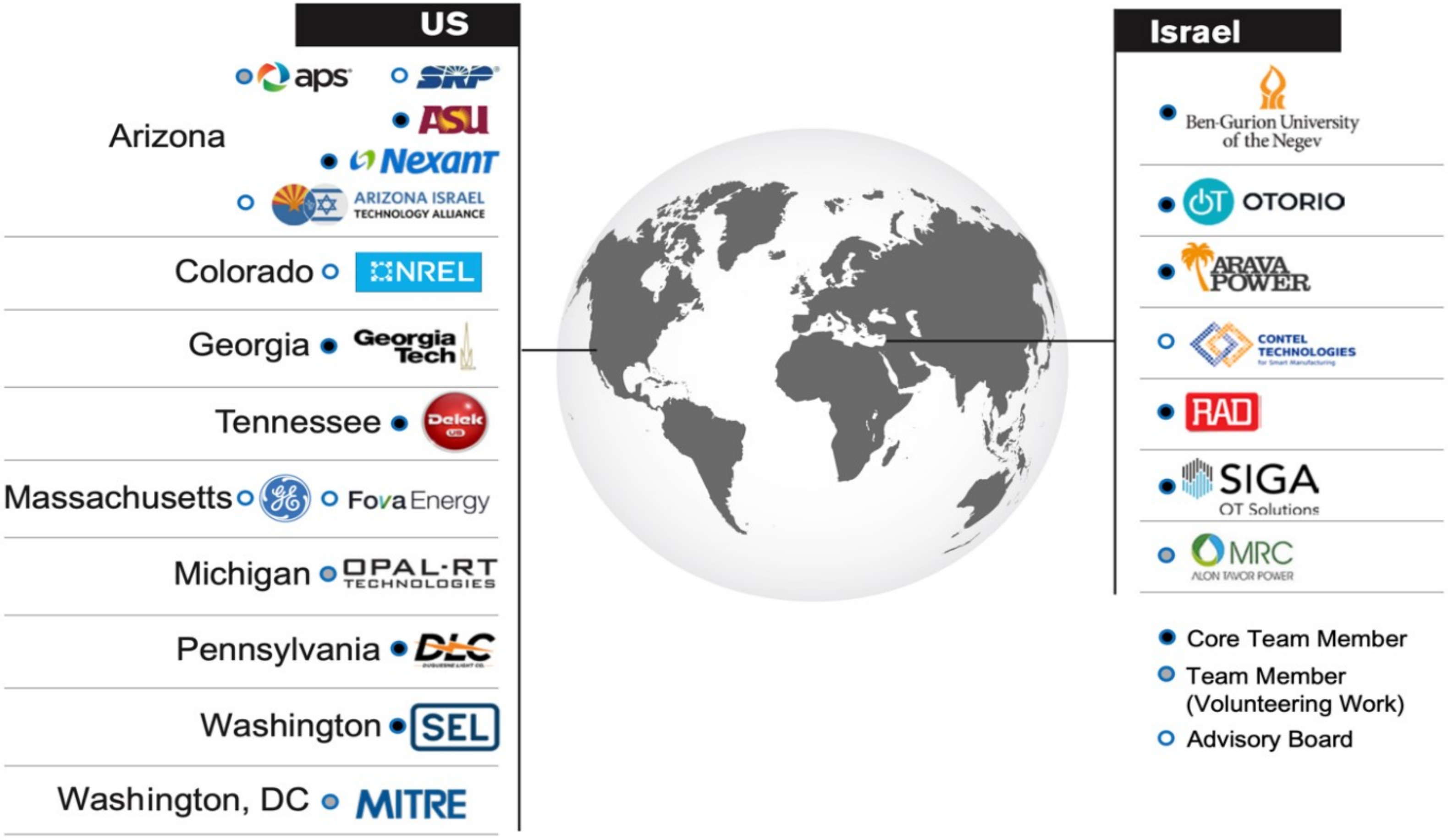
BIRD ICRDE: Task 17 - **ICS Security by Design**



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

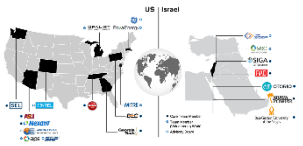
◉ Team Member (Volunteering Work)

○ Advisory Board

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

08/24/2022

Work Package 1 - requirements

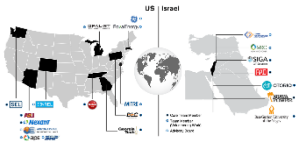


Dov Shirtz

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

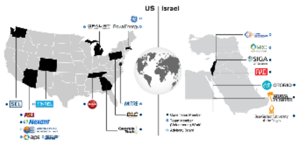


- We surveyed:
  - Academic and nonacademic papers;
  - International standards (e.g., IEC/TS 62443, NIST.SP.800-160, NIST.SP.800-218);
  - Best practice proposed by the industry (e.g., MITRE ATT&CK ICS, SANS);
- Identify and map:
  - Security issues;
  - Security-by-design requirements for future ICS;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

- **Note**

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

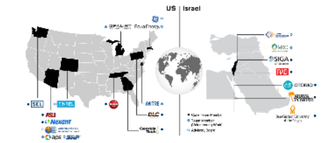
Security Issues



Dov Shirtz

- Definition
- Mapping and Categorization;

Security Issue – Definition



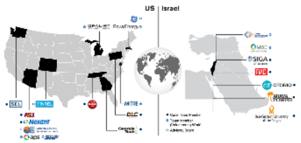
Fajarsari, defines **cybersecurity issue** as:

“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

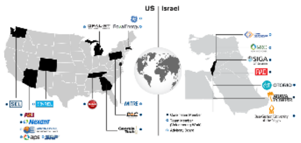


- **Our question is**
    - What types of security issue are today and will probably last to the future?

- We have come out of 3 groups of security issues.

    - Human related
    - Technological related
    - Policy / managerial related
    - A combination of the above

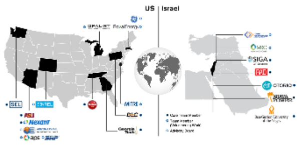
Security Issues - Mapping and Categorization



An example from the list

#	Security issue	Human related	Technology related	Policy/ managerial related
1	Lack of security policy	+		+
2	Bring your own device	+		+
3	Human factor	+		
4	Predictability in design		+	
5	Encryption		+	
6				
7				

Security-by-Design (SbD) Requirements for Future ICS

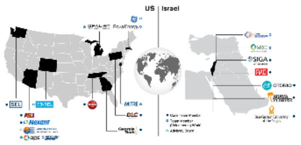


Dov Shirtz

- **The goal** is

  Suggest a security-by-design framework / list of requirements 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

Security by Design (SbD) - Introduction

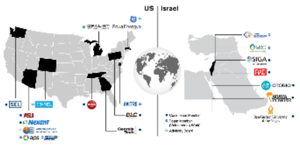


- SbD is not just for those techies i.e., programmers, engineers,…
- SbD is not just for my organization
- SbD is not just a technological subject

So, What is SbD?

Basically, as all standards and best practices it is a **list of requirements**
That should be **evolve over time**
Its goal
If implemented properly is to improve the overall security of the ICS

Security by Design (SbD) - Introduction

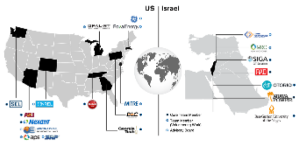


- SbD is not just for those techies i.e., programmers, engineers,…
- SbD is not just for my organization
- SbD is not just a technological subject

- SbD is a cross organizations effort my organization, business partners, manufacturers,…
- SbD is a managerial issue
  - SbD starts from the top – Management and Directorate
- SbD goes down to everyone in the organization
- SbD is a technological issue as well

WHY?

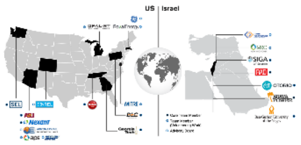
Security by Design (SbD) – Our point of view



Dov Shirtz

- Currently The suggested SbD is of two parts
  - A general part
  - Technological part

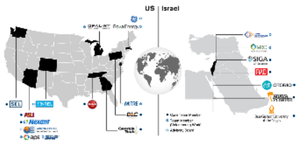
Security by Design (SbD) – Our point of view



Dov Shirtz

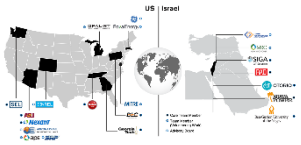
- **The general part that deals with aspects such as:**
  - "Soft requirements" e.g., management, directorate, and CISO, obligations, audit, …
  - Asset management e.g., inventory, ownership, mapping & classification
  - Security infrastructure e.g., access control, certification of devices and software, logs, data integrity, encryption, SIEM/SOC,
  - Architecture e.g., segmentation, DMZ, different environments, MFA, penetration tests,
  - Encryption, digital signature, certifications
  - Remote access

Security by Design (SbD) – Our point of view



- **The technological part includes**
  - Development life cycle
    - Requirement phase
    - Design phase
    - Development phase
    - Test phase
    - Deployment phase
    - Maintenance phase
    - Disposal phase
  - Some other technologies to be used

Security by Design (SbD) – Our point of view



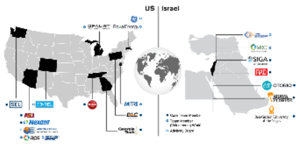
Dov Shirtz

- Development life cycle

Requirement phase

#	Activity	#	Activity
a	Risk analysis	i	Communication
b	Quality assurance	j	Remote access
c	Identification & authentication	k	Segregation of duties
d	Access control	l	Segmentation
e	Logs / Historians	m	Perimeter security
f	Audit	n	Backup and recovery
g	Tests	o	Physical security
h	Security	p	Low and regulations

Security by Design (SbD) – Our point of view



- Development life cycle

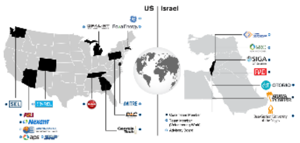
  - Design phase

  Design each requirement with respect to security

  - Examples of activities

  Decide on secure coding standards
  Check for possible violations of standards and best practices
  Build a threat modeling to identify threats = > ability to identify vulnerabilities
  Architecture risk analysis
  Perform review design
  Decide on test environment, test scenarios,
  Insert all the security remedies, and countermeasures inside the development
  Design the backup and recovery process what we need to do at emergency
  ::

Security by Design (SbD)



- Development life cycle

  - Development phase

  Secure coding

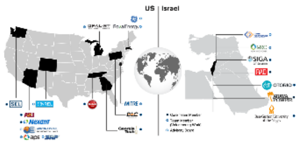
  Coed review – static analysis via COTS products and manually

  Version management

  Enhance testing scenarios

  ::

Security by Design (SbD)

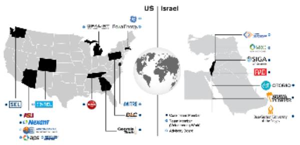


- Development life cycle

  - Test phase

  Build a testbed that is a small-scale replica of the real i.e., production, environment
  Use the risk analysis, from previous phases to design tests
  Run conventional and known test methods, Blackbox, Whitebox, …
  Run security test – e.g., scenarios for deferent inputs, …
  Run penetration tests – outside- inside and inside-outside,
  ::

Criteria to Check & Test the Future Energy ICS Architectures



Dov Shirtz

- From the SbD = > 1’st part of criteria
- Architecture survey is included in the next phase = > 2’nd part criteria