# Trustworthy Inter-connected Cyber-Physical Systems

**Chris Hankin**

**Imperial College London and Director of RITICS**

September 2020

Imperial College London

# Outline

- Context – RITICS and KIOS
- Some Contributions
  - Monitoring
  - Measuring
  - Diversifying
  - Defending
- The Broader Network

# Key Questions / Challenges for RITICS Phase 1 (2014-2018)

Do we understand the harm threats pose to our ICS systems and business?

Can we confidently articulate these threats as business risk?

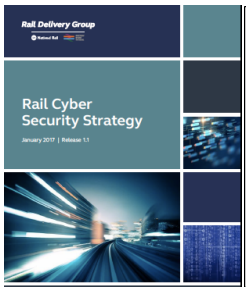
What could be novel effective and efficient interventions?

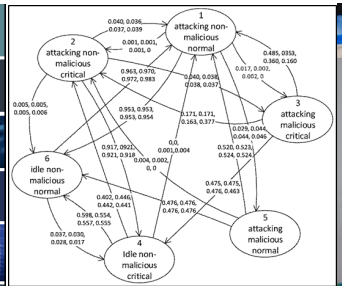
# RITICS Phase 1 Projects

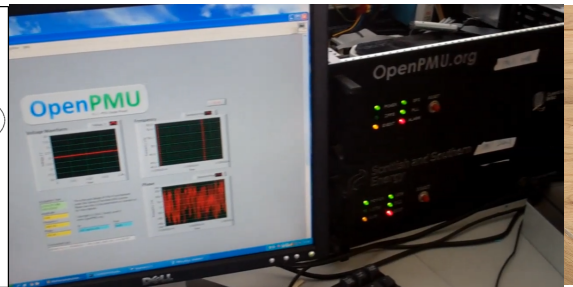
- RITICS (Hankin, Chana, Imperial College London)
- MUMBA (Rashid, Lancaster/Bristol)
- CEDRICS (Bloomfield, Popov, City)
- SCEPTICS (Easton, Chothia, Birmingham)
- CAPRICA (Sezer, Queen's University Belfast)

# Impact of Phase 1

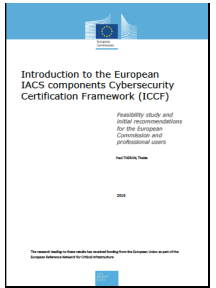
- Creation of a new research community
- Contribution to new Cyber Security Strategy for UK railways.
- Tools for building models of complex cyber physical systems.
- Testbeds.
- A serious game for studying security decisions.
- Secure implementation of gateway module compatible with IEC  and IEEE standards.
- Contribution to European work on certification of ICS components.



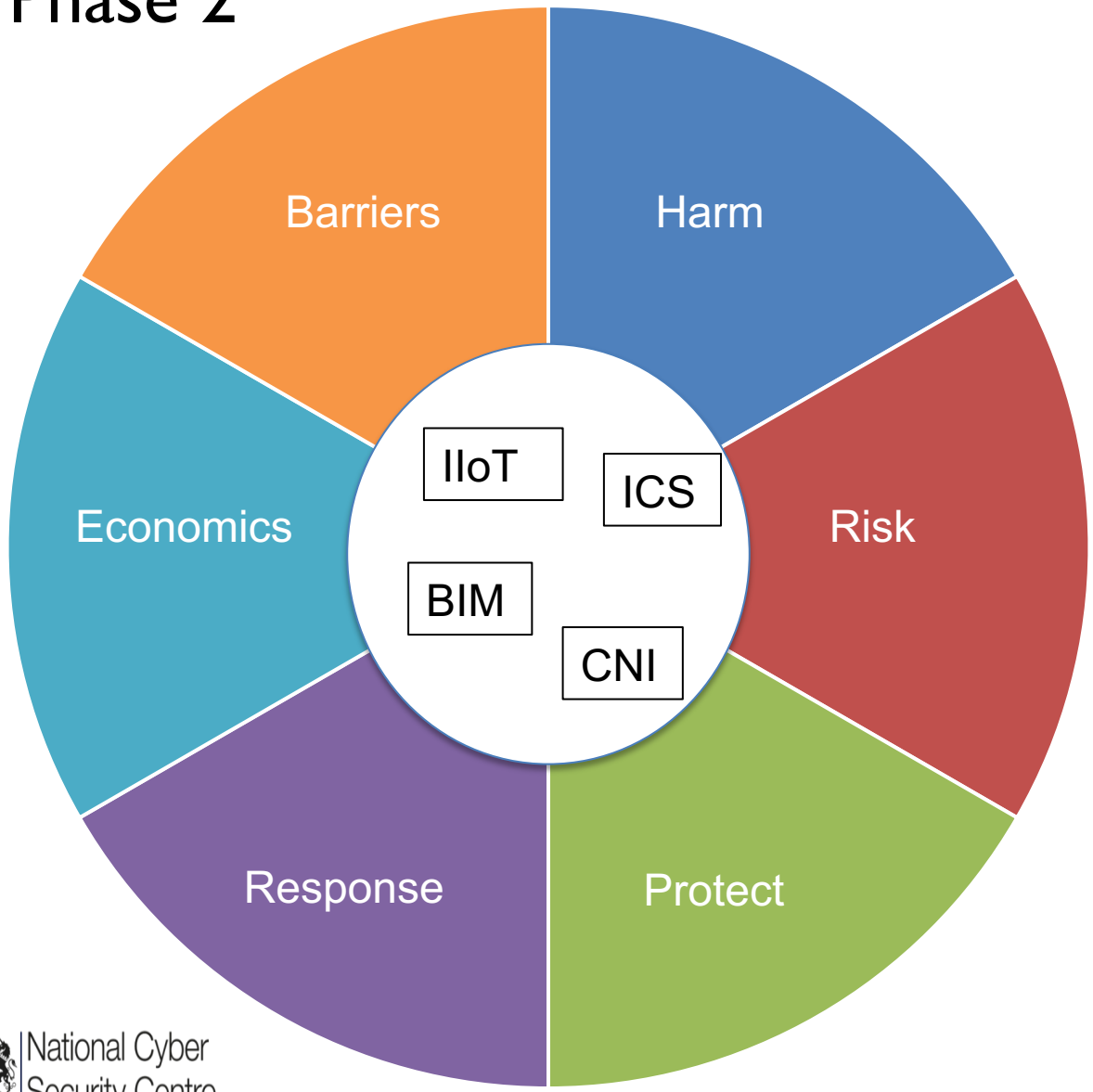







# RITICS Phase 2




EPSRC
Engineering and Physical Sciences Research Council

National Cyber Security Centre

# Teaming with the University of Cyprus

RITICS

KOIOS
Research and Innovation Center of Excellence

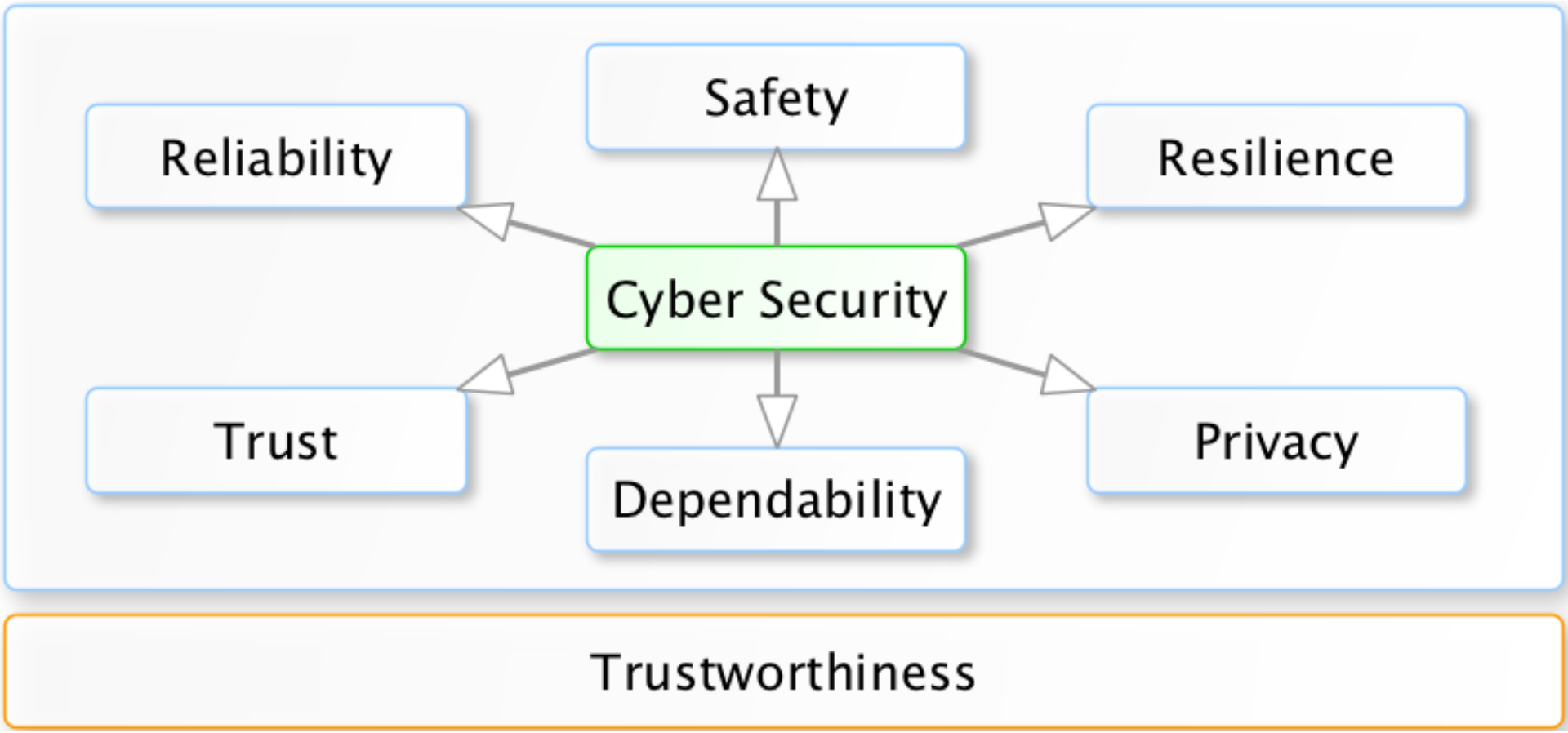
University of Cyprus

Imperial College London

**Official Launch Event**
University of Cyprus, Nicosia
16th March 2017

## Formal Addresses

| | |
|---|---|
| **10.00** | The Rector of the University of Cyprus<br>Professor Constantinos Christofides |
| **10.10** | H.E. the President of the Republic of Cyprus<br>Mr Nicos Anastasiades |
| **10.20** | Director-General, Research & Innovation, European Commission<br>Mr Robert-Jan Smits |


Safety
Reliability
Resilience
Cyber Security
Trust
Privacy
Dependability
Trustworthiness

# Challenges to Trustworthiness

- Cyber Security and Computer Science Education
- Inter-connectedness and inter-dependencies
- Digitalisation and homogeneity
- Reliance on AI/ML

RITICS

## Emerging Topics in ICS Security

- Bring Your Own Device (BYOD)
- Virtual Machine Technologies
- Security Monitoring in an ICS environment
- ICS Intrusion Detection and Prevention Systems
- Security Information and Event Management (SIEM) technologies
- ICS Supply Chain Management
- Managed Services and Outsourcing
- Leveraging Cloud Services in ICS

## ICS Attack Methods

- Exploiting Weak Authentication
- Network Scanning/Probing
- Removable Media
- Brute Force Intrusion
- Abuse of Access Authority
- Spear Phishing
- SQL Injection

## CISA ASSESSMENTS: FISCAL YEAR 2019 MOST PREVALENT IT AND OT WEAKNESSES AND RISKS

### Boundary Protection

**RISK**
Undetected unauthorized activity in critical systems

**RISK**
Weaker boundaries between ICS and enterprise systems

### Principle of Least Functionality

**RISK**
Increased vectors for malicious party access to critical systems

**RISK**
Opportunity for rogue internal access to be established

### Identification and Authentication

**RISK**
Lack of accountability and traceability for user actions if an account is compromised

**RISK**
Increased difficulty in securing accounts as personnel leave the organization, especially sensitive for users with administrator access

### Physical Access Control

**RISK**
Unauthorized physical access to field equipment provides increased opportunity to:

- Maliciously modify, delete, or copy device programs and firmware
- Access the ICS network
- Steal or vandalize cyber assets
- Add rogue devices to capture and retransmit network traffic

### Account Management

**RISK**
Increased opportunity for unapproved system access from shared or system accounts

KIOS
Research and Innovation Center of Excellence

RITICS

# Four contributions:

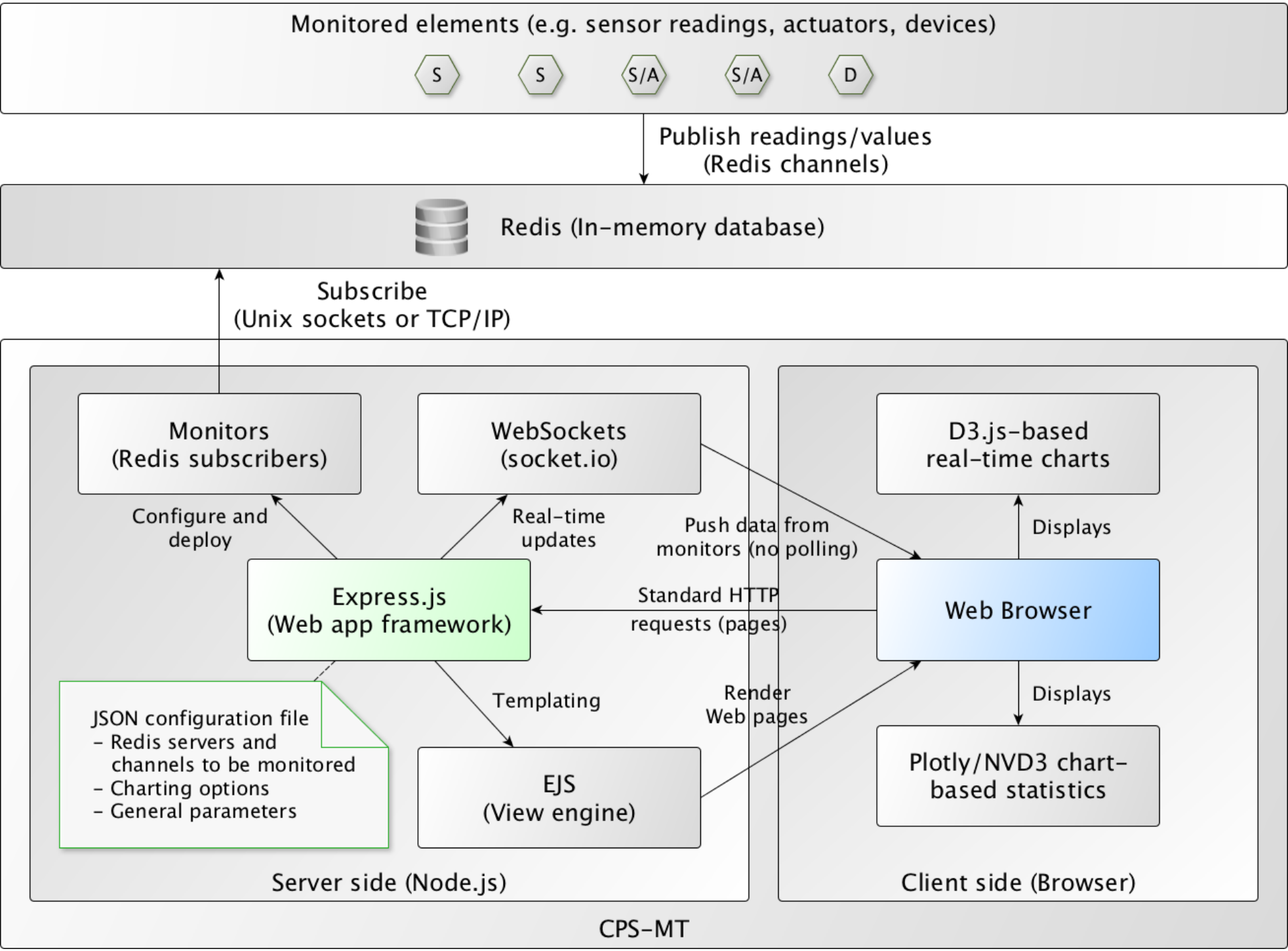
- Real-time CPS Monitoring
- Measuring Cyber-physical security
- Software Diversity
- AI and Intrusion Detection

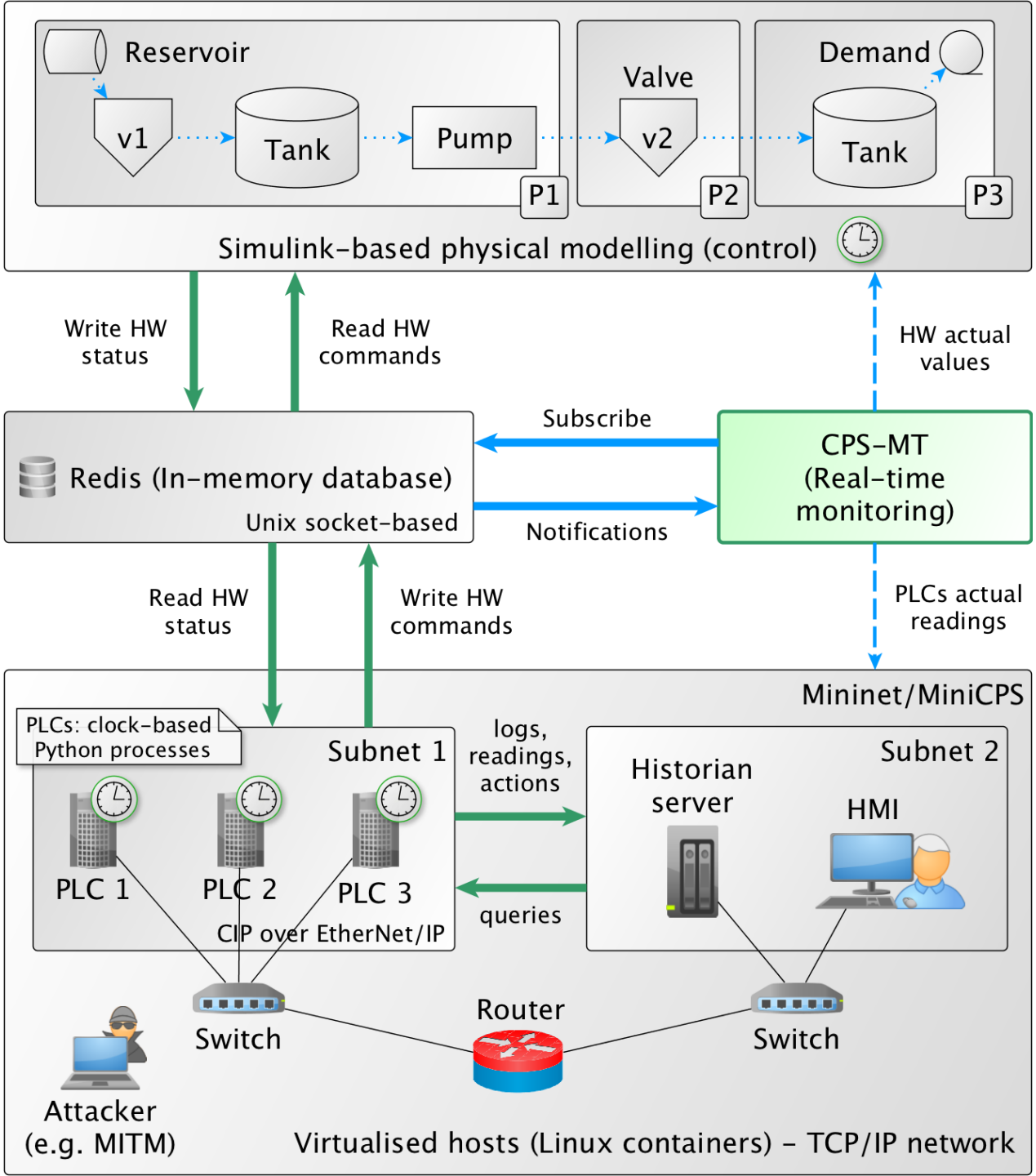
# CPS-MT

KIOS
Research and Innovation Center of Excellence

RITICS

- Proof-of-concept real-time monitoring tool.
- Focus on security research
- Monitored elements publish status/data via in-memory database
- CPS-MT subscribes to data base
- Deployment in water treatment study


Monitored elements (e.g. sensor readings, actuators, devices)
S
S
S/A
S/A
D
Publish readings/values
(Redis channels)
Redis (In-memory database)
Subscribe
(Unix sockets or TCP/IP)
Monitors
(Redis subscribers)
WebSockets
(socket.io)
D3.js-based
real-time charts
Configure and
deploy
Real-time
updates
Push data from
monitors (no polling)
Displays
Express.js
(Web app framework)
Standard HTTP
requests (pages)
Web Browser
JSON configuration file
- Redis servers and
channels to be monitored
- Charting options
- General parameters
Templating
Render
Web pages
Displays
EJS
(View engine)
Plotly/NVD3 chart-
based statistics
Server side (Node.js)
Client side (Browser)
CPS-MT




RITICS

KOIOS

Research and Innovation Center of Excellence

CPS-MT (DEMO)

Home Config Monitors Stats About

Imperial College London

## Monitors

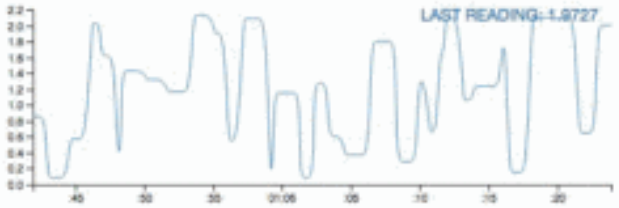
Capture | Download | Status: Stopped | Events captured: 196 | Clear

Show 10 entries Search:

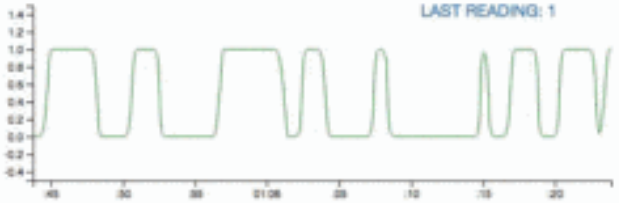
| Id | Name | Stream server | Channel | Display |
|---|---|---|---|---|
| _s1_plc1_get_lit101 | Tank 1 level (LIT101 read by PLC1) | 192.168.59.10:6379 | plc1:get:LIT101 | yes |
| _s1_plc1_get_mv101 | Mechanical valve 1 (MV101 read by PLC1) | 192.168.59.10:6379 | plc1:get:MV101 | yes |
| _s1_plc2_get_fit201 | Flow level pipe 2 (FIT201 read by PLC2) | 192.168.59.10:6379 | plc2:get:FIT201 | yes |

Showing 1 to 3 of 3 entries Previous 1 Next

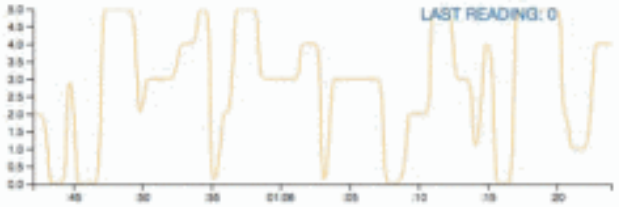
- **Tank 1 level (LIT101 read by PLC1) - Channel: s1:plc1:get:LIT101**




- **Mechanical valve 1 (MV101 read by PLC1) - Channel: s1:plc1:get:MV101**




- **Flow level pipe 2 (FIT201 read by PLC2) - Channel: s1:plc2:get:FIT201**




Institute for Security Science and Technology
Imperial College London © 2018

RITICS

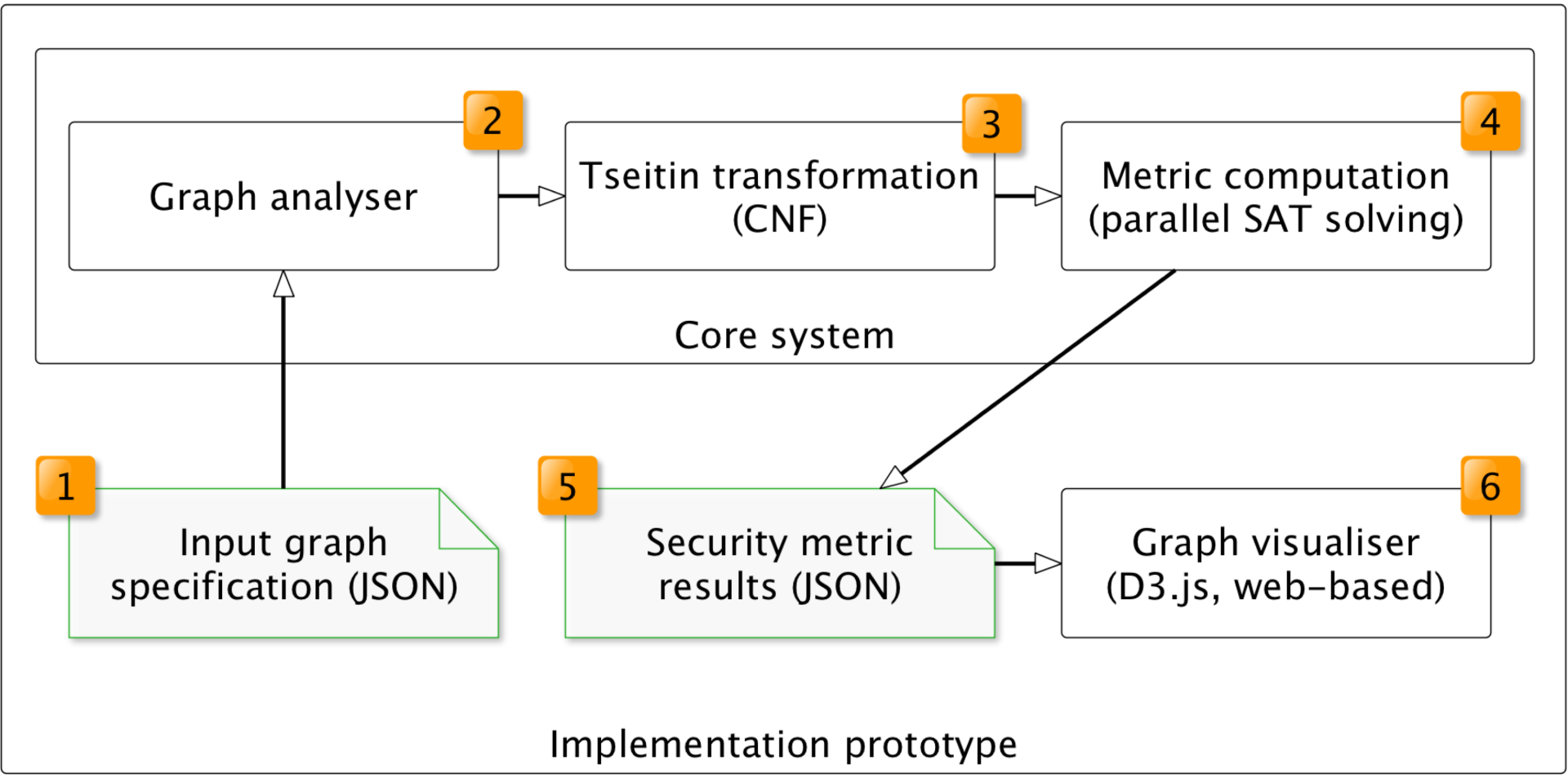
KOIOS
Research and Innovation Center of Excellence

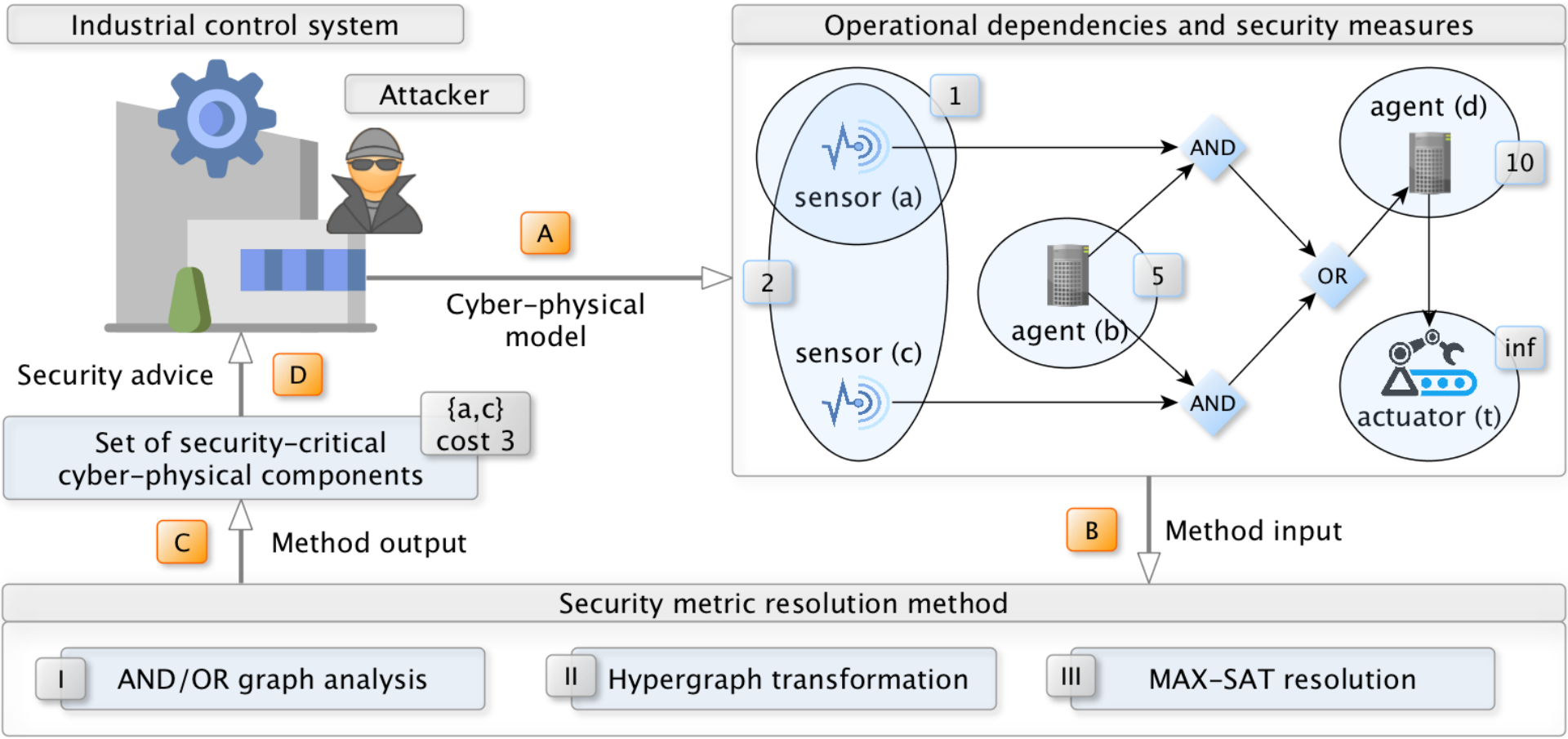
# META4ICS

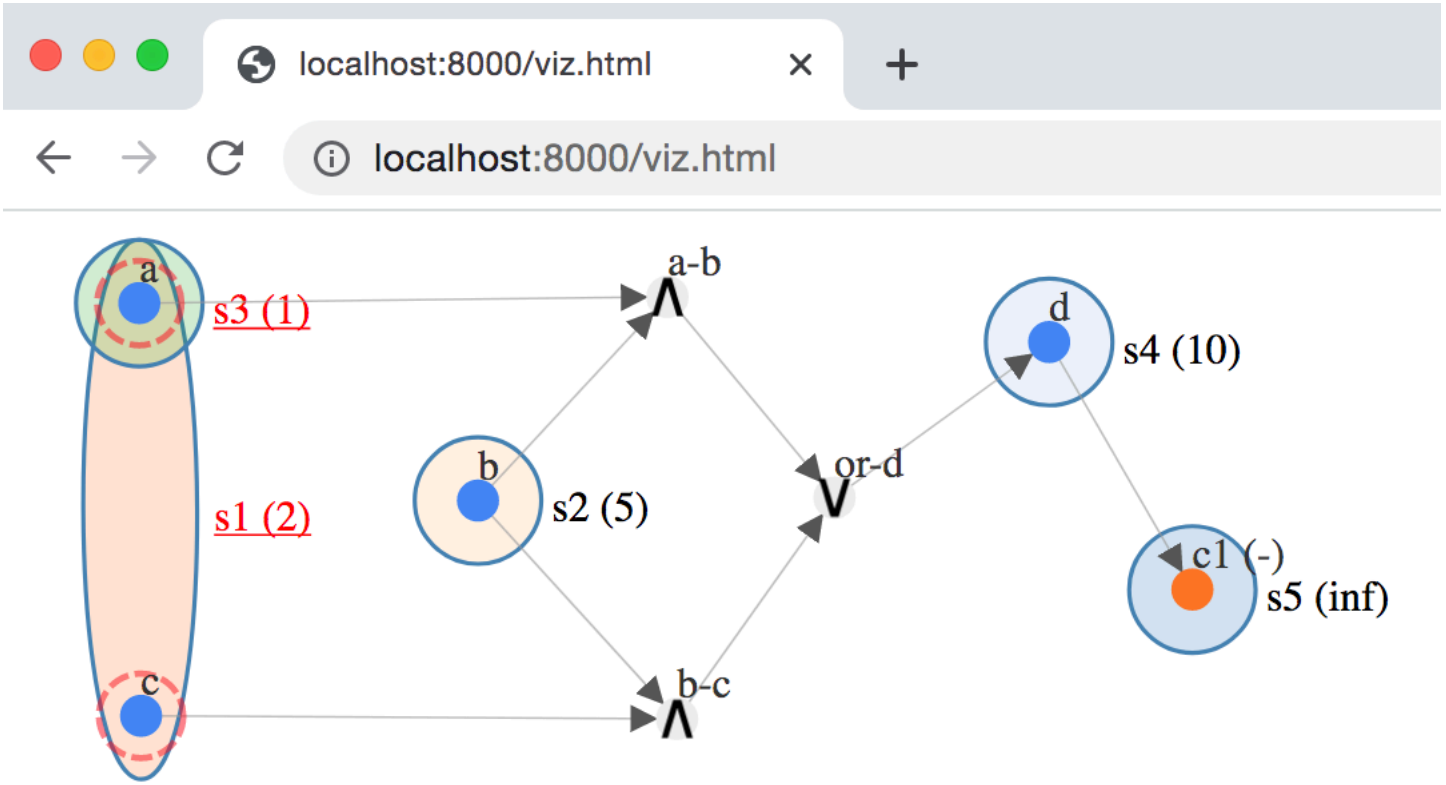
KIOS
Research and Innovation Center of Excellence

RITICS

- Proof-of-concept tool to identify critical cyber-physical components.
- AND/OR (hyper-)graph of dependencies.
- MAX-SAT solvers used in calculating critical components.
- Models physical protections as well as cyber aspects.


2
Graph analyser
3
Tseitin transformation
(CNF)
4
Metric computation
(parallel SAT solving)
Core system
1
Input graph
specification (JSON)
5
Security metric
results (JSON)
6
Graph visualiser
(D3.js, web-based)
Implementation prototype


Industrial control system
Attacker
A
Cyber-physical model
Operational dependencies and security measures
1
sensor (a)
2
sensor (c)
AND
AND
5
agent (b)
OR
agent (d)
10
inf
actuator (t)
Security advice
D
Set of security-critical cyber-physical components
{a,c}
cost 3
C
Method output
B
Method input
Security metric resolution method
I
AND/OR graph analysis
II
Hypergraph transformation
III
MAX-SAT resolution


localhost:8000/viz.html
localhost:8000/viz.html
a
s3 (1)
s1 (2)
c
a-b
b
s2 (5)
b-c
or-d
d
s4 (10)
c1 (-)
s5 (inf)

# Software Diversity

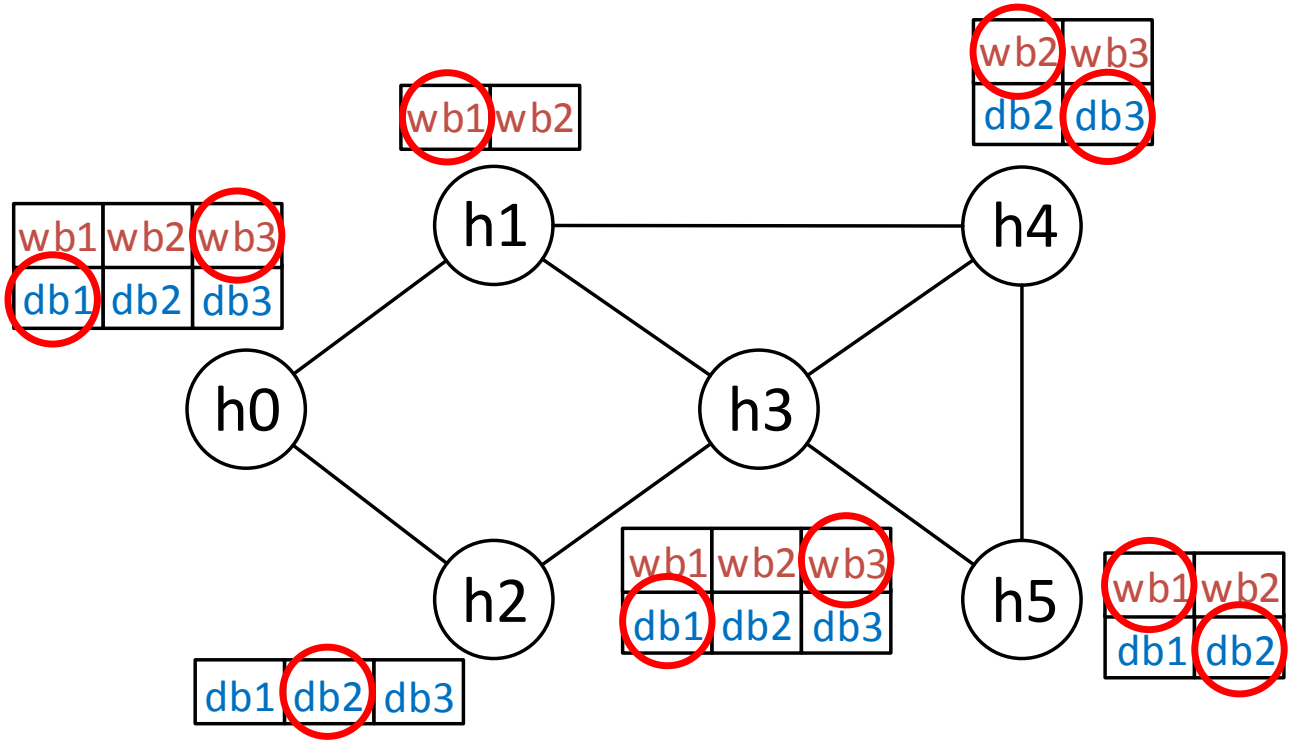
- Software diversity in networks as graph colouring problem
- Similar products facilitate spread of malware
- Optimal allocation across multiple products (respecting constraints) to slow spread

# Approach

RITICS

- Metric *vulnerability similarity of products* computed from a statistical study of *CVE/NVD*.
- Model the multi-labelled network by a discrete *Markov Random Field (MRF).*
- Optimal assignment of products by the *sequential tree-reweighted message passing (TRW-S)* algorithm – assign products to reduce similarity between neighbouring nodes whilst obeying any constraints.
- The result evaluated in a *NetLogo simulation* in terms of Mean Time To Compromise.
- Scalability analysis of our optimisation method against
  - Large-scale networks with *up to 10,000 hosts*.
  - High-density networks with *up to 50 degrees (# edges) per host*.
  - High-complexity networks with *up to 30 products/services per host*.
  - Most heavy cases converged from a couple of seconds to ~3 minutes.

# Example: Web and database diversity

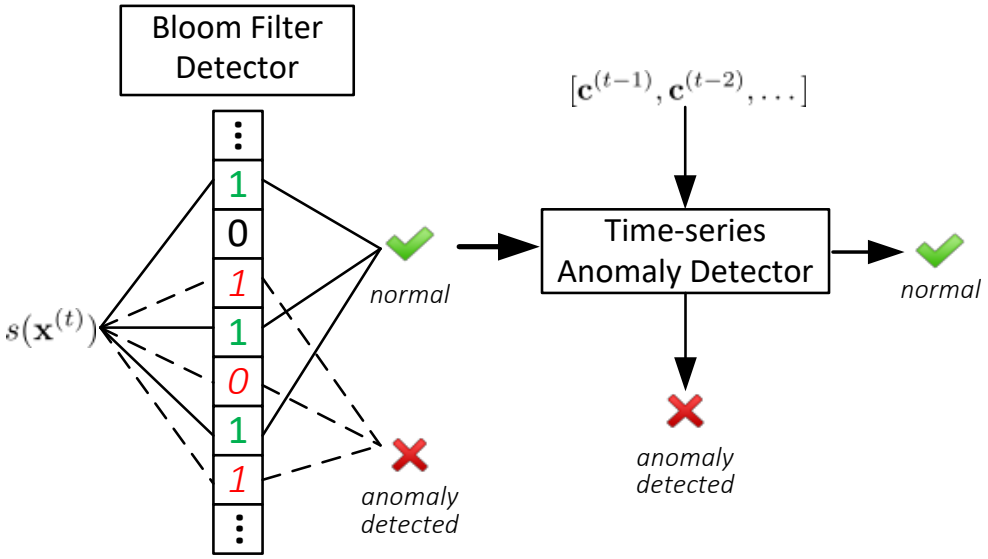


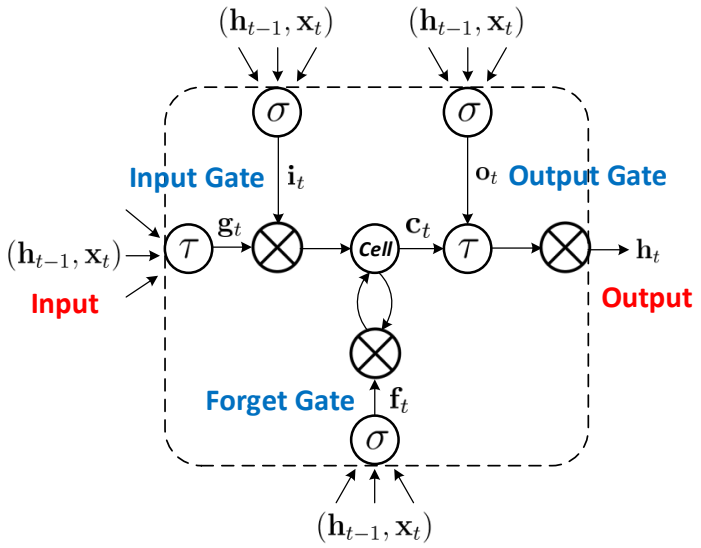
# Intrusion Detection

RITICS

- Deep learning to spot anomalous network traffic
- Evasion attacks
- Defence against adversaries

# Anomaly Detection



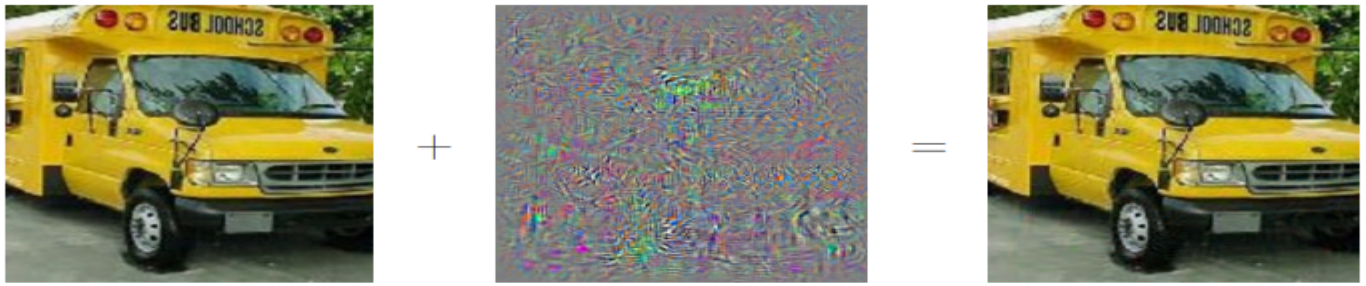




| Model | Precision | Recall | Accuracy | F-score |
|---|---|---|---|---|
| Our model | 0.94 | **0.78** | **0.92** | **0.85** |
| BF | **0.97** | 0.59 | 0.87 | 0.73 |
| BN | **0.97** | 0.59 | 0.87 | 0.73 |
| SVDD | 0.95 | 0.21 | 0.76 | 0.34 |
| IF | 0.51 | 0.13 | 0.70 | 0.20 |
| GMM | 0.79 | 0.44 | 0.45 | 0.59 |
| PCA-SVD | 0.65 | 0.28 | 0.17 | 0.27 |

C. Feng, T. Li . Chana". "*Multi-level Anomaly Detection in Industrial Control Systems via Package Signatures and LSTM networks*", *DSN'17*.

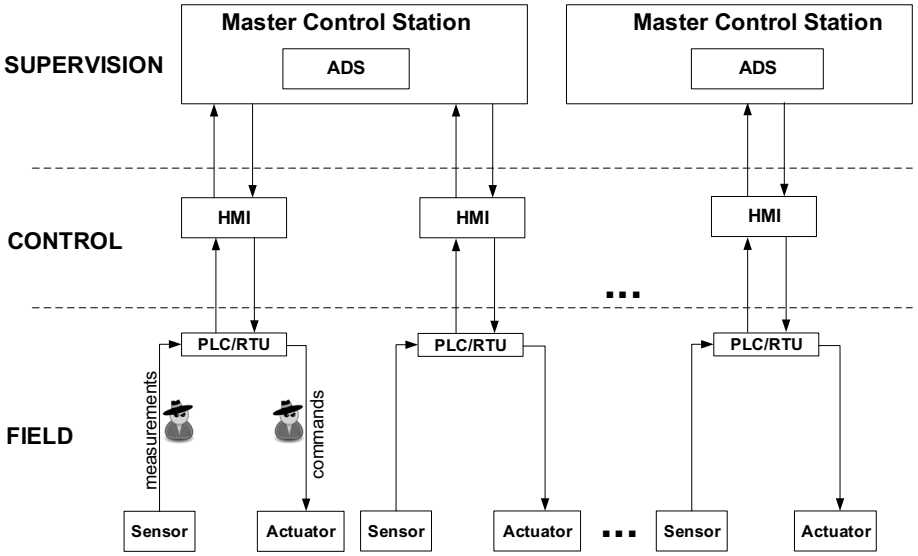
# Evasion Attacks

Originally discovered by researchers when trying to better interpret neural networks.




*Szegedy, Christian, et al. "Intriguing properties of neural networks." (2013).*

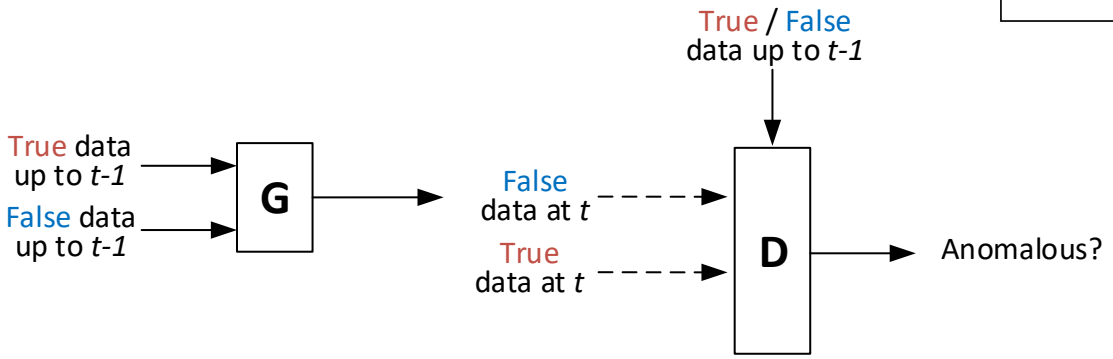
# Adversarial ML




*Monitoring signals*

| Attack Scenario | Ratio of goal achieved | Detected ratio | |
|---|---|---|---|
| | | by residual error | by CUSUM |
| 1 | 88.1% | 2.6% | 0.2% |
| 2 | 86.0% | 2.4% | 0.1% |
| 3 | 85.9% | 1.1% | 0.01% |
| 4 | 90.5% | 1.2% | 0.01% |

| Compromised Channels | Successful Ratio | |
|---|---|---|
| | by residual error | by CUSUM |
| Only PLC-AIT202, PLC-AIT203 | 90.1% | 93.8% |
| all channels | 92.4% | 94.6% |



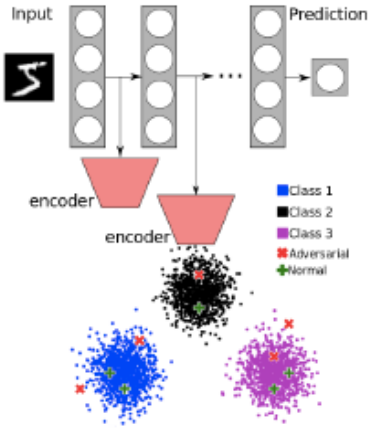

Cheng, Li and Chana

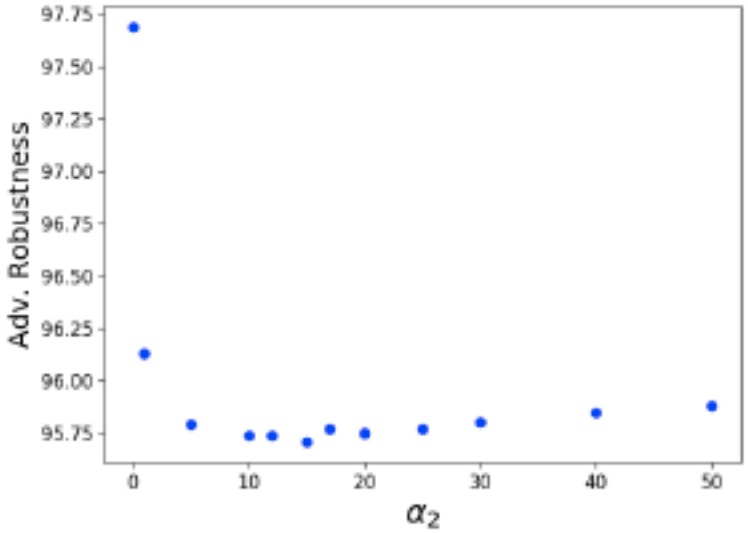
# Defences

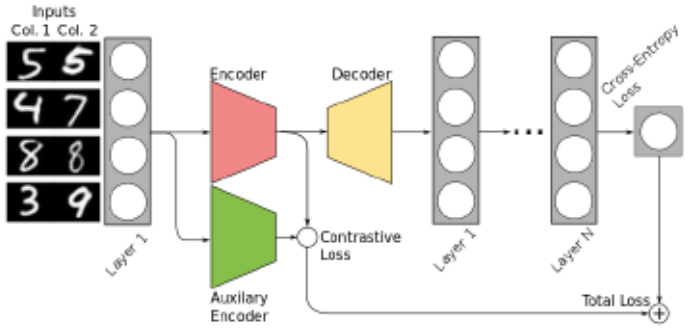
- Many defences proposed, no clear silver bullet:
  - Adversarial Training
  - Defensive Distillation – use information from training points to make the classifier model more robust to perturbations
  - Feature Squeezing – reduce degrees of freedom in feature input spaces
  - Neural Network Uncertainty – confidence and uncertainty for inputs
  - And many more…

# Deep Latent Defence

- Feed-forward Nets
- Lower dimensional latent space created by encoder.
- Classes clustered.
- K-nn algorithm to compare training data embeddings to test-time samples.
- Combined with adversarial training




Adversarial Machine learning Beyond the Image Domain, Zizzo, Hankin, Maffeis, Jones, DAC 2019

# The RITICS Programme

RITICS

NIS Directive – baseline, barriers, impact

Safety and Security

Autonomous Systems

Incident Response and Forensics

Cyber Controls

Interconnected Systems

Supply Chain

# NIS Directive

RITICS

How many shades of NIS: Understanding Organisational Cybersecurity and Sectoral Differences - Bristol

Effective Solutions for the NIS Directive: Supply Chain Requirements for Third Party Devices - Birmingham

Establishing a Scientific Baseline for Measuring the Impact of the NIS Directive on Supply Chain Resilience - Glasgow

# Second Call

AIR4ICS: Agile Incident Response For Industrial Control Systems – DMU

Cloud-enabled Operation, Security Monitoring, and Forensics (COSMIC) – QUB

Developing Pedagogy to Optimise Forensic Training in Safety-Related Industrial Control Systems (ICS) – Glasgow

Interconnected safe and secure systems ($IS^3$) - City

Thank you

ritics.org

c.hankin@imperial.ac.uk