This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Protection Against Cyber-Attacks: Introducing Resilience for SCADA Networks

Dr. Antonios Gouglidis
a.gouglidis@lancaster.ac.uk

Lancaster University

Symposium on Innovative Smart Grid Cybersecurity Solutions
Vienna, Austria, 13th-14th March, 2017

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Outline

- *Cyber-Attacks on Critical Infrastructures*
- *Resilience Strategy*
- *Resilience for SCADA networks*
  - *Resilience Policies & Resilience Architecture*
- *Results & Questions*

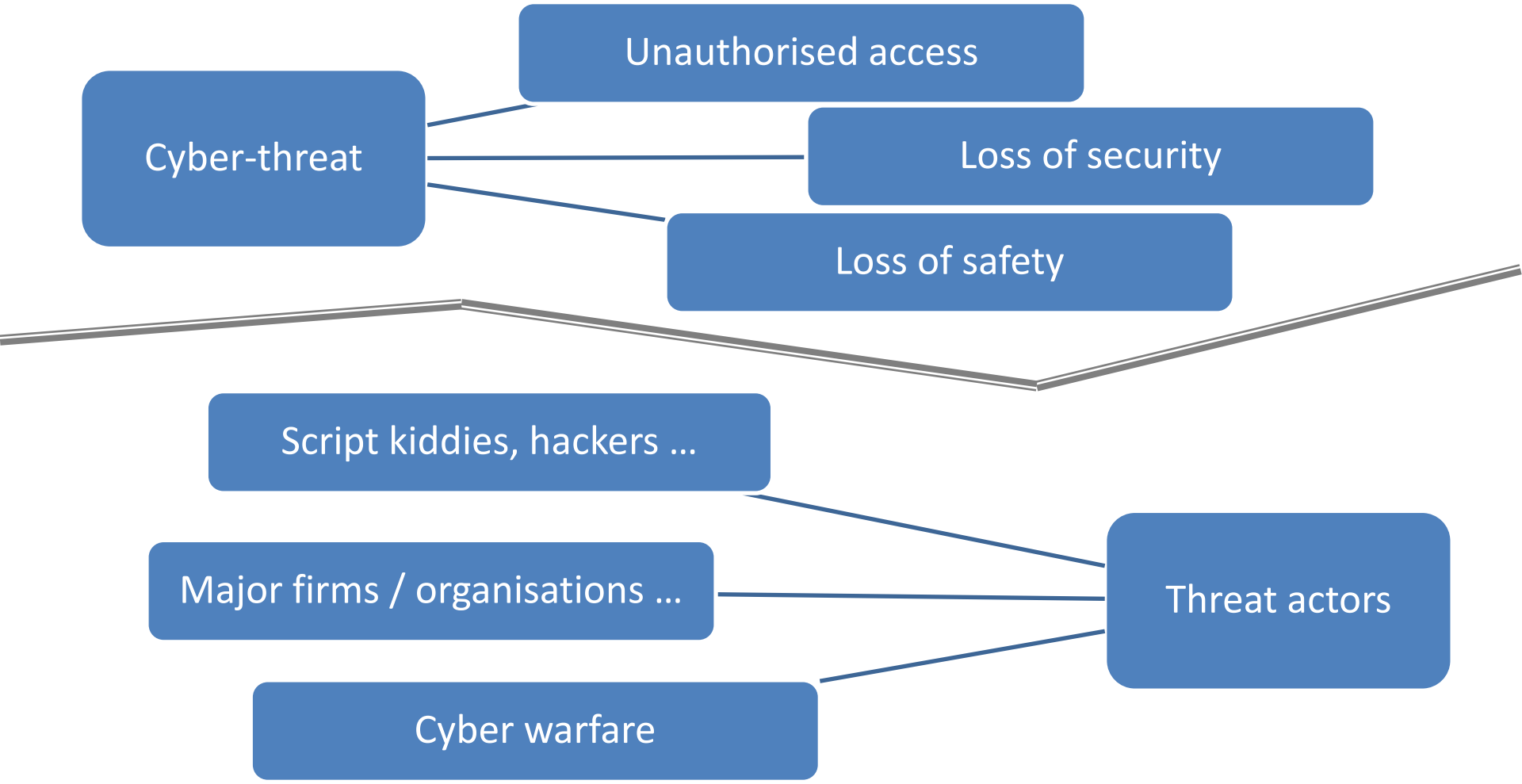
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Cyber-attacks on Critical Infrastructures

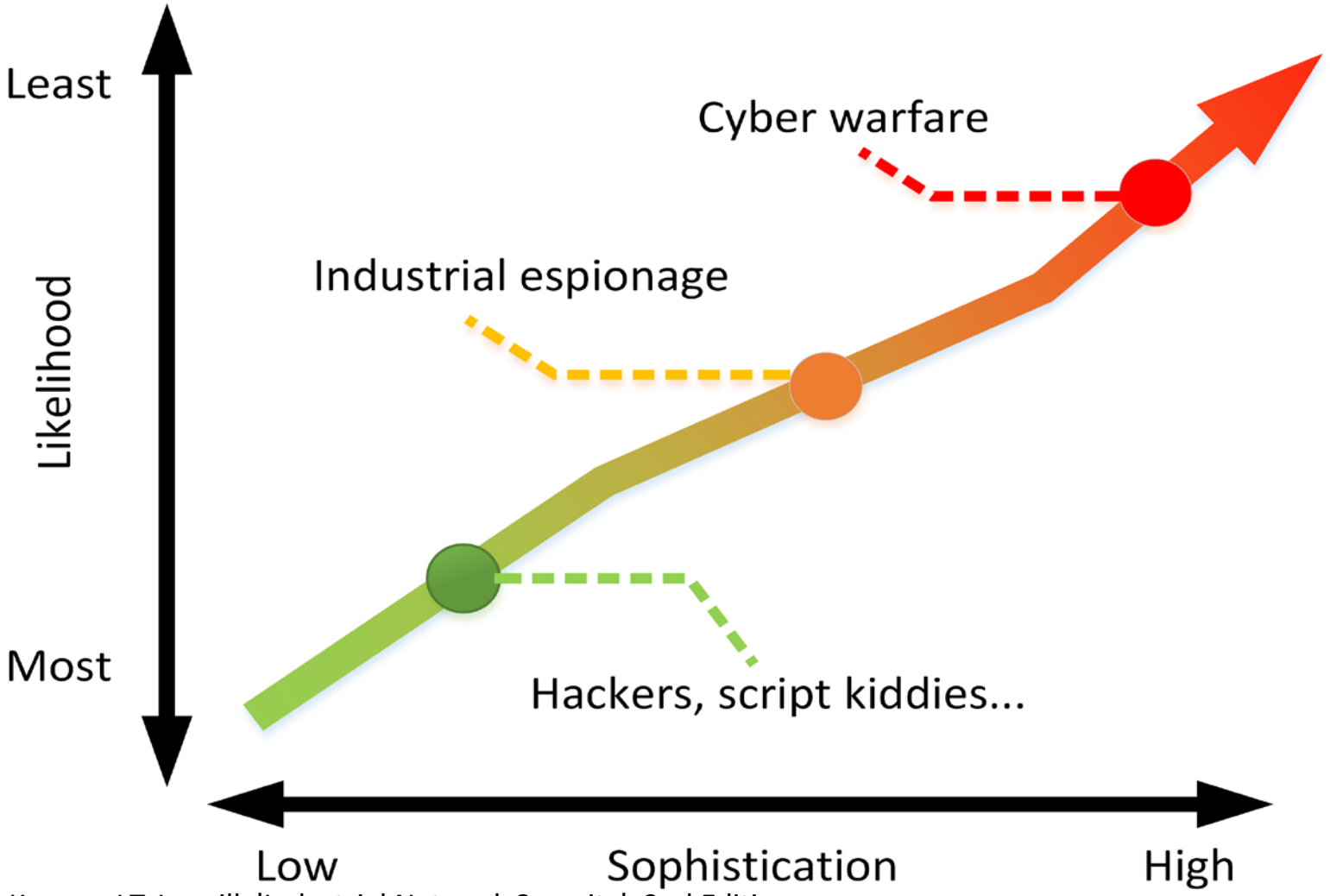
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Cyber-threats & actors to CI



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

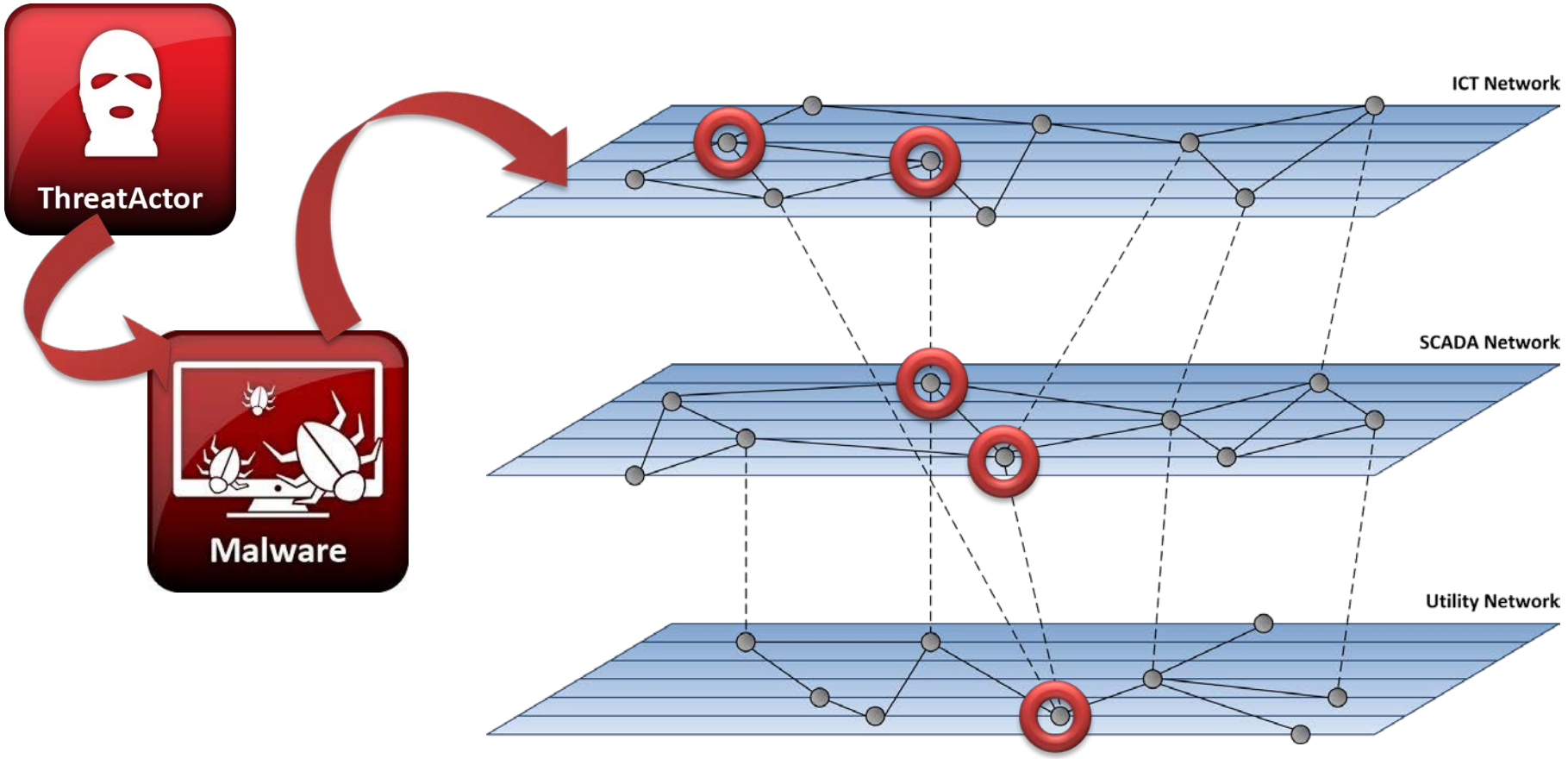
Likelihood vs. consequence*



* E. Knapp, J.T. Langill, 'Industrial Network Security', 2nd Edition

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Attack vectors



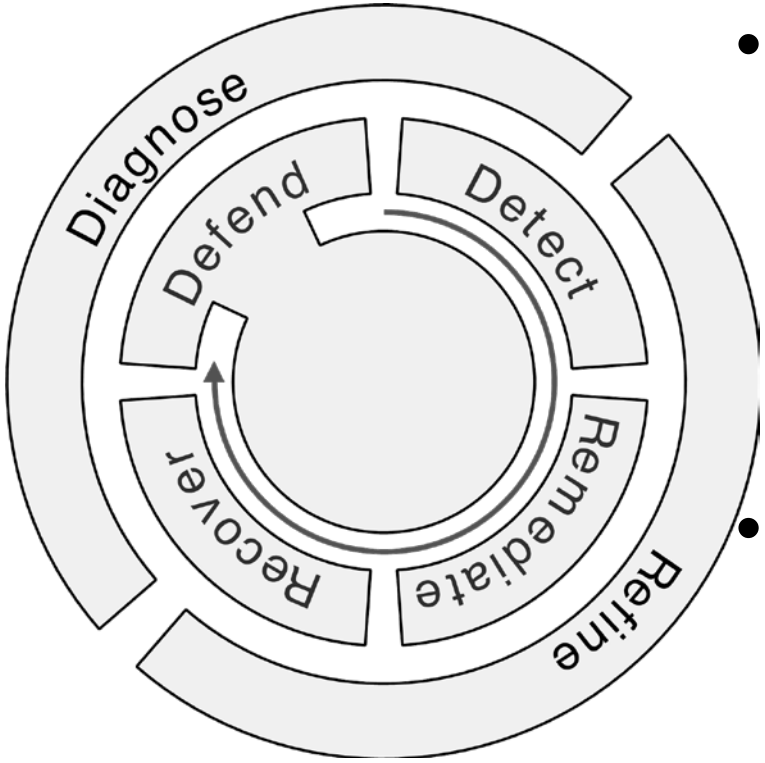
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Resilience Strategy

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Resilience and ways of achieving it…

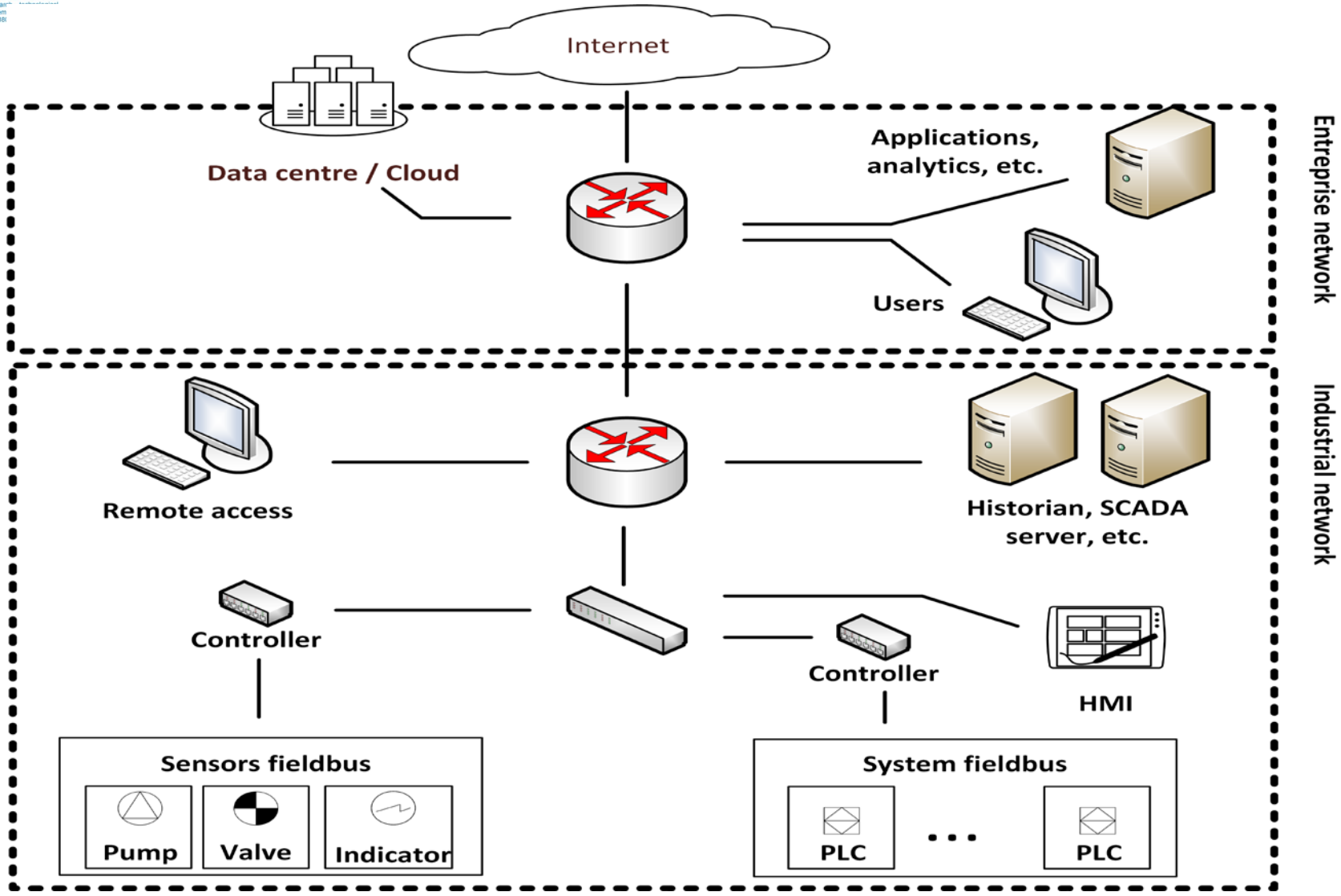


Resilience strategy

- *'… the ability of a network/system to defend against and maintain an acceptable level of service in the presence of challenges.' **
- D^2R^2+DR
  - Real-time control (internal) loop
  - Background (external) loop

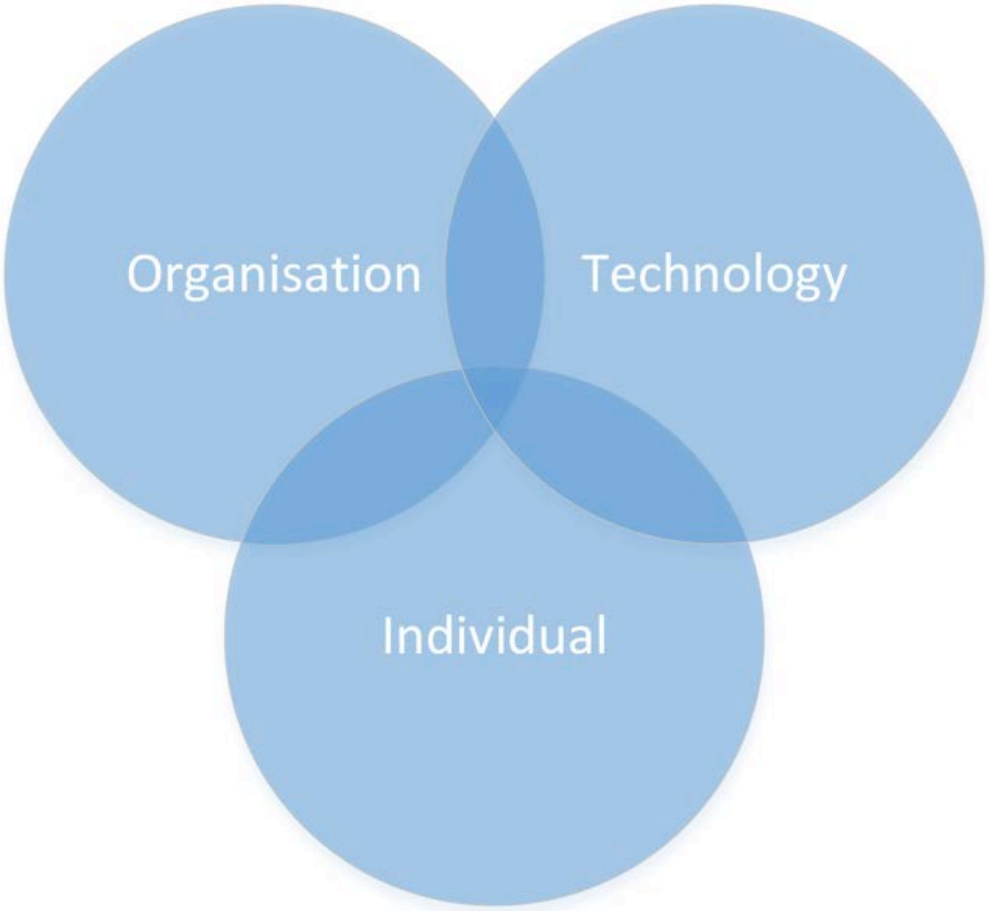
* J. Sterbenz, D. Hutchison, et al. 'Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines.' Computer Networks 54.8 (2010): 1245-1265.

Common network architecture



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Viewpoints for critical infrastructures



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

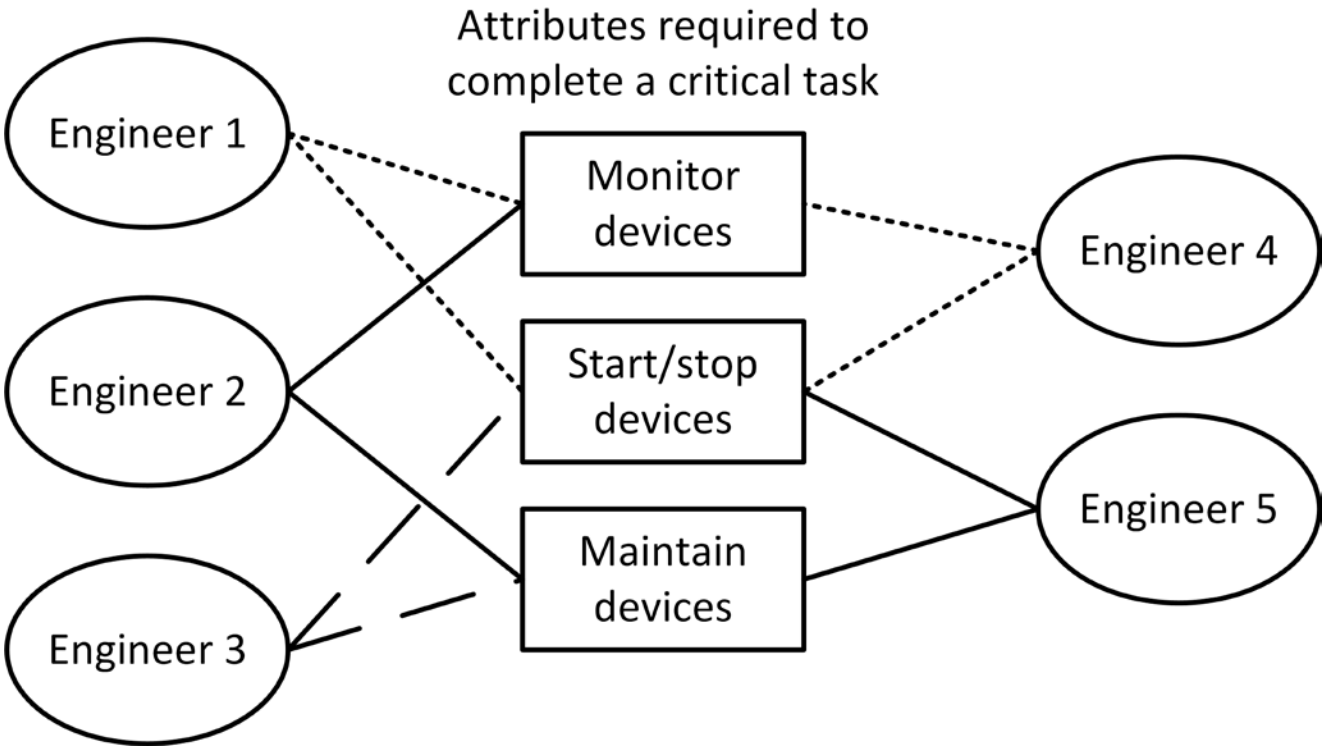
HyRiM

Resilience in Access Control Policies

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Resilience policies

Resilience in access control is the ability of a system not to restrict, but to enable access



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Resilience policies – tool chain

HyRiM

Access control policy tool (ACPT)

NIST

Model in NuSMV

+

Resilience specifications

NuSMV model checker

Detected resilience violations

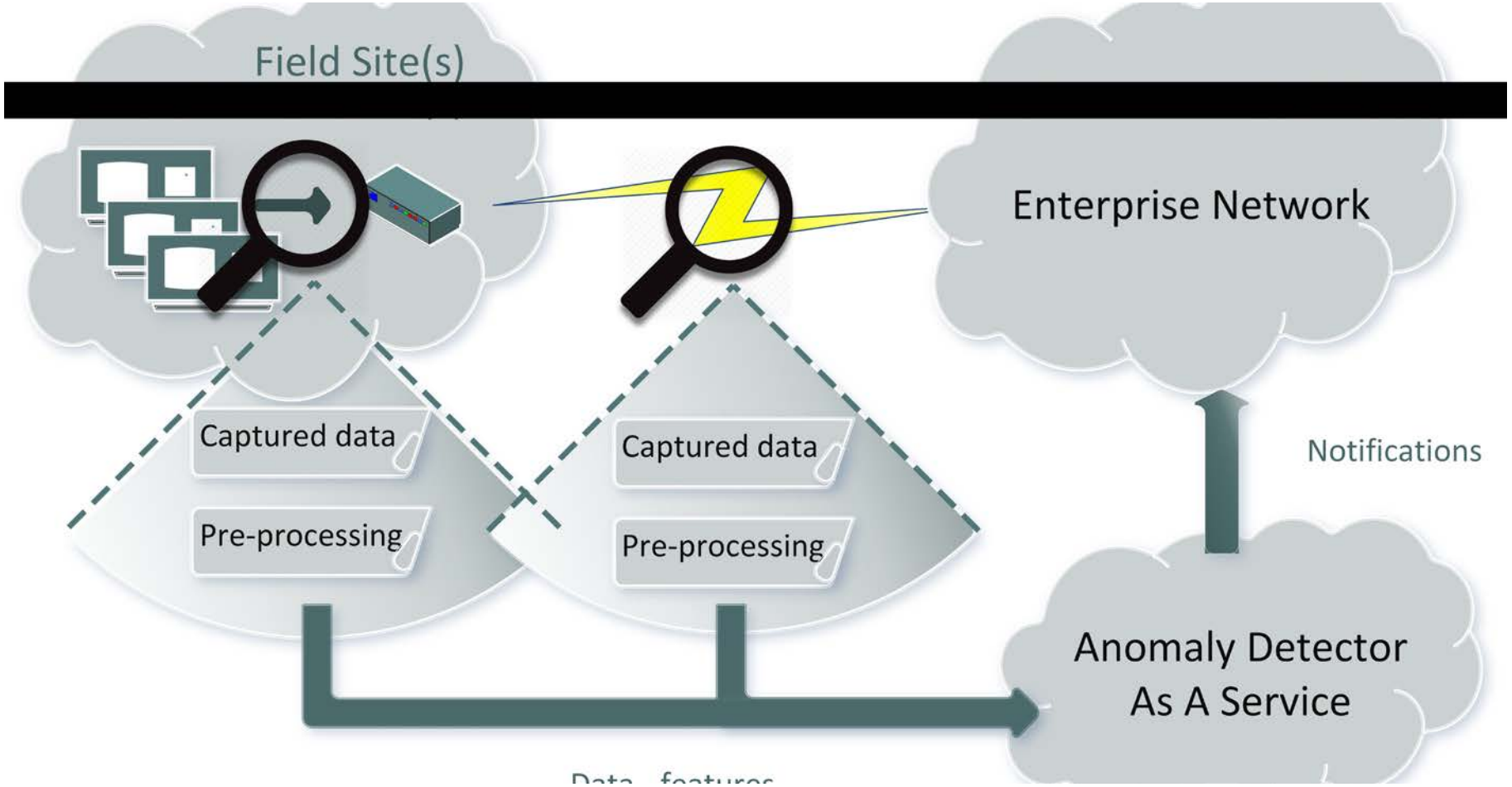
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Resilience Architecture for CI

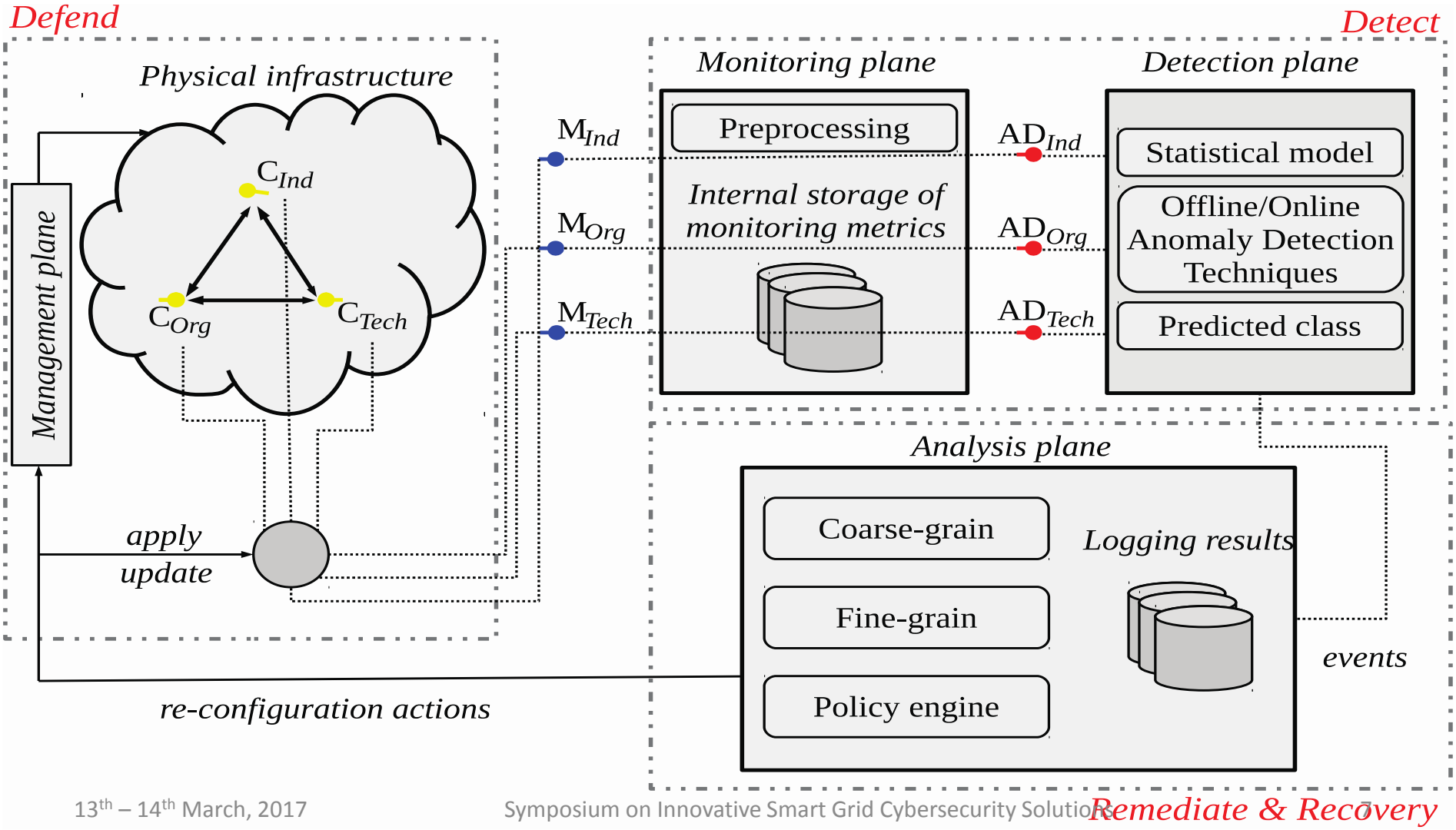
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Anomaly detection framework



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Resilience architecture



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Results and Discussion

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

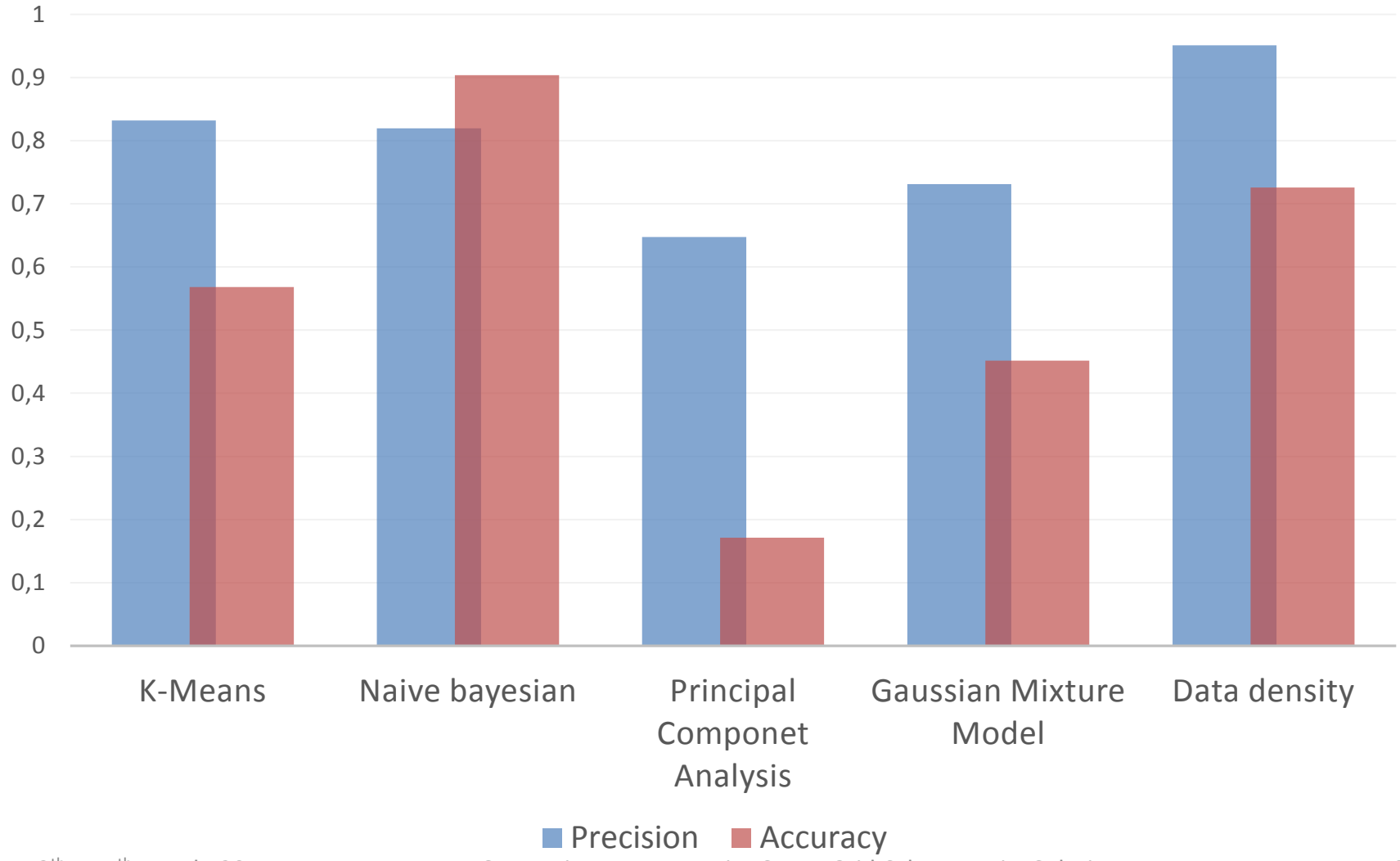
Evaluation of SCADA attacks

HyRiM

- Dataset: '*Morris, T., Thornton, Z., Turnipseed, I., Industrial Control System Simulation and Data Logging for Intrusion Detection System Research. 7th Annual Southeastern Cyber Security Summit. Huntsvile, AL. June 3 - 4, 2015.*'
- Gas pipeline log, captured in a laboratory environment, including:
  - Normal operation
  - Cyber-attacks
    - Reconnaissance
    - Denial-of-Service
    - Command injection

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

Comparison of techniques



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Questions?

Protection Against Cyber-Attacks: Introducing Resilience for SCADA Networks

Dr. Antonios Gouglidis
a.gouglidis@lancaster.ac.uk

Lancaster University

Symposium on Innovative Smart Grid Cybersecurity Solutions
Vienna, Austria, 13th-14th March, 2017