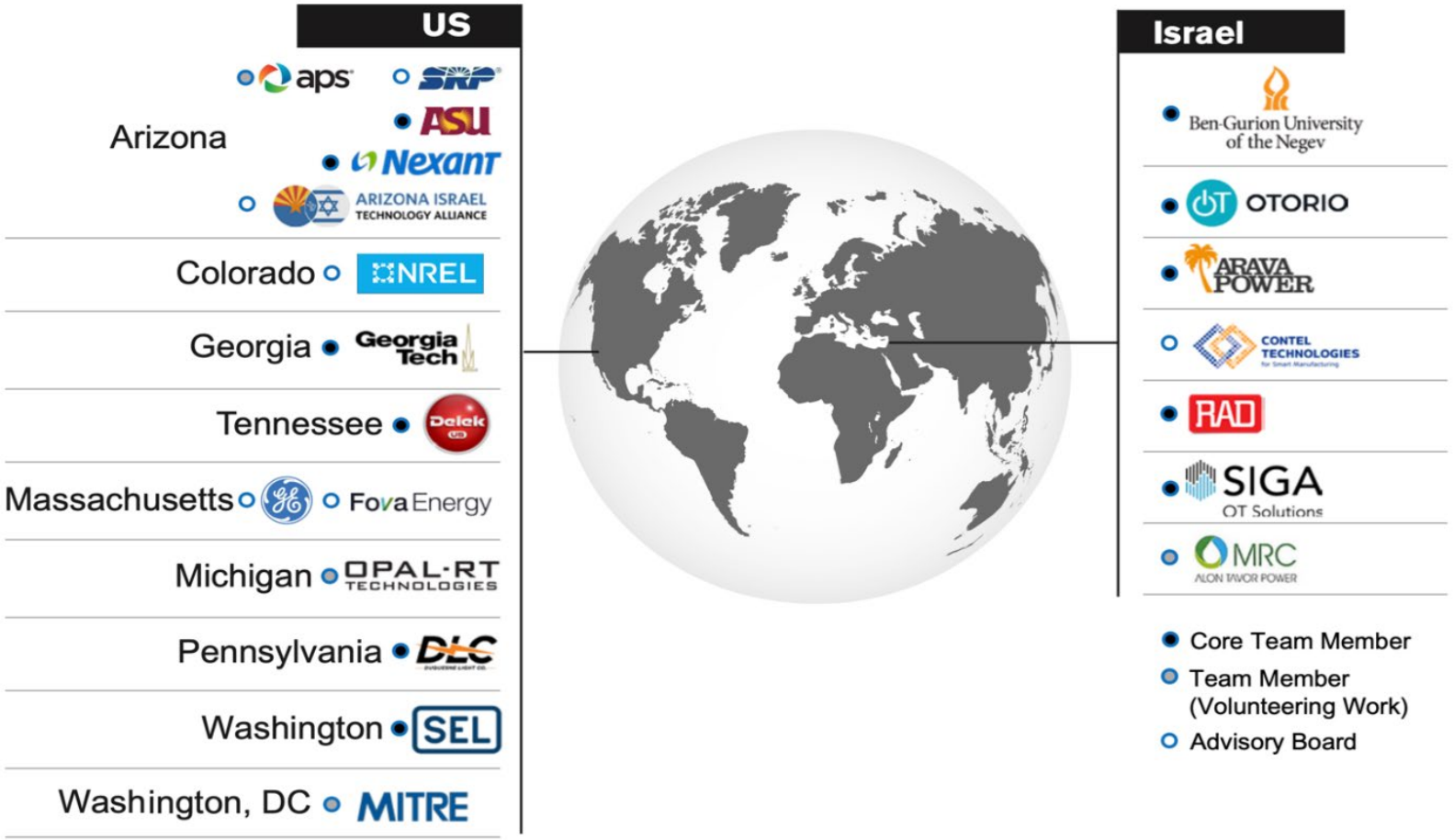
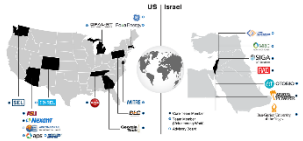
BIRD ICRDE: Task 17 - **ICS Security by Design**



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

2023.03.18

Introduction



Dov Shirtz

Task 17 deals with the future

= > We are not bound to current concepts

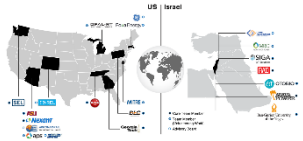
We are not trying to predict the future; we try to be visionary

We propose a framework for achieving the Security by Design goal

Security by Design

Dov Shirtz

Assumptions and prerequisite



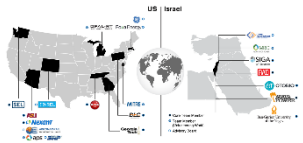
Dov Shirtz

Law and regulations

Industry requirements will force the use computerized devices at all levels of the Purdue model

We do not negate any security standard, or best practice, but rather, we mandate them

Framework

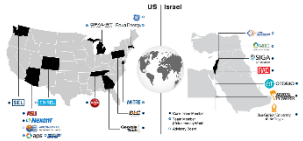


Dov Shirtz

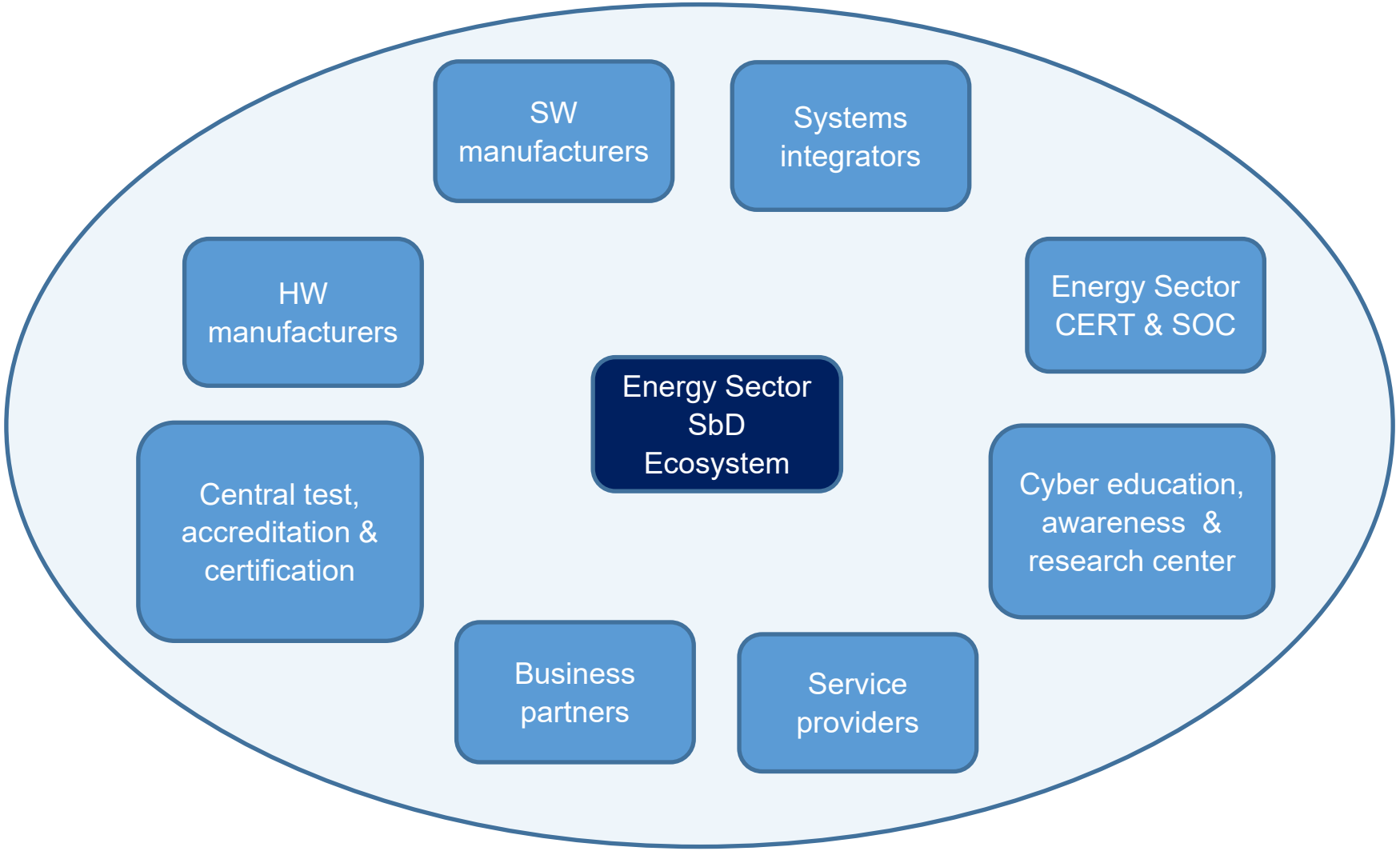
We propose a framework consists of

- **Proposing to construct an ecosystem that includes all participants**
- **Non-technological Issues**
- **Technological Issues**

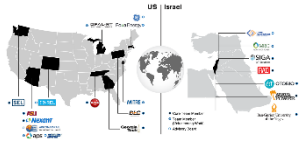
Framework - Ecosystem



Dov Shirtz



Framework – Non-Technological Issues



Dov Shirtz

Governance

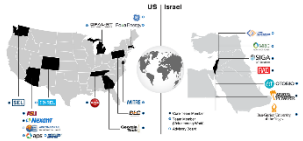
Board and Senior management

Internal audit

CISO

appointment, status in the organizational hierarchy, responsibilities

Framework – Technological Issues



Dov Shirtz

Standards, best practices and accreditation

Asset management

Inventory, ownership, acceptable use, mapping and classification

Security infrastructure requirements

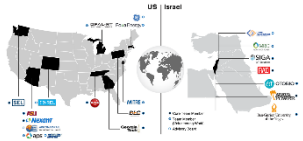
Access control, remote access control, encryption, certification, Date and time synchronization, audit logs, integrity, data, physical security, maintenance, risk assessment and audit, SIEM/SOC,…

Architectural elements

Network

Security by Design for system development

Framework – Technological Issues



Dov Shirtz

Standards, best practices and accreditation

Asset management

Security infrastructure requirements

Architectural elements

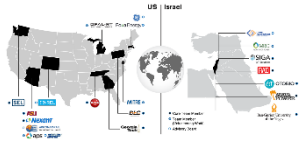
A list to requirements related to SbD implementation

Network

Network management, network elements, encryption

Security by Design for system development

Framework – Technological Issues



Dov Shirtz

Standards, best practices and accreditation

Asset management

Security infrastructure requirements

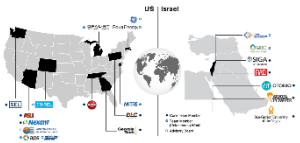
Architectural elements

Network

Security by Design for system development

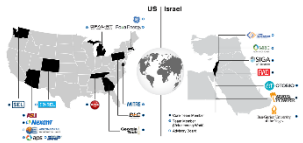
SbD requirements from each phase of the SDLC – requirements, design, development, testing, deployment, maintenance, disposal

Security solutions in academic papers – A survey



Dov Shirtz

Introduction



Dov Shirtz

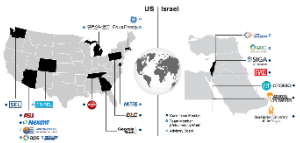
No silver bullet

= > searching and surveying suggested solutions

setting criteria for each solution type

setting some general criteria common to all solutions

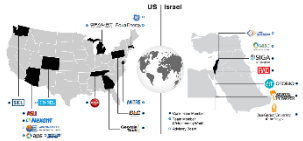
Proposed Method



Groups of solutions

- **Encryption**
- **Authentication**
- **Visibility**
- **Blockchain**
- **Zero trust**
- **Digital twin**
- **Network segmentation**

Common criteria



Dov Shirtz

Common

Performance – CPU overhead, Memory overhead, Latency

Testing – Theoretical, simulation test, lab test, real environment test

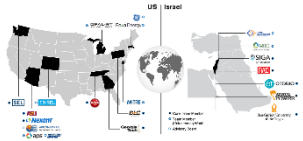
Scalability

Operational on – The environment the solution is designed to operate, communication protocols

Interaction – Interaction with other security solution,

Latency – Time to have results of a computational process

Encryption criteria



Dov Shirtz

Algorithm

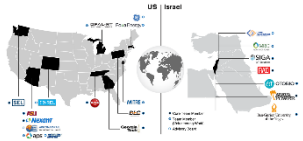
Target – Data-in-move, data-at-rest, data-in-use

Strength – Cryptographic strength

Implementation aspects

- **Implemented by** – Hardware, Software
- **Limitations** – Attack resistance, vulnerable to,
- **Compatibility** – Down version compatibility, HW

Authentication criteria



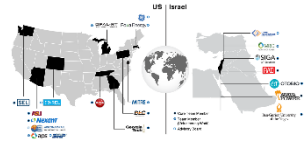
Dov Shirtz

Basic attributes – HW based, historical data, cryptography used, Inheritance

Implementation features

- **Requires additional components** - Tokens, TEVM
- **Encryption**
- **Mutual authentication**

Visibility criteria



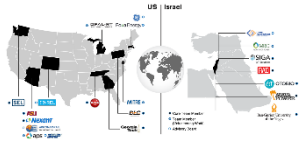
Dov Shirtz

Work environment

- **Device, user information** – CPU, communication and memory overhead
- **Memory**
- **Data, Data files**
- **Network**
- **Logs**

Detectability of irregularities

Blockchain criteria



Dov Shirtz

Type

Consensus algorithms

Platform

Governance model

Storage