Analyzing the Cyber-Resilience of Autonomic Software-defined OT Networks in Offshore Wind Power Plants.

PRESENTED BY:
Agrippina Mwangi, PhD Candidate

SUPERVISORS:
Prof.dr.Madeleine Gibescu, Main Supervisor (Utrecht University)
Ass.Prof. Elena.M.Fumagalli, Co-Supervisor (Utrecht University)
Dr. Mikkel Peter Sidoroff Gryning, Industrial Supervisor (Ørsted)

Partner Contributors:
Dr.Alfan Presekal, Ass. Prof. Alex Ştefanov
(IEPG TU Delft, The Netherlands)

Cyber-security Quagmire in Offshore Wind Power Plants

ENERCON
ENERGIE FÜR DIE WELT

Germany onshore WPP (February 2022)

5800 wind turbines affected
40000 VIASAT SATCOM compromised
~ Fully recovered in April 2022

S·POWER
An AES and AIMCo Company

March 2019 (Utah, USA)

Denial of Service Attack
vulnerable Cisco firewall
~12hr system unavailability

Deutsche Windtechnik

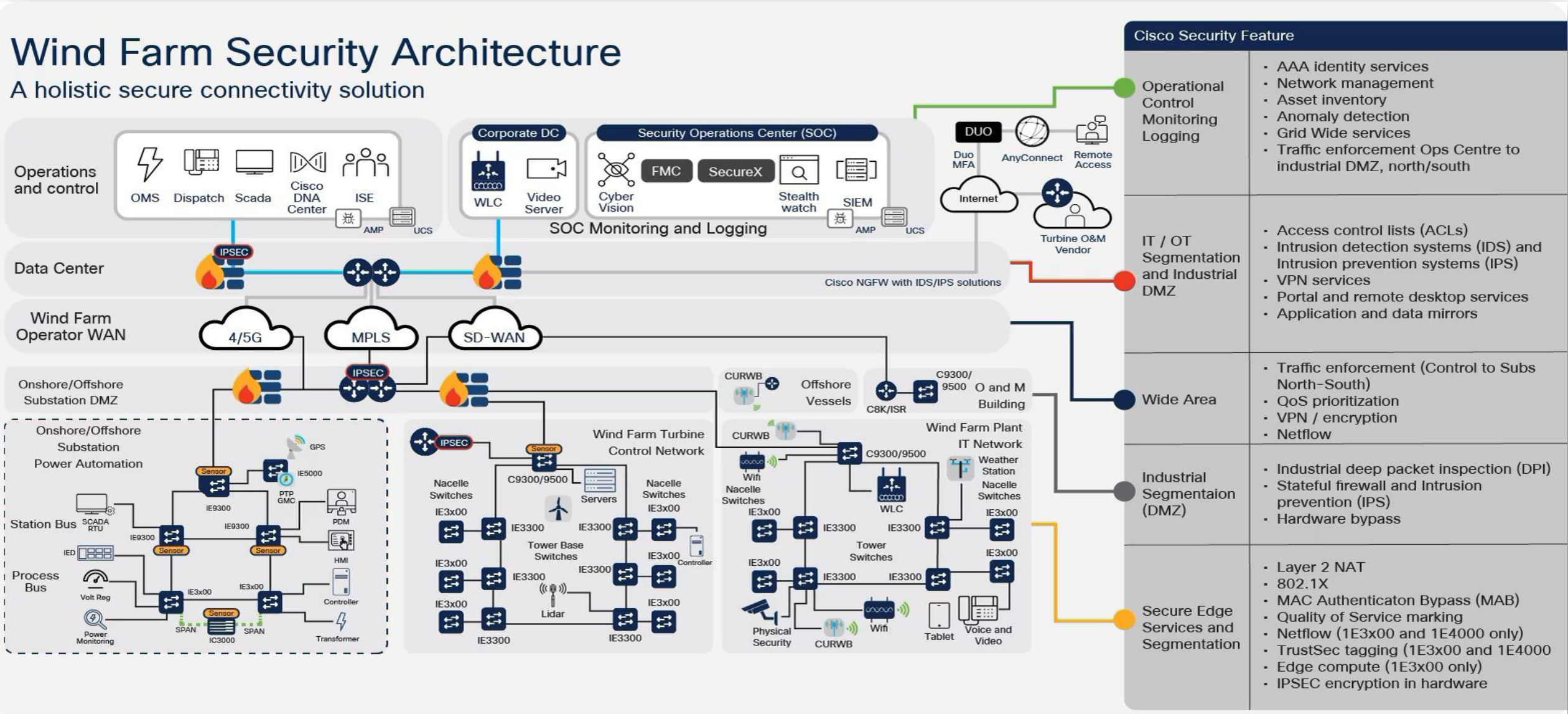
Germany onshore WPP (April 2022)

Attack on the IT systems managing monitoring and control of WTGs
~ 2 days time to recover (minor restrictions)

Utrecht University

Wind Farm Security Architecture

A holistic secure connectivity solution



Cisco Security Feature	
Operational Control Monitoring Logging	• AAA identity services • Network management • Asset inventory • Anomaly detection • Grid Wide services • Traffic enforcement Ops Centre to industrial DMZ, north/south
IT / OT Segmentation and Industrial DMZ	• Access control lists (ACLs) • Intrusion detection systems (IDS) and Intrusion prevention systems (IPS) • VPN services • Portal and remote desktop services • Application and data mirrors
Wide Area	• Traffic enforcement (Control to Subs North-South) • QoS prioritization • VPN / encryption • Netflow
Industrial Segmentaion (DMZ)	• Industrial deep packet inspection (DPI) • Stateful firewall and Intrusion prevention (IPS) • Hardware bypass
Secure Edge Services and Segmentation	• Layer 2 NAT • 802.1X • MAC Authenticaton Bypass (MAB) • Quality of Service marking • Netflow (1E3x00 and 1E4000 only) • TrustSec tagging (1E3x00 and 1E4000 • Edge compute (1E3x00 only) • IPSEC encryption in hardware

1) **Cisco Systems, Inc.**, "Renewable Generation: Operational Grid Solutions," Cisco, Sep. 8, 2022. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/design-zone/renewable-gen-og.html#UseCases.

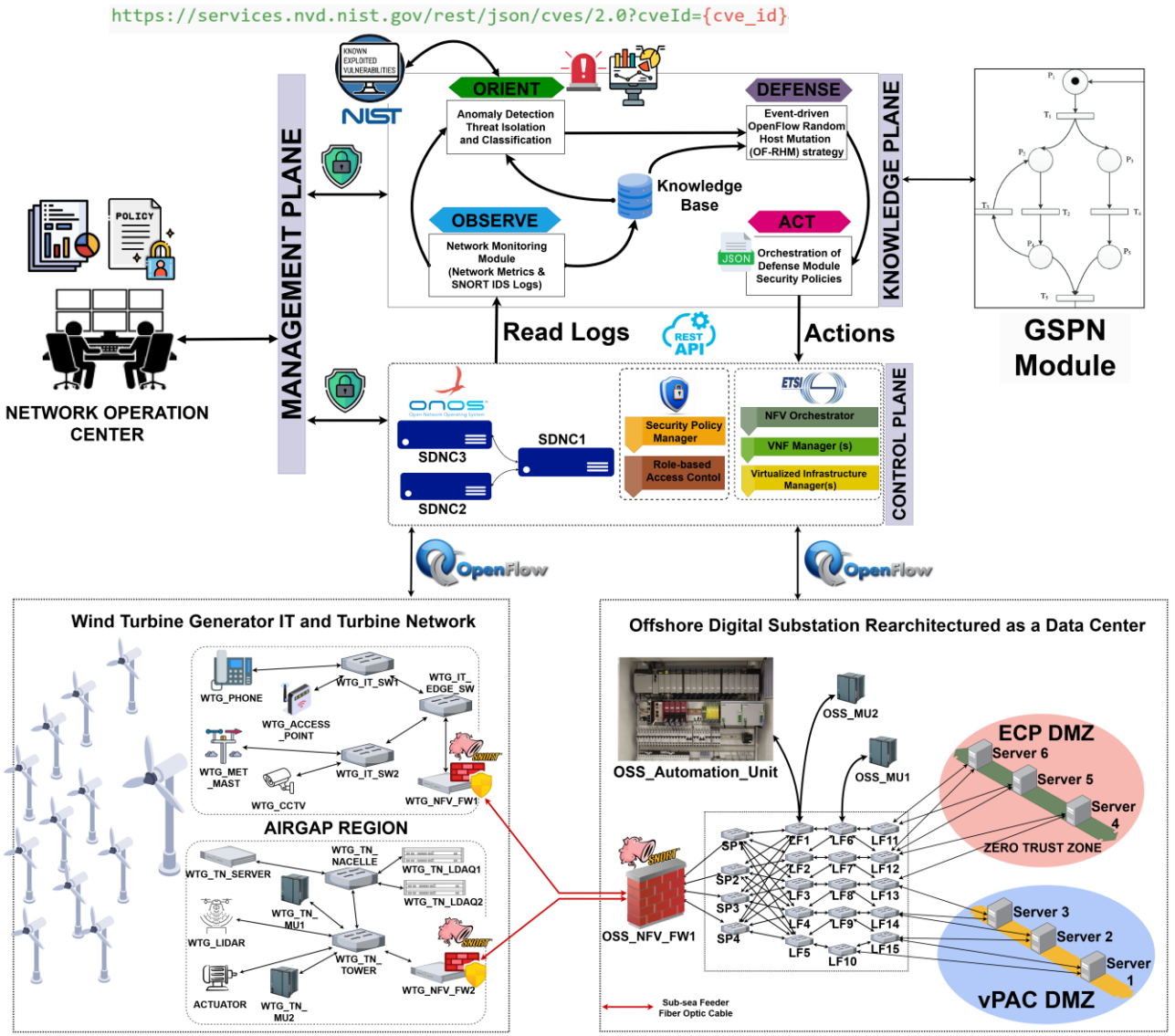
"The key notion of cyber resilience is
acceptance of cyber compromise as a likely event,
and the system suffering as a result;
the focus is on the system's ability to recover and adapt,
not just resist."

Alexander Kott & Igor Linkov (2021)
US Combat Capabilities Development Command's Army Research Laboratory

Utrecht University

1. *Kott, A. and Linkov, I., 2021. To Improve Cyber Resilience, Measure It. IEEE Computer, 54(2), Feb.2021, pp.80-85.*
2. *Kott, A. and Theron, P., 2020. Doers, Not Watchers: Intelligent Autonomous Agents Are a Path to Cyber Resilience. IEEE Security & Privacy, 18(3), pp.62-66.*
3. *I. Kamara, "European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience," Innovation: The European Journal of Social Science Research, pp. 1–20, 2024.*

Securing software-defined OT Networks in offshore wind power plants



Internet Research Task Force (IRTF)
Request for Comments: 7575
Category: Informational
ISSN: 2070-1721

M. Behringer
M. Pritikin
S. Bjarnason
A. Clemm
Cisco Systems
B. Carpenter
Univ. of Auckland
S. Jiang
Huawei Technologies Co., Ltd
L. Ciavaglia
Alcatel Lucent
June 2015

Autonomic Networking: Definitions and Design Goals

Abstract

Autonomic systems were first described in 2001. The fundamental goal is self-management, including self-configuration, self-optimization, self-healing, and self-protection. This is achieved by an autonomic function having minimal dependencies on human administrators or centralized management systems. It usually implies distribution across network elements.

Founded on Zero-touch network and Service Management (ZSM) and Experiential Networked Intelligence (ENI) initiatives.

Utrecht University

Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012). "OpenFlow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking." Proceedings of the First Workshop on Hot Topics in Software Defined Networks (HotSDN '12).

TABLE I
OFFSHORE WPP SPECIFIC VULNERABILITIES AND ATTACKS MAPPED TO CVE IDS [19] AND MITRE ATT&CK REFERENCES [20]

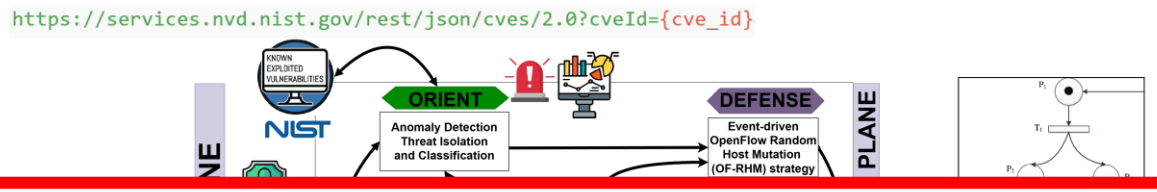
Category	Attack	CVE ID	MITRE ATT&CK	REFERENCE CODE
SCADA & ICS	Modbus TCP Write Single Register Attack	✓	✓	CVE-2019-10988, T0860
	DNP3 Malformed Packet	✓	✓	CVE-2015-7916, T0856
	IEC 60870-5-104 Exploit	✓	✓	CVE-2022-29544, T0859
	Modbus Read Device ID Spoof	✗	✓	–, T0859
IoT Exploits	IoT Botnet Infection	✓	✓	CVE-2016-10401, T0747
	MQTT Unauthorized Access	✓	✓	CVE-2017-7653, T0852
	CoAP Unauthorized Access	✓	✓	CVE-2019-15889, T0853
DoS/DDoS	UDP Chargen (RFC864) DoS Attack	✓	✓	CVE-1999-0103, T1498
	HTTP Slowloris (RFC793, RFC7230) DoS Attack	✓	✓	CVE-2007-6750, T1499
Unauthorized Access	FTP/SSH Brute-Force	✗	✓	–, T1110
	SNMP Unauthorized Access	✓	✓	CVE-2017-6736, T1021
	ICMP Redirect Attack	✗	✓	–, T1595
Network Scanning	Nmap XMAS/FIN/UDP Scan	✗	✓	–, T1046
Malware & Exploits	Malware Download	✓	✓	CVE-2016-0034, T1203
	SMB EternalBlue	✓	✓	CVE-2017-0144, T1210
	RDP BlueKeep	✓	✓	CVE-2019-0708, T1210
Credential Dumping	LDAP Credential Dumping	✗	✓	–, T1003
	SSL Strip Attack	✓	✓	CVE-2009-3555, T1557
DNS-based Attacks	DNS Exfiltration	✗	✓	–, T1071
	DNS Tunneling	✓	✓	CVE-2019-6487, T1572

```
mysql> select * from threat_severity;
+----+---------------------+--------------+--------------+----------+----------------+----------------+
| id | timestamp           | source_ip    | cve_id       | mitre_id | severity_level | severity_label |
+----+---------------------+--------------+--------------+----------+----------------+----------------+
|  1 | 2025-03-28 10:22:14 | 192.168.1.101 | CVE-2019-6487 | T1572    |              4 | Critical       |
+----+---------------------+--------------+--------------+----------+----------------+----------------+
```

Points to the vulnerabilities and is suited for threat severity classification (Z) in the DEFENSE Module.

Threat modelling, Incident classification, and attack behavior detection in the multi-log ingestion at the ORIENT Module.

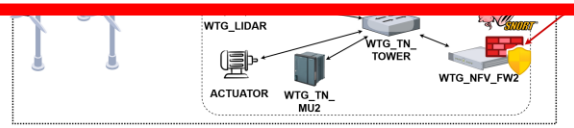
Securing software-defined OT Networks in offshore wind power plants

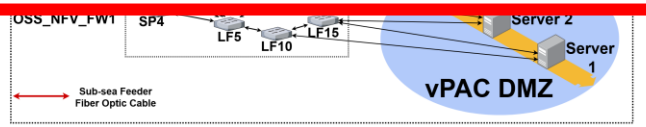


Proposed Approach:
Autonomic, event-driven OpenFlow Random Host Mutation (OF-RHM) Framework

OpenFlow Random Host Mutation (OF-RHM) is a key Moving Target Defense technique designed for use with OpenFlow-based software defined networks

"Moving Target Defense (MTD) is a cyber-resilience strategy introduces dynamism into the protected systems and networks, thereby increasing the uncertainty and complexity for attackers while maintaining usability for legitimate users."
Jafarian et al., 2012



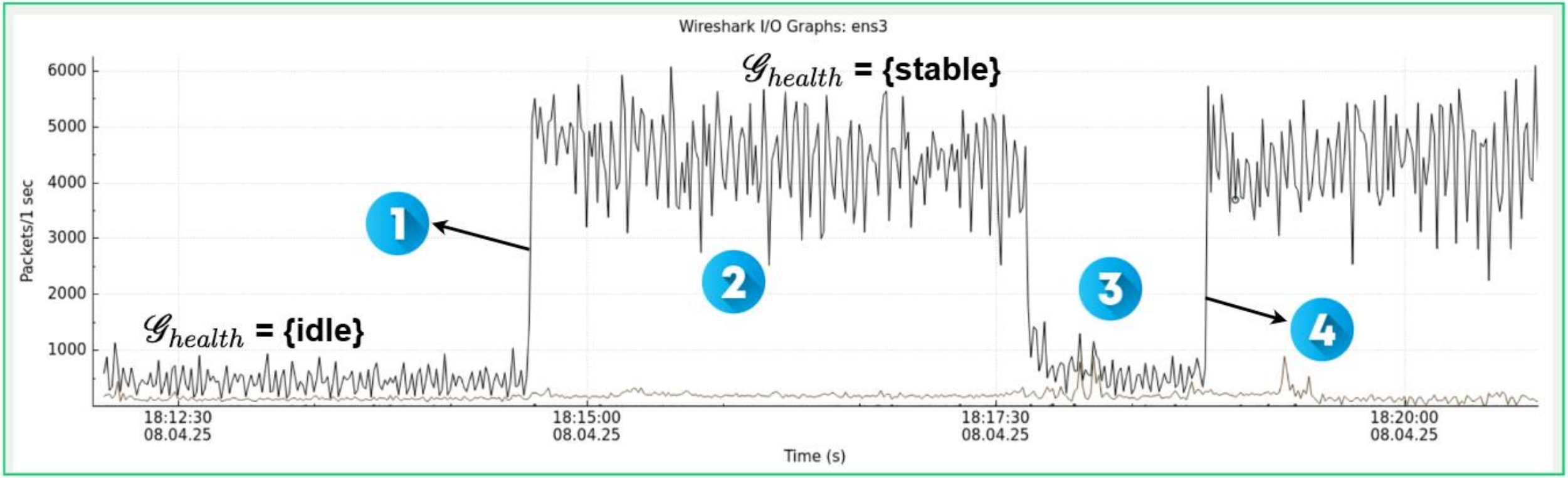


Utrecht University

Jafarian, J. H., Al-Shaer, E., & Duan, Q. (2012). "OpenFlow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking." Proceedings of the First Workshop on Hot Topics in Software Defined Networks (HotSDN '12).

Cyber Resilience? How do we measure it?

1. Network behavior and performance indicators of Cyber-Resilience



Wireshark capture of network throughput (packets/sec) under both reconnaissance and late-stage (DDoS) attacks for 10 minutes.

Cyber Resilience? How do we measure it?

2. *Quantitative Assessment using Generalised Stochastic PetriNets (GSPN)*

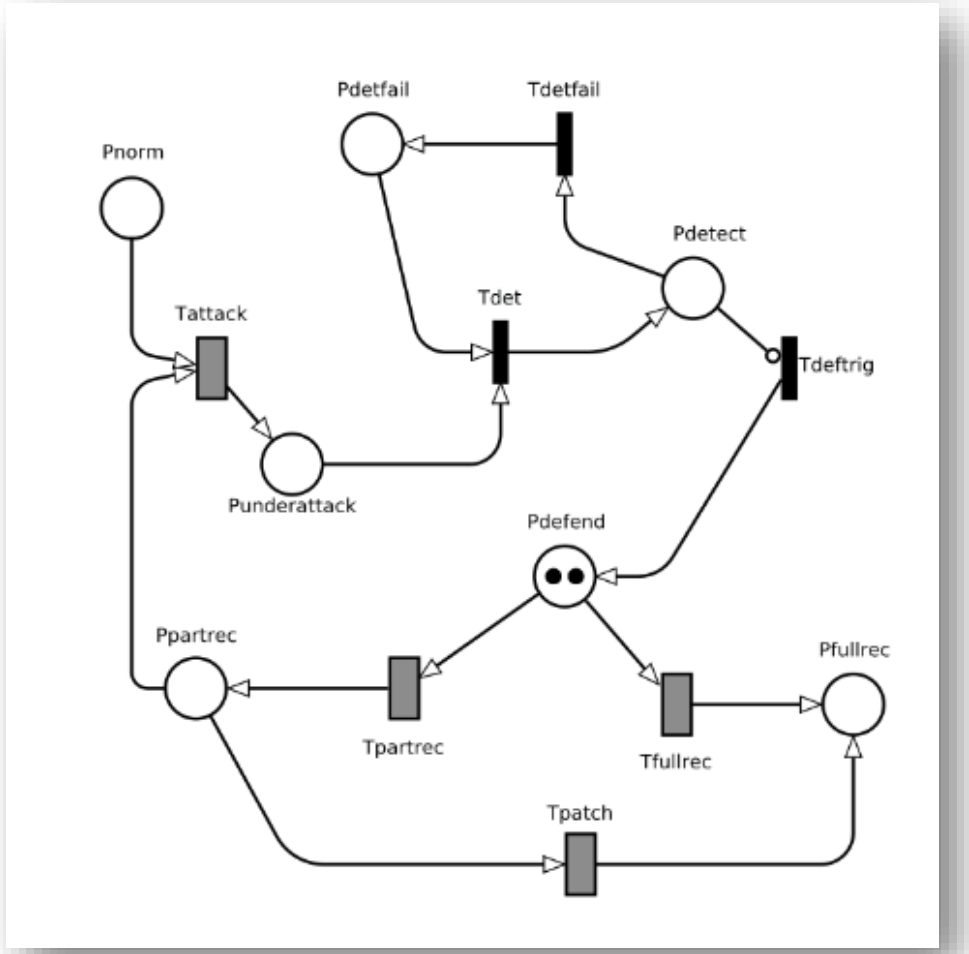


TABLE III
GSPN SCENARIOS FOR SIMULATING ATTACK-DEFENSE DYNAMICS

Scenario	λ_{attack}	$\mu_{compromise}$	δ_{detect}	$\rho_{recover}$
Passive Reconnaissance	0.01	0.001	0.85	0.3
Loud Scan (Stealthy Scan)	0.30	0.010	0.65	0.25
Slow Advanced Persistent Threats	0.02	0.010	0.25	0.1
Ransomware	0.70	0.500	0.35	0.05
Insider Leak	0.15	0.080	0.15	0.4
DoS Burst	0.90	0.050	0.60	0.15

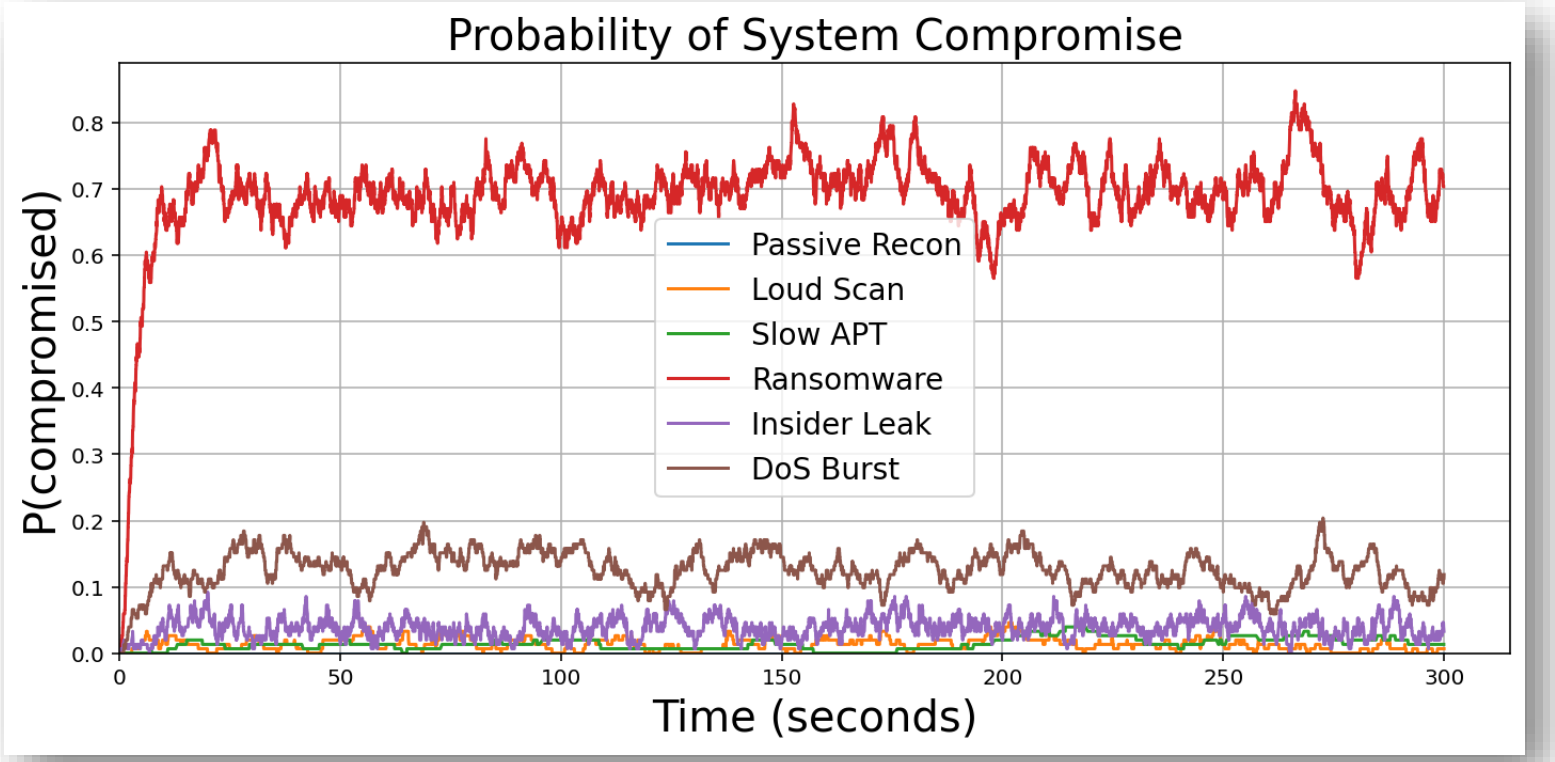
Cyber Resilience? How do we measure it?

2. *Quantitative Assessment using Generalised Stochastic PetriNets (GSPN)*

1) Probability of System Compromise: At time t, the proportion of markings in vulnerable or compromised states is given such that,

$$\mathbb{P}_{\text{comp}}(t) = \frac{\sum_{p \in \mathcal{P}_{\text{comp}}} \mathcal{M}_p(t)}{\sum_{p \in \mathcal{P}} \mathcal{M}_p(t)} \tag{11}$$

where $\mathcal{P}_{\text{comp}} \subseteq \mathcal{P}$ is the subset of places representing compromised states and $\mathcal{M}_p(t)$ is the number of tokens in place p at time t.

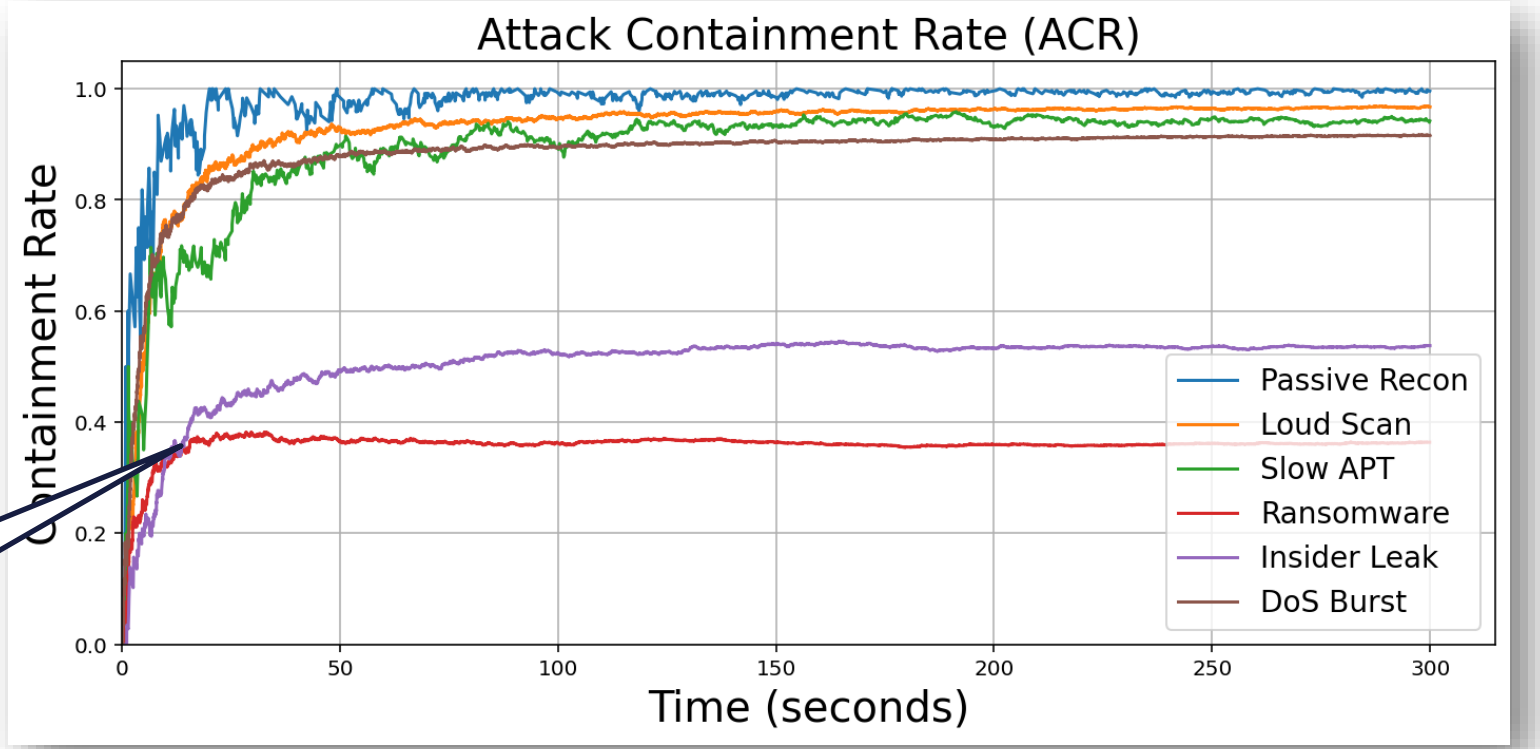


Cyber Resilience? How do we measure it?

2. *Quantitative Assessment using Generalized Stochastic PetriNets (GSPN)*

The attack containment rate ($ACR(\%)$) was computed as the ratio of the number of attacks detected and mitigated ($\mathcal{A}_{\text{mitigated}}$) to the total number of attacks launched ($\mathcal{A}_{\text{total}}$), as expressed in eqn. 9:

$$ACR(\%) = \frac{|\mathcal{A}_{\text{mitigated}}|}{|\mathcal{A}_{\text{total}}|} \times 100 \qquad (9)$$



Supplement with internal standard procedures

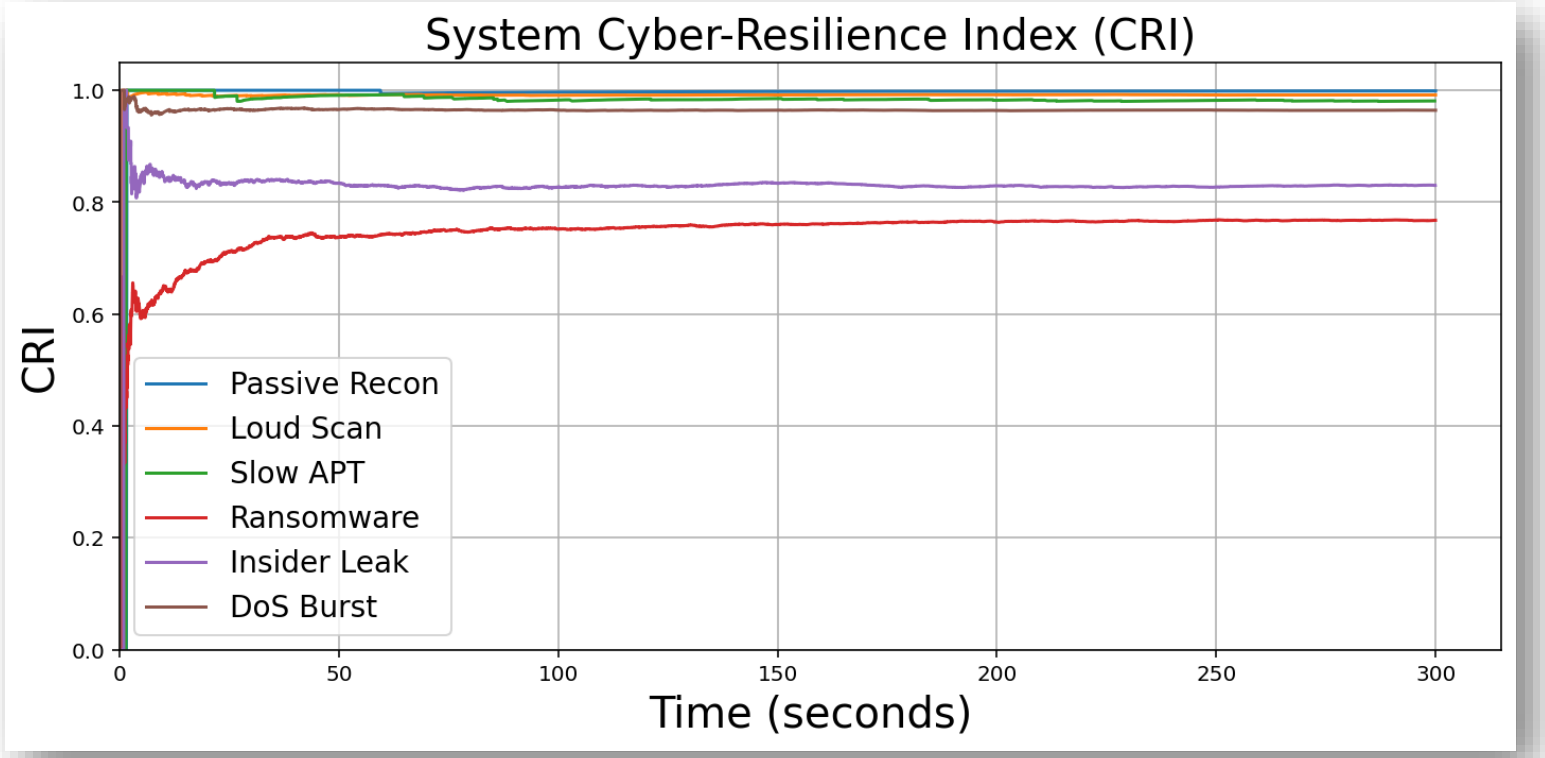
Cyber Resilience? How do we measure it?

2. *Quantitative Assessment using Generalized Stochastic PetriNets (GSPN)*

The cyber-resilience index (CRI) was computed as ratio such that

$$CRI(t) = \frac{RecoveryRate(t)}{DisruptionImpact(t) + \epsilon} \tag{12}$$

where the $RecoveryRate(t)$ is the number of tokens that return to place, $\mathcal{P}_{norm}$, and the $DisruptionImpact(t)$ is the total weighted transitions to degraded or failed states.



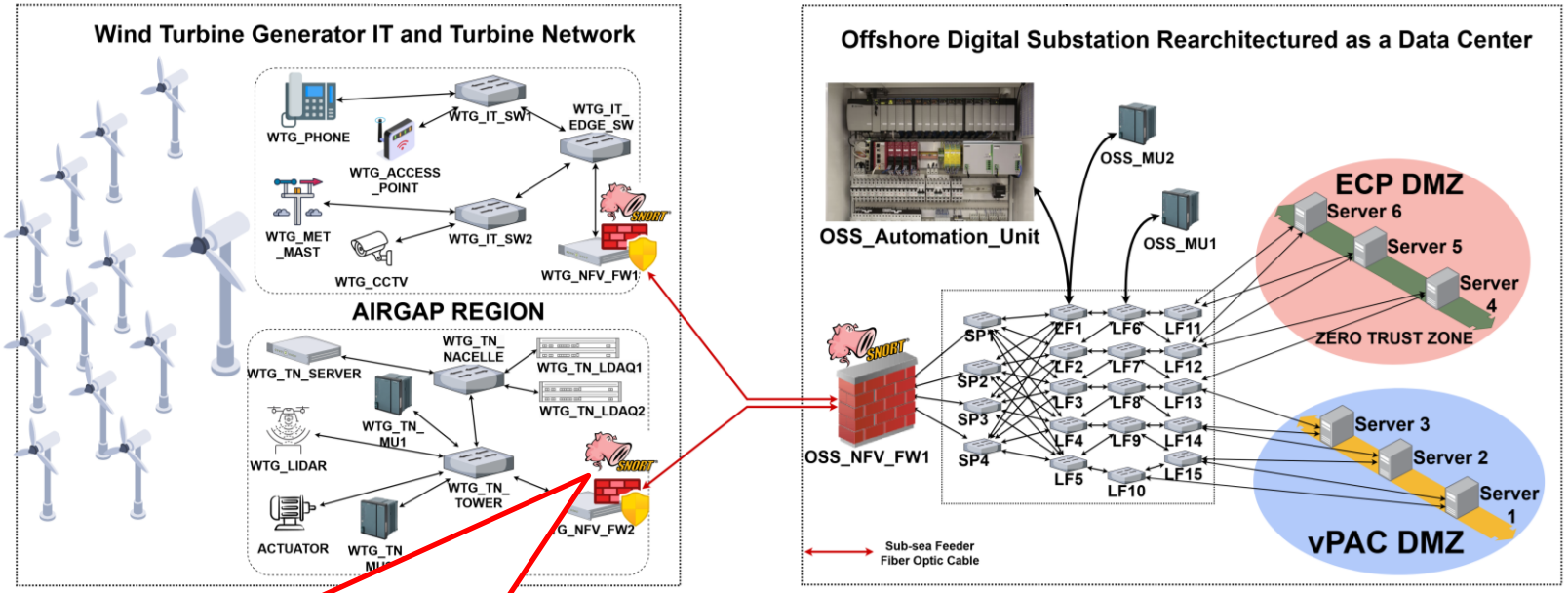
Insights from Testbed Transient Studies

False positive Rate or a case of over-defending?

The $FPR(\%)$ was computed as:

$$FPR(\%) = \frac{False\ Positives}{Total\ Alerts} \times 100$$

Average of 5.67% while the preferred is 1-2%



1. *Make IDS/IPS nodes more context-aware*
2. *Use traffic anomaly detection in the ORIENT Module*

Utrecht University

Utrecht University

Q&A

This presentation contains material that forms part of the research objectives of an ongoing doctoral thesis entitled "Resilient Autonomic Software-Defined Industrial Networks for Offshore Wind Power Plants." The content presented herein is intended solely for academic dissemination and reflects work in progress as part of a PhD research program. Any opinions, findings, or conclusions expressed are those of the author and do not necessarily reflect the views of affiliated support industrial partners.

Agrippina Mwangi, PhD Candidate | CCNA

Energy and Resources Group
Copernicus Institute of Sustainable Development
Utrecht University, The Netherlands

Email: a.w.mwangi@uu.nl
Github: https://github.com/PinaPhD

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 956433.