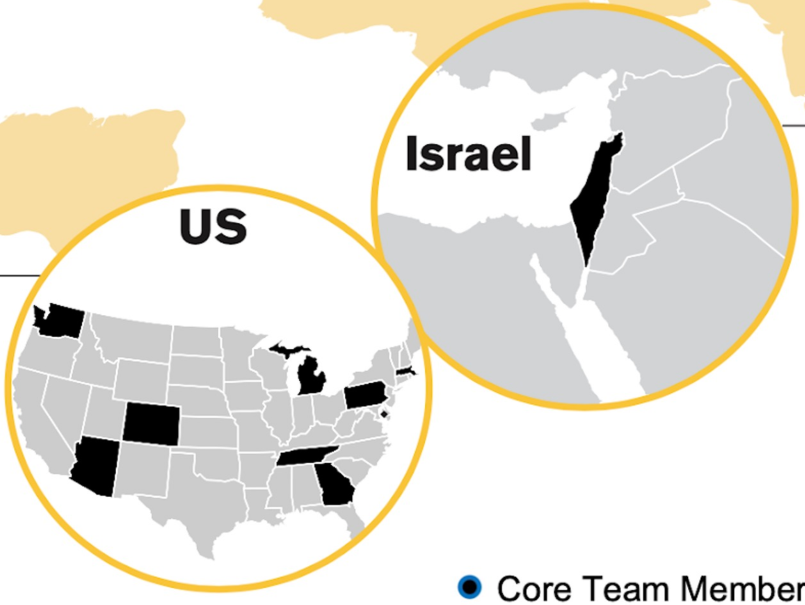
US-Israel Energy Center

US-Israel Cybersecurity Research and Development for Energy (ICRDE)

Arizona	●	ASU
	●	resource innovations
		ARIZONA ISRAEL TECHNOLOGY ALLIANCE
Colorado	○	NREL
Georgia	●	Georgia Tech
Tennessee	●	Delek US
Massachusetts	○	Fova Energy
Michigan	◉	OPAL-RT TECHNOLOGIES
Pennsylvania	●	DLC DUQUESNE LIGHT CO.
Washington	◉	SEL
Washington, DC	●	MITRE



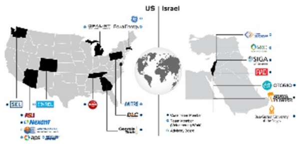
U.S.-Israel Energy Center

● Core Team Member

◉ Team Member (Volunteering Work)

○ Advisory Board

meptagon head for a better process	●
CONTEL TECHNOLOGIES for Smart Manufacturing	○
MRC ALON TAVOR POWER	◉
SIGA OT Solutions	●
Ben-Gurion University of the Negev	●
OTORIO	●
ARAVA POWER	●
cybereason	○
RAD	●
DK INNOVATION	●



PANEL B:

ATTACK DETECTION AND MITIGATION

Adam Hahn MITRE

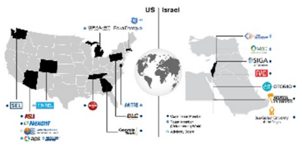
Principal Critical Infrastructure Security Engineer

@ The MITRE Corporation

MODERATOR @ PANEL B

PANELISTS @ PANEL B:

ATTACK DETECTION AND MITIGATION



John Geiger
Senior Sales Director
RAD Data Communications

Mayank Malik
Information Systems Spec
SLAC National Accelerator Laboratory

Ying-Chang Lai
Regents Professor
ASU

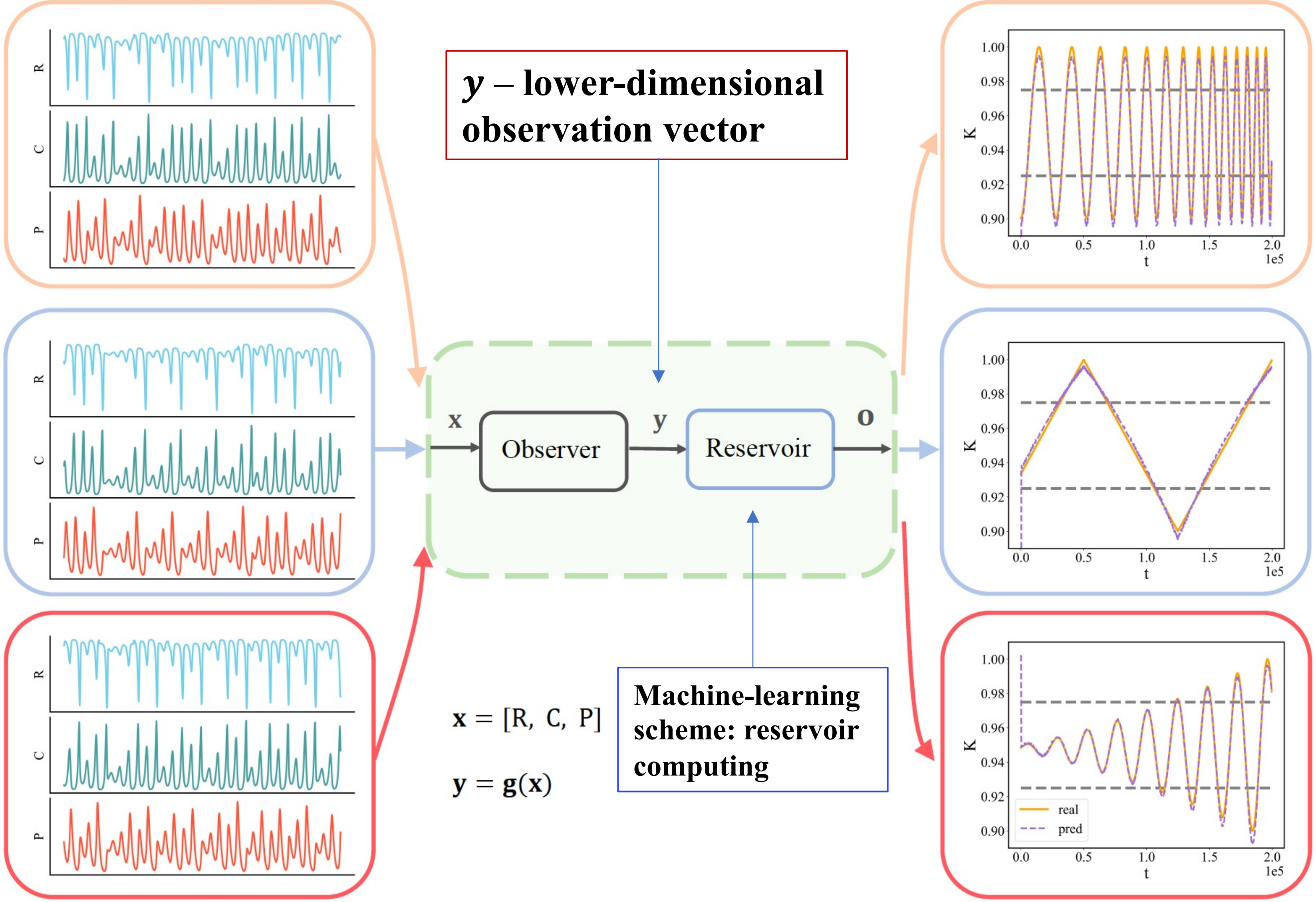
Michael Hylton
Senior Sales
Director of
Cybersecurity
SIGASec

Harry Thomas
OT Security
Advisor
OTORIO

Sherry Jacob
Senior Manager
Accenture

Partial State Observation for Parameter Tracking

Full state of the system



y **– lower-dimensional observation vector**

$\mathbf{x} = [\mathrm{R},\ \mathrm{C},\ \mathrm{P}]$

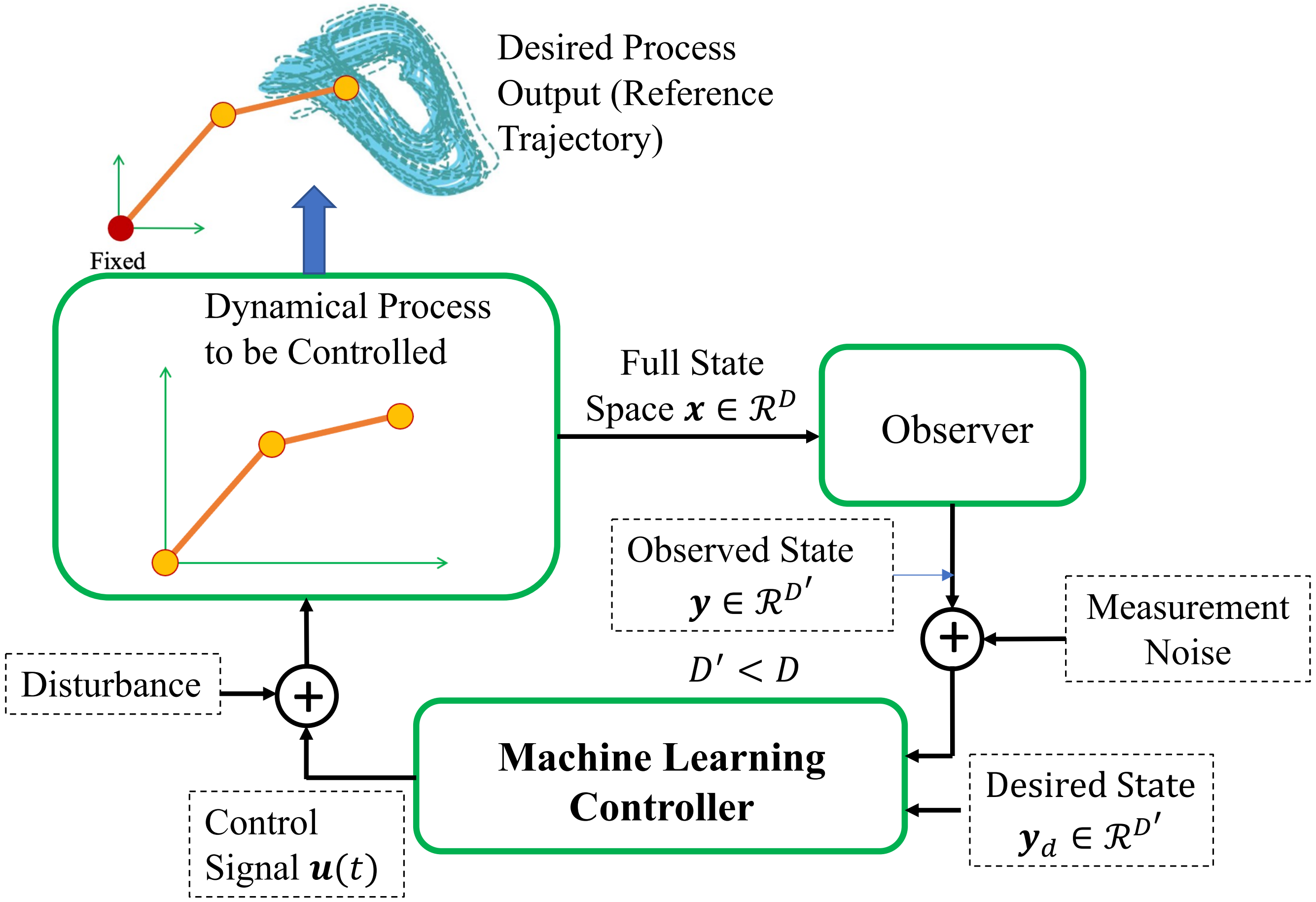
$\mathbf{y} = \mathbf{g}(\mathbf{x})$

Machine-learning scheme: reservoir computing

Parameter as a function of time

Z.-M. Zhai, M. Moradi, M. Haile, and Y.-C. Lai, "Tracking parameter variations in nonlinear dynamical systems using machine learning," preprint (2023)

Partial State Observation for Tracking Complex Dynamical Trajectories


Desired Process Output (Reference Trajectory)
Fixed
Dynamical Process to be Controlled
Full State Space $\boldsymbol{x} \in \mathcal{R}^D$
Observer
Observed State $\boldsymbol{y} \in \mathcal{R}^{D'}$
$D' < D$
Measurement Noise
Disturbance
Machine Learning Controller
Control Signal $\boldsymbol{u}(t)$
Desired State $\boldsymbol{y}_d \in \mathcal{R}^{D'}$

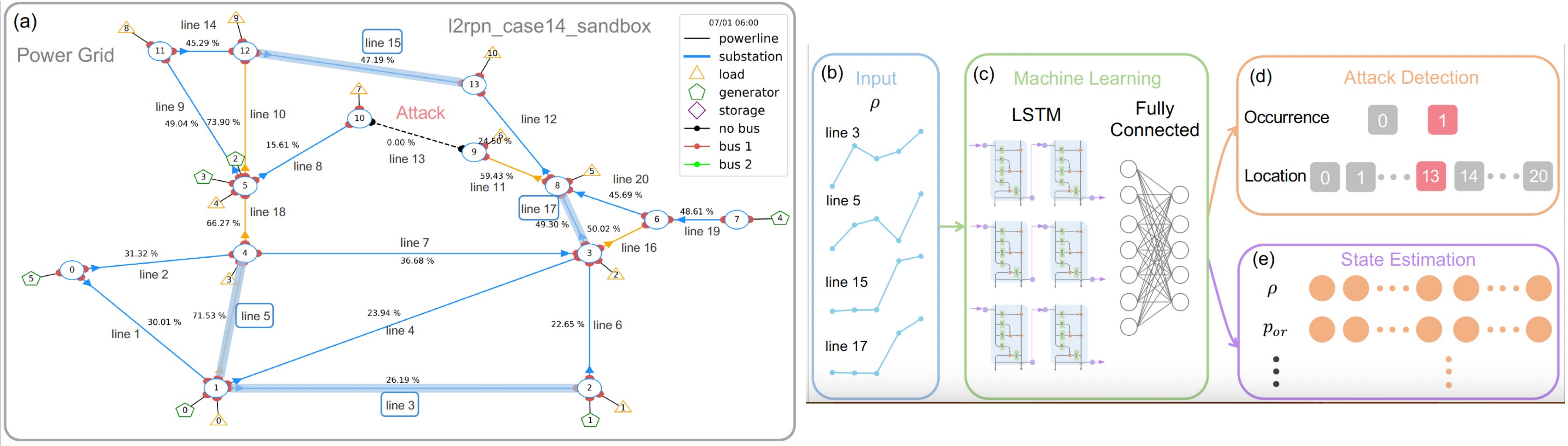
Unique features:

- Model-free
- Requiring only **partial observables**
- Stochastic signal for training
- Time-delayed input configuration for training

Z.-M. Zhai, M. Moradi, L.-W. Kong, B. Glaz, M. Haile, and Y.-C. Lai, "Model-free tracking control of complex dynamical trajectories with machine learning," *Nature Communications* **14**, 5698, 1-11 (2023). Highlighted as a Featured Article by Editors.

Partial State Observation for Attack Detection

- Investigate the practical issue of partial state observation by developing an LSTM (long short-term memory) based framework for attack detection and full state estimation. Commercialization will be explored.



Ongoing collaborative work

Secure Utility Networks

John Geiger

October 10, 2023

RAD

Your Network's Edge®

Delivering

INNOVATION

Critical Infrastructure

- Critical Infrastructure assets are often very long-lived and reflect massive investments in operational, reliability, and safety testing.
- Most of the legacy protocols common in Critical Infrastructure predate the internet and need for cyber security. This includes the US power grid.
- It's often not economically nor technically feasible to replace existing equipment and applications wholesale with newer alternatives in the short- or medium-term.
- Therefore, such equipment is at greater risk of attacks than equipment with the latest versions of security features and the latest security updates applied, deeply affecting security.
- IPD / IDS or other security application that can activate AI to detect attacks is required to protect Critical Infrastructure.

U.S. DEPARTMENT OF ENERGY | OFFICE OF Cybersecurity, Energy Security, and Emergency Response

April 2022

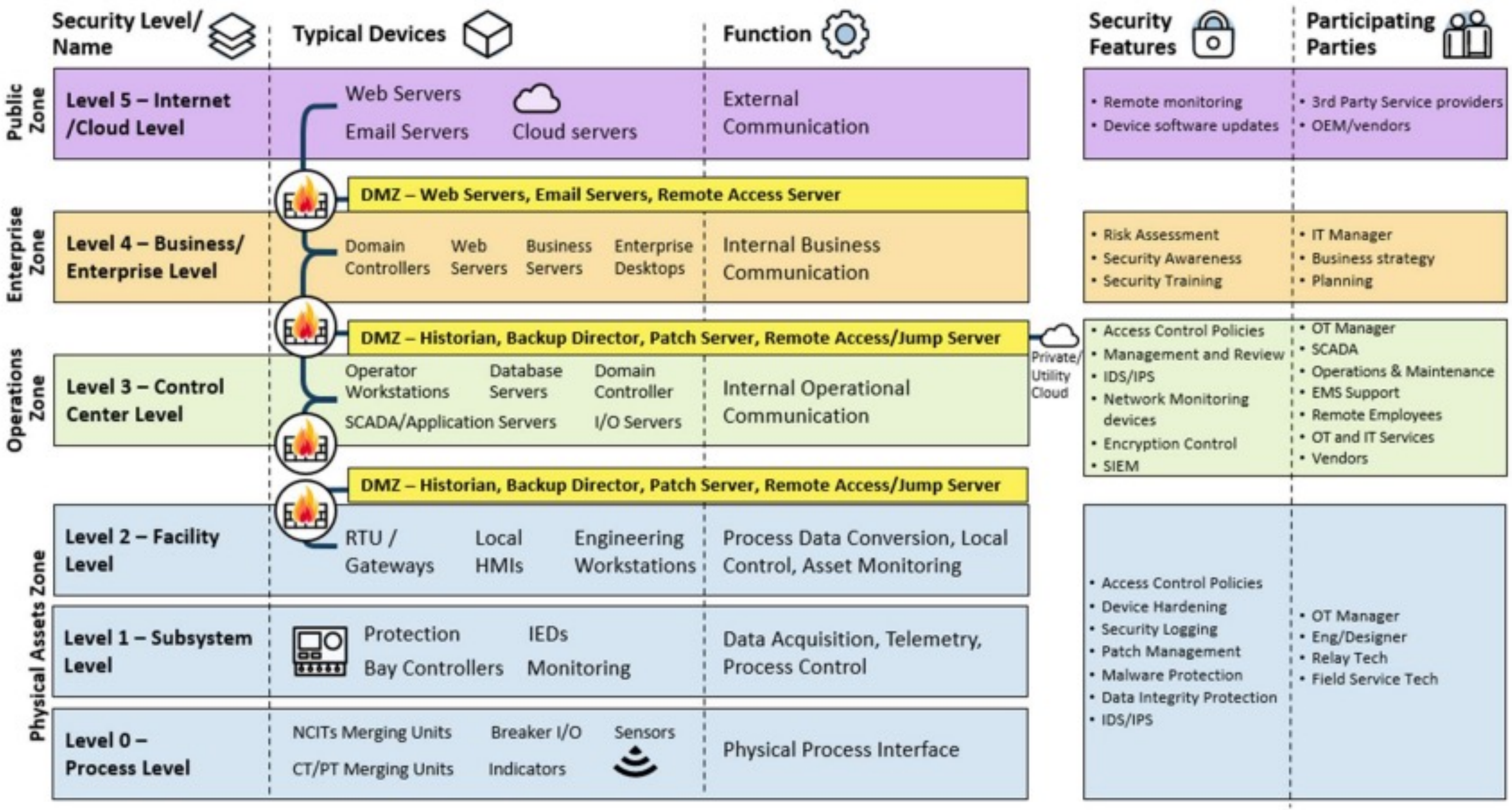
SEI ETF Securing Energy Infrastructure Executive Task Force

RAD Your Network's Edge®

CypherPlug

CypherPlug

SecFlow Gateway



	Security Level/ Name	Typical Devices	Function	Security Features	Participating Parties
Public Zone	Level 5 – Internet /Cloud Level	Web Servers Email Servers Cloud servers	External Communication	• Remote monitoring • Device software updates	• 3rd Party Service providers • OEM/vendors
		DMZ – Web Servers, Email Servers, Remote Access Server			
Enterprise Zone	Level 4 – Business/ Enterprise Level	Domain Controllers Web Servers Business Servers Enterprise Desktops	Internal Business Communication	• Risk Assessment • Security Awareness • Security Training	• IT Manager • Business strategy • Planning
		DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server	Private/ Utility Cloud	• Access Control Policies • Management and Review • IDS/IPS • Network Monitoring devices • Encryption Control • SIEM	• OT Manager • SCADA • Operations & Maintenance • EMS Support • Remote Employees • OT and IT Services • Vendors
Operations Zone	Level 3 – Control Center Level	Operator Workstations Database Servers Domain Controller SCADA/Application Servers I/O Servers	Internal Operational Communication		
		DMZ – Historian, Backup Director, Patch Server, Remote Access/Jump Server			
Physical Assets Zone	Level 2 – Facility Level	RTU / Gateways Local HMIs Engineering Workstations	Process Data Conversion, Local Control, Asset Monitoring	• Access Control Policies • Device Hardening • Security Logging • Patch Management • Malware Protection • Data Integrity Protection • IDS/IPS	• OT Manager • Eng/Designer • Relay Tech • Field Service Tech
	Level 1 – Subsystem Level	Protection IEDs Bay Controllers Monitoring	Data Acquisition, Telemetry, Process Control		
	Level 0 – Process Level	NCITs Merging Units Breaker I/O Sensors CT/PT Merging Units Indicators	Physical Process Interface		

Blockchain for Optimized Security and Energy Management (BLOSEM)

First ever blockchain-based cybersecurity testing environment that features **end-to-end integration**, including generation (inclusive to all sources), transmission, and distribution

Secure coordination of distribution-level assets to track and provide bulk services (example: influence on market structure or contracts, etc)

Novel, systems-based approach to evaluating blockchain-based applications by creating **tangible metrics and guidance** for performance benchmarks

Filling the R&D gap that the industry working groups need to push standards forward. Also, **minimizes risk** of fragmented DOE funding

Creation of a longstanding, foundational **reference architecture for grid cybersecurity** illustrating how blockchain can be used in a meaningful way

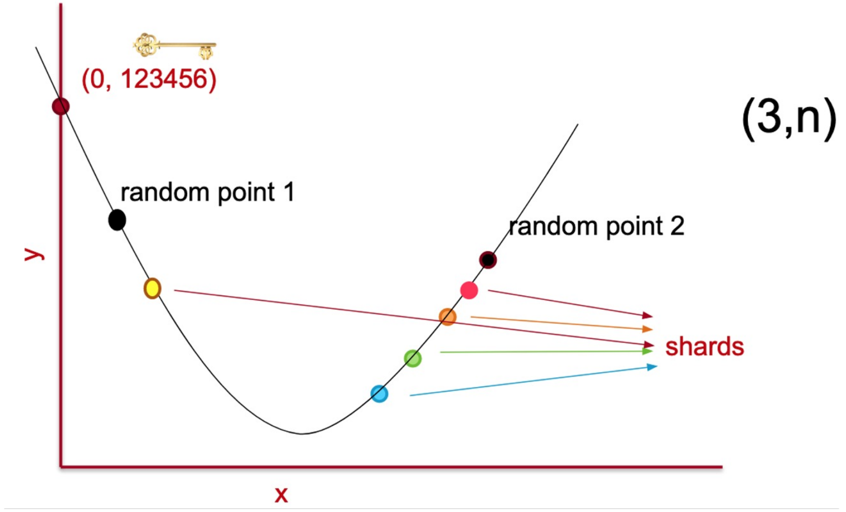
SLAC developed technology to ensure grid assets are protected from supply chain attacks and compromised devices are flagged prior to installation at the operator.

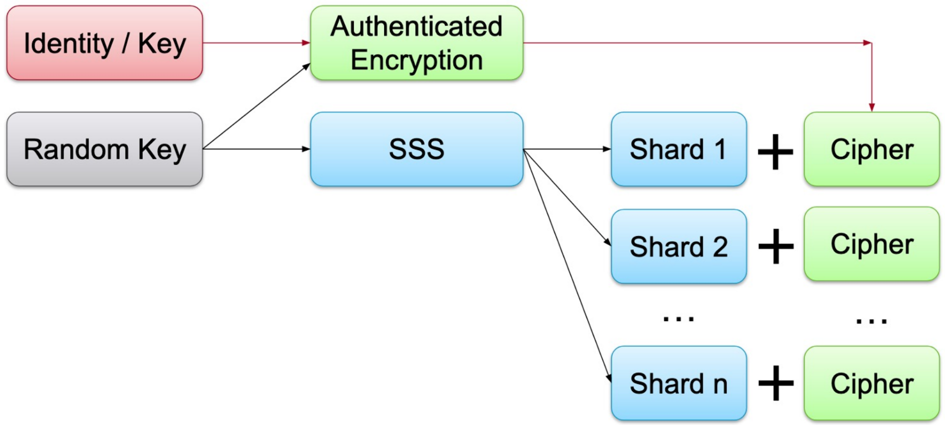
Lab Partners

Secure ID: Distributed Identity Management for Grid Assets

The main idea behind the Secure ID is to break a key into multiple shards. Each shard may be distributed to a node on a trusted network such that they abide by the following constraints:

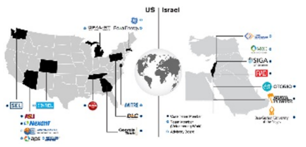
1. Only *k* shards are required perform social verification of the secret key, *k* < *n* where *n* is the total number of shards distributed to custodians
2. Any shard *Sx* must <u>not</u> be a subset of the key
3. All shards *S1, S2, ... , Sn* when combined together must not reveal the secret key





QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION



Question 1:

What is more helpful? Supervised or unsupervised machine learning?

QUESTIONS @ PANEL B:

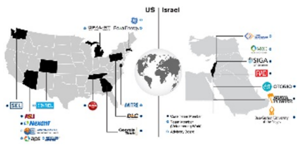
ATTACK DETECTION AND MITIGATION

Question 1:

What is more helpful? Supervised or unsupervised machine learning?

QUESTIONS* @ *PANEL B:

ATTACK DETECTION AND MITIGATION

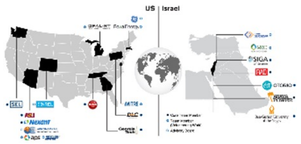


Question 2:

How do you balance the emerging digital transformation in ICS vs. the need to minimize attack surface of critical infrastructure?

QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION

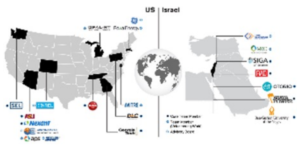


Question 3:

What are the available monitoring strategies for detecting attacks on the physical machines and process layer?

QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION

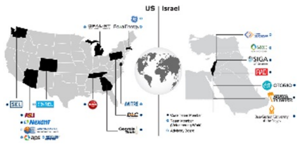


Question 4:

What approach do you propose for legacy environments where digital transformation is a real challenge?

***QUESTIONS** @ PANEL B:*

ATTACK DETECTION AND MITIGATION

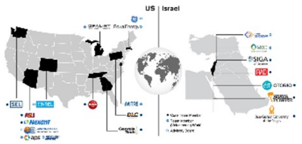


Question 5:

How do you detect attacks that are targeted to the assets themselves using methods like HMI spoofing?

***QUESTIONS** @ PANEL B:*

ATTACK DETECTION AND MITIGATION

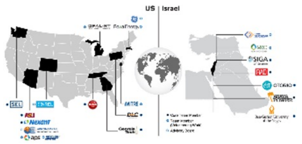


Question 6:

How could AI help detect and mitigate cyber vulnerabilities?

QUESTIONS* @ *PANEL B:

ATTACK DETECTION AND MITIGATION

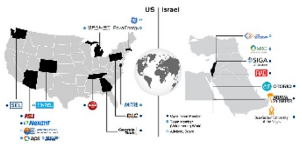


Question 7:

How emerging sensing technologies can be leveraged to protect the power system against cyber threats?

QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION

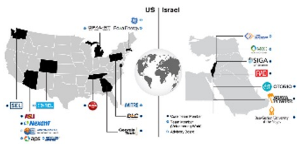


Question 8:

What is your approach or how do you consider the risks for ICS?

QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION

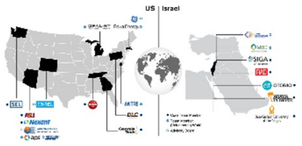


Question 9:

Which are among the following approaches preferable? Proactive or Reactive approach in OT security?

QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION

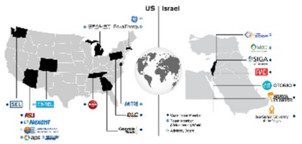


Question 10:

How can we use security plugables for attack detection and mitigation?

QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION

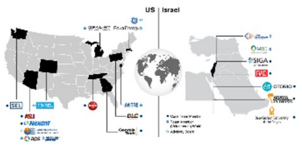


Question 11:

What kind of anomalies are the hardest to detect?

QUESTIONS @ PANEL B:

ATTACK DETECTION AND MITIGATION



Question 12:

How do the advanced language models and chatbots affect ICS attack detection?