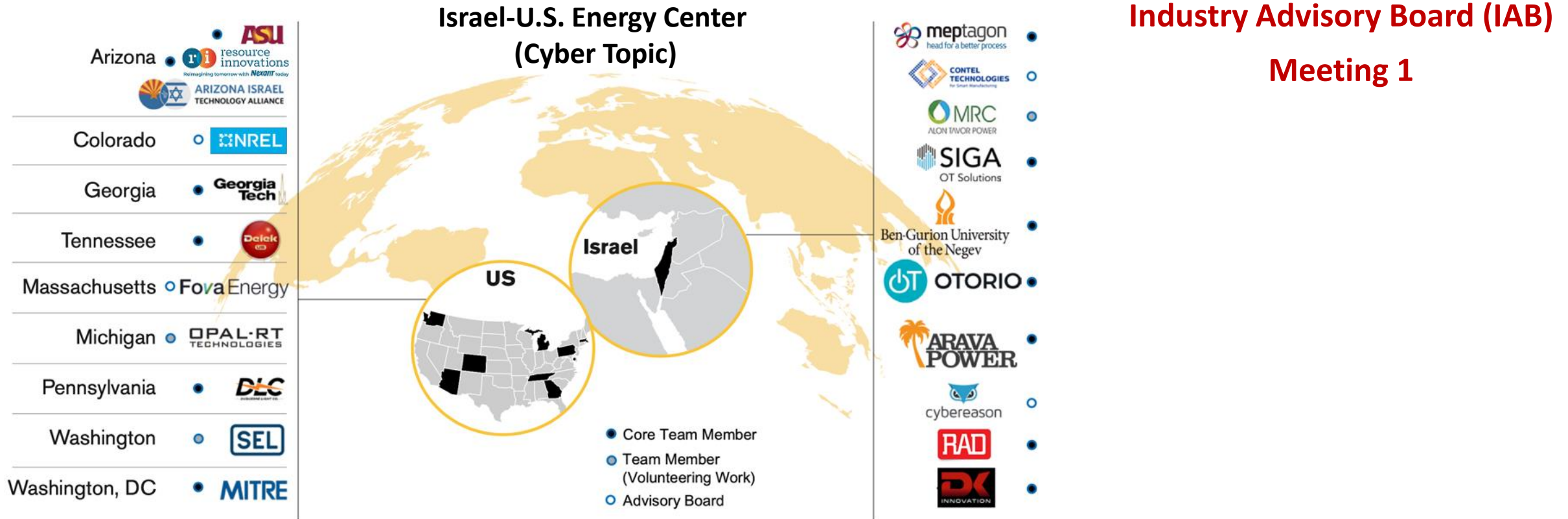


Comprehensive **Cybersecurity** Technology for Critical Energy Infrastructure **AI-Based** Centralized Defense and Edge Resilience



Commercialization - Industry Advisory Board Candidates



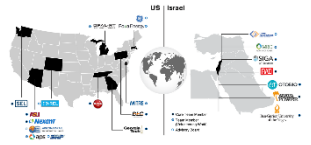
The Industry Advisory Board also includes:

- Arava Power
- Arizona Public Service
- Delek US
- Duquesne Light Company
- Salt River Project

Slides will be shared after the meeting.

Name	Title
Aganze Matembela	Cyber Security Analyst
Alexander Amaya	Senior Manager Cybersecurity
Bill Brandt	Director LightWorks, Strategic Integration
Bill Lawrence	Chief Information Security Officer
Brent Hamilton	Cybersecurity Professional
Charles MaGill	OT Cybersecurity
Dan Frechette	GBB/Technical Specialist IoT Security
David Dekker	Principal Cybersecurity Project Manager
Ed Budde	Regional Technical Manager SW Region
Francois Detroio	OT Cybersecurity Expert
George Kalavantis	Chief Operating Officer
Gisele Widdershoven	Managing Director
Greg Sisson	Managing Director- Energy, Resources and Critical Infrastructure Cybersecurity
Griffin Wiley	OT Cybersecurity Engineer
James Freeman	Cybersecurity Specialist
Jim Acord	Manager, Cybersecurity - Operational Technology
Jodi Wineman	Director, Cyber Security Software Engineering
Ketki Malhotra Patney	Deputy Manager
Laura Hussey	Transmission Compliance
Matt Rhodes	Principal Electrical Engineer
Patrick Popa	Cybersecurity Innovation Manager
Robert Ngabesong	Controls Engineer, OT Cybersecurity
Roderick Kaleho	Chief Information Security Officer
Ross Goulet	Cyber Security Specialist
Roya Gordon	OT/IoT Security Research Evangelist
Sherry Jacob	Senior Manager O&G/Utility

Commercialization - Approaches



Technical approach

Six target applications: 1. Energy Management Systems (EMS), 2. Distribution Management Systems (DMS), 3. Supervisory Control and Data Acquisition (SCADA), 4. Programmable Logic Controller (PLC), 5. Industrial Control Systems (ICS)/Cyber-Physical Systems (CPS), and 6. IoT devices

Integration/add on of new technology without need for wholesale replacement of systems/devices

Commercialization approach

Licensing mechanism is preferred

Market segments

EMS/DMS/SCADA: T&D utilities, IOU, municipal, and cooperatives in North America, T&D utilities in rest of the world

PLC/ICS/CPS/IoT: many potential applications

Key commercial partners, customers/advisors

Form Industry Advisory Board (IAB)

Composition of IAB will be utility personnel, vendors, system integrators, and academics

90 minute meetings via Teams approximately every six months starting in September

IAB will provide feedback/validation of our proposed approach and market strategy

The Lean Canvas

Designed for:

Startup Name

Designed by:













Name1, Name2, ...

Date:

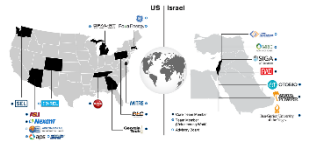
DD/MM/YYYY

Version:

X.Y

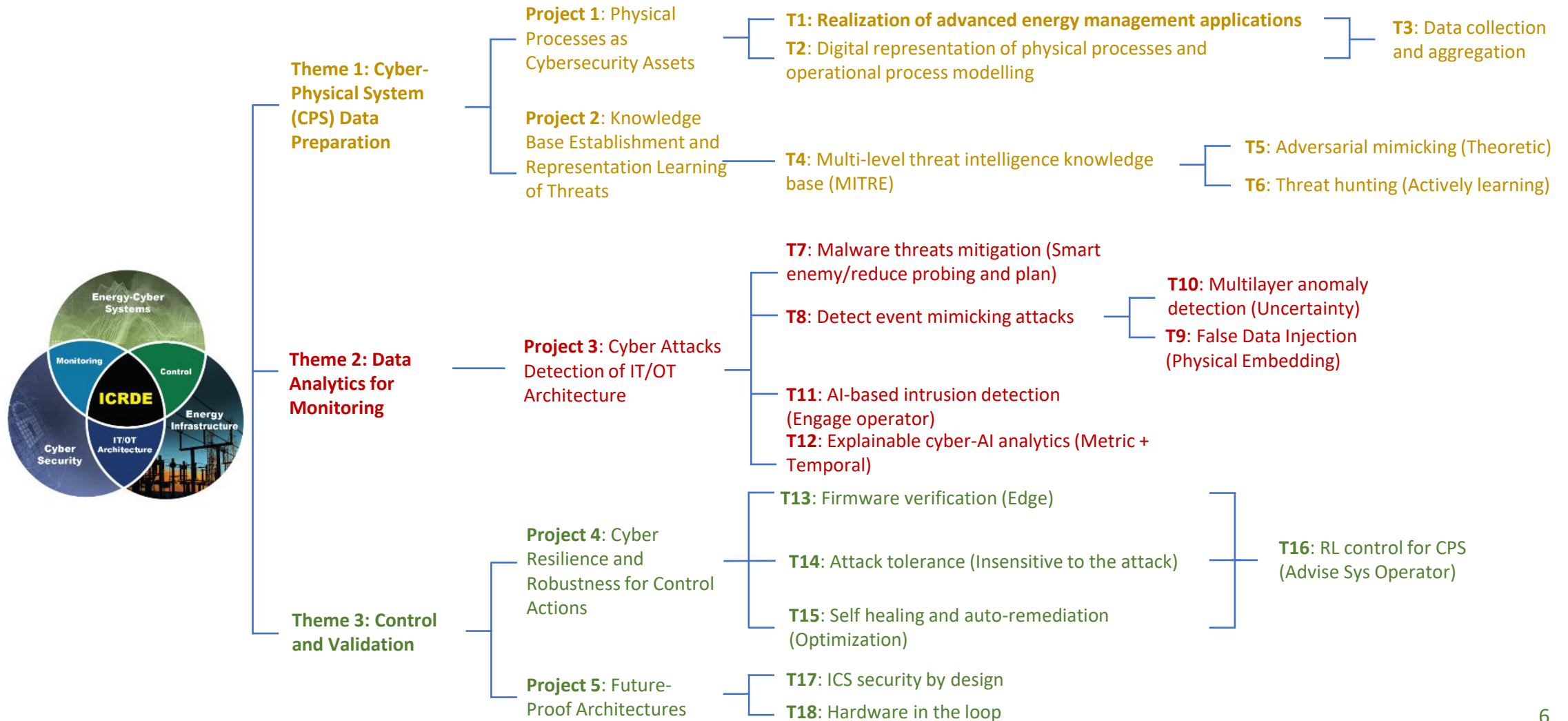
Problem  Top 3 problems	Solution  Top 3 features	Unique Value Prop.  Single, clear and compelling message that states why you are different and worth buying	Unfair Advantage  E.g. can't be easily copied or bought	Customer Segments  Target Customers
Existing Alternatives  List how these problems are solved today.	Key Metrics  Key activities you measure	High-Level Concept  List your X for Y analogy (e.g. YouTube = Flickr for videos)	Channels  Path to customers	Early Adopters  List the characteristics of your ideal initial customers.
Cost Structure  List your fixed and variable costs: <ul style="list-style-type: none">• Customer acquisition costs• Distribution costs• Hosting• People• Technology• Etc.		Revenue Streams  List your sources of revenue: <ul style="list-style-type: none">• Revenue Model• Life Time Value• Revenue• Gross Margin		

Key Questions for Consideration

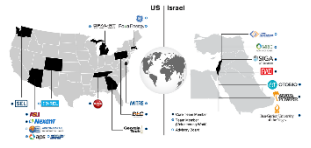


1. What is the potential for commercialization?
(Anonymous Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Comprehensive Cybersecurity Technology for Critical Energy Infrastructure AI-based Centralized Defence and Edge Resilience

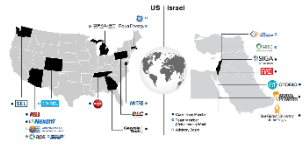


IAB Meeting 1 of 2 Agenda, 21 September 2022



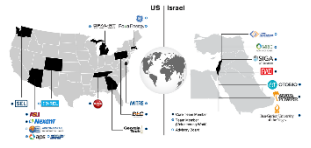
Time	Topic
8:00 to 8:04am Pacific	Kickoff
8:04 to 8:16am Pacific	Task 2. Digital representation of physical processes and operational process modeling - Yuval Elovici <elovici@bgu.ac.il>, Asaf Shabtai <shabtaia@bgu.ac.il> (BGU)
8:16 to 8:28am Pacific	Task 4. Multi-level threat intelligence knowledge base - Lior Rokach <liorrk@bgu.ac.il>, Rami Puzis <puzis@bgu.ac.il> (BGU)
8:28 to 8:40am Pacific	Task 6. Threat hunting - Yuval Elovici <elovici@bgu.ac.il>, Rami Puzis <puzis@bgu.ac.il> (BGU)
8:40 to 8:52am Pacific	Task 11. AI based intrusion detection - Ying-Cheng Lai <ying-cheng.lai@asu.edu> (ASU), Yisroel Mirsky <yisroel@post.bgu.ac.il> (BGU)
8:52 to 9:04am Pacific	Task 16. RL control for CPS - Ying-Cheng Lai <ying-cheng.lai@asu.edu> (ASU)
9:04 to 9:16am Pacific	Task 5. GANs for generating adversarial attacks - Lalitha Sankar <lsankar@asu.edu> (ASU)
9:16 to 9:28am Pacific	Task 8. Detect event mimicking attacks - Lalitha Sankar <lsankar@asu.edu> (ASU)

IAB Meeting 2 of 2 Agenda, 6 October 2022



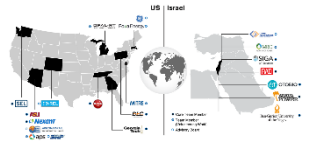
Time	Topic
8:00 to 8:04am Pacific	Kickoff
8:04 to 8:16am Pacific	<u>Task 7</u> . Malware threats mitigation - Wenke Lee <wenke@cc.gatech.edu> (GIT)
8:16 to 8:28am Pacific	Task 9. False data injection - Hagai Galili <hagai.g@sigasec.com>, Ilan Gendelman <Ilan@sigasec.com> (SIGA)
8:28 to 8:40am Pacific	Task 10. Multi-layer anomaly detection framework - Robert Moskovitch (BGU)
8:40 to 8:52am Pacific	Task 12. Explainable cyber AI analytics - Bracha Shpira <bshapira@bgu.ac.il>, Liat Antwarg <liatant@post.bgu.ac.il> (BGU)
8:52 to 9:04am Pacific	Task 13. Firmware verification - Michael Amar <amarmic@post.bgu.ac.il>, Yossi Oren <yos@bgu.ac.il> (BGU)
9:04 to 9:16am Pacific	Task 14. Cyber-attack tolerance - Sukarno Mertoguno <karno@gatech.edu> (GIT)
9:16 to 9:28am Pacific	Task 15. Self-healing and auto-remediation - Yuval Elovici <elovici@bgu.ac.il>, Asaf Shabtai <shabtaia@bgu.ac.il> (BGU)

Task 2 - Digital representation of physical processes and operational process modelling



- Problem:
 1. When investigating an alert a security analyst must understand the relevant OT processes at least at high level. When investigating a malfunction the operators should understand possible adversarial causes of the malfunction. But there is **no common language to describe operational processes** to Engineers, IT expert, Security analysts etc.
 2. Process specifications and project files are too detailed and contain too sensitive information to be shared with other organizations.
- Solution:
 - A database of OT design patterns common to many ICS environments (in similar sectors).
 - Definition of a model for OT processes whilst creating a repository of abstracted processes described by the model.
- Existing Alternatives:
 - Project files
 - BPML
- Unique Value Proposition:
 - Ability to sharing information about OT processes without exposing sensitive details.
 - Enables tight cooperation between Security and Engineering personnel.

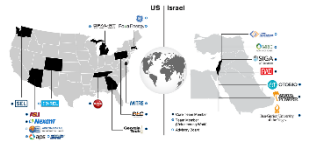
Task 2 - Digital representation of physical processes and operational process modelling



Task Details:

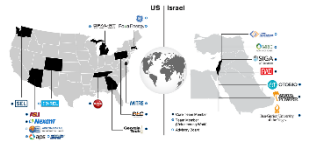
- Definition of a model for OT processes whilst creating a repository of abstracted processes described by the model.
- The model would include sub processes modeled the same way, the patterns of the sensors when the process is taking place and short description of it.

Task 2 - Key Questions for Consideration



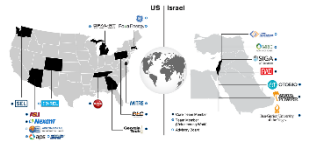
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 4&6 - Multi-level threat intelligence knowledge base and threat hunting



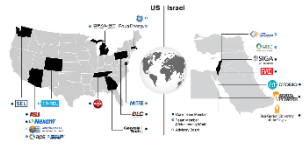
- Problem:
 - Disparate disconnected sources of threat intelligence make it **hard to use both high-level and low-level threat intelligence** for mitigating campaigns.
 - For example cyber attack techniques recognition given observable artefacts was not possible.
- Solution:
 - Build a **unified Knowledge Based** of ICS attack data by fusing data from multiple open sources of threat intelligence data within a graph database (Neo4j).
 - Use machine learning and graph algorithms to **infer techniques from observables**
 - Given prospective techniques use reinforcement learning to highlight important observables to **guide the investigation**

Task 4&6 - Multi-level threat intelligence knowledge base and threat hunting

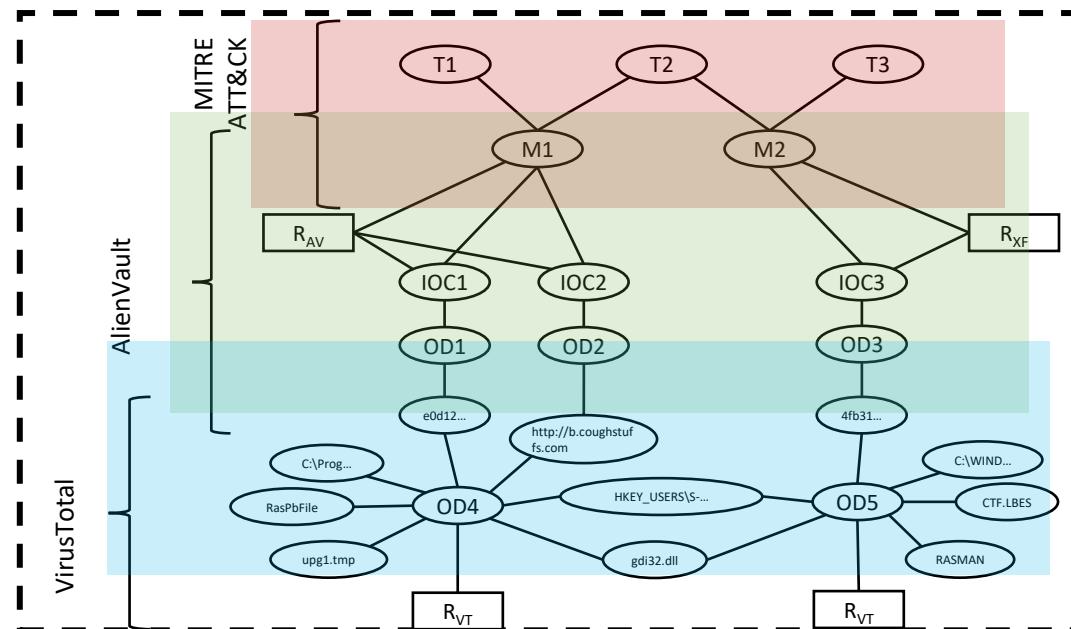


- Existing Alternatives:
 - MITRE ATT&CK (only high level data),
 - OTX/AlienVault (only low level data),
 - VirusTotal Graph (getting close to what we have but not yet)
- Unique Value Proposition:
 - **Inference of techniques from observables**
 - **Targeted data collection**
- Unfair Advantage:
 - Multi-level knowledge base
- Channels:
 - Approaching CISOs in ICS orgs, cooperation with existing ICS cyber security firms
- Revenue Streams:
 - ????

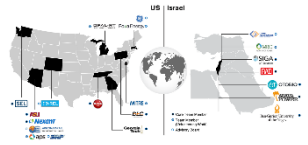
Task 4 - Multi-level threat intelligence knowledge base



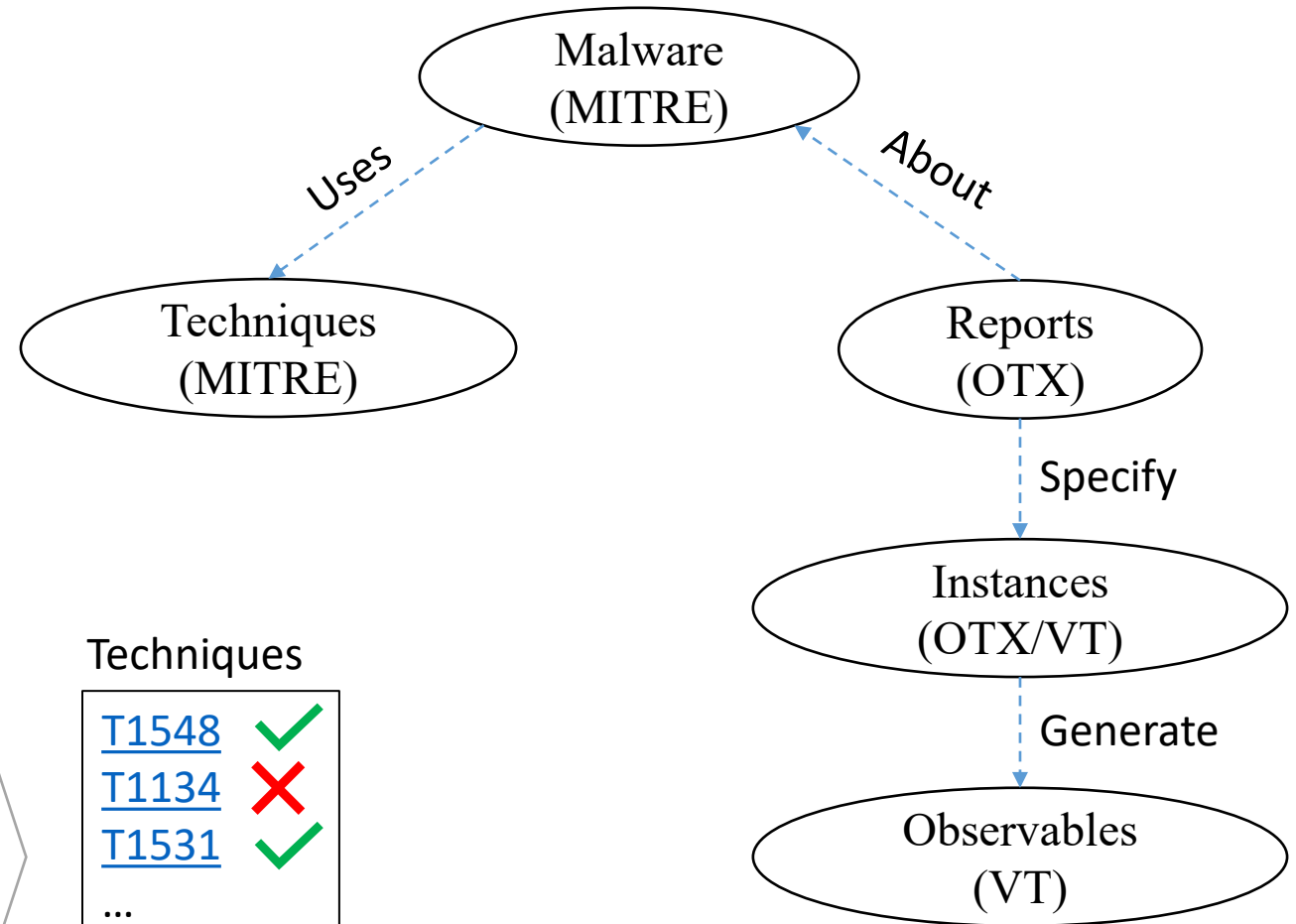
- Merge information regarding ICS cyber attacks from multiples sources and level into a unified graph database
 - Analyze multiple data sources
 - Develop mechanisms to get the data
 - Structure the data into a unified KB, with a relevant Ontology
 - Perform data cleanup and loading



Task 4 - Attack Techniques Classification - approach



- We have a graph KB composed of data collected from (Task 4):
 - MITRE ATT&CK
 - VirusTotal
 - AlienVault OTX
- The artifacts are used as input to a classification algorithm and the output is the techniques used



ML multi-label classification

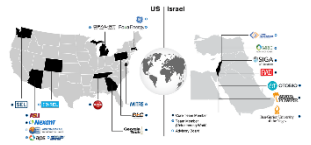


Techniques

T1548	✓
T1134	✗
T1531	✓
...	
T1220	✗

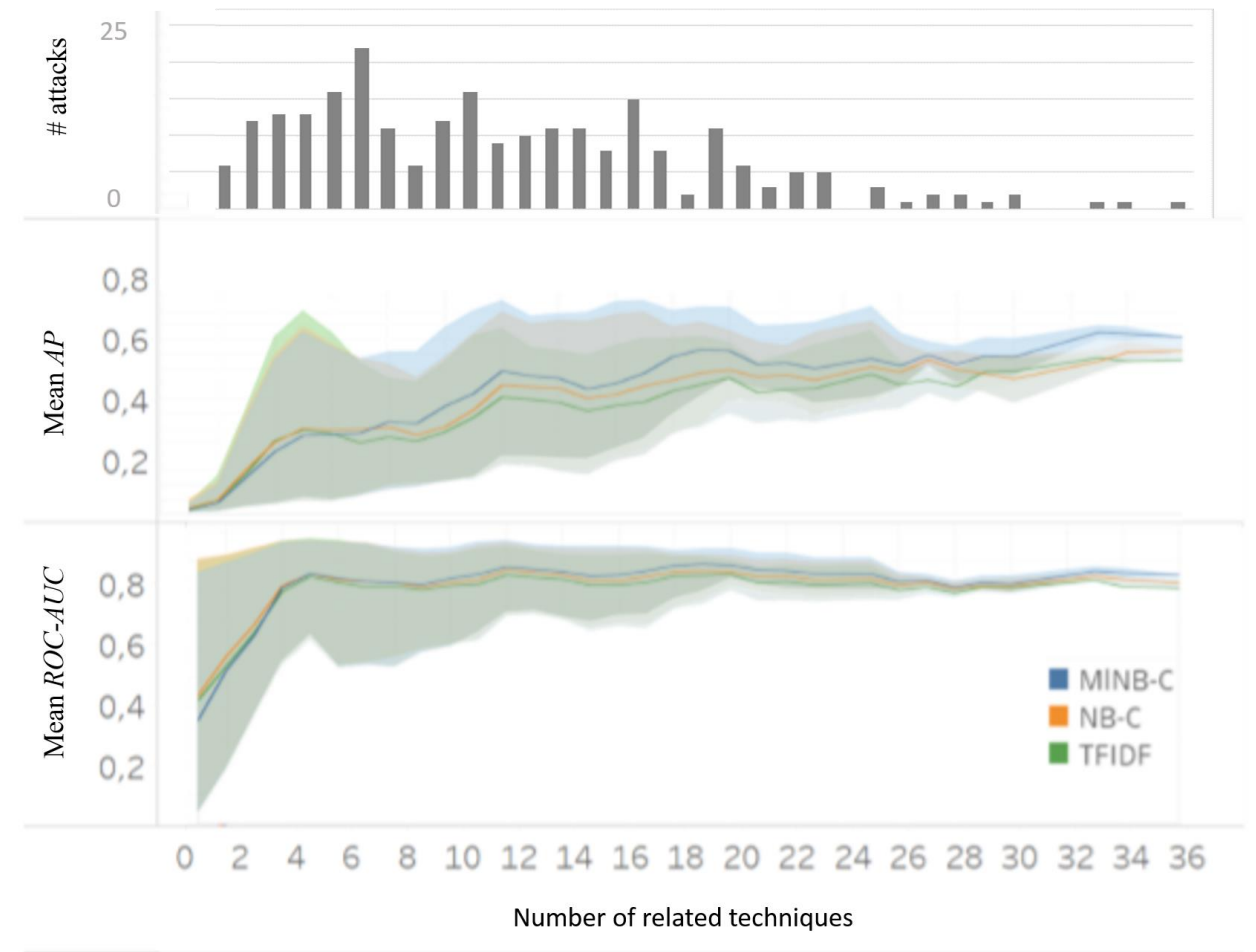
Task 4&6 - Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph

Florian Klaus Kaiser, Uriel Dardik, Aviad Elitzur, Polina Zilberman, Marcus Wiens, Frank Schultmann, Yuval Elovici, and Rami Puzis



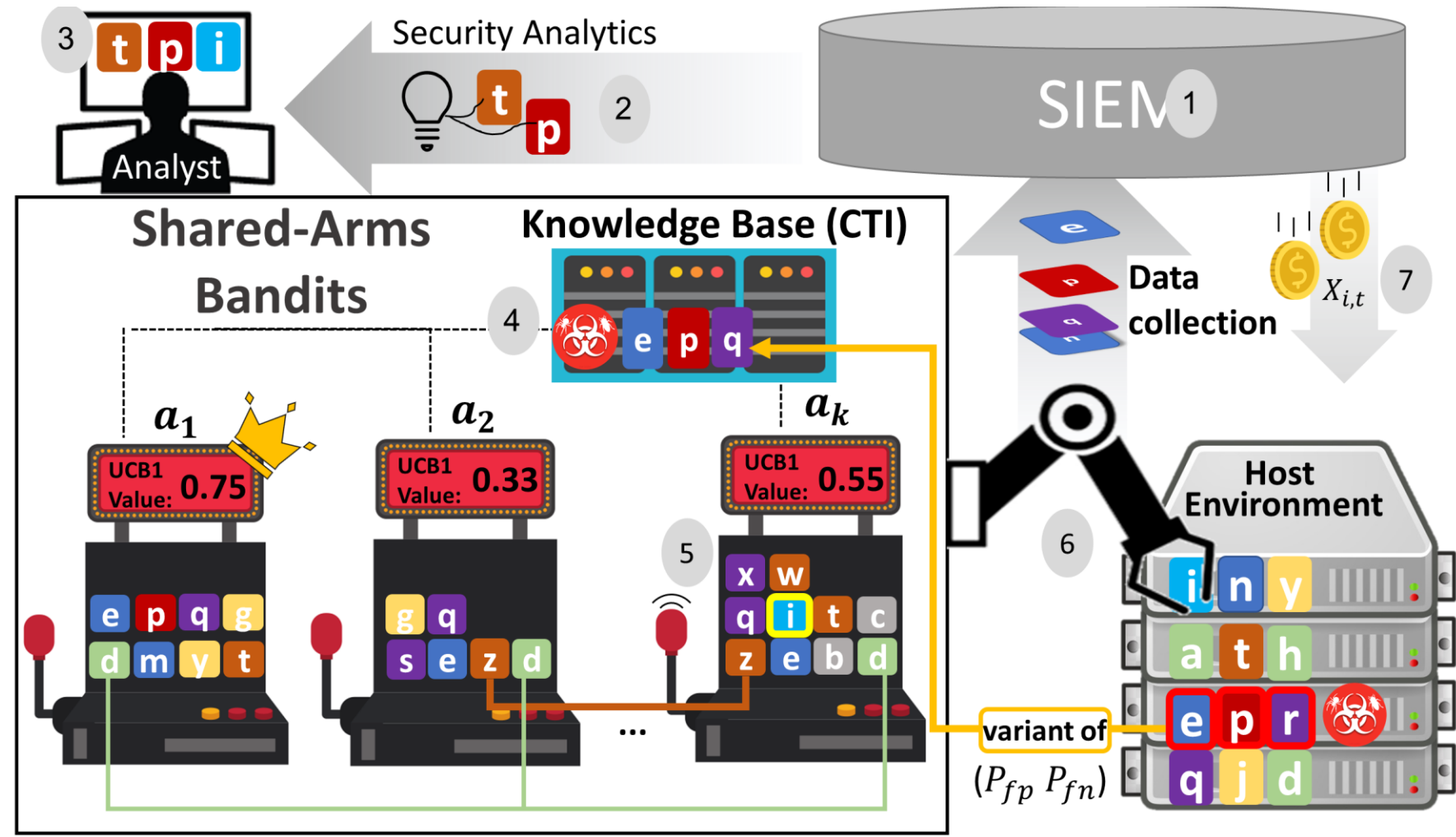
- Pending major revision
- IEEE transactions on dependable and secure computing (IF=7.329)

Focus on the privilege escalation, lateral movement, discovery, and C&C tactics



Task 6 - MABAT: A Multi-Armed Bandit Approach for Threat-Hunting

Liad Dekel, Ilia Leybovich, Polina Zilberman, and Rami Puzis



Task 6

An autonomous deep dive into for advanced cyber-security forensics



Do not sit back and wait for the Intrusion Detection Systems to raise alerts.

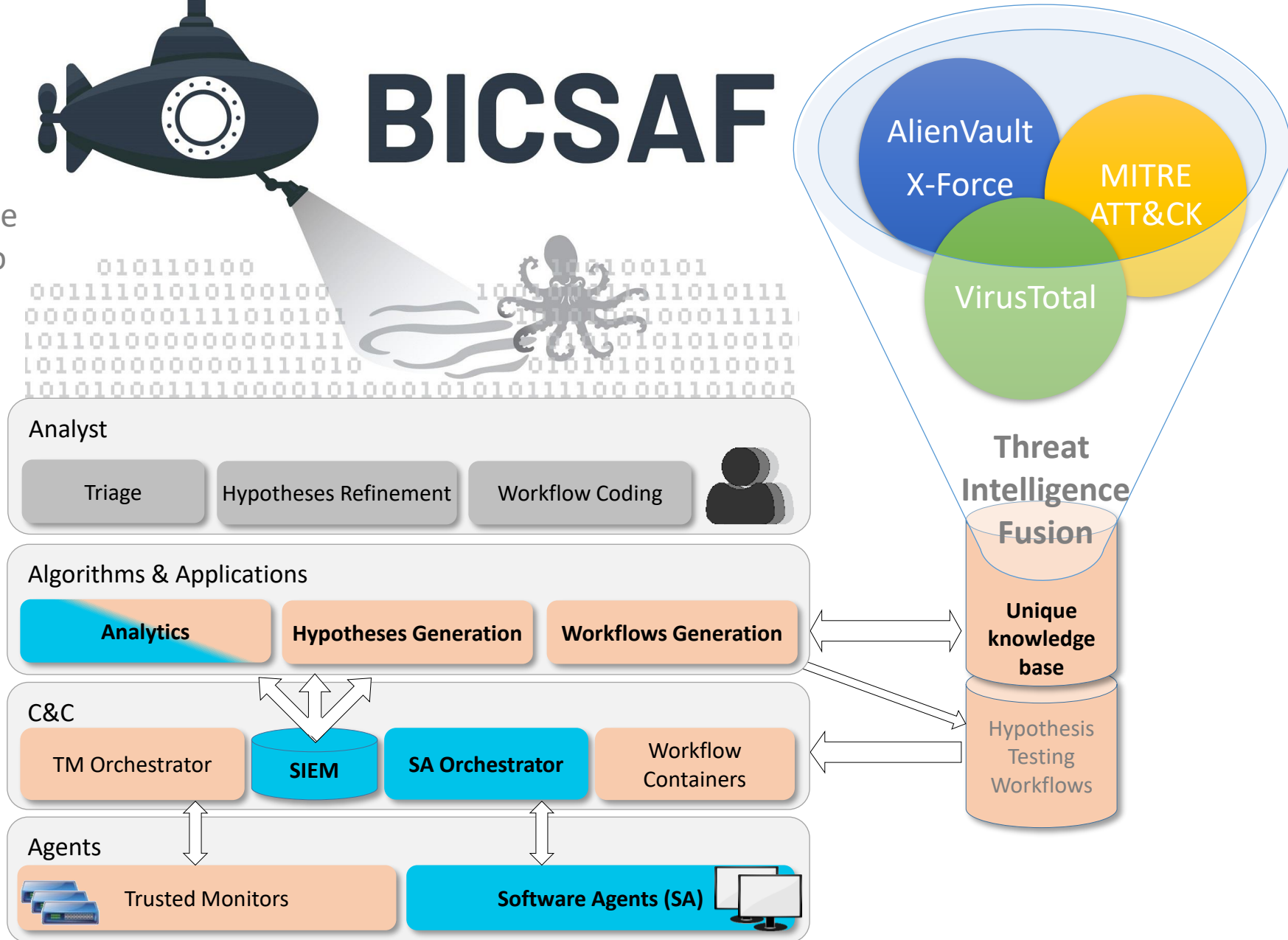
Actively hunt down artifacts that will lead to the attacker.

Agile and adaptive data collection process feeds on attack hypotheses

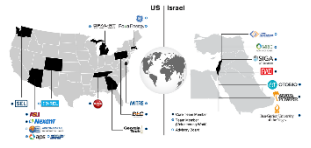
constantly generated by BICSAF. **Hunting workflows**

(a.k.a. playbooks) are **automatically generated**

relying on a **unique knowledge base** constructed relying on multiple threat intelligence sources.

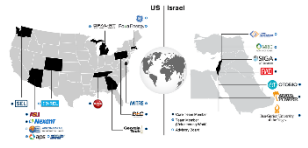


Tasks 4&6 - Key Questions for Consideration

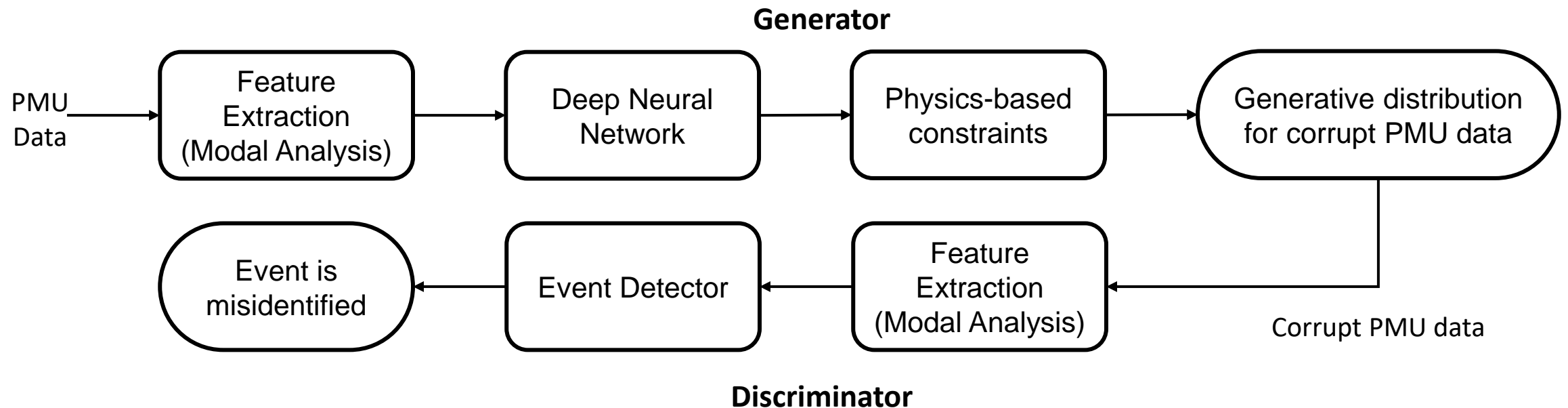


1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

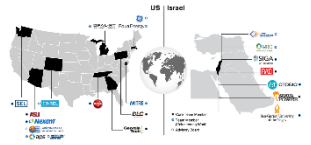
Task 5 - GANs for generating adversarial attacks



- **Lead PI: Dr. Lalitha Sankar (Arizona State University)**
- **Problem:** Generate intelligent event-mimicking attacks that can spoof conventional event detectors
 - Potential to disrupt grid operations by creating local outages that can percolate widely
- **Solution:** Learn generative model of corrupt PMU data in an adversarial manner
 - utilize knowledge of feature extraction and detection process
 - first step is to start with simpler physics-based models (on-going)



Task 5 - GANs for generating adversarial attacks

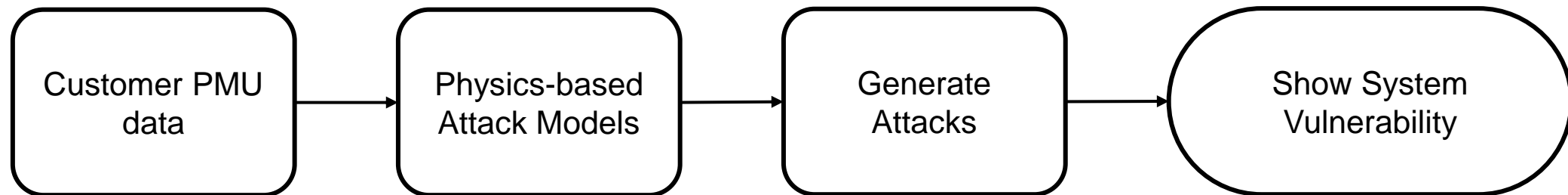


- **Problem:** Generate intelligent event-mimicking attacks that can spoof conventional event detectors
 - Potential to disrupt grid operations by creating outages that can percolate widely
- **Solution:** Learn generative model of corrupt PMU data in an adversarial manner
 - utilize knowledge of feature extraction and detection process
 - first step is to start with simpler physics-based models (on-going)
- **Existing Alternatives:** Black-box approaches involve adding random noise for data corruption
 - EMS/DMS algorithms are generally robust to random noise attacks
 - Misleads operators to assume their detectors/algorithms are robust
 - Systems are still vulnerable to attacks utilizing system knowledge (gray-box / white-box)
 - Future solutions need to assume that attackers are powerful entities with system knowledge (given critical infrastructure)
- **Unfair Advantage:** We have worked with EMS vendors and simulation companies
 - Commercialize simple implementable algorithms to test robustness of SCADA and PMU measurements
 - Use our existing methodology for vendors to test EMS algorithms against a range of attacks

Task 5 - GANs for generating adversarial attacks

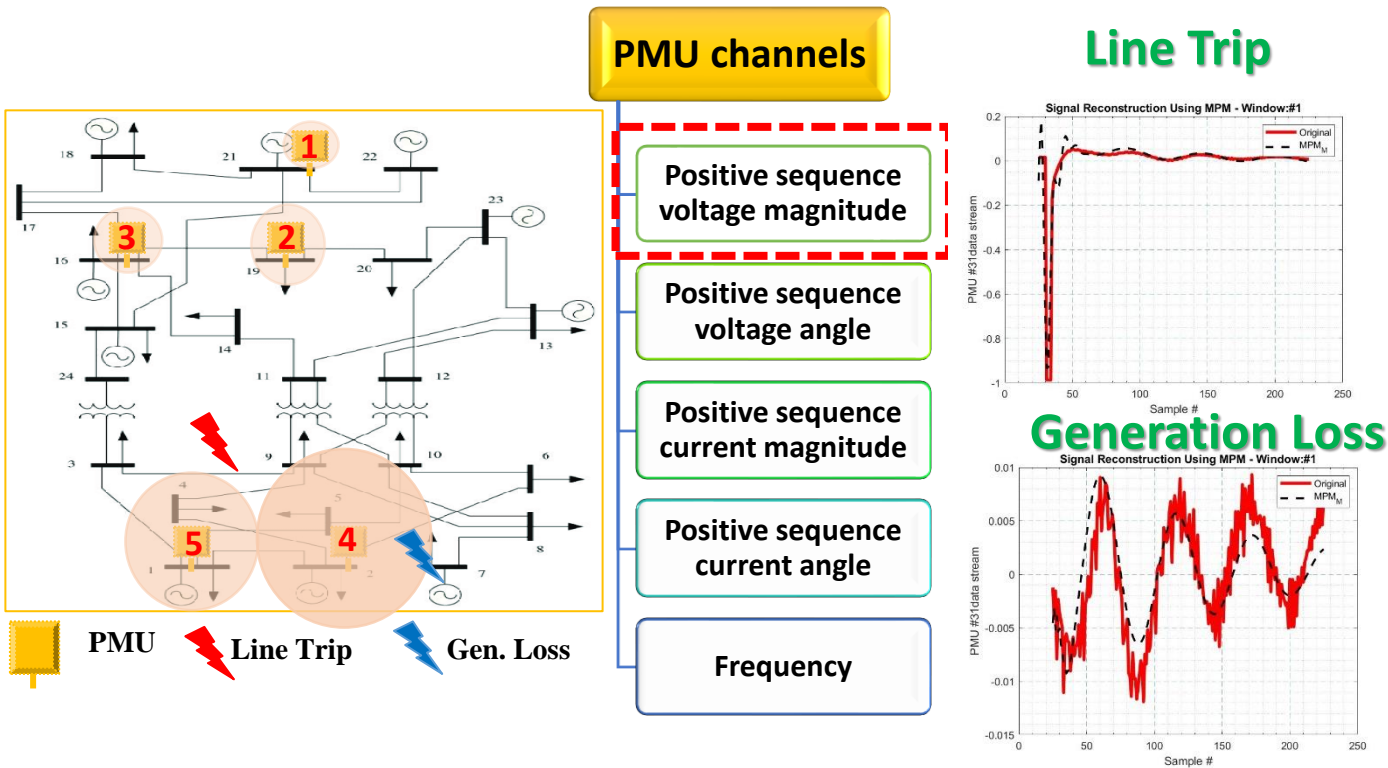
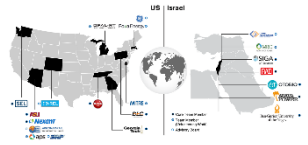


- **Unique Value Proposition:** creation of realistic false data using physics encoded in the PMU data
 - (e.g., mode damping, frequencies, residues, etc) differentiates this research from standard approaches
- **Unfair Advantage:** Task-lead has a decade-long expertise on evaluating cybersecurity of EMS
 - Group has strong background in power systems, machine learning, and cybersecurity
 - Access to 100 TBs of proprietary PMU data to design such attacks
- **Channels:** Work closely with RII



- **Revenue Streams:** Commercialization of research in collaboration with Resource Innovations, Inc.
 - Prospective clients include distribution utilities and private companies developing cybersecurity solutions
 - Examples: Schneider Electric, GE, Siemens, ComEd, Ameren, etc.

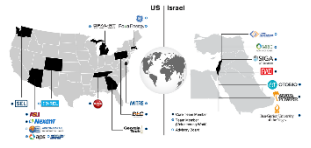
Task 5 - GANs for generating adversarial attacks



Can we identify physically realizable attacks (e.g., event-mimicking) ?

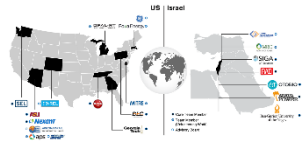
Yes! By identifying key event features that are easy to synthesize by changing measurements!

Task 5 - Key Questions for Consideration



1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

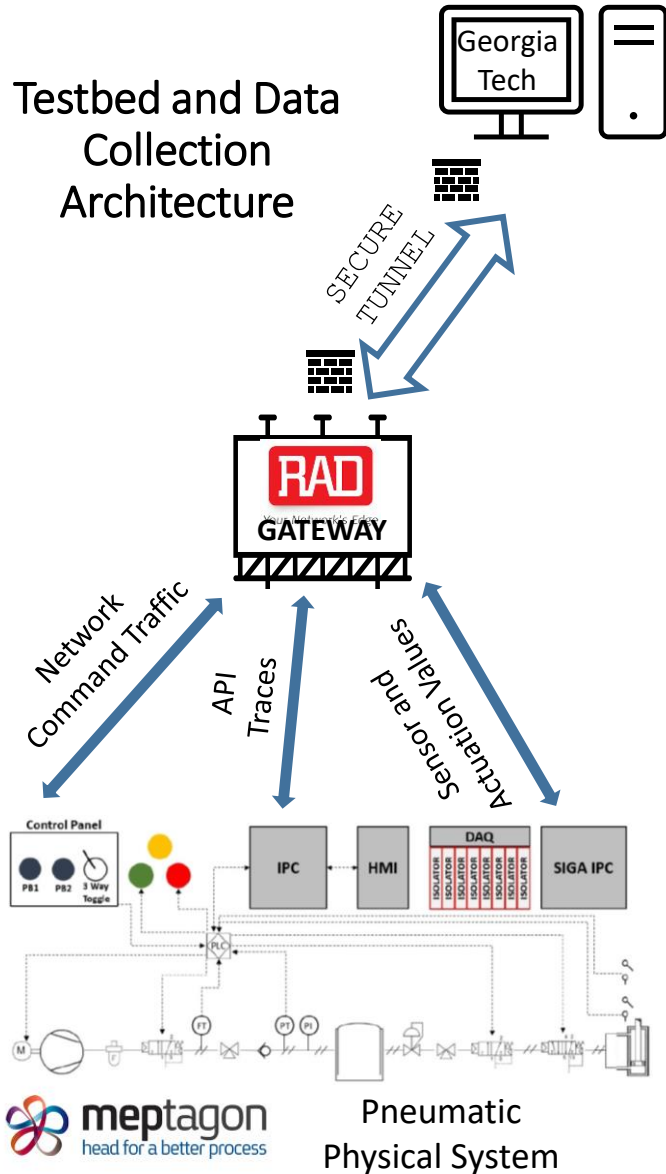
Task 7 - Malware threats mitigation



- **Problem:** Host-based ICS malware attacks are hard to detect in SCADA control systems because they blend with normal host execution and network behaviors, causing physical disruptions and damages.
- **Solution:** We propose to correlate anomalous "physical-targeted" executions in SCADA with anomalies in physical sensors and actuator behaviors
- **Existing Alternatives:** Existing work analyze either SCADA host network or sensor behaviors in isolation which raise many false alarms and missed attacks
- **Unique Value Proposition:** The correlation between SCADA and physical is both novel and unique, but help to increase detection accuracy as well as reduce false positives
- **Unfair Advantage:** Our technique leverages industry domain knowledge and host systems in ICS, such as how malware infects SCADA systems to attack physical devices
- **Channels:** Prototype demonstration as a passive monitoring and alerting system in an industrial environment.
- **Revenue Streams:** Based on future deployment and market scenarios

Task Details

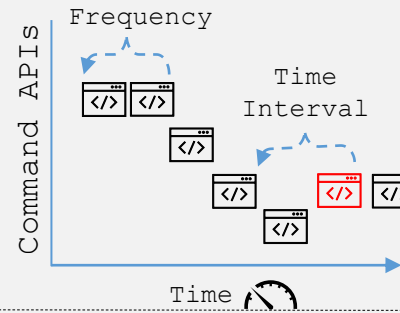
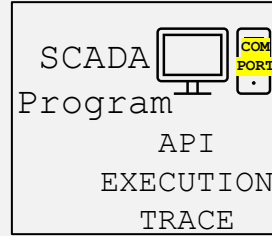
Testbed and Data Collection Architecture



Approach: Correlate execution traces in the control hosts with physical sensor effects/anomalies. Georgia Tech is leveraging domain knowledge and real systems from Industry Collaborations, such as Meptagon and RAD

Learn normal SCADA control semantics using frequency and timing dependency features of control API calls

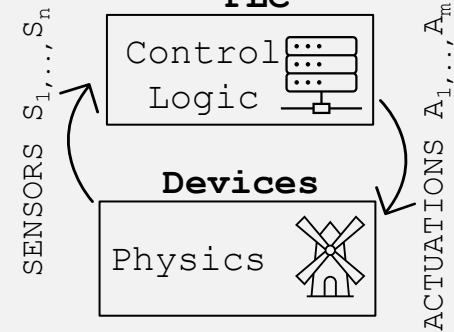
SCADA SERVER



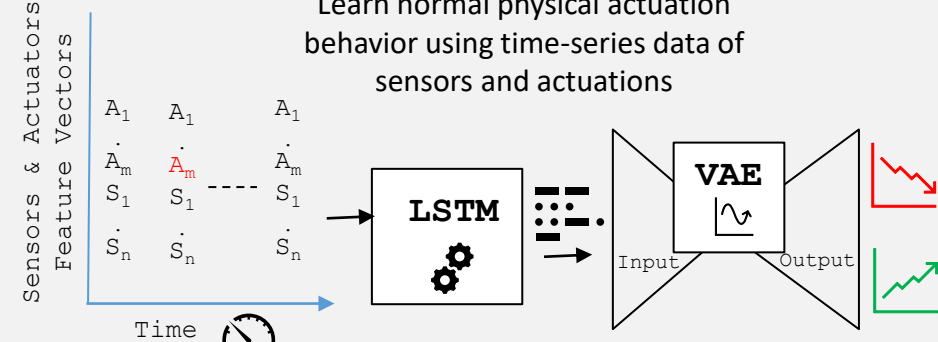
SCADA + Physical Correlation Approach

1. Check SCADA API trace for anomalies in Window W
2. If yes, check if anomaly exist at the physical side in $W, W+1$
3. If yes, check if physical anomalies in $W-1$
4. If yes, it's a False Positive.
5. If No, Raise **Alert**
6. Locate the anomalous actuator from the SCADA API command argument

PLC



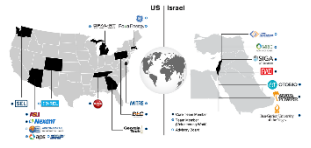
Learn normal physical actuation behavior using time-series data of sensors and actuations



Domain Knowledge-Informed Feature Engineering

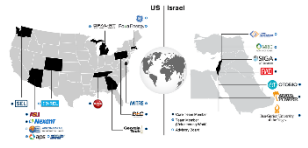
1. Selection of Important Sensors and Actuators, and pruning of unimportant ones
 - Sensor partitioning, operator selection, and forward sensitivity analysis
2. Selection of Time Window W , Object Length L , and Sampling Interval I
3. Each Feature F will include "aggregation" of the sampled value, e.g., mean and SD of values from I_1 to I_2

Task 7 - Key Questions for Consideration



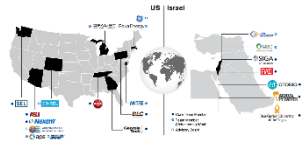
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 8 - Detect event mimicking attacks

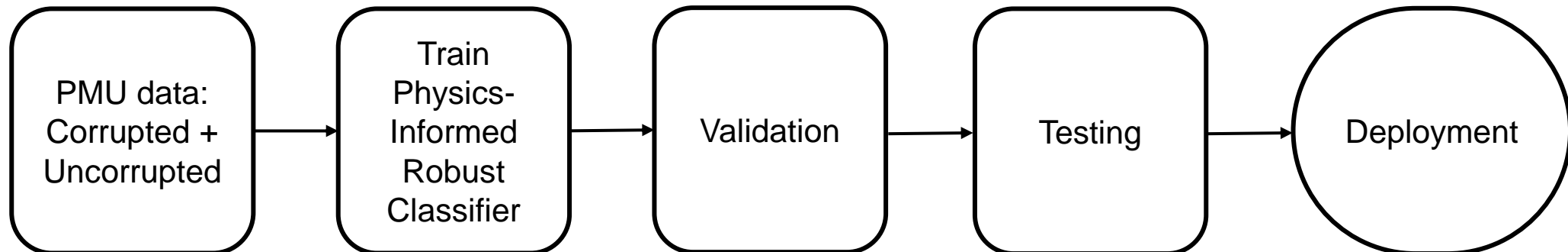


- **Lead PI: Dr. Lalitha Sankar (Arizona State University)**
- **Problem:** Robust detection of intelligent event-mimicking attacks
- **Solution:** Robustness of classifier can be ensured by:
 - exploiting physics-based models for grid to explore meaningful feature engineering
 - Identifying the complete set of features to make system more robust – design trade-off between ML algorithm complexity and robustness
- **Existing Alternatives:** PMU event detectors are presently based on simple signal processing methods; their robustness to attacks haven't been explored
 - Basic linear and non-linear classifiers are susceptible to attacks, particularly for low-dimensional feature space

Task 8 - Detect event mimicking attacks



- **Unique Value Proposition:** Analysis of classifier trade-off — robustness, interpretability, accuracy
- **Unfair Advantage:** Task-lead has a decade-long expertise on evaluating cybersecurity of EMS
 - Group has strong background in power systems, machine learning, and cybersecurity
 - Access to 100 TBs of proprietary PMU data
- **Channels:** Work closely with RII

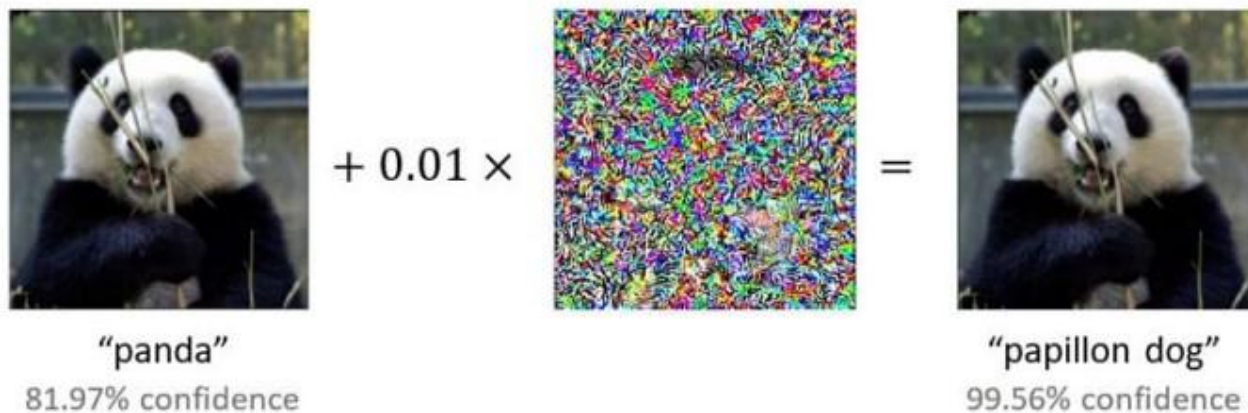


- **Revenue Streams:** Commercialization of research in collaboration with Resource Innovations.
 - Prospective clients include RII clients and private EMS and DERM systems

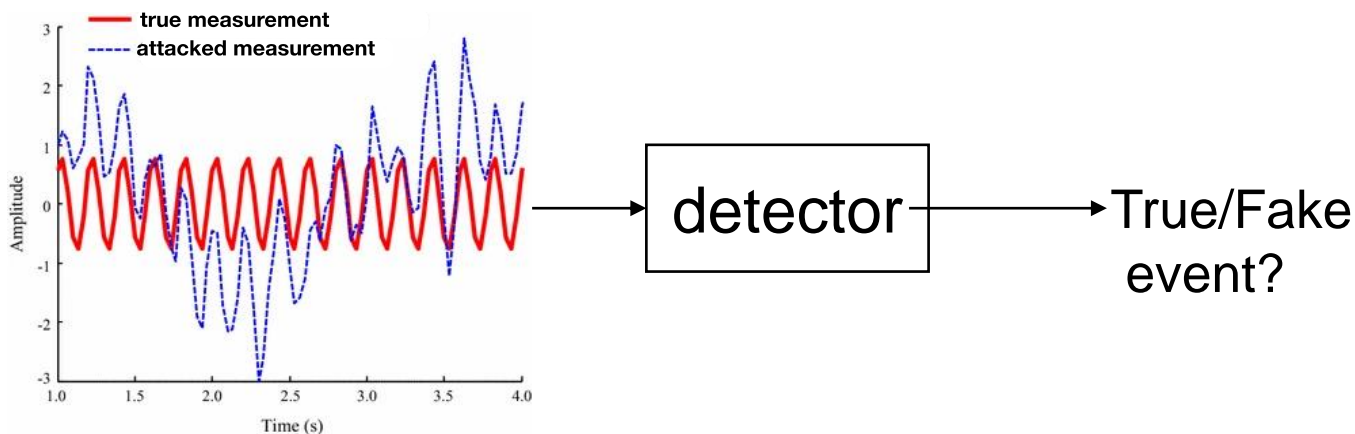


Task 8: Detect Sophisticated (Mimicking) Attacks

- Existing robust detectors of **static data**



- Power system data is dynamic

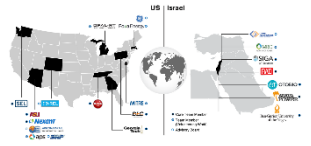


Objective: Design modular detectors capable of detecting anomalies via PMU measurements

Our Method: Online ML detector that exploits **event features** to:

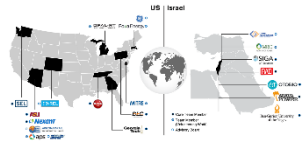
- compare **features** of true events against fake events
- Incorporate (**physics-based prior**) to make detectors robust
- Include **event characteristics** (e.g., frequency, source of event) to enhance distinguishability

Task 8 - Key Questions for Consideration



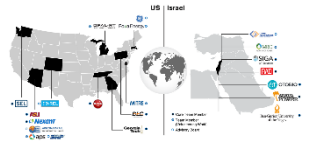
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 9 - False data injection



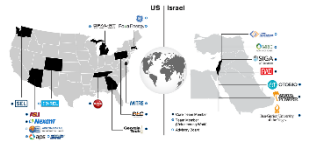
- **Problem**: OT plays a crucial role in electrical & power infrastructure assets, especially in Sub-stations, that have long ago been identified as having enormous potential for cyber attacks, as they cannot tolerate downtime by any means. The most critical layer of the OT environment, Level 0 (the physical layer), is exposed to numerous kinds of cyber-attacks. Some of these cyber attacks, as identified by SIGA, can go unnoticed by operators, causing wide outages and serious damage to equipment
- **Solution**: SigaGuard, is a unique comprehensive OT cyber security solution for critical infrastructure and industrial assets using ICS/SCADA electrical signal-based advanced Machine Learning. SIGA is providing out-of-band real-time OT processes monitoring and analytics for safeguarding the critical industrial assets. SigaGuard is monitoring the most reliable source of data for OT environments, namely the non-penetrable physical source – the raw electrical signals of Level 0 coming from the sensors, breakers and actuators. This source of data is rich & unfiltered, un-hackable, and often unavailable to operators.
- **Existing Alternatives**: There are several cyber protection tools in use in the OT environment of sub-stations today, all of them are focusing on Level 1 or the above levels of the Purdue Model, aiming at the protection of the OT network and its components.

Task 9 - False data injection



- **Unique Value Proposition**: SigaGuard is the only solution that provides the operator with complete visibility into its operations and machinery by performing the analysis of electrical signals directly from the OT/ICS Level 0. SigaGuard's process signals oriented ML models deliver anomaly detection and elaborated insights to allow the operators to really feel their machinery pulse, and act upon potential threats quickly and effectively, so that downtime is avoided or reduced to the minimum.
- **Unfair Advantage**: process-oriented ML, highly protected with patents and was developed from scratch specifically for ICS electrical signals; only solution for level 0 monitoring in the market; scalable solution with vast "know-how" knowledge and experience; agnostic to asset process type and to ICS equipment and network type.
- **Channels**: SIGA is distributing its product and serving customers mainly via partners and re-sellers (there are some direct sales processes as well).
- **Revenue Streams**: Mainly by SaaS when HW and services are sold separately

Task 9 - False data injection



Task 9 will focus on R&D of new capabilities of anomaly detection at Level 0 of the electrical grid physical process. There are 2 main use cases for cyber-attacks on the grid that was assessed and found to be relevant for developing new capabilities to mitigate them by SIGA:

- **Early detection of malicious Voltage Collapse**

The attacker will gain control on the AVR mechanisms controller and disrupt the tap changer operation, causing the voltage to drop to a low level.

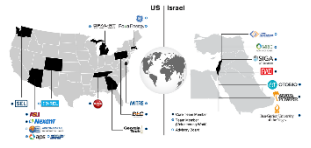
- **Malicious loss of grid's inertia**

The attacker will take control of an energy storages control systems and reverse their stabilizing effect on the grid (resulting in divergence of the grid instead of stabilizing it).

The following R&D activities will be conducted by SIGA:

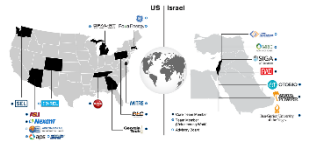
- **SIGA will develop new ML models** for the given sub-station's setup for learning of the the normal behavior of all its monitored components, combining a new shift from <100Hz data to a 1KHz of its unsupervised learning algorithms.
- **SIGA will build a lab**, simulating a sub-station and grid, to demonstrate these use cases. This will create the required data and allow for test after the development made by SIGA

Task 9 - Key Questions for Consideration



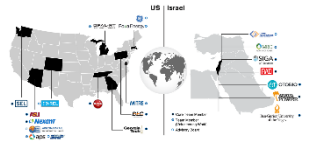
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 10 – Multi Layer Anomaly Detection



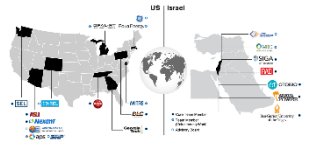
- Problem:
 - Unknown cyber attacks are hard to detect, since it is not clear how they appear
 - A common way to detect unknown attacks is through the detection of anomalous behavior
- Solution:
 - Develop an anomaly detection method through heterogeneous multivariate temporal data analysis
- Perform frequent temporal patterns based anomaly detection, through monitoring the metrics of the temporal patterns
 - Use of negative temporal patterns, to incorporate the meaning of NON APPEARANCE

Task 10 – Anomaly Detection



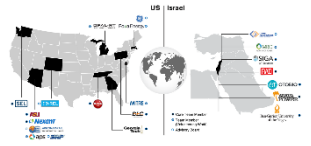
- Existing Alternatives:
 - Not known negative temporal patterns based anomaly detection
 - There are various anomaly detection methods
- Unique Value Proposition:
 - Discovery of frequent negative temporal patterns
 - Explainable anomaly detection based on the actual anomalous temporal patterns
- Unfair Advantage:
 - Almost two decades of Temporal Patterns based Applications
- Channels:
 - Approaching CISOs in ICS orgs, cooperation with existing ICS cyber security firms
- Revenue Streams:
 - ????

Task 10 - Key Questions for Consideration



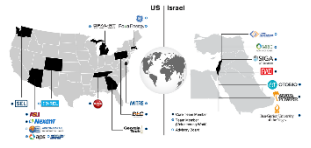
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 11 - AI based Intrusion Detection



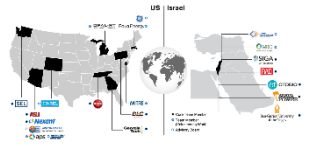
- **Problem:** Developing a network nonlinear dynamics and machine-learning based framework to detect external perturbations that can potentially cause catastrophic damages to cyberphysical systems.
- **Solution:** Creating digital twins of cyberphysical systems
- **Existing Alternatives:** many anomaly and intrusion detection algorithms are available, including the state-of-the-art network intrusion detection software for ICS
- **Unique Value Proposition:** Creating AI-based digital twins for intrusion detection is scientifically innovative and represents a new approach in this field
- **Unfair Advantage:** ASU Task-11 team has expertise in adaptable machine learning with significant recent works on developing machine learning for predicting critical transition, tipping point, and catastrophic bifurcations in a variety of nonlinear dynamical systems
- **Channels:** Working closely with Resource Innovations/Nexant
- **Revenue Streams:** Unable to speculate

Task 11 - AI Based Intrusion Detection: Task Details



- **Main Objective:** to develop a network nonlinear dynamics and machine-learning based framework to detect external perturbations that can potentially cause catastrophic damages to cyberphysical systems.
- **Cascading Failures:** catastrophic for power networks with heterogeneous energy sources.
- **Research Focus:** identifying the type of perturbations or intrusion that will result in cascading failures and developing real-time detection schemes based on digital twins.
- **Digital Twin for Cyberphysical Systems:** recurrent neural-network based machine-learning architecture as required by the intrinsic nonlinear dynamics of the power systems.
- **Training Data:** from real-world power systems - possibly through enterprise Operational Technology (OT) management tools and Industrial Control System (ICS) tools.
- **Anticipated Outcome:** enabling a systematic identification of all types of possible attack (intrusion) scenarios that can potentially lead to cascading failures, resulting in a “library” of such intrusion types.

Task 11 - Key Questions for Consideration



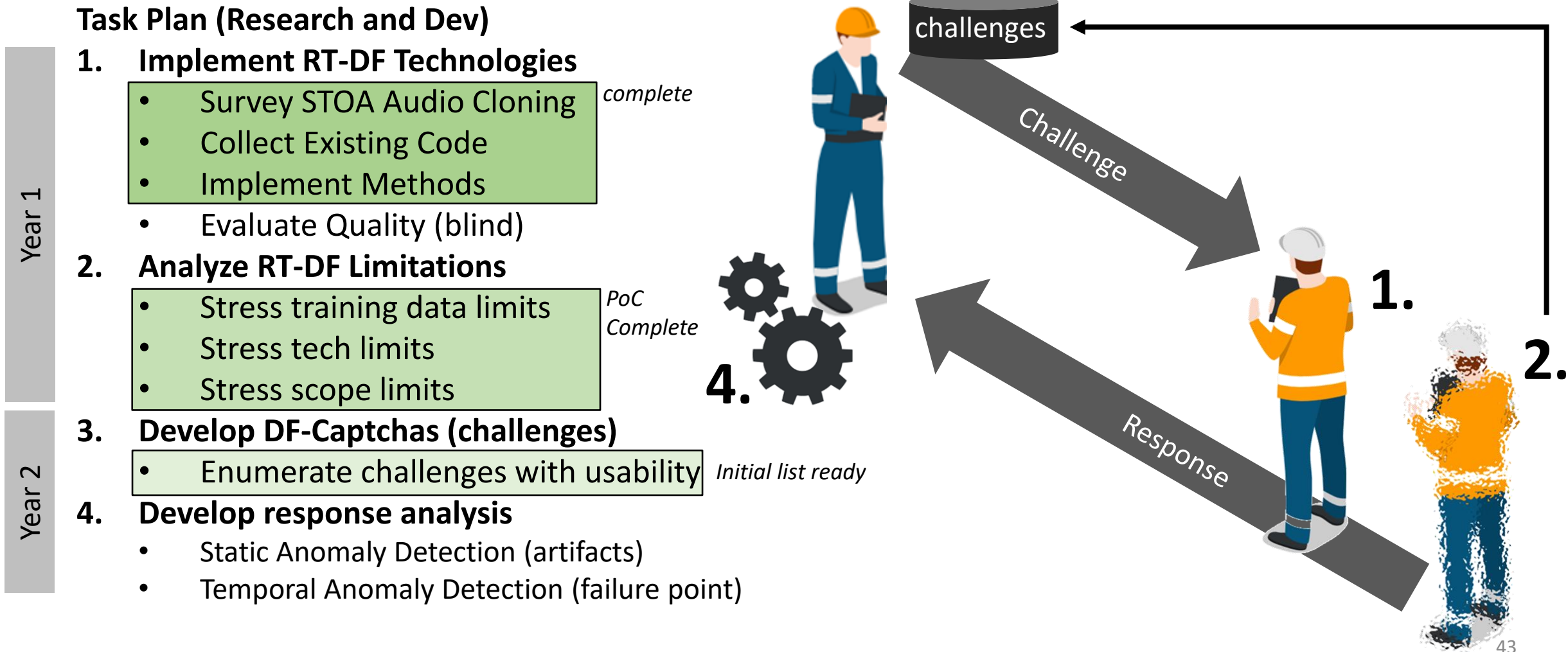
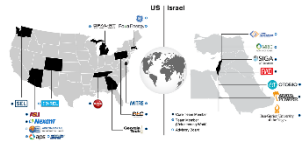
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 11 - AI based intrusion detection – RT-DF Prevention

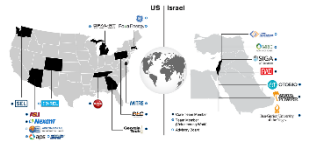


- **Problem:** With deepfake technology, attackers can impersonate voices and faces to make phone calls and join meetings to steal information, perform scams, and carryout espionage
- **Solution:** Captcha – send caller challenge (e.g., press cheek) which is extremely hard for the attackers deepfake technology to reproduce, then detect massive anomalies
- **Existing Alternatives:** Existing solutions use machine learning classifiers or anomaly detectors to identify subtle artifacts in the audio/video content
- **Unique Value Proposition:** With our solution, high risk communications/meetings can be secured with minimal hinderance.
- **Unfair Advantage:** Deepfakes will be hyper realistic in the next year or so –existing solutions will be obsolete. We use an *active* defence to expose the attacker. WE also know when/where to look due to the challenge response setup.
- **Channels:** Call center security, virtual meeting waiting rooms, cell phone firewalls, ...
- **Revenue Streams:** subscription-based cloud firewall (voip), app on phone with paid updates (new challenges, detectors,...)

Task 11 - AI based intrusion detection – RT-DF Prevention



Task 11 - Key Questions for Consideration



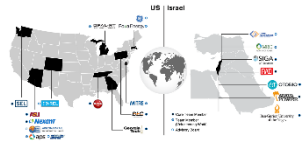
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 12 - Explainable cyber AI analytics



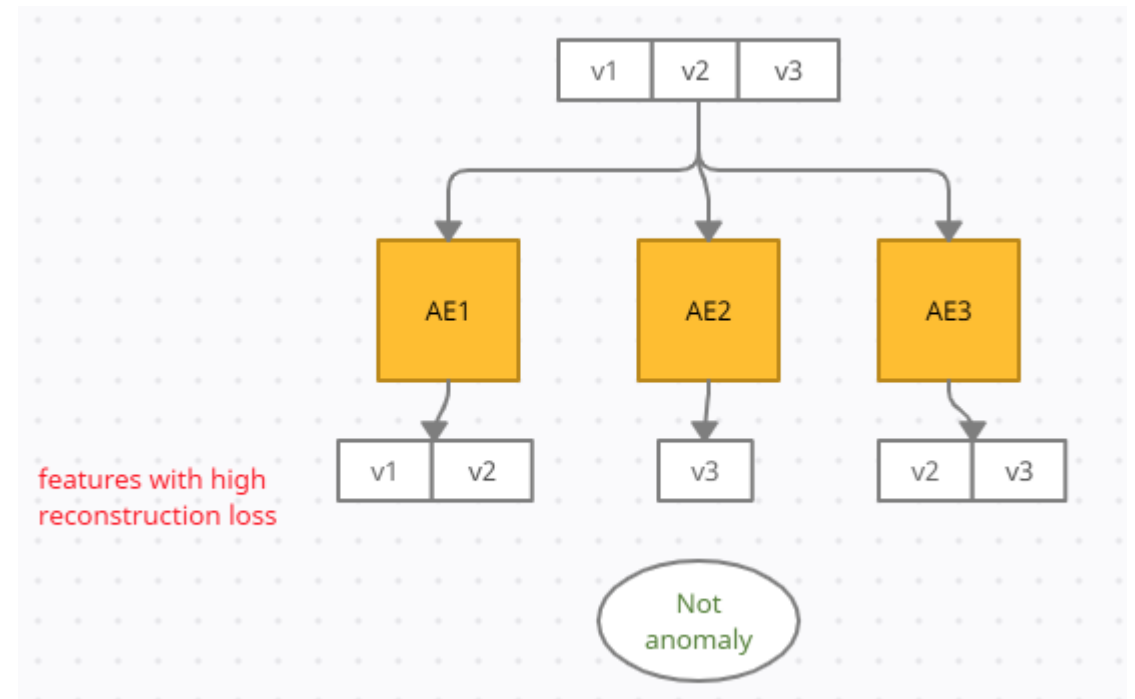
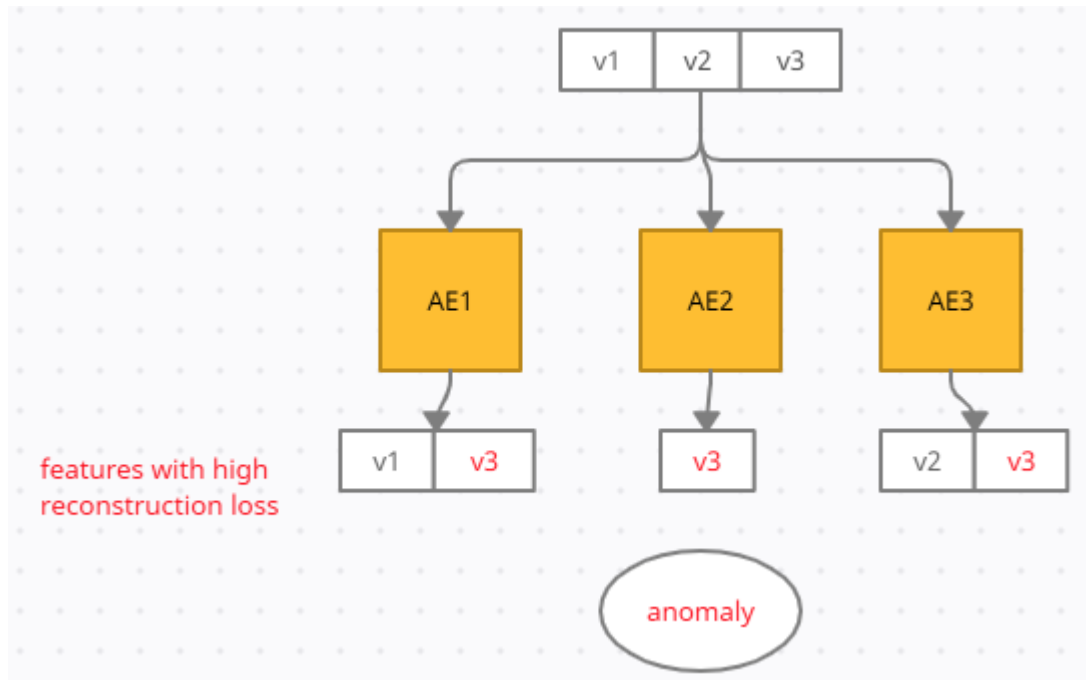
- Problem: Anomalous instances usually include rare but not interesting anomalies
- Solution: An algorithm based on the explanations to the results of a few (any) anomaly detectors, that decides if a record is anomalous
- Existing Alternatives: Ensemble of anomaly detectors, without the explanations to the anomalies
- Unique Value Proposition: Save time and money for your domain experts/analysts by providing them anomalies that their explanations are agreed by most anomaly detectors
- Unfair Advantage: Proficiency in the field of XAI (Explainable AI)
- Channels:
- Revenue Streams: By decreasing domain experts/analysts' time in investigating anomalies with a higher probability to be real anomalies and not rare events

Task 12 - Explainable cyber AI analytics

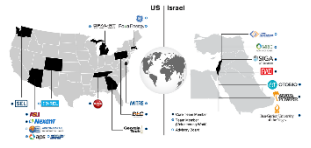


- **Method:** Ensemble of anomaly detector models

- Train multiple models independently
- Decide using an ensemble of anomaly detectors' **explanations** which records are anomalous

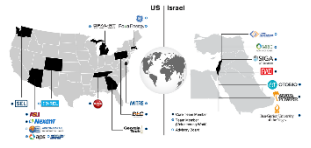


Task 12 - Key Questions for Consideration



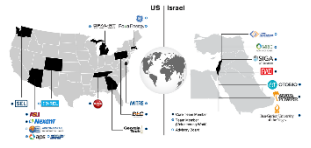
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 13 - Firmware verification



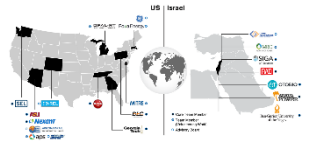
- Problem: Verify the firmware installed on PLC devices
- Solution: Profiling the side channel signals (Power, EM) of legitimate software execution
- Existing Alternatives: whitelist/blacklist antiviruses
- Unique Value Proposition: External monitor, No OS interference
- Unfair Advantage: additional hardware(oscilloscope), access to the source code, (possibly) long training time.
- Channels: Through a PLC vendor, provide a demonstration of detecting recent malwares
- Revenue Streams: Additional security layer

Task 13 - Firmware verification



- Preliminary stage:
 - Detecting peak frequency and strongest emission point – EM side channel
- Phase 1: static analysis of the source code, generating full coverage tests for the code. We assume here that PLC code is not branch-heavy (High risk assumption)
- Phase 2: Executing the test cases with deactivated outputs and collecting the side channel signals (Power, EM)
- Phase 3: Data preprocessing and feature extraction (noise removal, signal smoothing, etc)
- Phase 4: Training a ML classifier
 - Class = Execution path
 - Anomaly = low confidence in all classes
- Challenge: OS context switches

Task 13 - Key Questions for Consideration



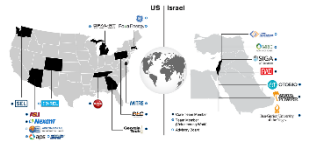
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 14 - Cyber-attack tolerance



- Problem:
 - End point device (controller) are susceptible to exploits.
 - Compromised devices behaves as insider threat;
 - Lies (e.g. Stuxnet) & compromises operation (incl. monitoring).
- Solution:
 - Prevent device/controller compromise by leveraging physical properties of the systems, hence
 - Agnostic to the attack vectors (malwares/exploits techniques), without
 - Relying that the controller software is devoid of any vulnerability
- Existing Alternatives:
 - Guaranteeing of the controller that controller software devoid of any vulnerabilities, which generally requires an expensive engineering (formal methods), or
 - Inserting many layers of sanitation and protections into controller software, which can violate real time property of controller.
- Unique Value Proposition:
 - Exploiting system's invariant (physical property) and established Fault-Tolerant Method, to provides Cyber-attack-Tolerant method, agnostic to exploits' methods, easily and efficiently deployable in new and legacy controllers
- Unfair Advantage:
 - Enhancement over a novel (overlooked & scarcely published) methods, invented & proved within US Navy.

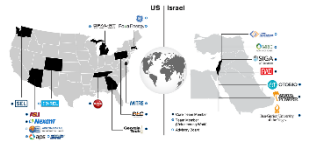
Task 14 - Cyber-attack tolerance



- Task Details

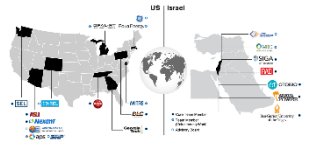
- Develop SubProcess BFT++ software architecture into OpenPLC development environment.
- Scientific Foundation:
 - Investigation of theory & principles of sub-process sensitivity rankings to cyber attack, leading to identification of candidate sub-processes to be protected
 - Investigation of principles for selecting specific BFT++ resilience methods for particular sub-process to be protected
- M14.2 Insert BFT++ software into OpenPLC dev environment with all features
- M14.3 Integration and validation of BFT++ software in OpenPLC dev environment
- M14.4 Demonstrate a case of BFT++ implementation on OpenPLC

Task 14 - Key Questions for Consideration



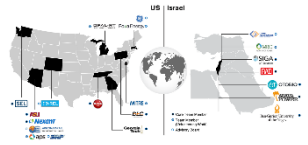
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 15 - Self-healing and auto-remediation



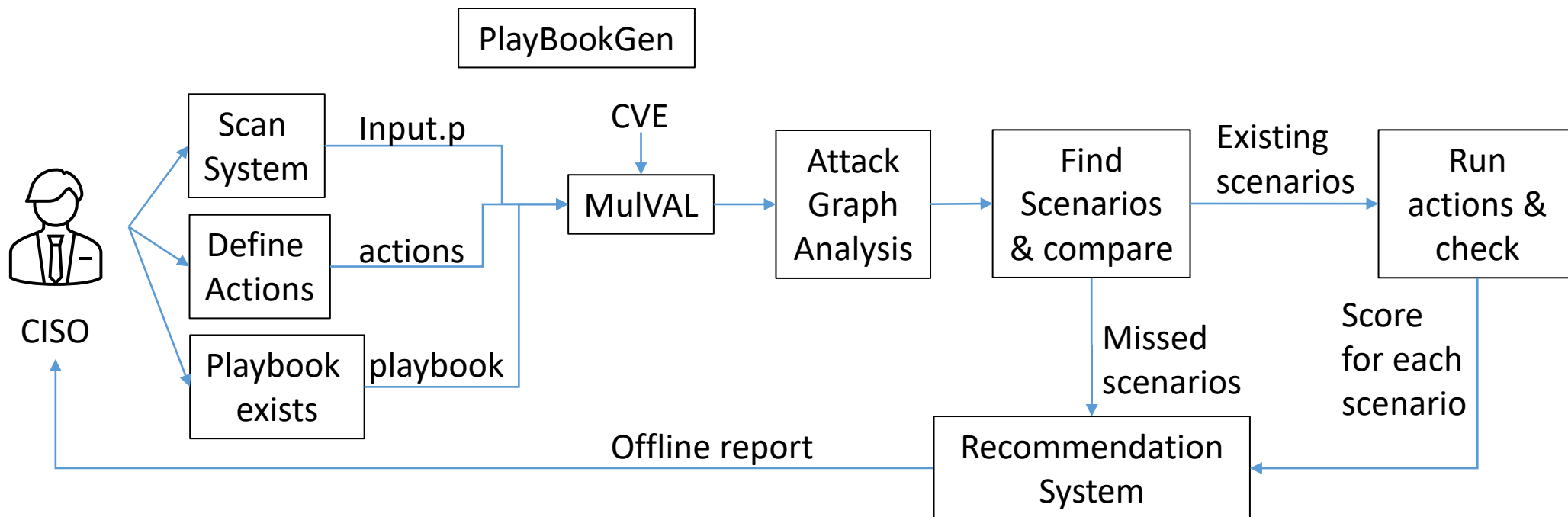
- **Problem:** Critical facilities requires a fast and effective response to cyber security incidents that can be implemented as playbooks.
- **Solution:** Use attack graphs as a support tool for generating effective playbooks for cyber-physical systems.
- **Existing Alternatives:** Playbooks are manually generated by experts.
- **Unique Value Proposition:** Continuous update, possible to take existing playbook and enhance it, attack graphs can serve the red team.
- **Unfair Advantage:** Non.
- **Channels:** Critical sites, Industrial facilities.
- **Revenue Streams:** *As Product:* on-premise software to constantly enhance the facility's playbook and readiness.
SAAS: online service to get recommendations for better defenses.
Support: used by Security consultants to support the factory's defense planning.

Task 15 - Self-healing and auto-remediation

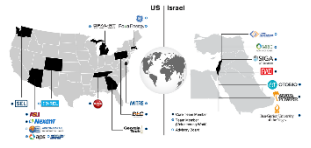


- Task Details:

- Use case: Facility CISO takes (1) defensive Playbook (if exists), (2) the system description and (3) the actions that he can do to defend against intruders (ex. Replace PLC, reset router, restore backup) – insert those into PlayBookGen system which analysis the attack graphs, compare scenarios, check the existing ones and provide a report for better playbook.

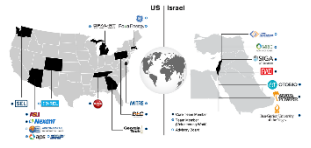


Task 15 - Key Questions for Consideration



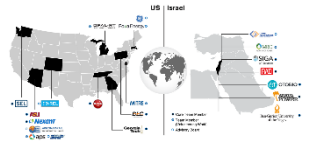
1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?

Task 16 - RL control for CPS



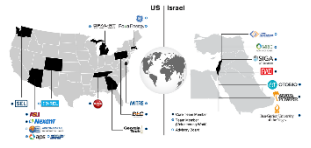
- **Problem:** Developing a RL framework for devising the “best” control policies to significantly suppress or even eliminate cascading failures in distributed electrical power networks
- **Solution:** Exploiting deep RL (e.g., deep-Q learning), stochastic game theory, and optimization to understand the dynamics of interplay between attackers and defenders and accordingly developing effective control strategies for cyberphysical systems
- **Existing Alternatives:** RL is being studied widely to control all kinds of physical and engineering systems, even quantum systems
- **Unique Value Proposition:** A combination of deep Q-learning, game theory, and mathematical optimization for controlled protection of cyberphysical systems
- **Unfair Advantage:** The ASU Task-16 team has expertise in RL, game theory, nonlinear dynamics and complex systems
- **Channels:** Working closely with Resource Innovations/Nexant
- **Revenue Streams:** Unable to speculate

Task 16 - RL Control for CPS: Details



- **Main Objective:** developing a machine-learning framework for devising the “best” control policies to significantly suppress or even eliminate cascading failures in distributed electrical power networks.
- **Idea:** exploiting deep reinforcement learning, stochastic game theory, and optimization to understand the dynamics of interplay between attackers and defenders and accordingly developing effective control strategies for cyberphysical systems.
- **Anticipated Outcome:** a library of control scenarios that can be implemented in the real world to prevent cascading failures in distributed power networks.
- **Reinforcement Learning:** finding the optimal control path for any given attack scenario.

Task 16 - Key Questions for Consideration



1. What is the potential for commercialization? (Poll: 1 Very Low to 5 Very High)
2. Are the methods presented useful to your organization?
3. Do you see any roadblocks to implementation?
4. What changes would you propose?
5. What other related R&D topics would you suggest?