Engineering Institute of Technology.

Watch Webinar Recording Here

Authentication for Remote Critical Infrastructure (IT/OT) Assets

8 November 2023 | Technical Topic Webinar

A/Prof. Zubair Baig, EIT Lecturer

About EIT

We are dedicated to ensuring that you receive a world-class education and gain skills that you can immediately implement in the workforce.

World-Class Australia Accredited Education

Our vocational programs and higher education degrees are registered and accredited by the Australian Government. We have programs that are also recognized under three international engineering accords.

Engineering Specialists

EIT is one of the only institutes in the world specializing in Engineering. We deliver professional certificates, diplomas, advanced diplomas, undergraduate and graduate certificates, bachelor's and master's degrees, and a Doctorate of Engineering.

Industry Experienced Lecturers

Our lecturers are highly experienced engineers and subject specialists with applied knowledge. The technologies employed by EIT, both online and on-campus, enable us to source our lecturers from a large, global pool of expertise.

Industry Oriented Programs

Our programs are designed by industry experts, ensuring you graduate with cutting-edge skills that are valued by employers. Our program content remains current with rapidly changing technology and industry developments.

Unique Delivery Model

We deliver our programs via a unique delivery methodology that makes use of live and interactive webinars, an international pool of expert lecturers, dedicated learning support officers, and state-of-the-art such as hands-on workshops, remote laboratories, and simulation software.

Introduction - Presenter

A/Prof. Zubair Baig

- Zubair Baig is an Associate Professor in Cyber Security at Deakin University.
- He is the Head of Research Translation, Cyber Security at the Strategic Centre for Cyber Resilience and Trust.
- Zubair has authored over 105 journal papers, conference articles, book chapters, and 5 white papers.
- He holds 2 Cyber Security Technologies patents from the USPTO.
- Zubair has served on technical program committees for international conferences and delivered numerous keynotes on cyber security.
- His research interests include cyber security, artificial intelligence, critical infrastructures, and the Internet of Things.
- He possesses a diverse skillset for conducting risk assessments in areas such as IoT, critical infrastructures, and sensor networks.

IIoT or Industry 4.0

- Convergence of IoT, Cyber Physical Systems (CPSs), and cloud/edge computing for industrial operations
- A vast ecosystem of interconnected devices defines IIoT

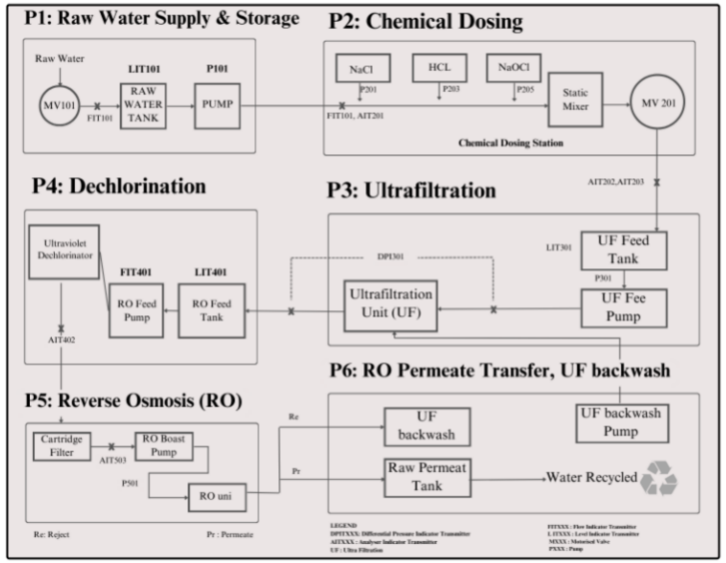
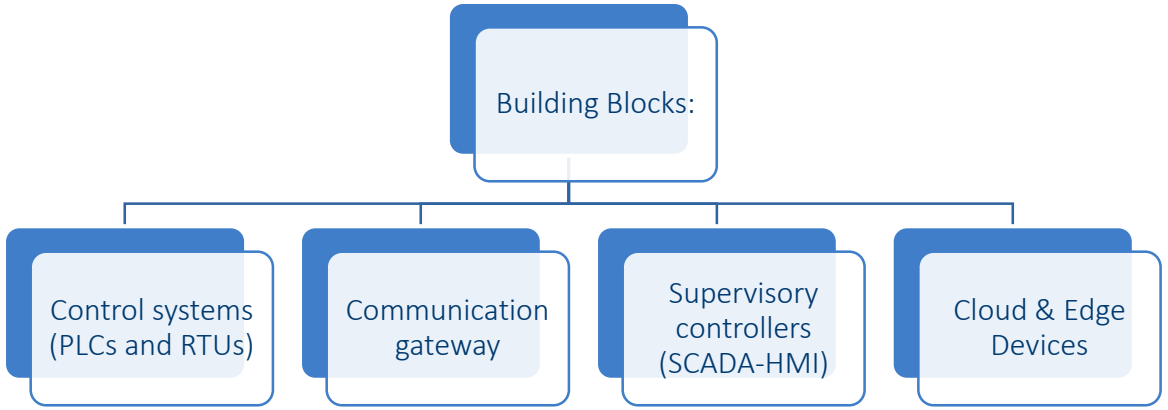


Fig. 1: Six stages of the water treatment plant



Security Challenges

Security challenges:

- Interconnected nature, complex structure, and connectivity

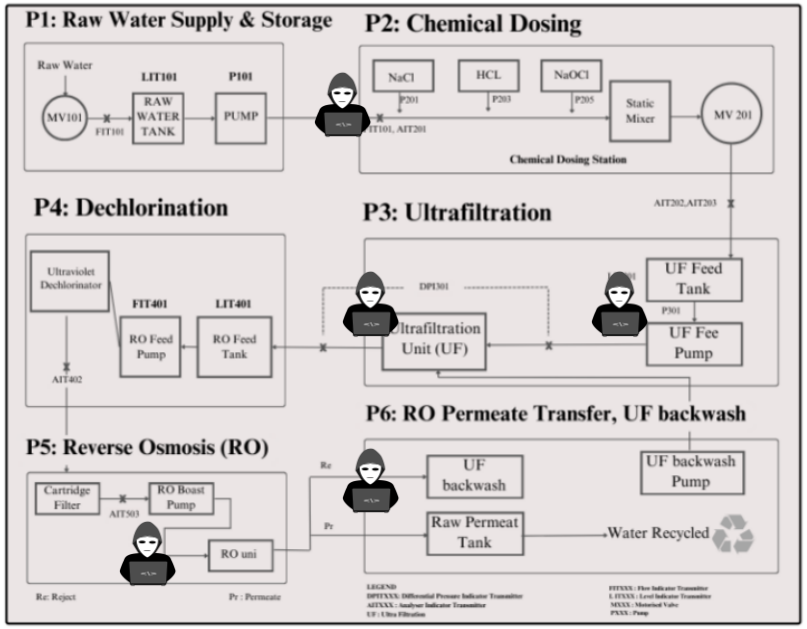


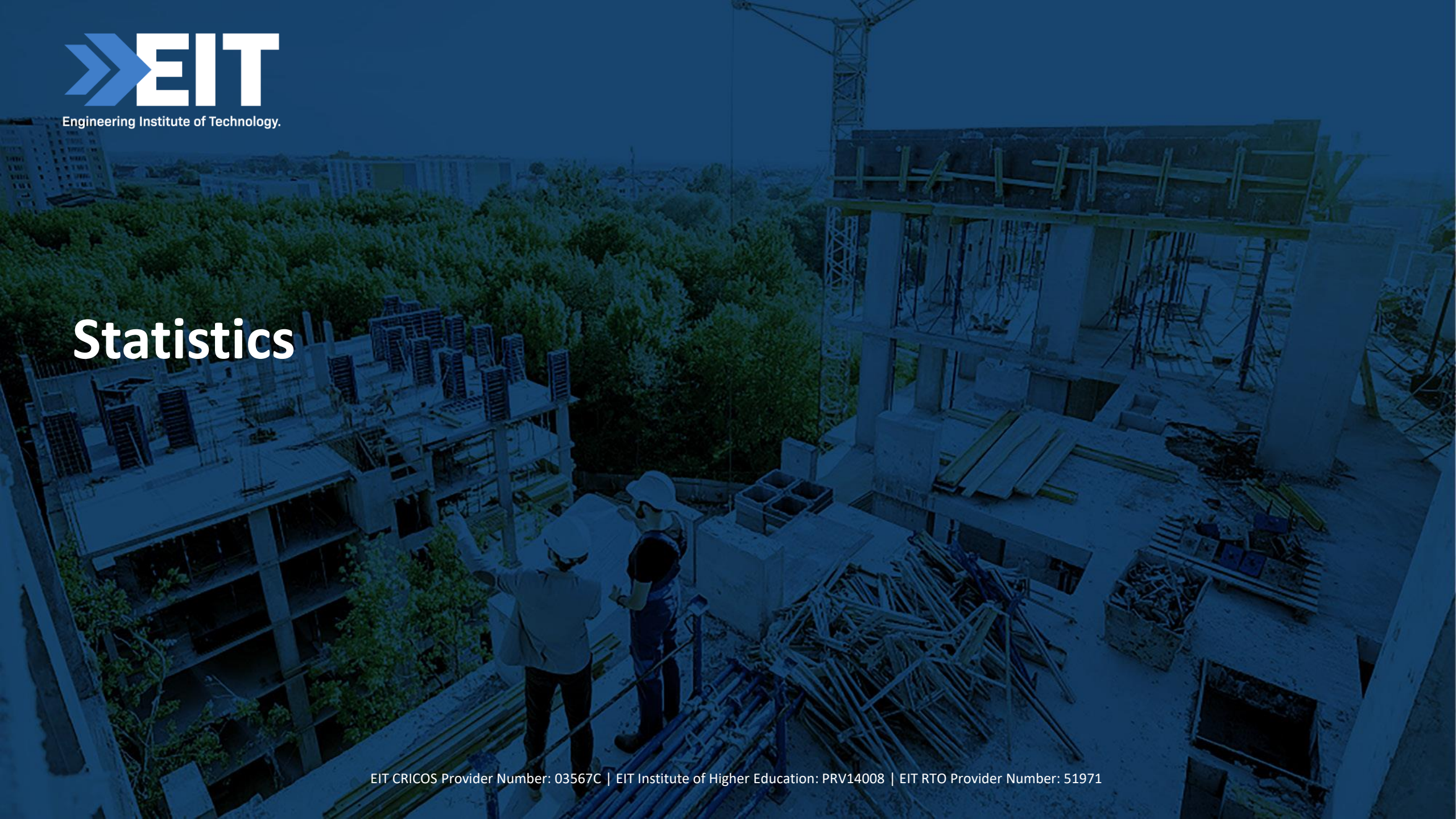
Fig. 1: Six stages of the water treatment plant

Influence of Human factors:

- Human factors play a pivotal role in vulnerability exposure

Engineering Institute of Technology.

Statistics



Industrial Control Systems in a CI

Analysis of a large number of security advisories (988 data points. Between **2013 to 2018**) by Gonzalez and team <> **Rochester Institute of Technology** :

-**Which ICS components are most vulnerable?**

- HMI, SCADA, PLC

What Percentages of ICS Vulnerabilities had an architectural Root Cause?

- 62.82 % (This is due to the products were designed without security in mind)

What are the most common architectural Weakness in ICS?

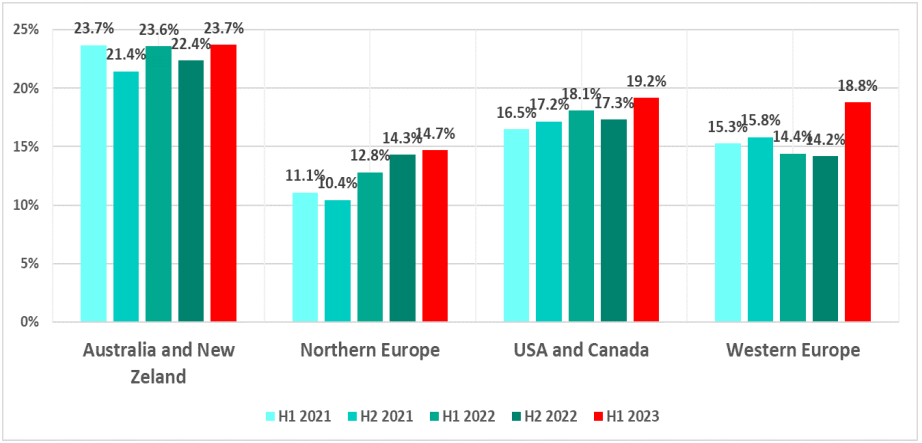
- Improper Input Validation (26.29%), Weak Authentication and Access Control (24 %)

Which Architectural Tactic Implementations are most often compromised in ICS ?

- Input validation, authentication, authorization

- Denylisting is #1
- Malware and phishing pages are #2

- Traditionally safer regions noticed spikes in attacks!
- Australia, NZ, US and Canada, Western & Northern Europe
- Africa remains highest at 40.3 %
- Building Automation Systems – Prime target – 38%
- Energy – increase of 36%



https://www.kaspersky.com/about/press-releases/2023_attacks-on-industrial-sector-hit-record-in-second-quarter-of-2023

Threats and Vulnerabilities

Cyber Threats & IIoT

IIoT in Mining

Cyber espionage

Phishing Attack

Third-Party Access

IIoT in Manufacturing

Malware

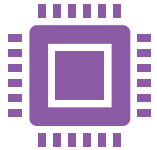
Ransomware

DDoS

Spear phishing

Device hacking

Vulnerabilities in legacy systems



IIoT in Electricity/Grid

DDoS

Ransomware

Malware injection

Man-in-the-Middle (MITM)

Phishing

Advanced persistent threat (APT)

IIoT in Healthcare

Botnets

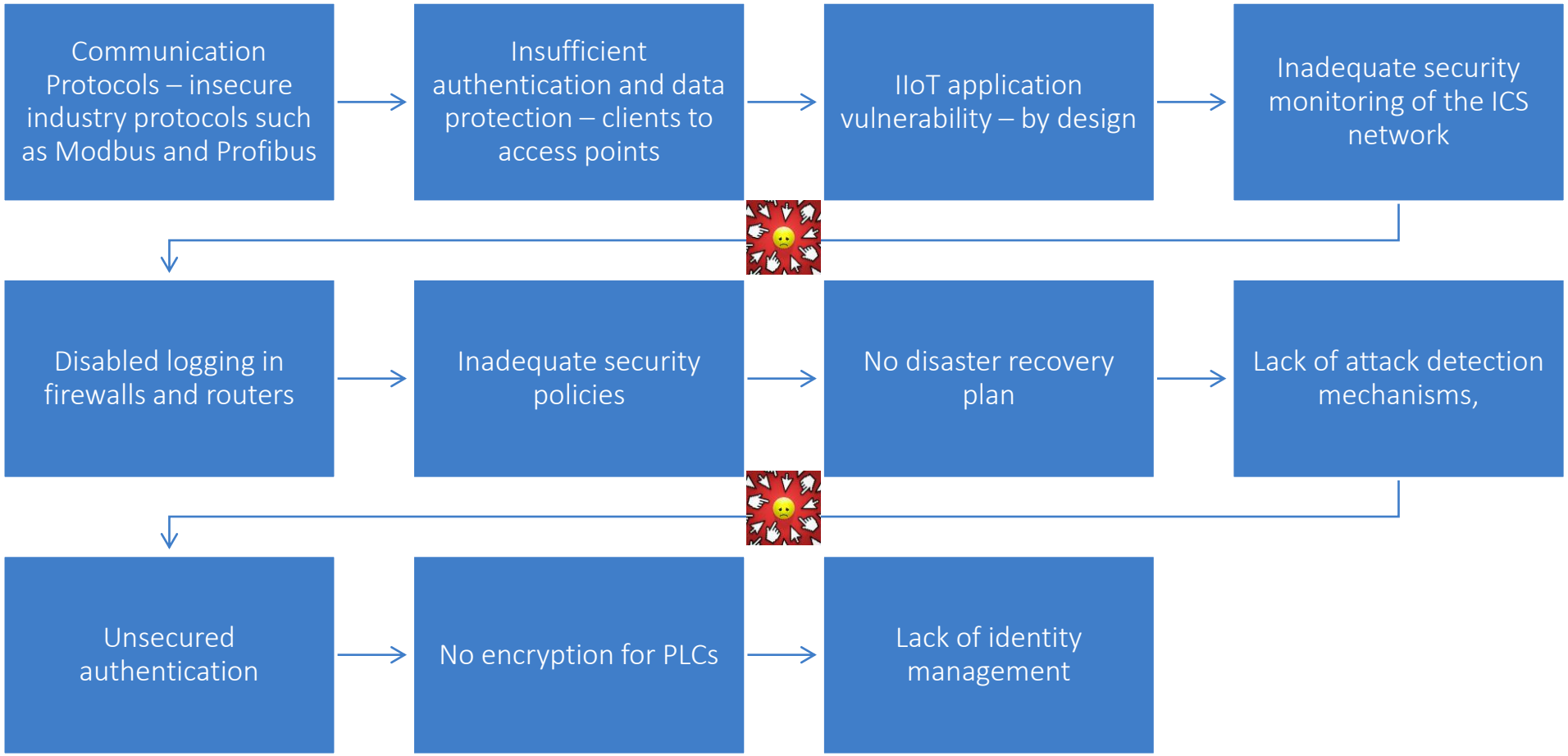
DoS/DDoS

Ransomware

Advanced persistent threats (ATP)

Medjacking

Common Vulnerabilities



Top 20 Architectural Weaknesses (CAWEs) in ICS

Tactic	CWE	#Freq.
Validate Inputs	CWE-20 Improper Input Validation	142
Validate Inputs	CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	75
Authenticate Actors	CWE-287 Improper Authentication	70
Authorize Actors	CWE-284 Improper Access Control	63
Validate Inputs	CWE-352 Cross-Site Request Forgery (CSRF)	45
Authenticate Actors	CWE-798 Use of Hard-coded Credentials	44
Validate Inputs	CWE-89 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	37
Authenticate Actors	CWE-259 Use of Hard-coded Password	20
Encrypt Data	CWE-522 Insufficiently Protected Credentials	18
Validate Inputs	CWE-94 Improper Control of Generation of Code ('Code Injection')	17
Authenticate Actors	CWE-306 Missing Authentication for Critical Function	16
Authorize Actors	CWE-434 Unrestricted Upload of File with Dangerous Type	14
Authorize Actors	CWE-269 Improper Privilege Management	13
Encrypt Data	CWE-326 Inadequate Encryption Strength	13
Encrypt Data	CWE-312 Cleartext Storage of Sensitive Information	12
Validate Inputs	CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	12
Authorize Actors	CWE-285 Improper Authorization	11
Encrypt Data	CWE-319 Cleartext Transmission of Sensitive Information	10
Encrypt Data	CWE-311 Missing Encryption of Sensitive Data	10
Encrypt Data	CWE-256 Unprotected Storage of Credentials	10

10 Compromised Architectural Tactics

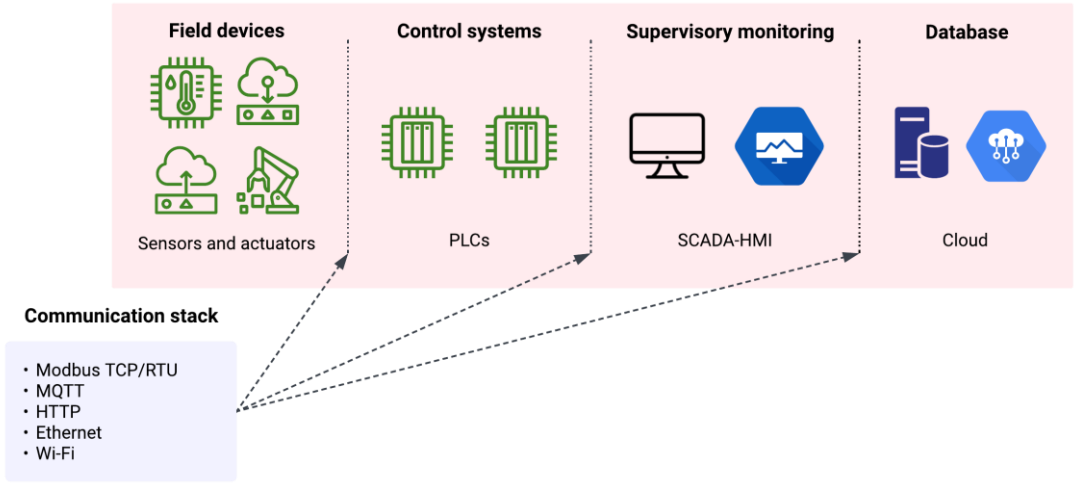
Tactic	# of Reports
Validate Inputs	351
Authenticate Actors	174
Authorize Actors	133
Encrypt Data	114
Limit Access	18
Identify Actors	13
Manage User Sessions	11
Cross Cutting	8
Verify Message Integrity	4
Audit	2

This triggers: Need for a "Strong Authentication Framework" for resilient CI.

Engineering Institute of Technology.

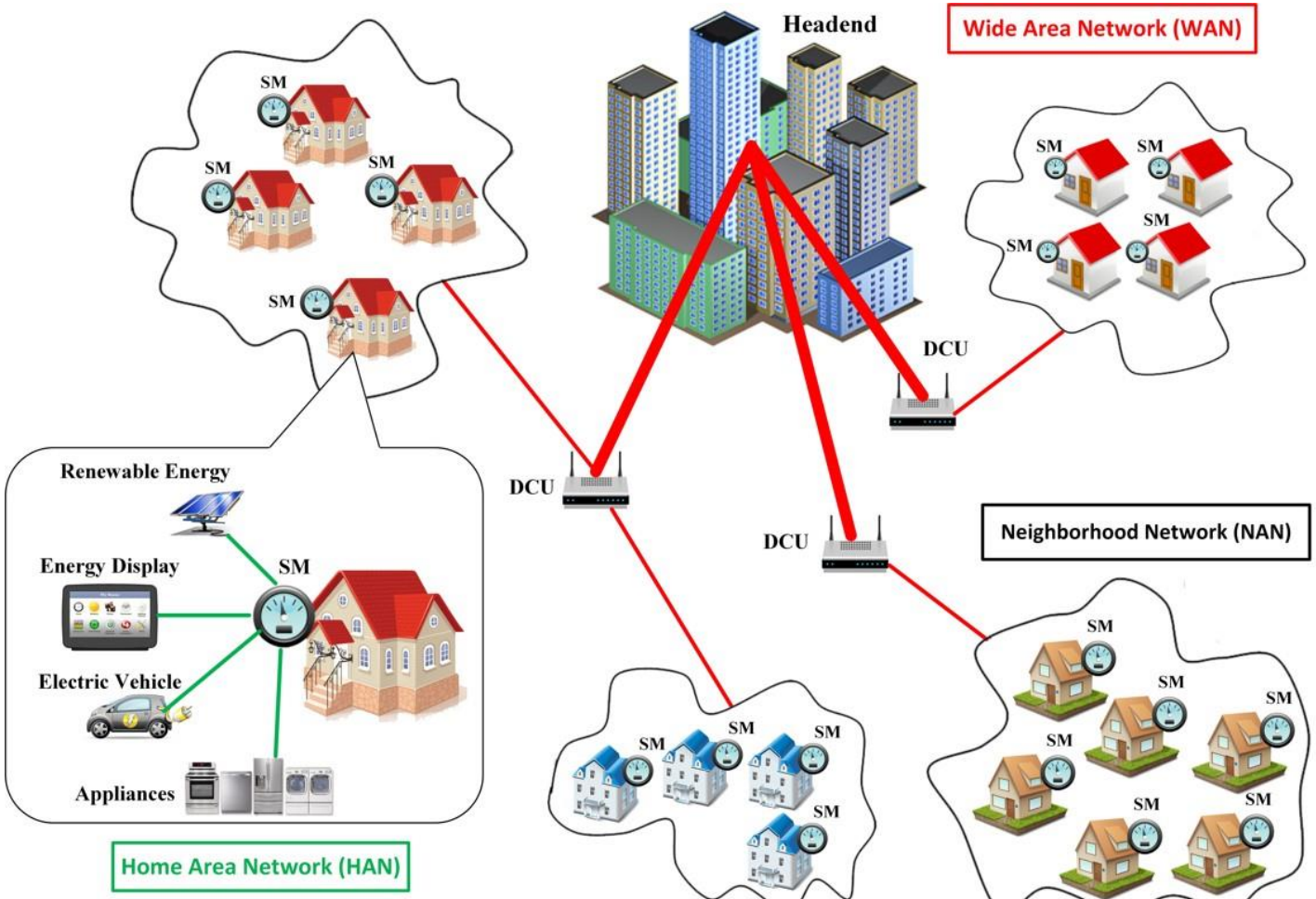
Architectures

IT/OT Architecture - Generic



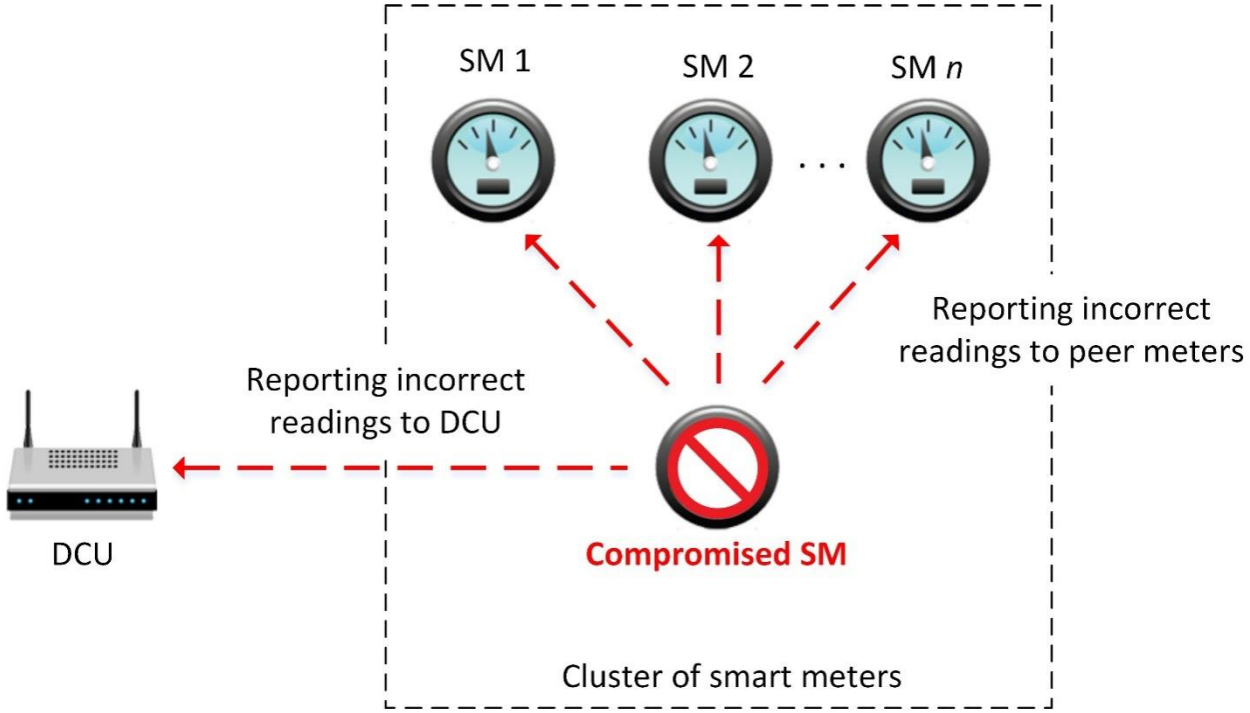
- Communication is achieved via Modbus TCP/RTU, MQTT, DNP3, CoAP, and Ethernet or Wi-Fi
- Customised security – distinct protocols
- Varied packet sizes
- Varied transmission rules and reliability standards
- Specific communication requirements that facilitate effective communication between devices

IT/OT Architecture – Smart Grid

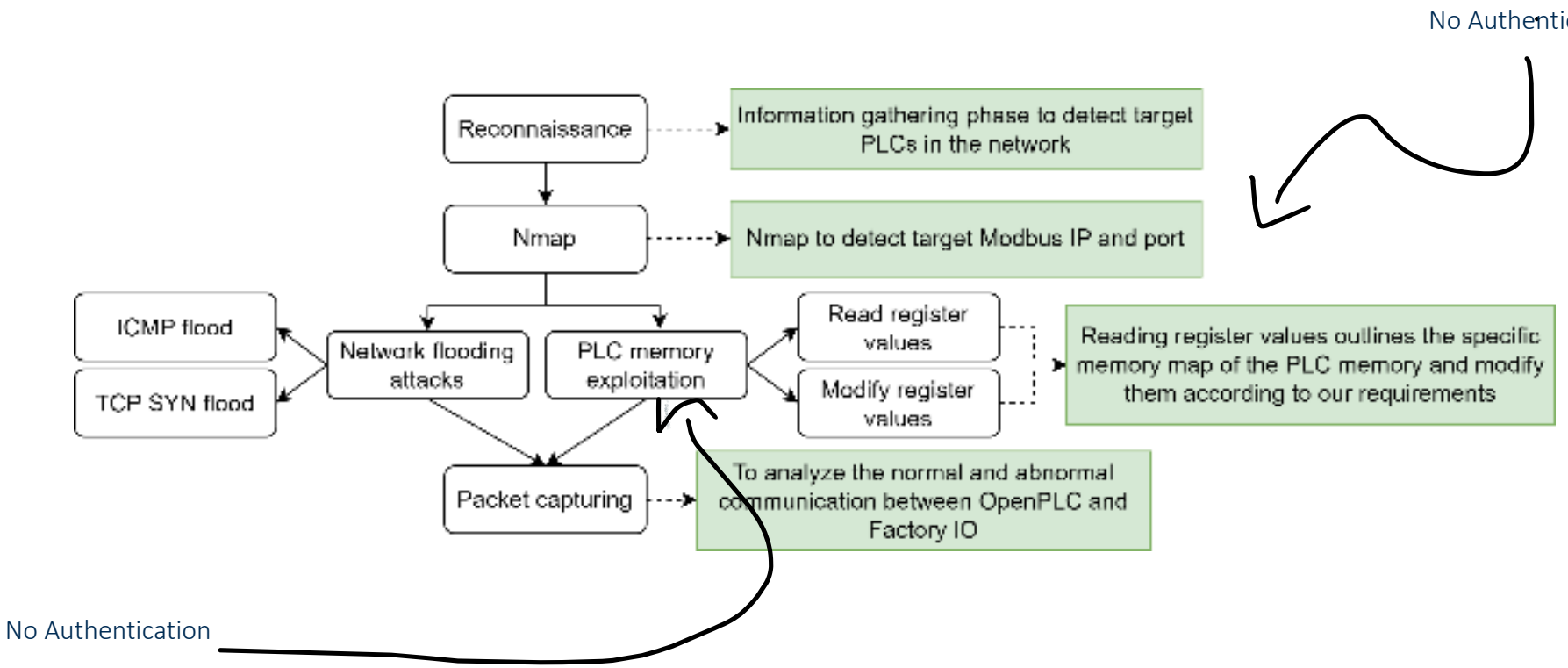


Attack Models & Mapping

Smart Meter Attack



Sample Attack Model



MITRE Mapping

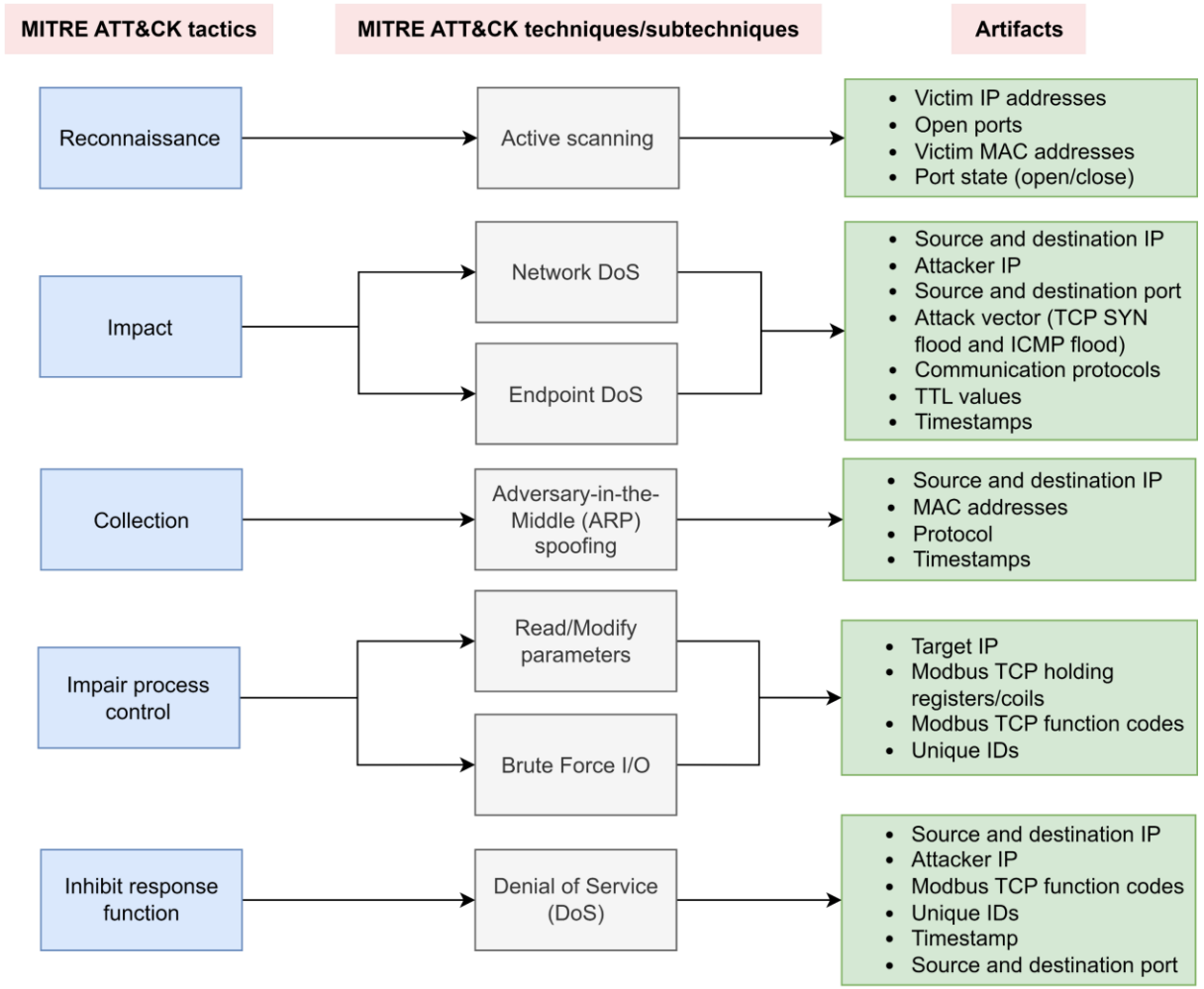


TABLE 2: Correlating key artifacts of Modbus TCP flood attack against the proposed data artifact template.

Artifact name	Attack vector	Data source	Artifact sample data	Purdue level	Artifact relevance
Field devices data (Modbus register and coil values)	Brute force I/O Read/modify parameters	Metasploit framework interface [12]	**Holding registers:** Before: [0, 0, 0, 0, 0] After: [99, 0, 0, 0, 0] **Holding coils:** Before: [0, 1, 1, 1, 0] After:[1, 1, 1, 0, 0]	Level 0, 2	High
IP addresses	Brute force I/O Read/modify parameters Modbus TCP flood	Metasploit and Smod framework interface Network traffic	192.168.211.130 (victim) 192.168.211.131 (victim) 192.168.211.128 (attacker)	Level 0, 1, 2	High
Ports	Brute force I/O Read/modify parameters Modbus TCP flood	Network traffic	502	Level 0, 1, 2	Medium
MAC addresses	Brute force I/O Read/modify parameters Modbus TCP flood	Network traffic	00:0c:29:4b:dc:d1 00:0c:29:2d:88:81	Level 0	Medium
Communication protocol	Brute force I/O Read/modify parameters Modbus TCP flood	Metasploit and Smod framework interface Network traffic	Modbus TCP TCP	Level 0, 1, 2	High
Timestamps	Brute force I/O Read/modify parameters Modbus TCP flood	Network traffic	N/A	Level 0, 1, 2	Low
Modbus TCP function codes	Read/modify parameters Modbus TCP flood	Network traffic	Function code 2: Read discrete inputs Function code 15: Write multiple coils	Level 1, 2	Medium
Unique ID	Brute force I/O	Smod framework interface	10	Level 1	Medium
OpenPLC runtime logs	Brute force I/O Read/modify parameters Modbus TCP flood	OpenPLC runtime interface	N/A	Level 1	Medium
Cloud access logs	Read/modify parameters Modbus TCP flood	Network traffic	Timestamped logs of database access events (IP address and type of access (write/read))	Level 3	Low
Packet count	Modbus TCP flood	Network traffic	10,147 10,477	Level 0, 1, 2	Low

1. Denylist
2. Protocol type
3. Relevance for Security Analysis

Engineering Institute of Technology.

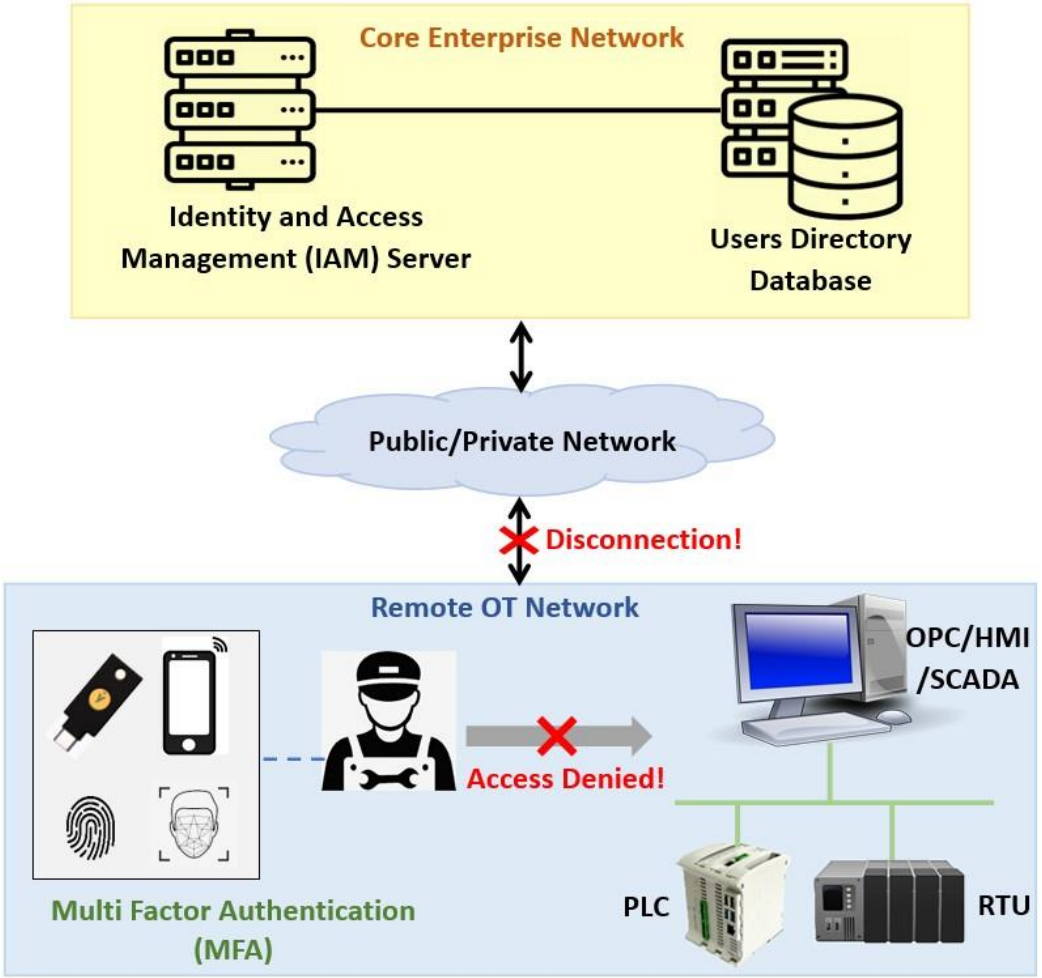
Authentication

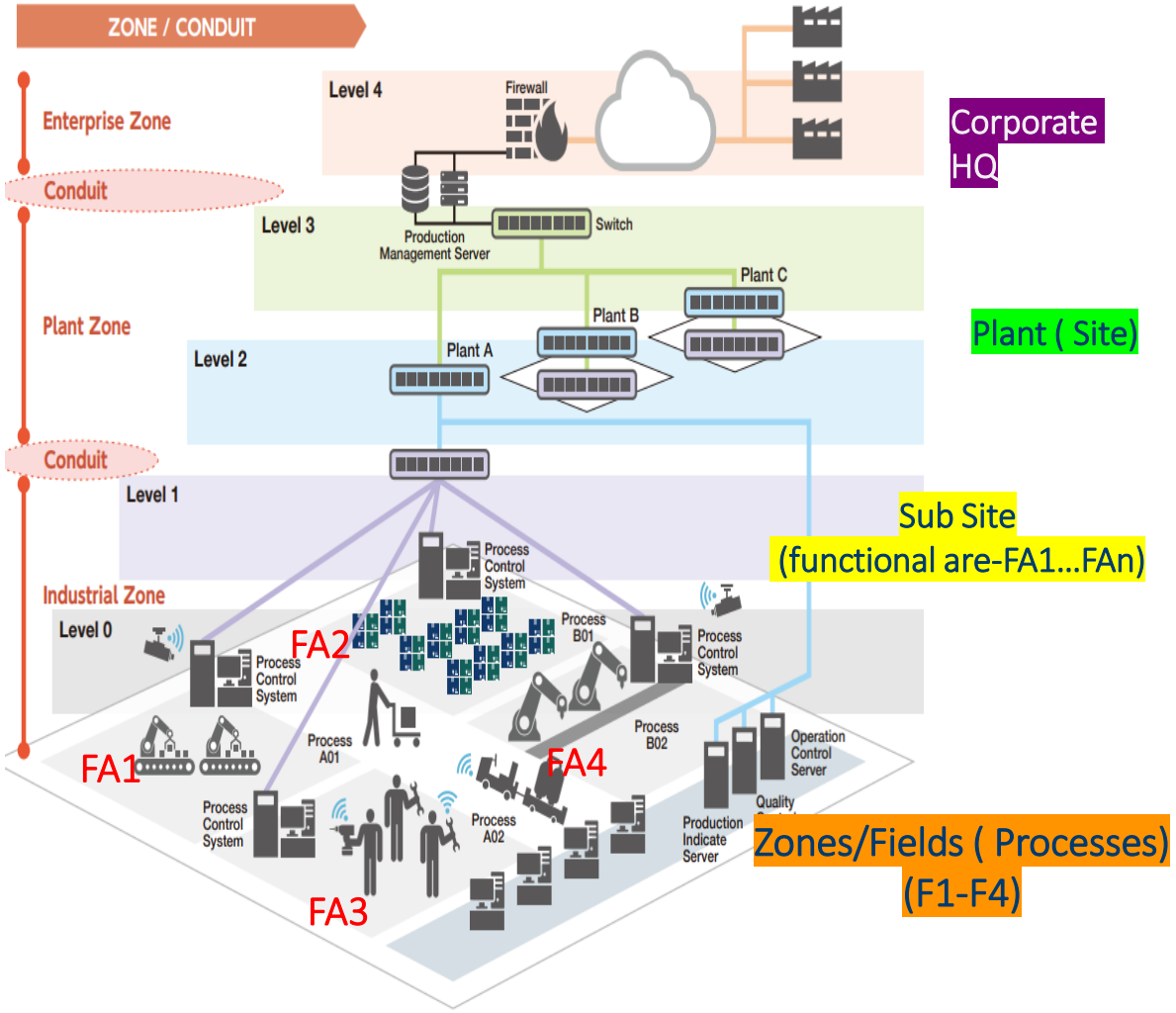
Authentication? Can or Can't?

- Implementing strong authentication (i.e., MFA) at remote OT sites is challenging
- Identity and Access Management (IAM) servers are typically deployed at the core segment of the network
- A stable network connection between the remote site and the core segment of the network is required

- **Problem statement:**

How can we enable MFA in remote and disruption-prone OT sites?





Conceptualize and build a framework to address the following 7 requirements

1. Strong Authentication
2. Distributed and Remote Connectivity
3. Resilience
4. Access Control

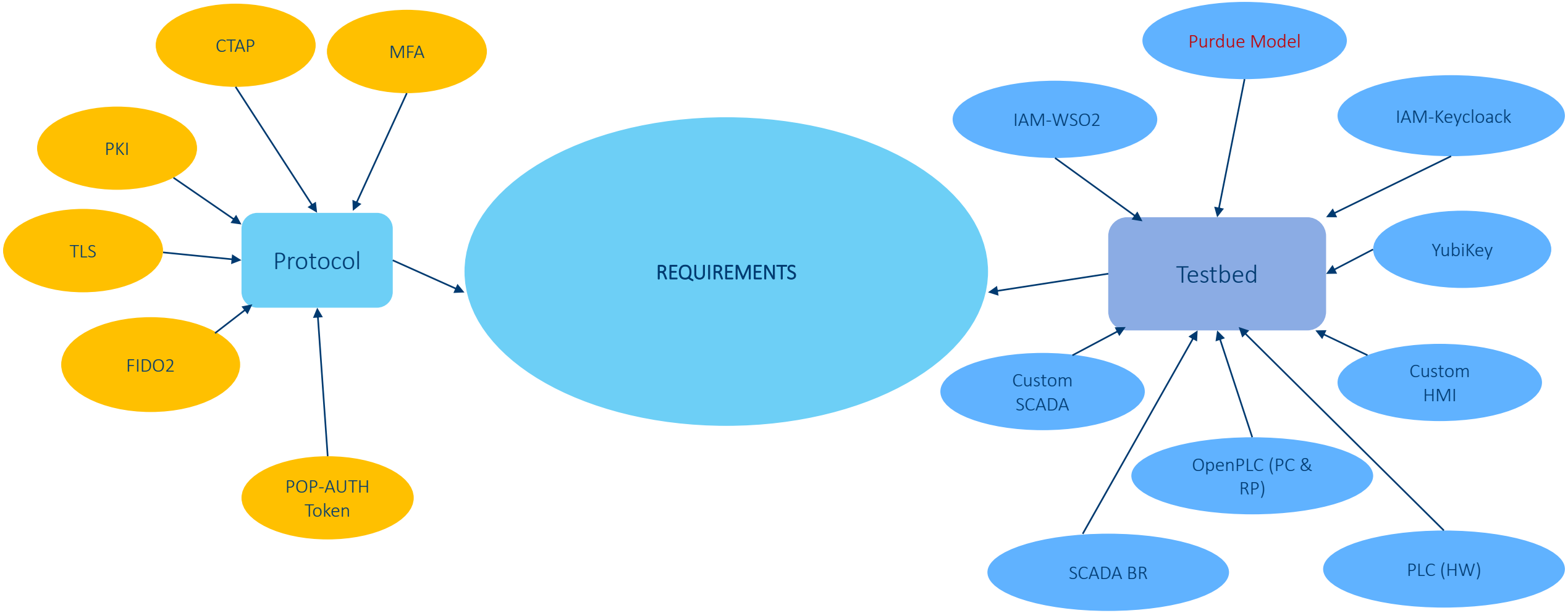
Data Authentication

1. All data communicated between the SGI devices will have the following format:

$$a \leftrightarrow b : \{M|Ctr_{ab}\}_{K^{ab}_{enc}}, MAC\{M|Ctr_{ab}|K^{ab}_{enc}\}_{K^{ab}_{maq}}$$

2. The MAC is the message authentication code to verify the origin of the message.
3. Two separate keys are used for communication, to ensure that the compromise of one does not affect the integrity check, done using the second key
4. In addition, having a MAC ensures that message replay attacks are not practicable
5. The message counter serves to ensure message freshness

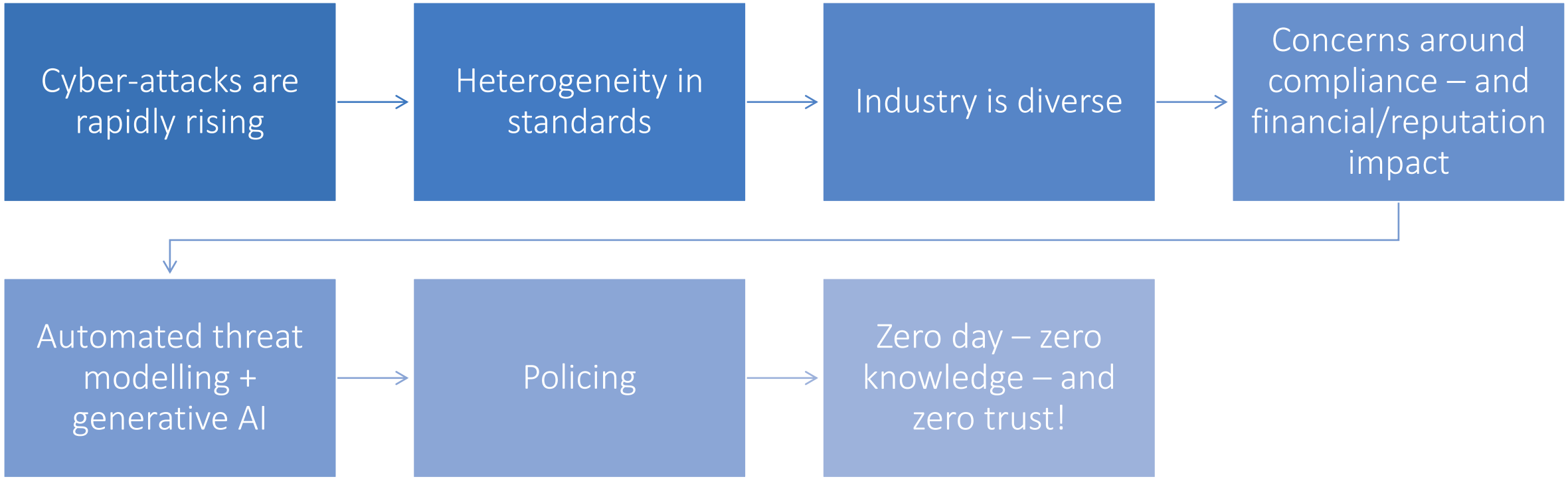
User to Device Authentication



Impact/Utilisation

- User to remote device authentication for varied ICS industries
- Secure authentication and authorization for seamless integration with known standards and established PLC/IIoT families

Summary


Cyber-attacks are rapidly rising
Heterogeneity in standards
Industry is diverse
Concerns around compliance – and financial/reputation impact
Automated threat modelling + generative AI
Policing
Zero day – zero knowledge – and zero trust!

Go against threats – but stay ahead!

Thank you!

Upcoming Courses

Engineering Institute of Technology.

We have a range of courses in Electrical Engineering.

Courses	Start Date
Graduate Diploma of Engineering (Electrical Systems)	2 January 2024
Online – Master of Engineering (Electrical Systems)	2 January 2024
Professional Certificate of Competency in Substation Design (Main Equipment)	16 January 2024
52882WA Advanced Diploma of Electrical and Instrumentation (E&I) Engineering for Oil and Gas Facilities	16 January 2024
Professional Certificate of Competency in Hydrogen Energy – Production, Delivery, Storage, and Use	23 January 2024
Professional Certificate of Competency in Industrial Internet of Things	23 January 2024
52883WA Advanced Diploma of Applied Electrical Engineering (Electrical Systems)	6 February 2024
Undergraduate Certificate in Engineering Foundations	12 February 2024
Undergraduate Certificate in Electrical Engineering	12 February 2024
Online – Bachelor of Science (Electrical Engineering)	12 February 2024

Find MORE courses here: www.eit.edu.au/study-areas/electrical-engineering/

Upcoming Webinars

Engineering Institute of Technology.

All upcoming Events & Webinars:
www.eit.edu.au/news-events/events/

Power System Support From Photovoltaic Systems
15 Nov 2023

Strategies for Effective Data Analytics in Incident Investigation
30 Nov 2023

Mastering the Art of Effective Investigation Techniques
07 Dec 2023

HVDC Technology for Power Transmission
13 Dec 2023

Certificate of Attendance

To receive your digital certificate of attendance for participating in this webinar, please fill out the form and survey here (or scan the QR Code):

https://qrco.de/beWXuc

Kindly note that this form will close on Sunday, 12 November 2023 and no further requests for certificates will be accepted after the form has closed

SCAN ME

Q&A

Engineering Institute of Technology.

Website
www.eit.edu.au

Head Office
1031 Wellington Street West Perth
Perth, WA 6005

Phone
Inside Australia: 1300 138 522
Outside Australia: +61 8 9321 1702

Email
webinars@eit.edu.au

Courses
https://www.eit.edu.au/schedule/