62443, NIST.SP.800-160, NIST.SP.800-218);
  - Best practice proposed by the industry (e.g., MITRE ATT&CK ICS, SANS);
- Started to take-in and map:
  - Security issues;
  - Security-by-design requirements for future ICS;
  - Criteria to check and test the future energy ICS architectures;

- **Note**

  We assume the following WPs of task 17 (e.g., mapping relevant commercial solutions and so on) may influence the 1st WP deliverables.

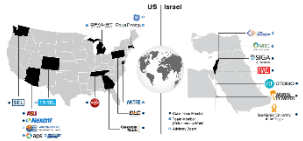
Security Issues



Dov Shirtz

- Definition
- Mapping and Categorization;

Security Issue – Definition



Dov Shirtz

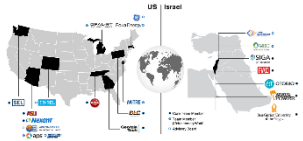
Fajarsari, defines **cybersecurity issue** as:

> **“any unmitigated risk or vulnerability”** [Fajarsari 2018].

This definition includes possible risks and unmitigated vulnerabilities **resides in any component within the** industrial control system (ICS) e.g., hardware, firmware, software, networking, protocols, and human factor.

Fajarsari, Herlia M. "Managing Cybersecurity Risk in Process Control System." (2018).

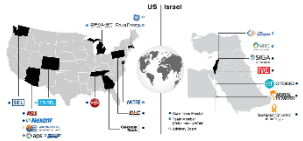
Security Issues - Mapping and Categorization



Dov Shirtz

- **Identify Cybersecurity issues** found in
  - Academic papers
  - Available Blogs
  - MITRE
  - Best practice documentation
  - …
  - **Categorize them**

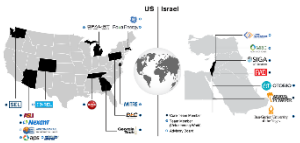
Security-by-Design Requirements for Future ICS



Dov Shirtz

- **The goal** is to suggest a security-by-design framework for future ICS
- Security is to be integrated at the **very beginning** stage of an ICS planning and be prioritize at the highest level
- Therefore, each component within the ICS should follow the security requirements imposed by the future Security-by-design document.
- Embrace advanced security remedies used in IT environment into the ICS environment
  - e.g., isolation, redundancy, segmentation, diversity, visibility, monitoring,…
  - e.g., frameworks such as:
    - Zero Trust
    - Cyber–Kill Chain methodology
    - Blockchain technology
    - Moving target defense

Criteria to Check & Test the Future Energy ICS Architectures



Dov Shirtz

- We only have a brief investigation into this subject
- Currently, we do not have any solid conclusions regarding this subject