



University of Cyprus
Department of Electrical
and Computer
Engineering



Cybersecurity for Next Generation Critical Infrastructure Systems (CIS)

Prof. (Asst.) Dr. Angelos Marnerides, SMIEEE
Department of Electrical & Computer Engineering
KIOS Research & Innovation Centre of Excellence
University of Cyprus
marnerides.angelos@ucy.ac.cy



Imperial College
London

Funded by:

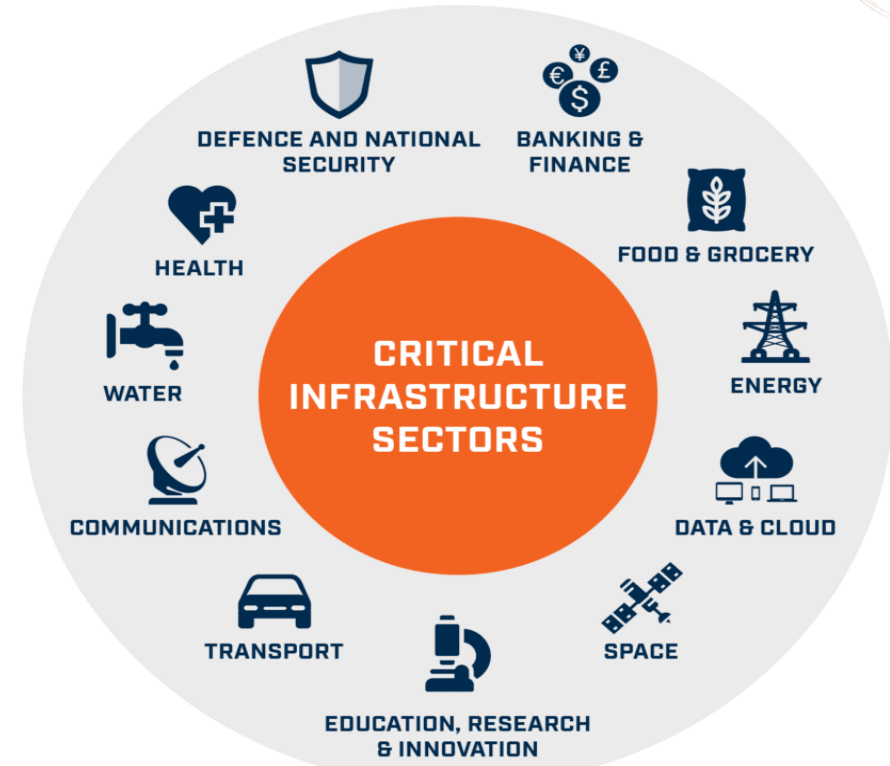


Critical Infrastructure Systems (CIS)

- Definition varies depending on the region

- Examples:

- Water
 - treatment/ distribution
- Power Grid
 - generation/transmission/distribution
- Defence & National Security
- Manufacturing
- Oil & Gas
- Health
- Telecommunications



Credits: [huntsmansecurity.com](https://www.huntsmansecurity.com)

- Most constitute: **Critical National Infrastructures (CNIs)**
- All rely on: **Industrial Control Systems (ICS)**

The problem – Internet-enabled CNI an attacker's playground

- **Reality:** a world of threats against CNI ..

- IoT-“exposed” CNI

- Nation-sponsored cyberwarfare

- Organised cyber-crime/terrorism

- In the depths of the DarkWeb...
 - Crime-as-a-Service (CaaS)
 - Bots-as-a-Service (BaaS)
 - Malware-as-a-Service (MaaS),
 - DDos-as-a-Service (DDoSaaS) etc....

- Complex systems → inadequate security

- IT/OT convergence (IoT-enabled ICS)
 - too challenging to profile/monitor *

Ukrainian power grid 'lucky' to
withstand Russian cyber-attack

12 April 2022



Russia-Ukraine war

The New York Times

**Hackers Are Targeting Nuclear
Facilities, Homeland Security Dept.
and F.B.I. Say**

Share full article



The Wolf Creek Nuclear power plant in Kansas in 2000. The corporation that runs the plant was targeted by hackers. David Eulitt/Capital Journal, via Associated Press



World Business Markets Sustainability Legal Breakingviews Technology In

Energy Data Privacy Grid & Infrastructure Solar Wind

**Insight: Cyberattacks on renewables:
Europe power sector's dread in chaos of
war**

By Nora Bull, Nina Chestney and Christoph Steitz

June 15, 2023 8:15 PM GMT+3 · Updated 3 months ago



**SektorCERT reports cyber attack against Danish critical
infrastructure, raises concerns of state involvement**

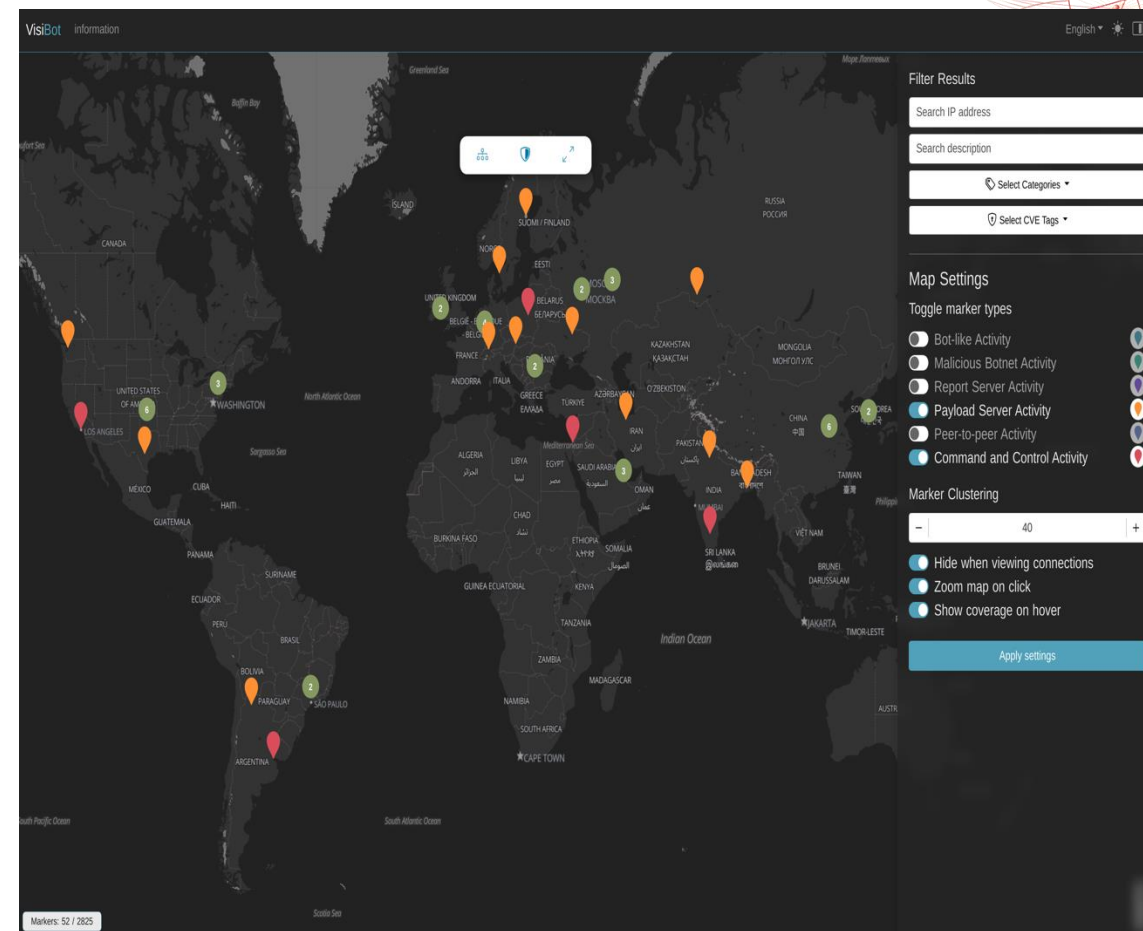
NOVEMBER 13, 2023



Beginning of a journey...

VisiBot @ UCY KIOS

- “ICS is seen as IoT”
- How many IoT devices are vulnerable or exploited in the wild?
 - As parts of greater large-scale attack vectors
→ IoT botnets
- Botnets: networks of compromised IoT devices
 - Controlled centrally or peer-to-peer
 - Biggest infrastructures rented in the Darkweb for large-scale attacks
 - E.g., Phishing, DDoS, Cryptohijacking etc
- Requirements:
 - Internet vantage points
 - Ground truth
 - Learning/profiling
- Result: **VisiBot**



SPAMHAUS
TECHNOLOGY

MaxMind



ipinfo.io



RIPE NCC
RIPE NETWORK COORDINATION CENTRE



SHODAN

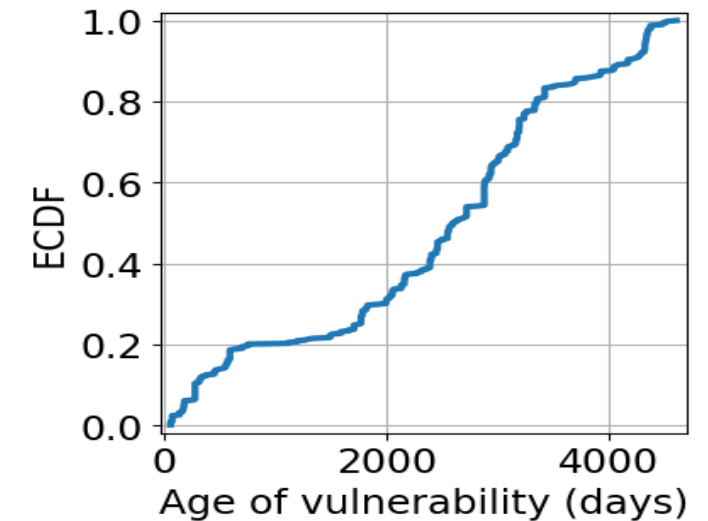
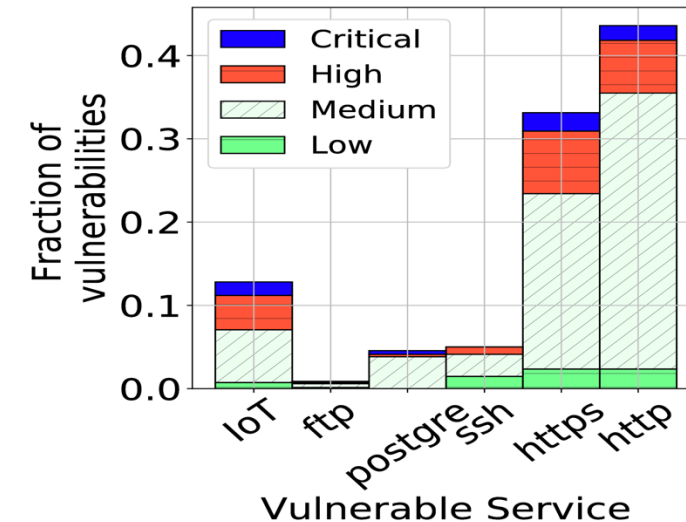
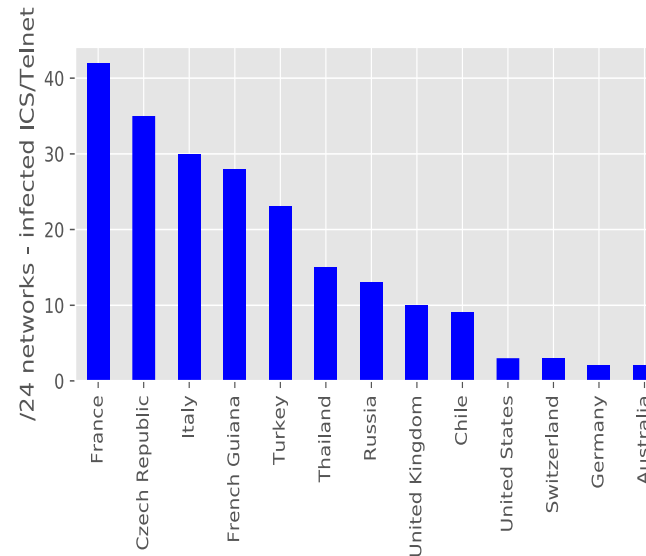
ABUSE|ch

VIRUSTOTAL



VisiBot on ICS

- Sep 22 – Sep 23
- # of infected ICS-related IPs → 1.6K
 - 64.2% ModBus (1.3K IPs)
 - 21.2% Tridium/Fox
 - 14.3% BACnet
 - 0.3% Siemens S7
 - 0% DNP3
- 832 unpatched types of vulnerabilities. 20% of the vulnerabilities have high or critical severity (75% older than 5 years old!)
- 37 different services behind the infected IP addresses (only 34% use HTTPS!)
- Some with unpatched vulnerabilities.. (for more than 10 years!)



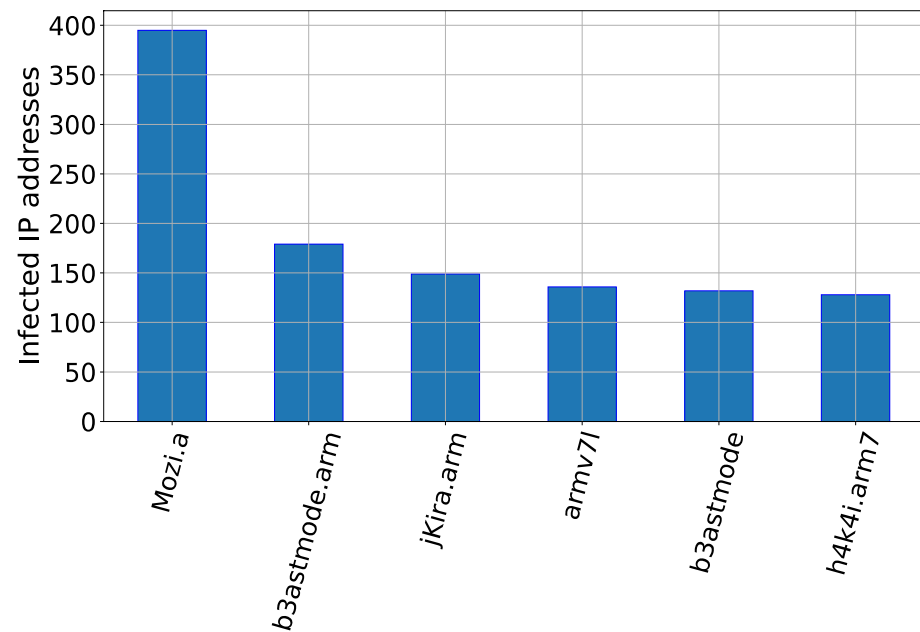
Note: these are already **exploited**, and not just vulnerable...and it's for less than 15% of the global IPv4 Internet!



VisiBot: Tendency malware

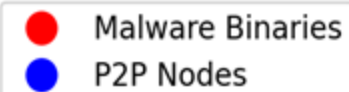
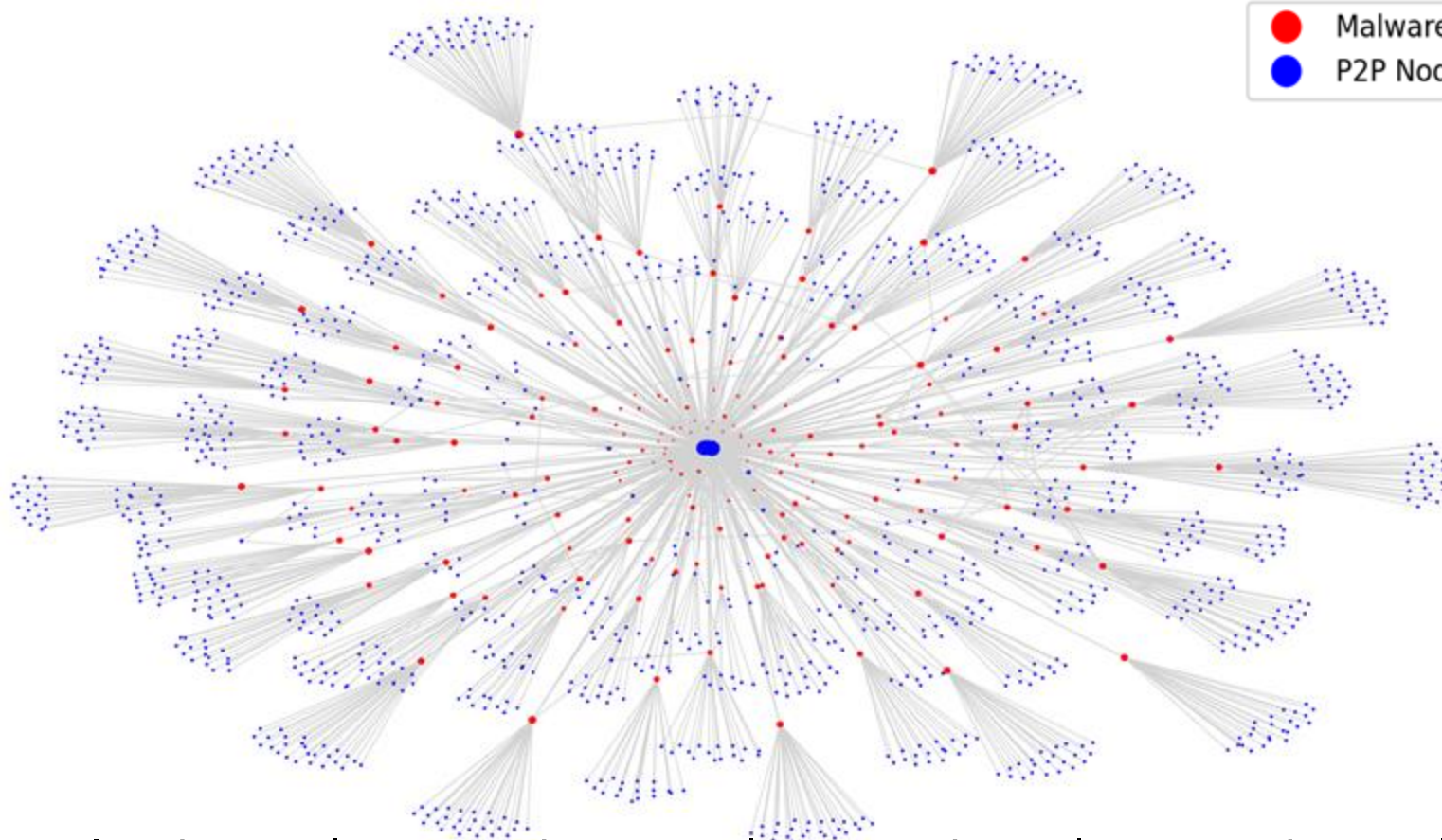


- Period: Sep 22 – Sep 23
- Mozi.a – Modbus/TCP
 - Energy systems
- B3astmode.arm – Fox/Tridium
 - water utilities
- jKira.arm – Modbus/TCP & BACnet
 - water, energy and building automation
- Conclusion: ICS devices → strategic botnet components





VisiBot Botnet graph



Top P2P DNS queries

dht.transmissionbt.com

router.bittorrent.com

router.utorrent.com

bttracker.debian.org

Payloads: 137 | P2P Nodes: 2114 | Min nodes: 1 | Max nodes: 42 | Avg nodes: 13

Finding: ICS Devices -**including Programmable Logic Controllers –PLCs-** can be P2P botnet “supernodes” !



PLC-oriented defense approaches– an issue!



Over 100 Siemens PLC Models Found Vulnerable to Firmware Takeover

Jan 12, 2023 Rave Lakshmanan

Firmware and Hardware Security



Critical Architectural Vulnerabilities in Siemens SIMATIC S7-1500 Series Allow for Bypass of All Protected Boot Features



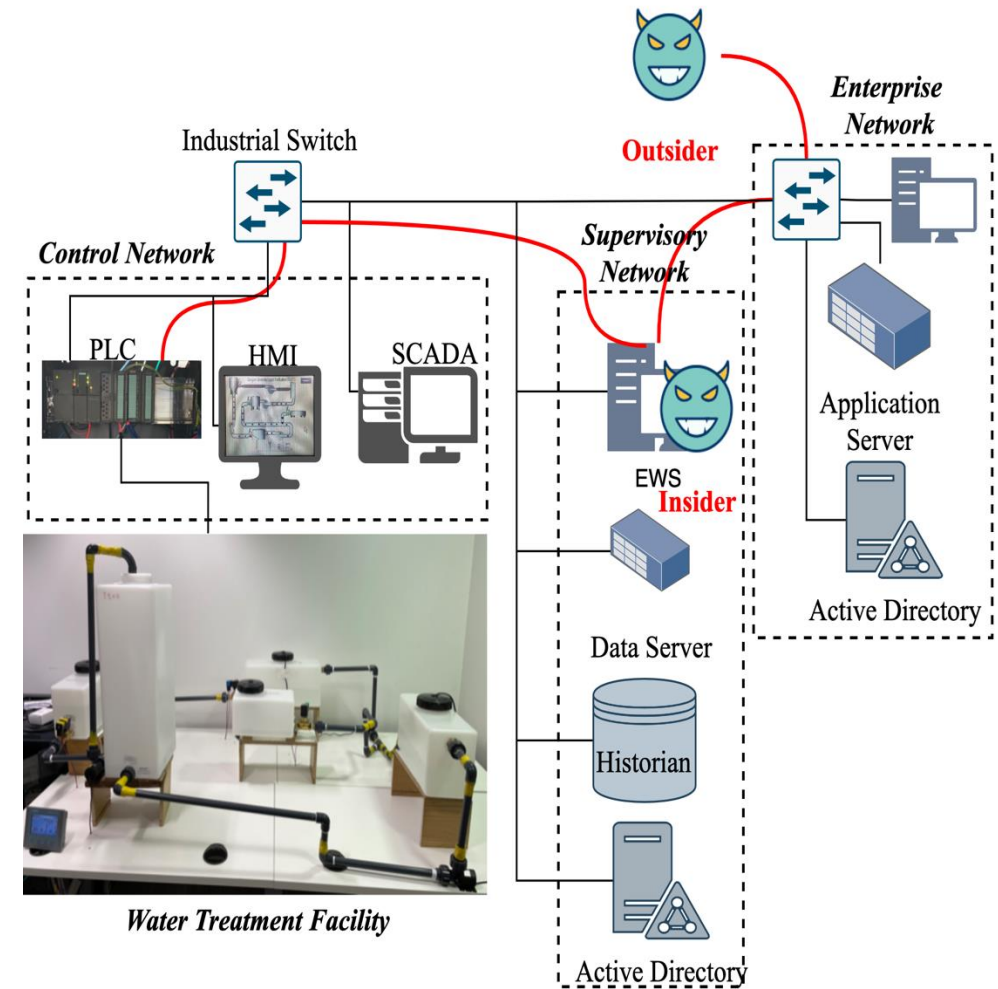
Are your PLCs an easy target? A mindset shift can significantly reduce PLC firmware vulnerabilities





PLCPrint - setup

- **Goal:** *vendor-independent* real-time PLC memory-level anomaly detection
- **Scenarios:**
 - Sectors: utilities & national defence
 - “Phishing” threat vectors
 - I/O module anomalies
 - malicious & operator “legit” faults

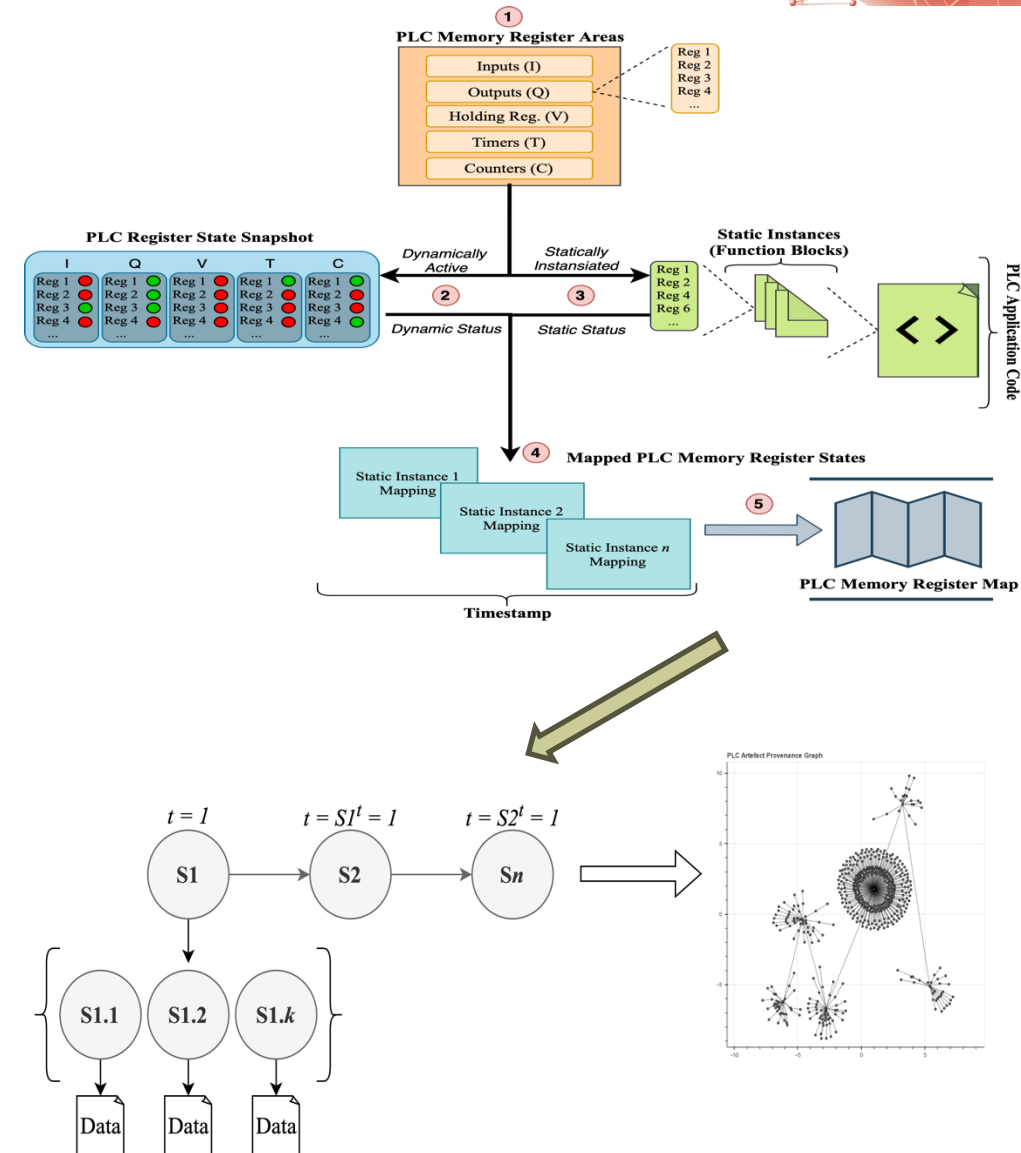


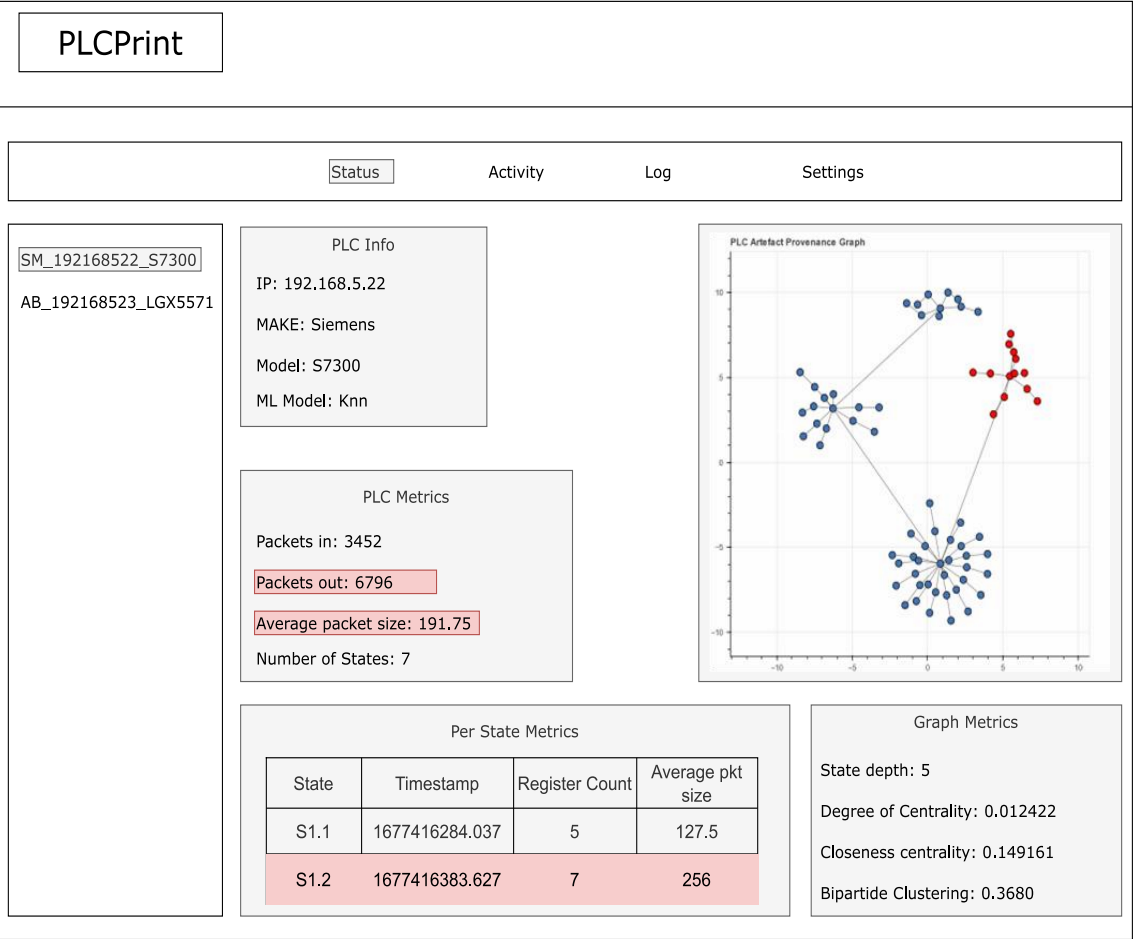


PLCPrint – composition

PLC vendor-independent:

- Define PLC registers within memory register areas
- Actively acquire snapshot of register states
 - Register given *dynamic status*
- Acquire PLC application code
 - Register given *static status*
- Cross-referenced to give each register mapping type
 - i.e., a “**fingerprint**”
- Anomaly **detection**:
 - OC-SVM || LOF,
- Anomaly **diagnosis**:
 - Deviation distance-based $\leftrightarrow$ graph-based provenance





Classifier	PLC Model	Test Set	Precision	Recall	F1	Time
OCSVM	S7-300	Cyber Intrusion	97.2%	95.5%	96.4%	19ms
		System Fault	99.2%	96.6%	97.9%	23ms
		Cyber Intrusion and System Fault	97.0%	95.4%	96.2%	28ms
	CL-1756	Cyber Intrusion	96.7%	99.5%	98.1%	29ms
		System Fault	93.0%	99.1%	96.0%	18ms
		Cyber Intrusion and System Fault	94.8%	99.1%	97.0%	14ms
LOF	S7-300	Cyber Intrusion	99.7%	97.8%	98.9%	38ms
		System Fault	99.8%	98.7%	99.3%	41ms
		Cyber Intrusion and System Fault	99.7	99.3%	99.7%	42ms
	CL-1756	Cyber Intrusion	99.3%	98.9%	99.5%	38ms
		System Fault	99.3%	98.1%	99.0%	33ms
		Cyber Intrusion and System Fault	99.4%	99.2%	99.6%	31ms
IF	S7-300	Cyber Intrusion	76.3%	87.9%	81.7%	88ms
		System Fault	99.3%	92.3%	96.0%	87ms
		Cyber Intrusion and System Fault	88.4%	90.0%	89.3%	84ms
	CL-1756	Cyber Intrusion	99.4%	95.7%	97.8%	85ms
		System Fault	99.2%	91.2%	95.4%	84ms
		Cyber Intrusion and System Fault	98.8%	94.0%	97.0%	81ms



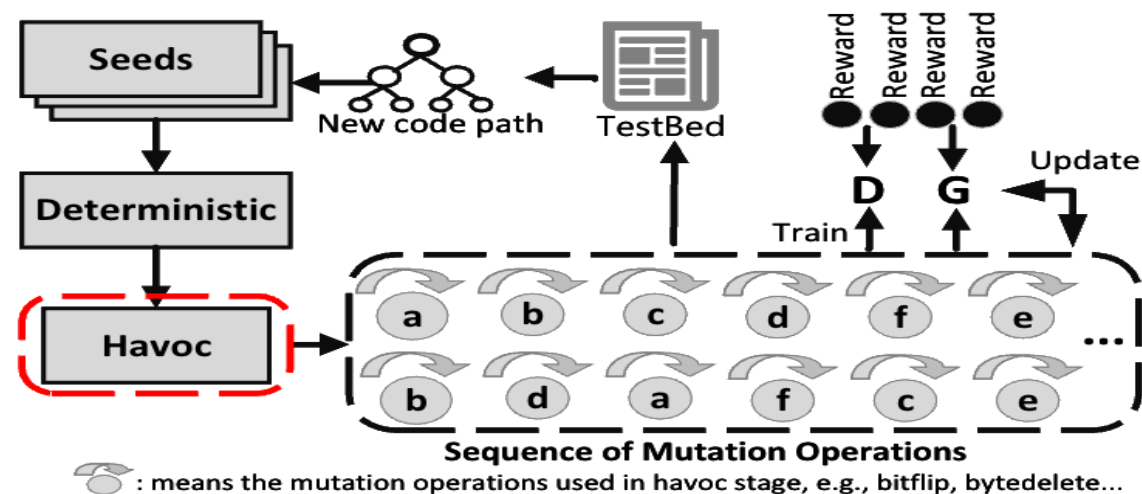
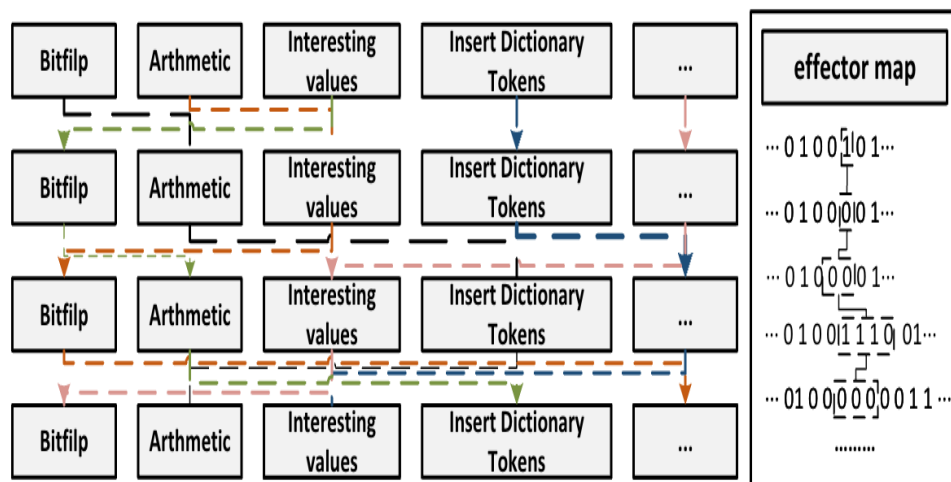
“Zero day” exploits & vulnerability discovery in PLCs

- **Goal:** vulnerability discovery for building “zero-day” exploit defense on PLCs
- **Challenges:**
 - Tools, frameworks, and techniques for reverse engineering of application binaries in the IT world do not directly translate to the OT world.
 - Strong vendor dependency
 - ICS binary reverse engineering remains a tedious manual procedure.
 - PLC application binaries differ from conventional IT-oriented application binaries
 - Execution model: sequential in normal application vs. scan cycle dictating PLC applications
 - I/O operations & file formatting: well-documented compilation for “normal” binaries
 - Even for experimentation/development: ...close to impossible on emulating PLC firmware



Sizzler: Sequential fuZZing in LadderER diagrams for vulnerability detection and discovery in PLCs

- **Vendor-independent** vulnerability discovery framework
 - specific to PLC applications operating on ladder logic diagrams
 - optimal synergy of a mutation-based fuzzing strategy
 - → learned through Sequence-Generative Adversarial Networks (Seq-GANs)



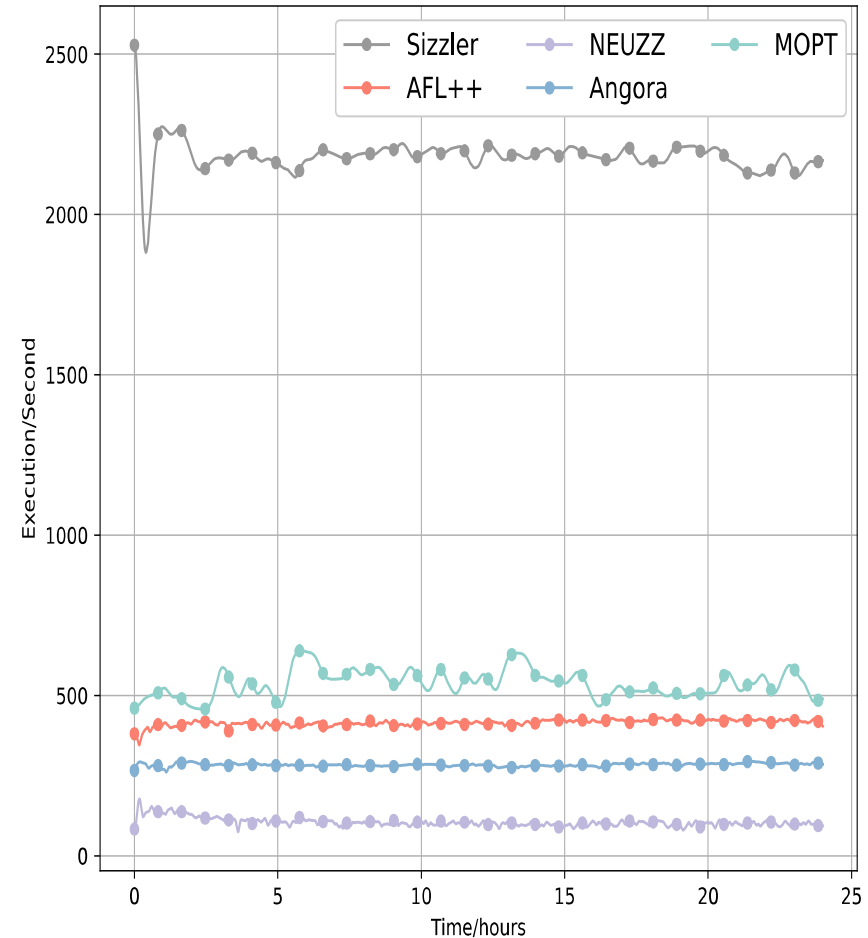


Sizzler: Some findings



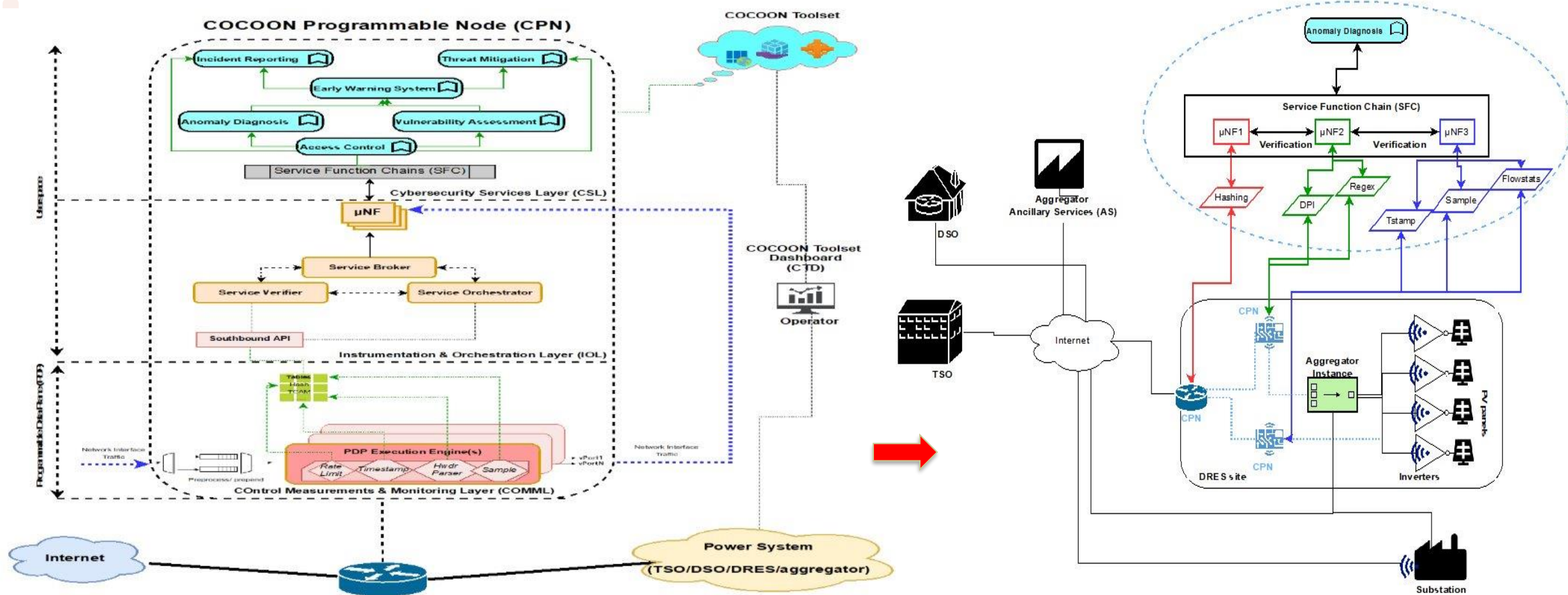
MCU	Program	Vulnerability	Crash	Time(min)	Coverage(%)		
					Function	Basic-block	Edge
PIC1616F628	test-i2c	RC	Y	64	93.8	78.1	69.5
	test-water	UT	Y	49	85.7	77.3	66.7
	test-electric	IL	Y	61	76.3	66.4	51.1
	test-i2c-lcd	MJL	Y	57	88.7	77.4	71.6
	test-leds	IL+UO+MJL	N	41	72.5	60.0	44.1
	test-pwm	UT+CH+ORR	Y	60	94.1	81.4	77.1
PIC1616F88	test-spi	ORR	Y	55	91.6	77.4	64.8
	test-uart	UO	Y	49	93.7	71.1	58.5
	test-timer	RC+UT	Y	43	91.6	67.7	51.7
	test-var-timer	UO+CH	Y	31	91.9	61.1	33.7
	test-coil	RC+IL	Y	52	87.5	78.8	67.4
	test-masterrelay	RC+UO	Y	67	94.5	81.4	71.9
AVR ATmega 2560	test-switch	MJL	Y	50	96.3	88.9	84.4
	seg-display	CH	Y	53	97.1	88.4	76.5
	asm-demo	IL+UT	Y	41	89.8	73.4	51.1
	test-blink	UO+ORR	Y	50	89.6	64.7	40.1
	test-lift	RC+HJ	Y	67	97.6	88.7	80.7
	test-alarm	UO+IL	Y	66	93.7	81.6	74.4
AVR ATmega 128	test-traffic	HJ	Y	63	91.8	81.1	76.0
	test-train	RC+IL+HJ	Y	63	99.6	89.6	84.6
	test-polution	UT+IL+ORR	Y	61	99.7	81.1	75.9
	test-counter	RC+MJL+UO	Y	31	97.4	76.7	61.2
	test-pressure	UT+IL+HJ	Y	44	82.4	71.1	61.7
	test-control	CH+RC+HJ	Y	49	88.1	63.5	59.4
ARM STM32F40X	test-clamb	IL	Y	57	87.1	71.4	66.6
	test-intustion	RC+ORR	Y	51	94.6	89.7	78.5
	test-modbus1	UT+CH	Y	61	81.6	74.4	71.7
	test-modbus2	RC+CH	Y	48	83.1	76.5	64.0
	test-tem	UT+CH+ORR	Y	55	88.0	80.0	74.3
	test-mov	RC+CH+HJ	Y	43	91.8	82.9	74.6

Vulnerability: Race condition competition (RC), Unconditional transfer (UT), Infinite loop (IL), Comparator hardcoded (CH), Missing jumps and links (MJL), Hidden jumpers (HJ), Object repeat reference(ORR), Unused objects (UO)



How can we orchestrate E2E defence?

- Applied architecture in power setups





Factsheet



- CIS are prone to complex cyber-attacks –
→ Advanced Persistent Threats (APTs)
- Attacks mutate, progress and evolve
- Defense mechanisms need to be adaptive and exploit available measurements from various components
 - Space for both fundamental and applied research (AI, Cryptography, network programmability. etc.)
- Need to go beyond vendor dependencies
- **Conclusively:** End-to-End (E2E) security in CIS → on-going "battle"

Related EU research projects

- **COCOON:** EU Horizon Europe (Innovation Action)

- UCY – Coordinator



- **ACTING:** European Defence Fund (EDF)



- **GuardAI:** EU Horizon Europe (Research Innovation Action)

- UCY – Coordinator



- Past related projects: EU H2020 Easy-RES



Some related publications

- K. Feng, M. M. Cook and A. K. Marnerides, "Sizzler: Sequential Fuzzing in Ladder Diagrams for Vulnerability Detection and Discovery in Programmable Logic Controllers," in *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 1660-1671, 2024
- H. A. Almazarqi, M. Woodyard and A. K. Marnerides, "Macroscopic Insights of IoT Botnet Dynamics Via AS-level Tolerance Assessment," *ICC 2024 - IEEE International Conference on Communications*, Denver, CO, USA, 2024
- M. M. Cook, A. K. Marnerides and D. Pezaros, "PLCPrint: Fingerprinting Memory Attacks in Programmable Logic Controllers," in *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 3376-3387, 2023
- H. A. Almazarqi, M. Woodyard, T. Mursch, D. Pezaros and A. K. Marnerides, "Tracking IoT P2P Botnet Loaders in the Wild," *ICC 2023 - IEEE International Conference on Communications*, Rome, Italy, 2023
- H. A. Almazarqi, M. Woodyard, T. Mursch, D. Pezaros and A. K. Marnerides, "Macroscopic Analysis of IoT Botnets," *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil, 2022
- M. Cook, C. Paterson, A. K. Marnerides and D. Pezaros, "Anomaly Diagnosis in Cyber-Physical Systems," *ICC 2022 - IEEE International Conference on Communications*, Seoul, Korea, Republic of, 2022



I will leave you with the following:

“Anyone who thinks that security products alone offer true security is settling for the illusion of security.”

— Kevin D. Mitnick, The Art of Deception: Controlling the Human Element of Security



University of Cyprus
Department of Electrical
and Computer
Engineering



KIOS
Research and Innovation Center of Excellence