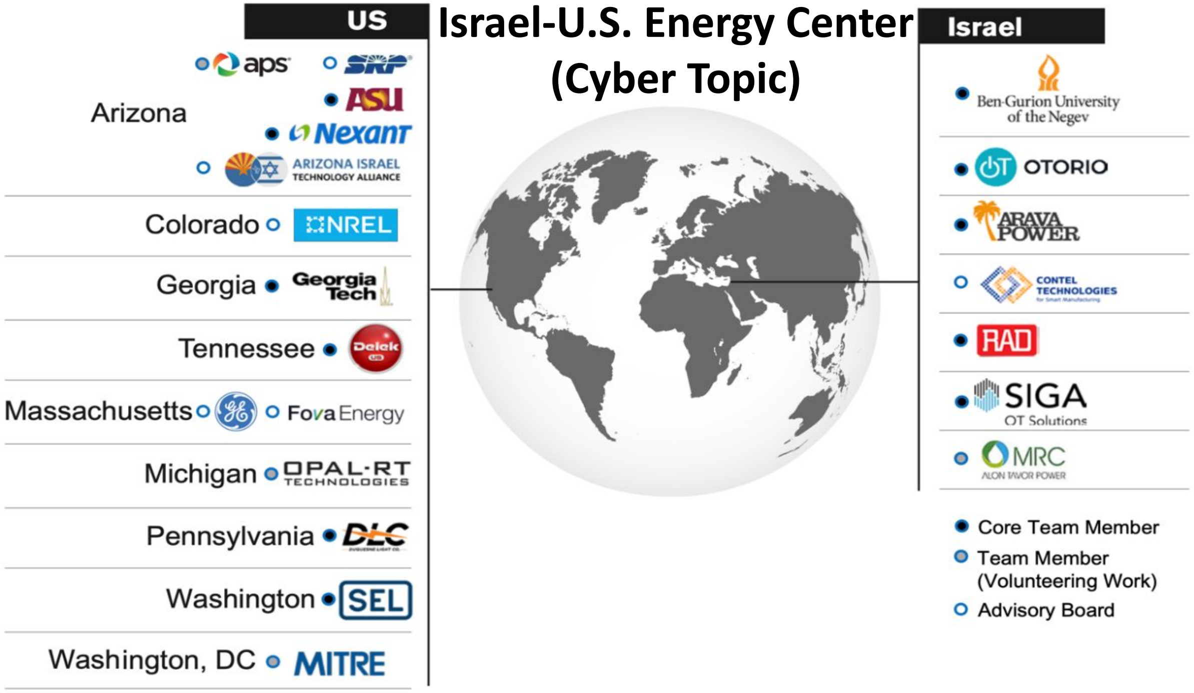
BIRD ICRDE: Closing the Gap



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

US

Arizona
- ◉ aps
- ○ SRP
- ● ASU
- ● Nexant
- ○ Arizona Israel Technology Alliance

Colorado ○ NREL

Georgia ● Georgia Tech

Tennessee ● Delek US

Massachusetts ○ GE ○ Fova Energy

Michigan ◉ OPAL-RT Technologies

Pennsylvania ● DLC Duquesne Light Co.

Washington ● SEL

Washington, DC ◉ MITRE

Israel

- ● Ben-Gurion University of the Negev
- ● OTORIO
- ● Arava Power
- ○ Contel Technologies for Smart Manufacturing
- ● RAD
- ● SIGA OT Solutions
- ◉ MRC Alon Tavor Power

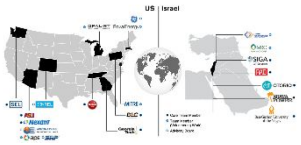
● Core Team Member

◉ Team Member (Volunteering Work)

○ Advisory Board

Oct. 2023

Closing the Gap



Dov Shirtz

Migration to the Cloud

Except for the Physical layer – i.e., sensors actuators etc., all other layers of OT and IT can reside in the cloud. It is especially challenging in the energy sector due to its unique characteristics, such as real-time, safety issues, etc.

ICS cyber protection mechanism using AI and ML

In this research, we aim to create a mechanism that continuously checks the systems for vulnerabilities, potential risks, etc. Utilizing internal and external information. Identifying and investigating techniques for prioritizing and remediating vulnerabilities.

Supply chain security

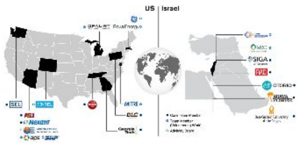
Research methods to secure the supply chain components and software. Developing methods for evaluating, assess, and test the security of 3rd party vendors and contractors.

Integrate cyber security and quality assurance regulation, standards, and best practices (*)

When it comes to cyber security and quality assurance, regulations, standards and best practices are quite prevalent. There may be a need for the industry to establish a list of cyber security and quality assurance requirements, together with SbD requirements. Implementing that can serve as a guide for product development, network design, software design and coding, testing, and implementation. Furthermore, this research can lead to the creation of commercial products.

(*) These ideas have been mentioned in the following "Security by Design Requirement for the Energy Sector“. document. Published on May 2023 to the consortium.

Closing the Gap



Security event logging

Currently the improve the capabilities OT lower-layer devices (e.g., PLCs) have limited logging capacity.

Research aims:

- To improve and security visibility of lower-layer devices.
- Create an evolving configuration of log security events based on the updated information.
- Develop a method for aggregating and correlating different events – security and operational

In light of the energy sector unique characteristics e.g., real time, safety issues, etc.

Integrate threat detection and device health check information

In some cases, Cyber-attacks on the OT level can cause damage to the device, organizational network and the environment.

Continues measurements of device behavior or results may indicate an ongoing attack or malfunction.