British Embassy Kuwait

المركز الوطني للأمن السيبراني
National Cyber Security Center

cerc 2024

THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

RESICS: Resilience and Safety in Industrial Control Systems (ICS) and Cyber-Physical Systems (CPS)

Dr. Sridhar Adepu

Assistant Professor
University of Bristol, UK

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY
•1966•

UK Science & Innovation Network

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

Industrial Control Systems (ICS)

- ICS are across different sectors: energy, Oil & Gas, Water, Transportation, manufacturing, etc.
- ICS are combination of physical process, computation and communication.

Safety critical systems and Great target for attacks

- Ukraine power blackout 2016.
- Florida water plant hack in 2021.

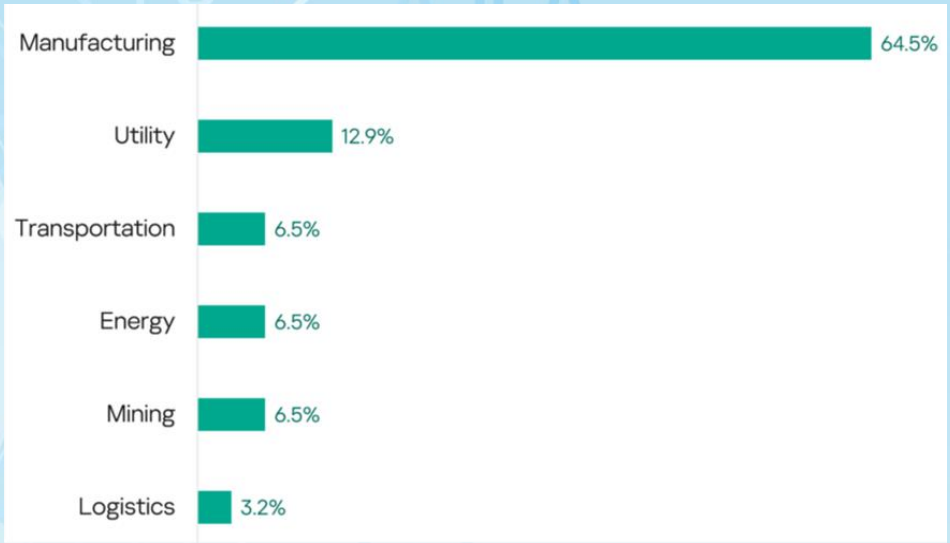
Electric Power Grid

Factory Automation

Q1 2024 Report on OT Cyber Incidents

cerc 2024
THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

- A total of **30 major incidents** were confirmed by large scale corporations.
- 37% of victims reported **denial of operations**.
- Half (~47%) of all incidents resulted in the **disruption of digital services**.



- Average **cost of security incidents** on OT systems : $ 3,000,000 (3 million)
- 1% of incidents reported **>$100 million damages** in each incident

المركز الوطني للأمن السيبراني
National Cyber Security Center

British Embassy Kuwait

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

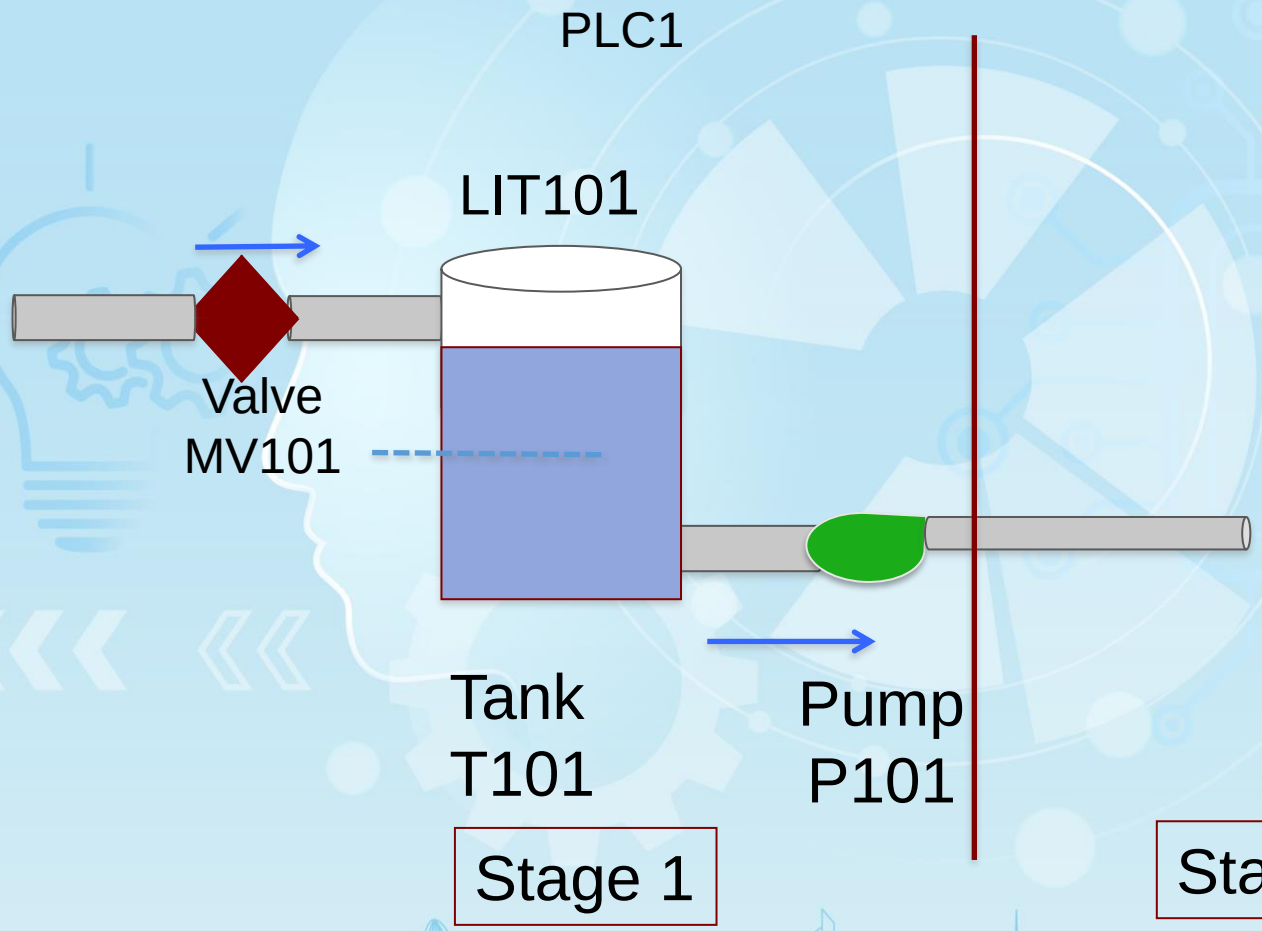
جامعة الكويت
KUWAIT UNIVERSITY

UK Science & Innovation Network

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

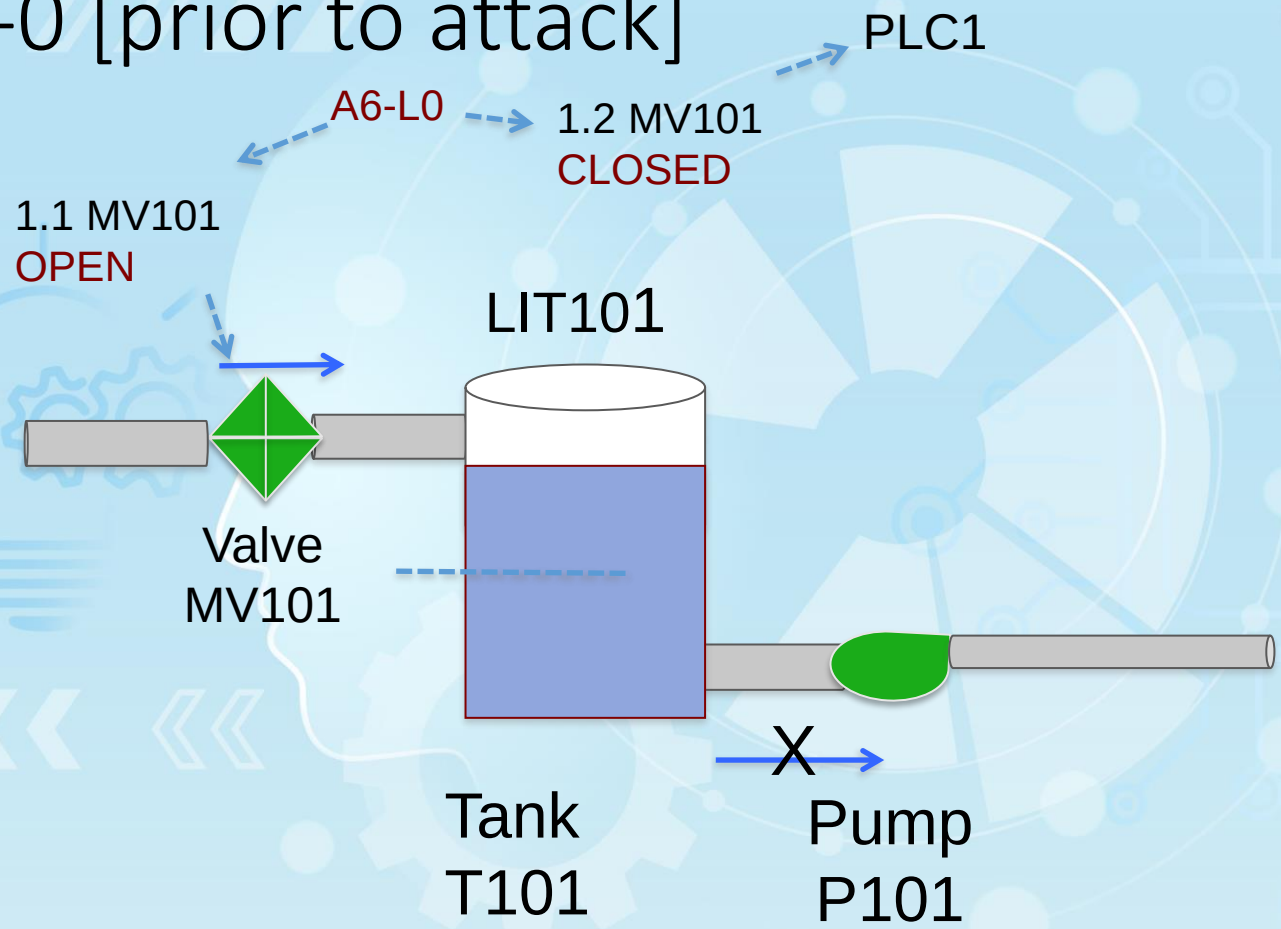
Time: -1 [prior to attack]

A6



Single-Point
Overflow Tank T101

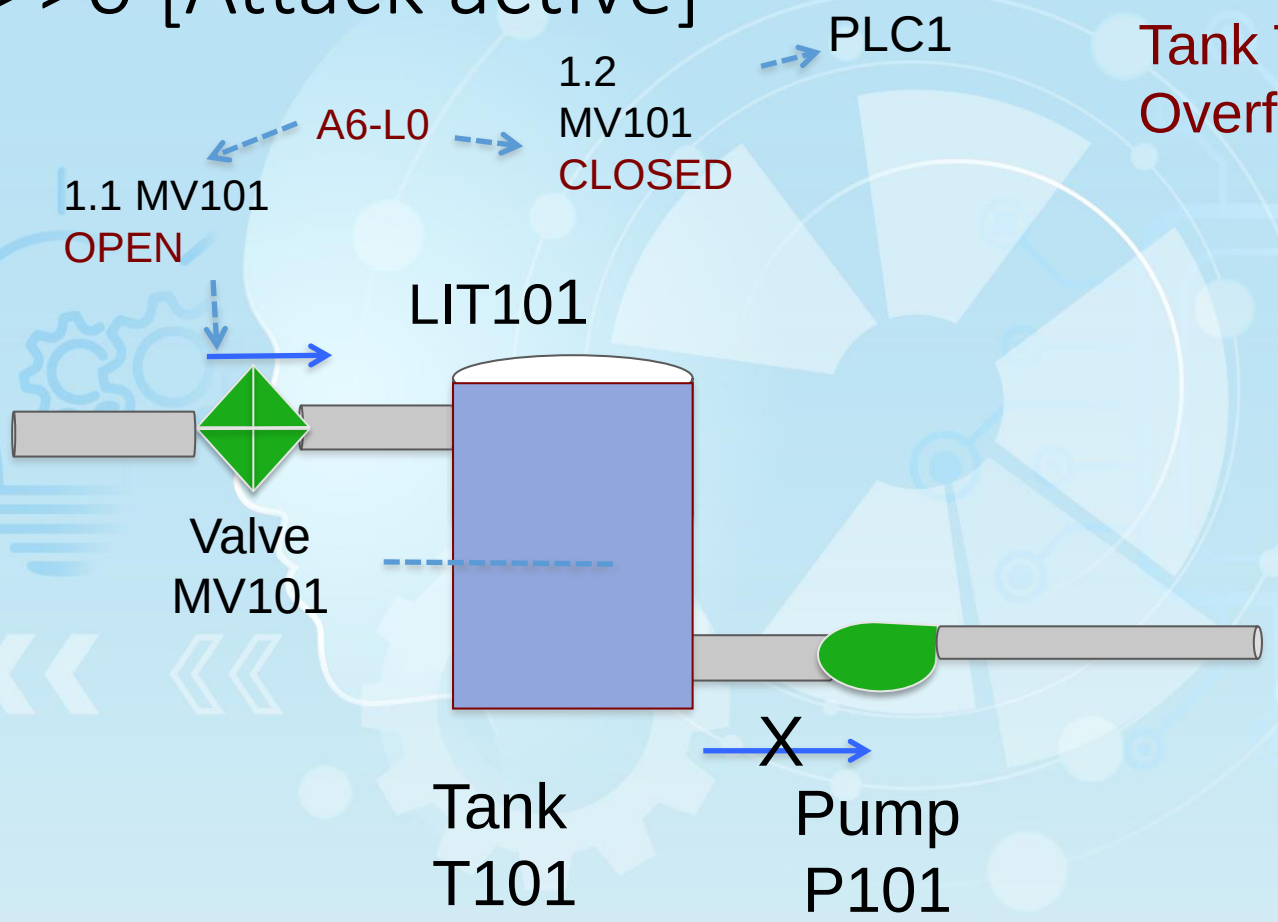
Time: -0 [prior to attack]



Stage 1

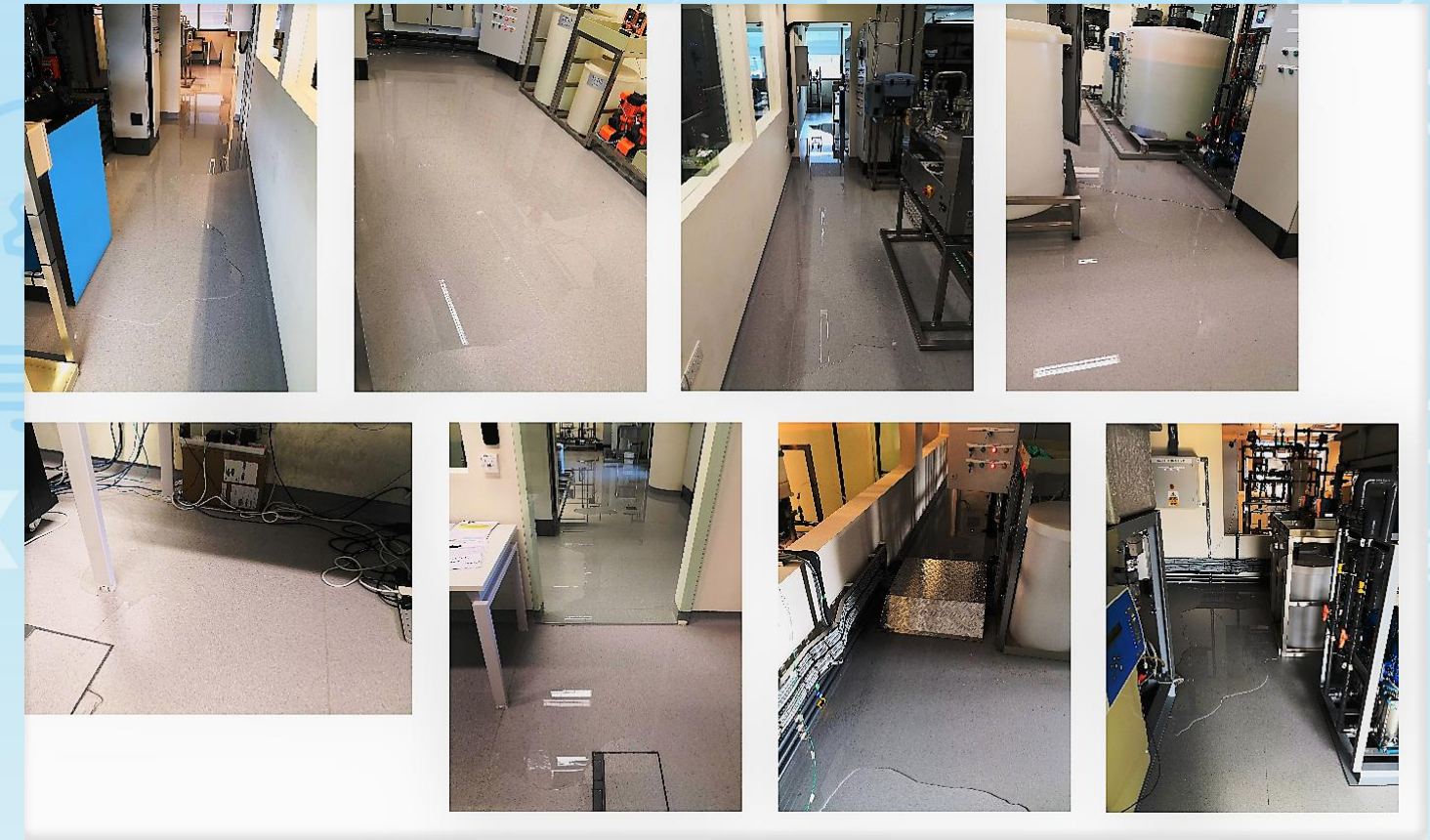
Stage 2

Time: >>0 [Attack active]



Tank T101
Overflow!

Overflow Flooding Scenario



Industrial Control Systems: Interconnection

cerc 2024
THE 6TH CYBERSECURITY EDUCATION & RESEARCH CONFERENCE

Water Treatment

Water Distribution

SWaT

WADI

iTrust
Centre for Research in Cyber Security

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Electric power generation, transmission, distribution, AMI

EPIC

المركز الوطني للأمن السيبراني
National Cyber Security Center

British Embassy Kuwait

KUWAIT COLLEGE OF SCIENCE & TECHNOLOGY
كلية الكويت للعلوم والتكنولوجيا

جامعة الكويت
KUWAIT UNIVERSITY
1966

UK Science & Innovation Network

125 عاماً من الشراكة الكويتية البريطانية
125 YEARS OF KUWAITI-BRITISH PARTNERSHIP

RESICS: Resilience and Safety to attacks in ICS and CPS

- Funded by DSTL and managed by EPSRC as part of the "*Research aligned with Cybersecurity Research Institutes*".
- Aligned with the Research Institute in Trustworthy Interconnected Cyber-Physical Systems (RITICS)
- Collaboration between Imperial College London and University of Bristol
- *Industry Collaborators*:
  Adelard (NCC), Airbus, QinetiQ, Reperion, Siemens, Thales
- *Academic Collaborators*: CMU (USA), SUTD (Singapore), Univ. of Naples (Italy)

The path that led us here

Security and Safety must co-exist in Safety-Critical systems

However, their relationship can be uneasy

Security often seeks to restrict access to data or function

Safety often relies on the availability of services and data

ICS systems must be safe and “secure”!

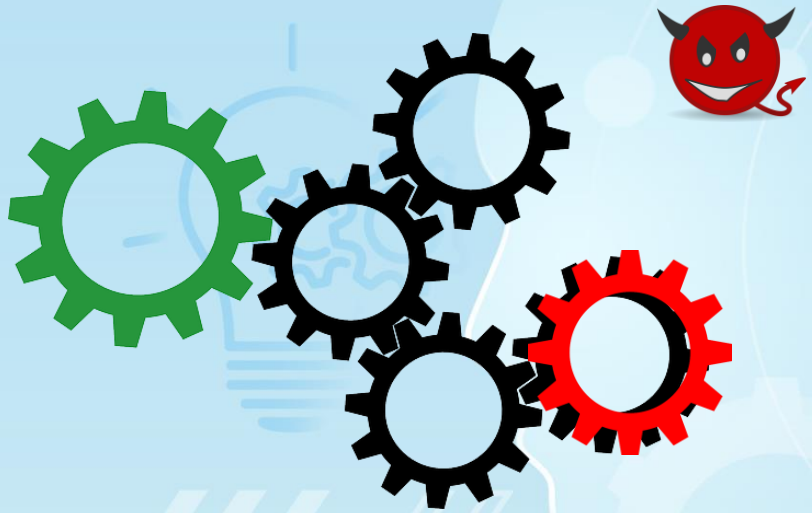
- Convergence of OT/IT
- IoT augmenting ICS systems
- Broader attack surface
- Contested environment
- Increasingly complex systems

What questions should we ask at the intersection of security and safety?

- …
- **Which attacks can compromise safety?**
- Which mitigating (counter) measures do not?
- Can a system be “safe” but vulnerable, or even partially compromised?
- …

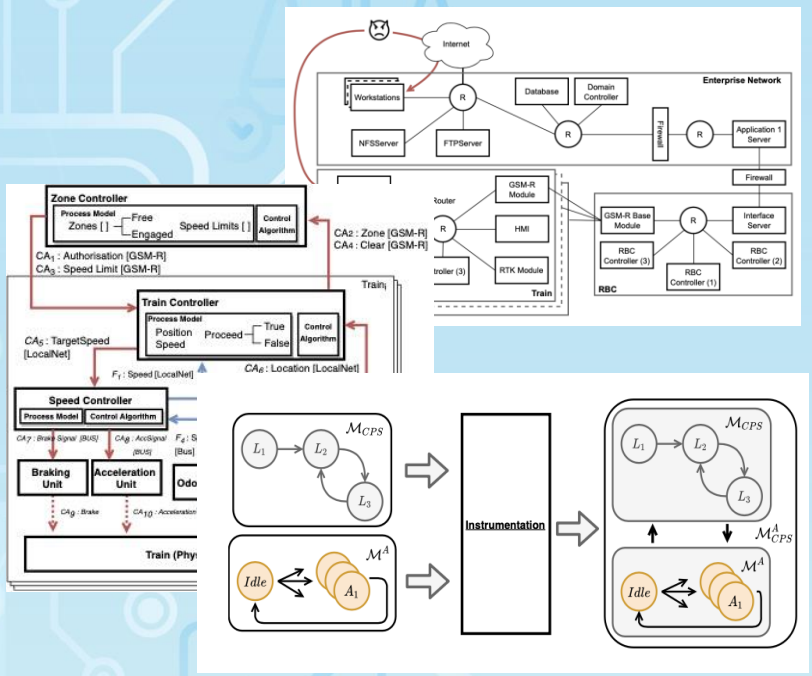
Given the broad attack surface can we systematically identify the attacks that may lead to safety violations?

The problem is difficult because …



Cascading Effects

Safety Engineers
Security Engineers
System Designers



Lack of integrated tools

Combining Safety and Security Analyses

Security Analysis

- Threats
- Attack Paths

System Models

- Architecture
- Behaviour

Safety Analysis

- Hazards, Losses
- Safety Properties

Align Models

Formal Methods

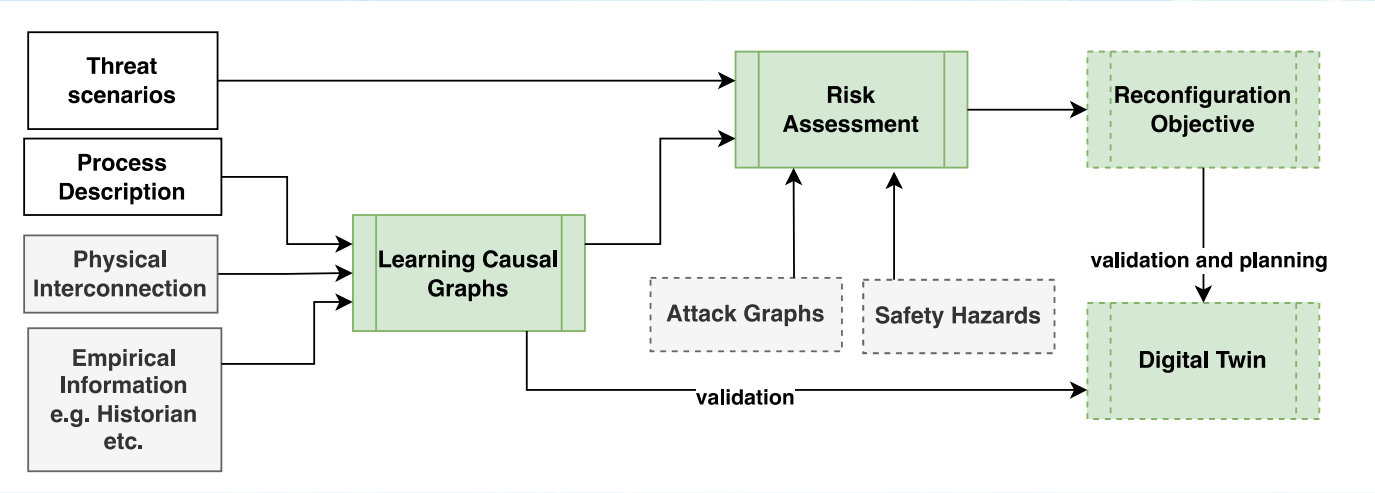
Attack Sequences

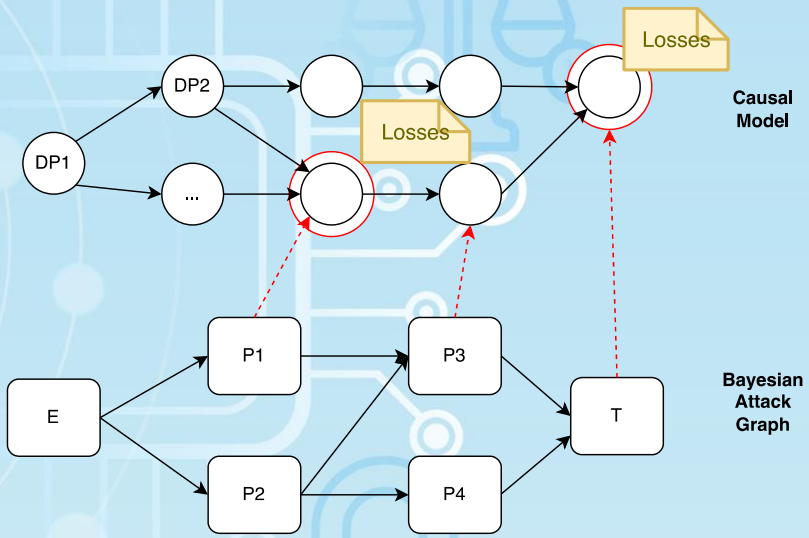
Attack Paths

Critical Protection Sets

Risk and Impact Assessment

- *How to assess the cascading effects of safety and security events?*

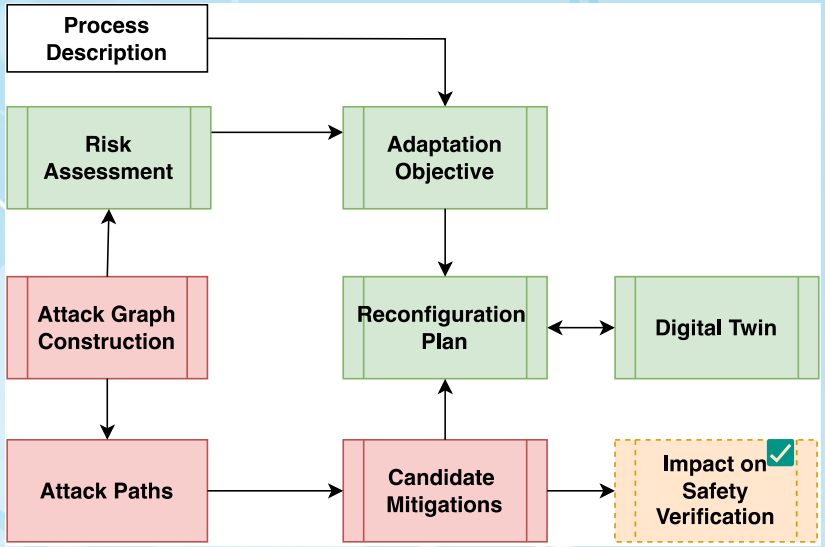




Causal graphs to determine dependencies, the impact of action parameter values and their discretisation. Combine with attack graphs and safety analysis for risk and impact assessment.

Resilience and Countermeasure Selection

- *How can we select or synthesise countermeasures that:*
  - Mitigate the threats.
  - Do not endager safety.
  - Keep the system in one of its operational states.
  - Maximise performance.



- Based on Risk Assessment identify degraded operation modes that reduce risk. Synthesize system adaptation.
- Analyse impact on safety and determine if it is acceptable. Evaluate effect of changes.
- Identify countermeasures that would mitigate the threat and reduce risk.

Related publications

- M, Kornkamon, S. Venugopalan, and S. Adepu. "WaXAI: Explainable Anomaly Detection in Industrial Control Systems and Water Systems." 10th ACM Cyber-Physical System Security Workshop. 2024.
- R. Wang, S. Venugopalan and S. Adepu. “Safety Analysis for Cyber-Physical Systems under Cyber Attacks Using Digital Twin” under submission with IEEE Cyber Security and Resilience 2024.
- Maiti, R. R., S. Adepu, and E Lupu. "ICCPS: Impact discovery using causal inference for cyber attacks in CPSs." arXiv preprint arXiv:2307.14161 (2023). Submitted: with ACM Transactions on Privacy and Security.
- L. M. Castiglione and E. C. Lupu. Which Attacks Lead to Hazards? Combining Safety and Security Analysis for Cyber-Physical Systems. IEEE TDSC *(to appear) https://doi.org/10.1109/TDSC.2023.3309778.*
- L. M. Castiglione, Z. Hau, P. Ge, K. T. Co, L. Muñoz-González, F. Teng, E.C. Lupu. HA-Grid: Security Aware Hazard Analysis for Smart Grids. IEEE Int. Conf. on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm).

ILLUSIONIQ Limited

https://www.illusioniq.com

Actionable and Relevant Intelligence from Globally Deployed Decoys

Sridhar Adepu PhD
Director and Founder

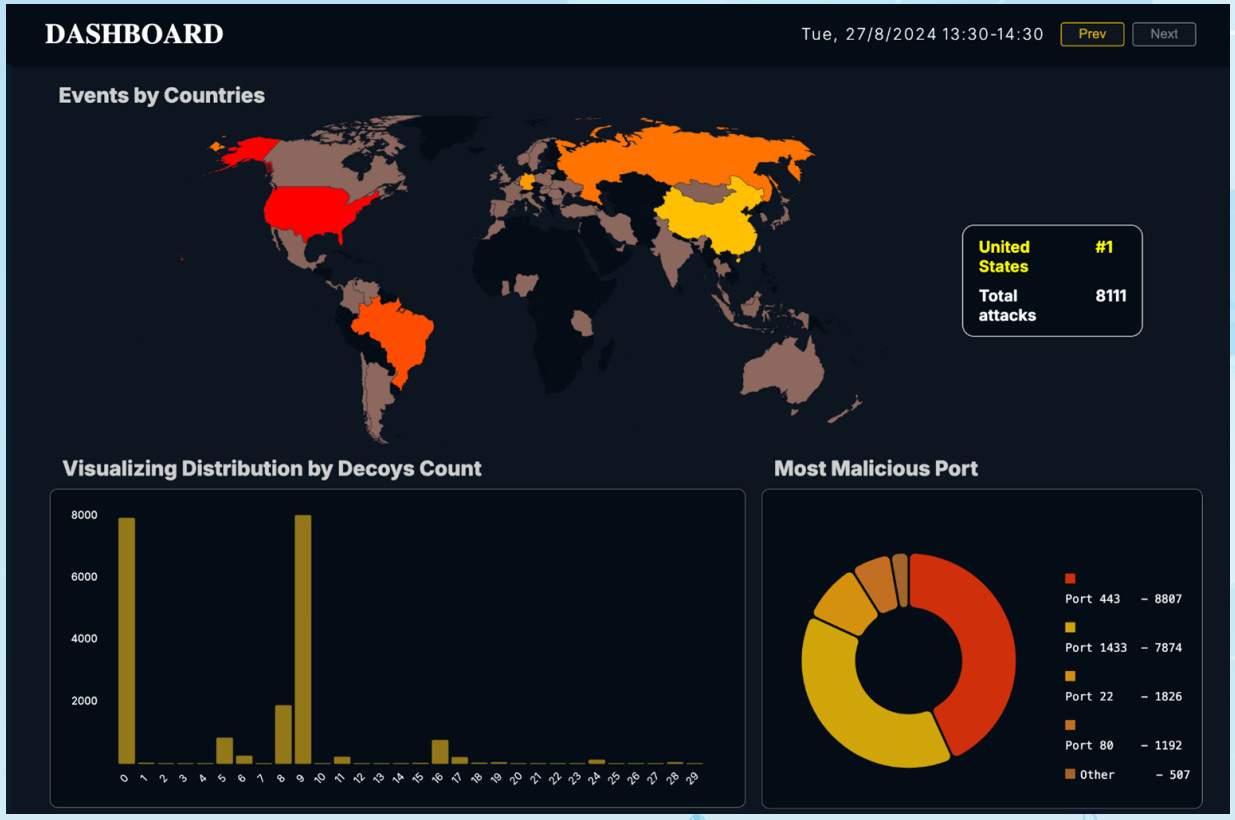
Deception Technology for Industrial Systems

- ILLUSIONIQ decoys resemble a **real system emulation** to deceive attackers.
- In house (70) and custom decoys
  - PLC/SCADA and OT-IT integrations
  - **Hardware in The Loop**
  - Applications and Services
  - **AI Enabled Decoys**
- Detect **high fidelity** alerts
- Redirect attackers to gain time
- Preparedness of defences

Energy

Manufacturing

Global Threat Visualisation



- Interactive map of **adversaries** locations and offering a visual understanding of worldwide patterns.
- Automatically identifying and **dynamically blocking** malicious threat actors across the globe.

Actionable and Relevant Intelligence

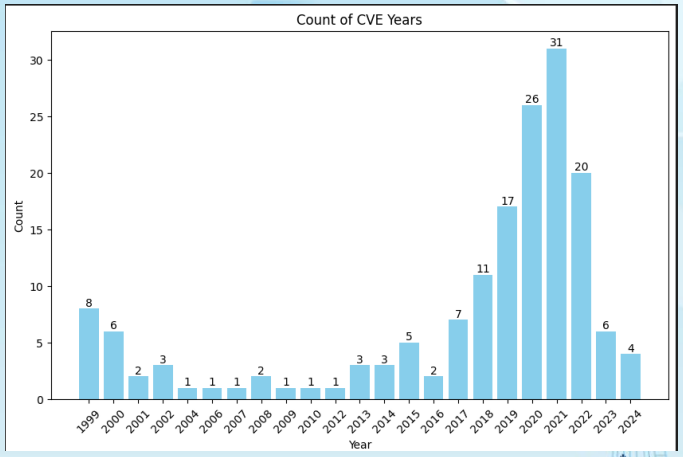
- Who - Attribution of attacker or team
- Where - Beacon files
- When - First seen, last seen, flow
- How - TTPs /APTs
- Why - Adversary behaviour

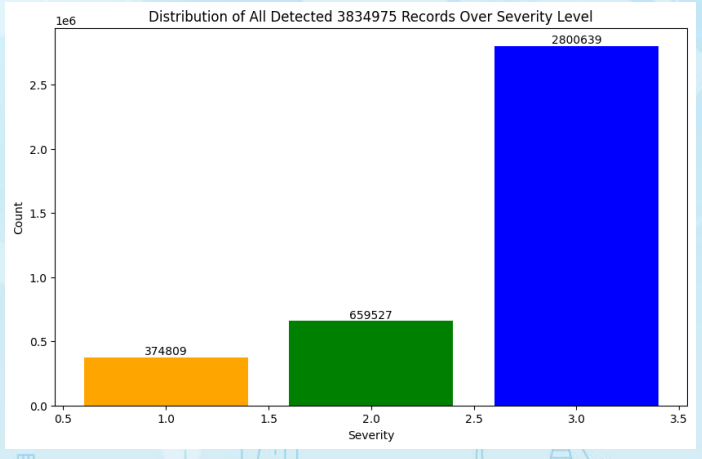
- Detailed Mapping of Attacker Vectors
  - Tactics
  - Techniques

MITRE ATT&CK™

Actionable Intelligence from Platform

- 3+ million attacker actions: Dynamic adversary blocking, Exploited CVEs, Malwares and MITRE ATT&CK
- 86000 times CVEs exploited and 162 of them are unique
- MITRE TTPs: 48 unique techniques mostly used false under 12 tactics
- Number of adversaries: 45000 +





What value do you get?

- **High fidelity** alerts
- **Reveal adversaries** and uncover their activities
- Intel from globally deployed decoys.
  - Most exploitable **CVEs**
  - Dynamic **IP blocking**
  - Active **malwares/ransomwares**

- Reduce **MTTD/MTTR**
- Augment your **SoC capacity** through **prioritisation**
- Reduce the **cost of breach**

The guarantee to always be a step ahead.

Ready to protect your Industrial system?

Dr. Sridhar Adepu

ILLUSIONIQ Limited

sridhar@illusioniq.com

https://www.illusioniq.com/demo