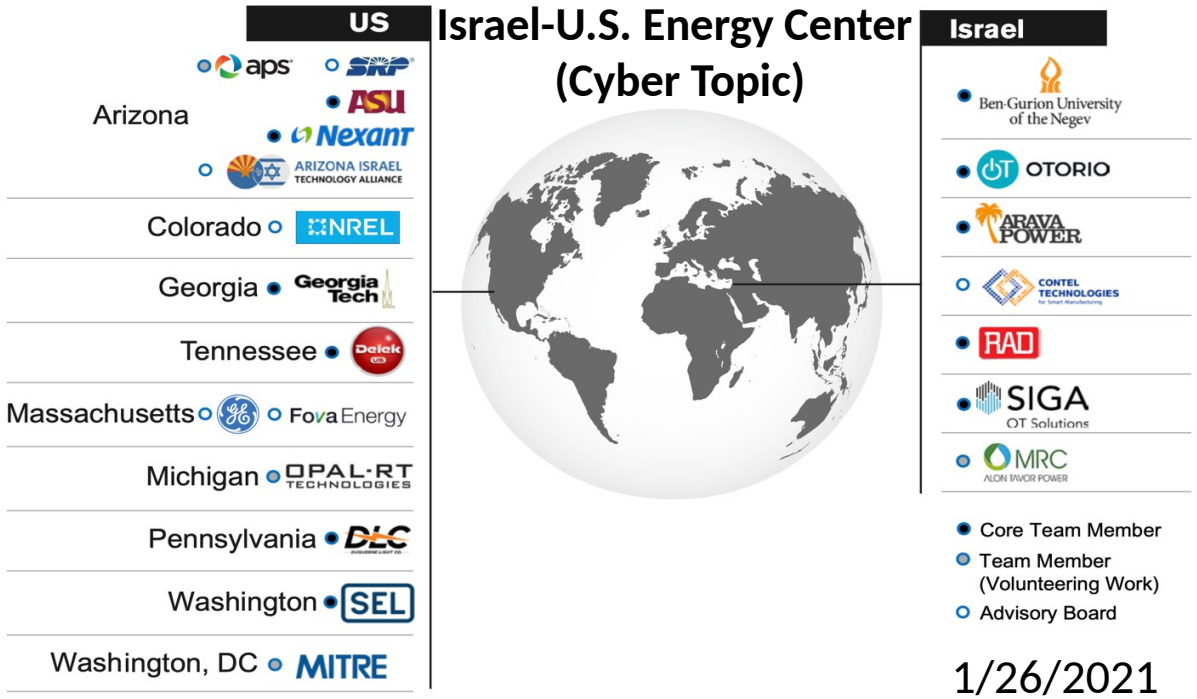
Comprehensive Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience



1/26/2021

Prepared for

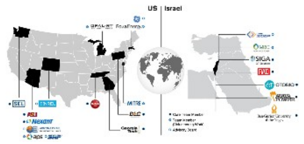
Itai Ganzer and **Ofer Goldhirsh**

Israel Innovation Authority

Avi Shavit and **Eynan Lichterman**

Israel Ministry of Energy

Cyber Security News



December
Iranian wiper malware was deployed against the network of Bapco, the national oil company of Bahrain.

January 2020
A Russian hacking group infiltrated a Ukrainian energy company where Hunter Biden was previously a board member, and which has featured prominently in the U.S. impeachment debate.

April 2020
Government and energy sector entities in Azerbaijan were targeted by an unknown group focused on the SCADA systems of wind turbines.

April 2020
Suspected Iranian hackers unsuccessfully targeted the command and control systems of water treatment plants, pumping stations, and sewage in Israel.

May 2020
Israeli hackers disrupted operations at an Iranian port for several days, causing massive backups and delays. Officials characterized the attack as a retaliation against a failed Iranian hack in April targeting the command and control systems.

May 2020
German officials found that a Russian hacking group associated with the FSB had compromised the networks of energy, water, and power companies in Germany by exploiting IT supply chains.

July 2020
Israel announced that two cyber attacks had been carried out against Israeli water infrastructure, though neither were successful.

August 2020
New Zealand's stock exchange faced several days of disruptions after a severe distributed denial of service attack was launched by unknown actors.

September
An electric utility in Pakistan that services 2.5 million customers fell victim to a ransomware attack by unknown actors. The attack did not disrupt the power supply but prevented customers from accessing their accounts and demanded almost $4 million in Bitcoin as ransom.

September
French shipping company CMA CGM SA saw two of its subsidiaries in Asia hit with a ransomware attack that caused significant disruptions to IT networks, though did not affect the moving of cargo.

October 2020
Iran announced that the country's Ports and Maritime Organization and one other unspecified government agency had come under cyberattack.

2020…

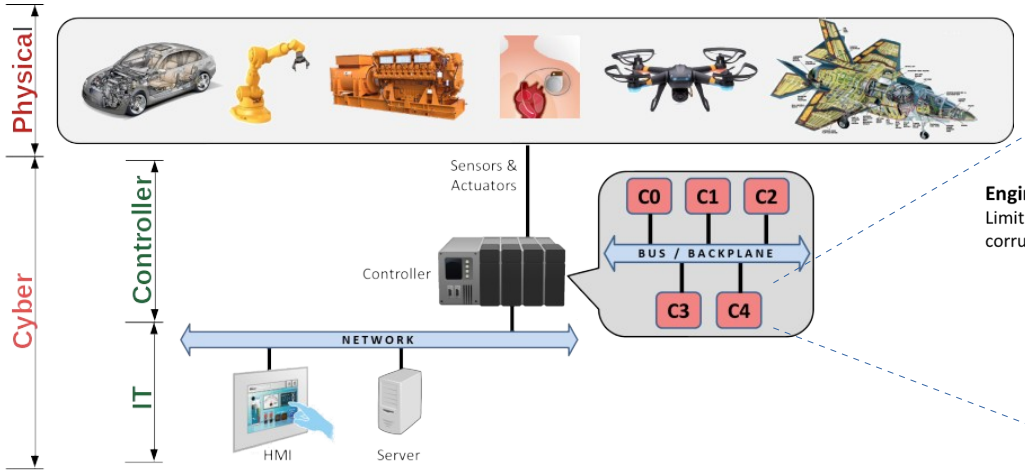
CSIS, Significant Cyber Incidents, https://www.csis.org/programs/strategic-technologies-program/significantcyber-incidents

Cyber-Attack Resilience for CPS – Part A

Goal:

- Continuous, uninterrupted operation under direct cyber-attack campaign
- Develop an economical and robust cyber attack resilience at controller level (level 0 & 1), relying on the physical properties of the controlled physical systems.

- Past Methods:
- BFT++ is a new approach to resiliency, leveraging established Fault Tolerant systems.
- Proposed SubProcess BFT++ will reduce the deployment cost for BFT++ cyber-attack-resilience.

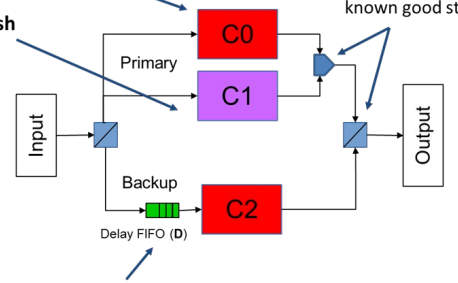


$$T_{crash} \leq D * T_{SC} \leq T_d - T_r$$

Artificial diversity
Protects controllers from being owned

Controller recovery
Detects variance and restores controller(s) to known good state

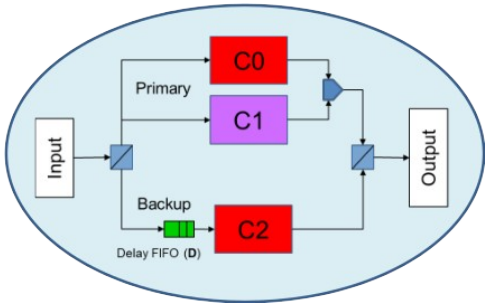
Engineered FastCrash
Limits time spent in corrupted state



Delayed input sharing
Keeps backup in clean state and isolates malicious trigger

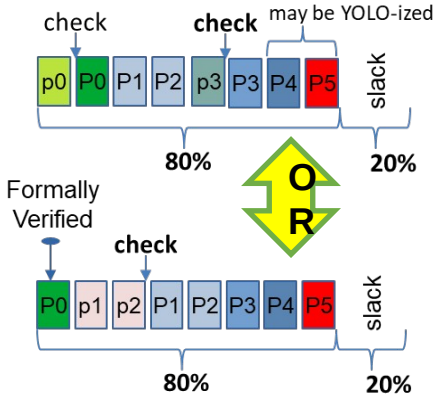
Successful attack requires:
1. Success on derailing targeted program → targeted program loses control
2. Success on capturing control → attacker controls program execution

Cyber-Attack Resilience for CPS – Part B



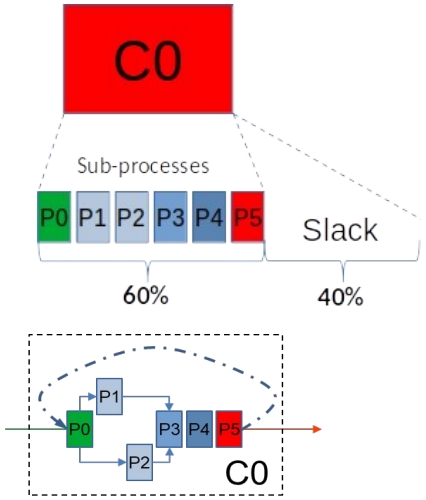
BFT++

Similar



SubProcess BFT++

SubProcess BFT++ Engineering **Tool**



We plan to integrate the SubProcess BTF++ engineering tool into Schweitzer Engineering Laboratories (SEL) PLC design tools and environment.

Impact:

- Providing cyber attack resilience for application which cannot afford device redundancy, alleviate the need for redundant device in BFT++,
- Significantly widen the applicability of BFT++ and resilience against direct cyber-attack
- Automated isolation of offending data, can be communicated to other system components, e.g. SCATOPSY, RAM2., to prevent repeat attack.
- Integration into SEL design environment for ease of deployment and dissemination.

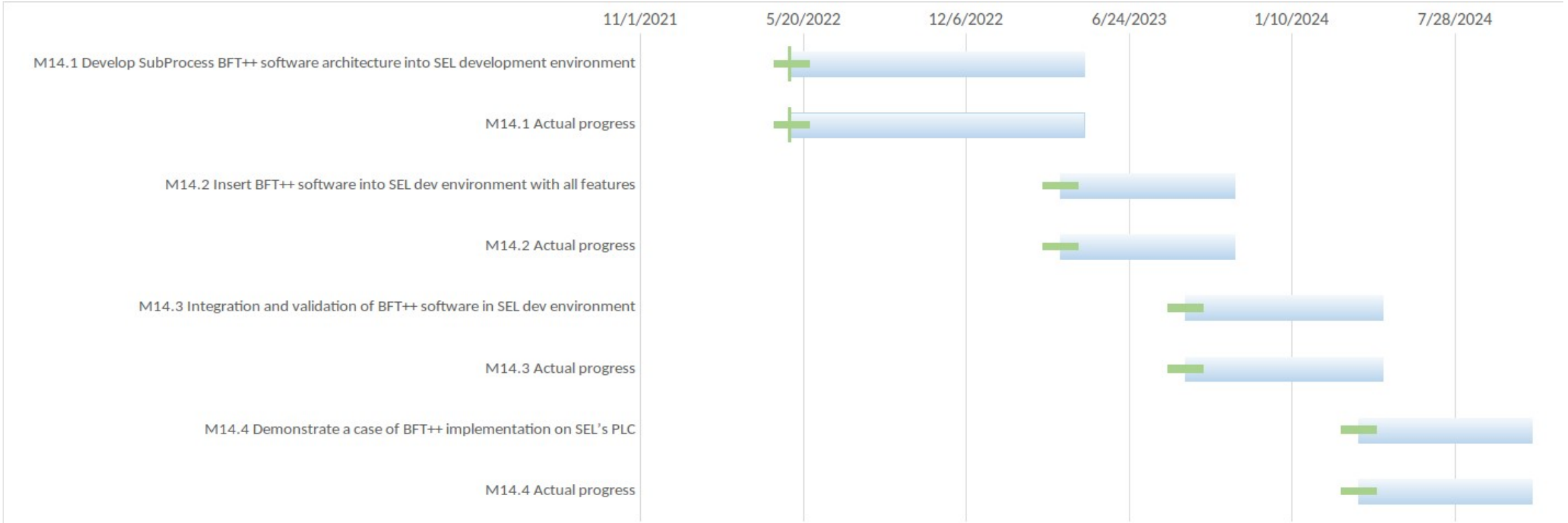
Cyber-Attack Resilience for CPS – Progress

Current status:

- Coordination meetings with SEL:
  - Initial Coordination meeting on April 5th 2022
  - Training for SEL RTAC development tools and environment on April 18th 2022
  - Meeting for further deep dive into SEL's:
    - Operating System implementation
    - Compiler and code generation process
    - Real time scheduler
    - Etc.
  - is currently being scheduled
- Commercialization through integration into Vendor's development environment (SEL, and other vendors).

- Started on May 1st 2022
- Initial research will use an open source PLC environment: **ClassicLadder**.
  - For experimentation platform and
  - For analyzing generated codes for PLCs
    - Understanding scheduling structure
    - Studying design trade offs for integrating sub-process BFT++
  - A Linux toolset, as oppose to Windoze
- We'll revisit this decision after SEL RTAC deep dive.
- Future: integration into SEL design tools and environment

Schedule & Milestones:

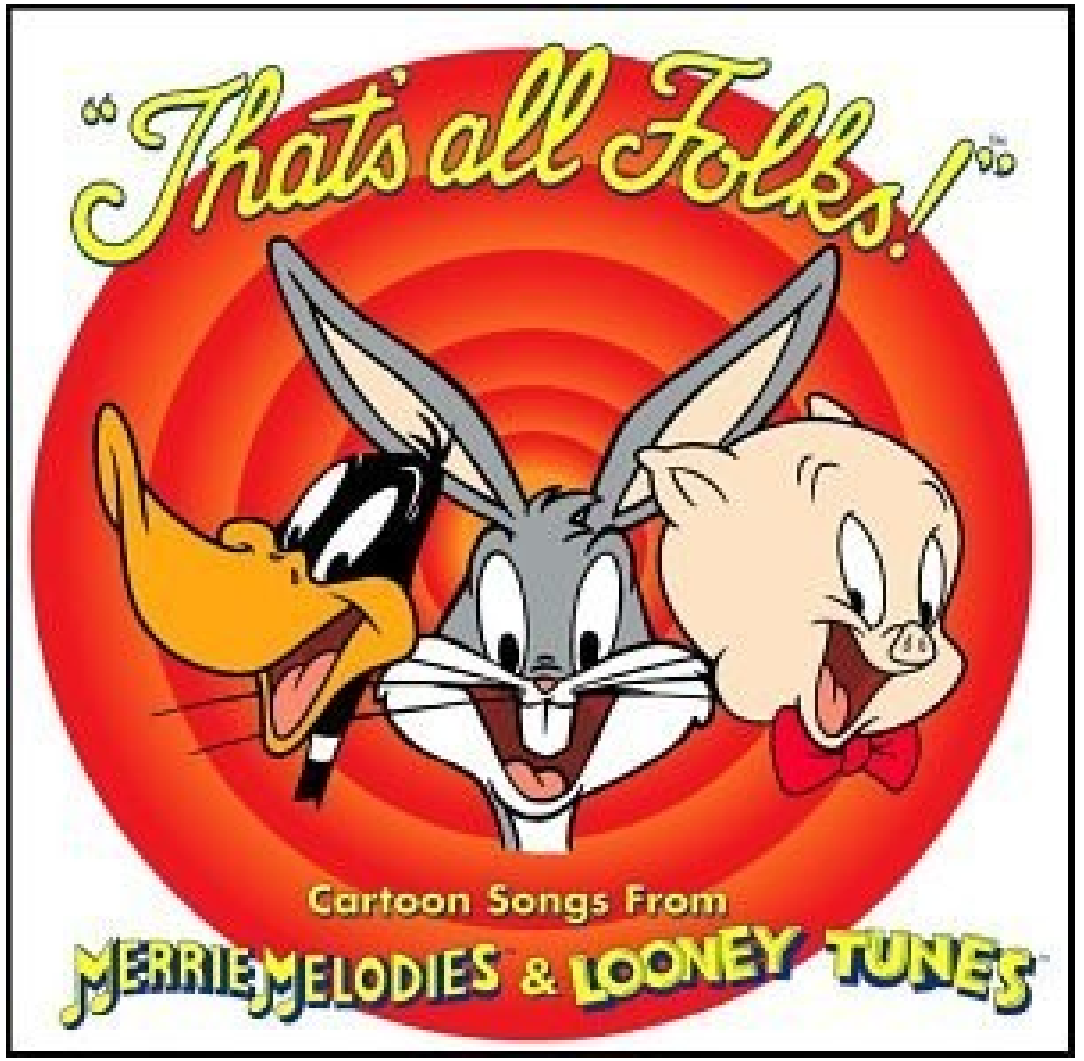


- We are starting in May 2022
- Team:
  - Dr. Sukarno Mertoguno
  - Dr. Michail Alexiu
  - Martin Ivanchev, joining in August 2022

The End

Georgia Tech

Cyber Physical System



Physics Rules !!!