CYBER RANGE CASE STUDY: RESEARCH

Computer Security Incident Response and Analysis for Nuclear Facilities

Michael T. Rowland[1], Mislav Findrik[2] and Paul Smith[2]

[1] IAEA (M.T.Rowland@iaea.org)

[2] AIT Austrian Institute of Technology (mislav.findrik@ait.ac.at | paul.smith@ait.ac.at)

CRPJ02008 AND THE SIREN PROJECT

- Technologies for Ensuring Safe and Secure Incident Response Strategies for Nuclear Facilities

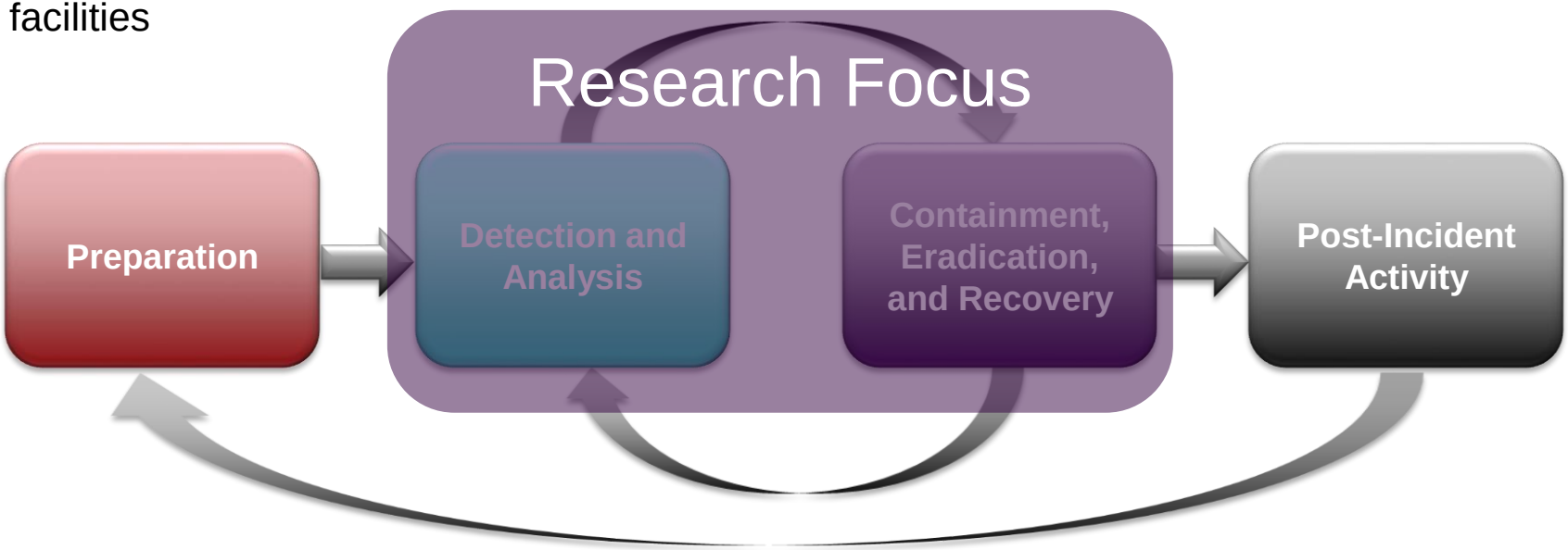
- **The Basics**
  - A project supported by IAEA CRP: Enhancing Computer Security Incident Analysis and Response Planning at Nuclear Facilities (CRP J02008)
  - Started end of November 2016
  - Expected duration: 3 years

- **Overall Goals**
  - Provide insights into how novel security technologies and processes can enhance computer security incident response
  - Support the safe and secure design and operation of industrial control systems (ICS) for nuclear facilities

CRP J02008 INSTITUTIONS

INCIDENT RESPONSE

The ability to detect and resolve problems that threaten people, process, technology and facilities



Paul Cichonski, Tom Millar, Tim Grance, Karen Scarfone, “Computer Security Incident Handling Guide,” NIST Special Publication 800-61 R2, August 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2

AIT INCIDENT RESPONSE AND ANALYSIS SOLUTIONS

Automatic Event Correlation for Incident Detection

- Monitors system events, their dependencies and occurrence, learns normal system behaviour, and detects anomalies

- **Example Research Questions:**
  - How do logging policies affect detection performance?
  - How can ÆCID be used in combination with other detection systems?
  - How can operators act upon alerts from detection systems?

Collaborative Analysis Engine for Situational Awareness & Incident Response

- Integrated framework to enable organizations to consume and efficiently apply threat intelligence

- **Example Research Questions:**
  - What information should be shared between operators?
  - How is this achieved in a secure and trustworthy fashion?
  - How can operators act upon threat intelligence that is derived from CÆSAIR?

DETECTION UNCERTAINTY

AVG

Antivirus Business

During July and August 2017 we continuously evaluated 14 endpoint protection products using settings as provided by the vendor. We always used the most current publicly-available version of all products for the testing. They were allowed to update themselves at any time and query their in-the-cloud services. We focused on realistic test scenarios and challenged the products against real-world threats. Products had to demonstrate their capabilities using all components and protection layers.

	July	August	Industry average
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 198 samples used	100%	99.0%	100%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 10,793 samples used	99.2%	99.2%	99.9%
Protection Score		●●●●●	5.0/6.0

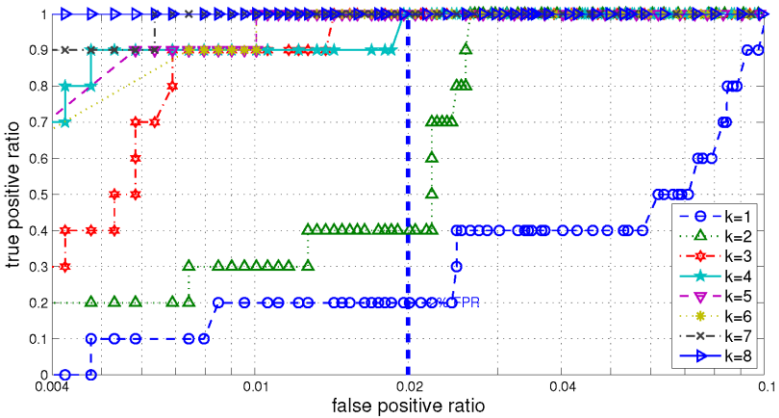
Source: AV Test (https://www.av-test.org/)

Detection systems can fail to identify malicious behaviour

(False Negatives)

Detection systems can incorrectly identify normal behaviour as malicious

(False Positives)

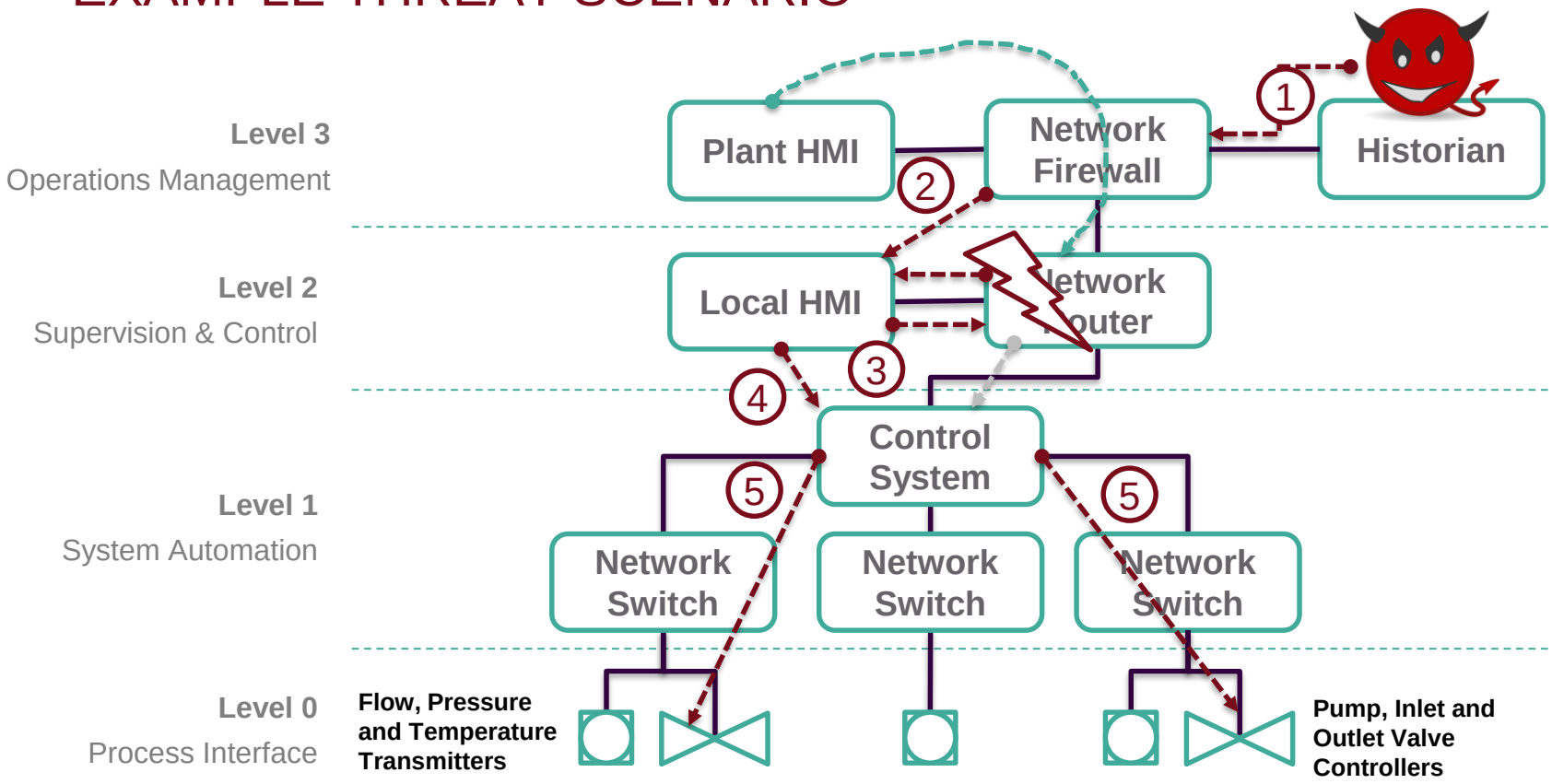


REASONING WITH UNCERTAINTY: EVIDENTIAL NETWORKS

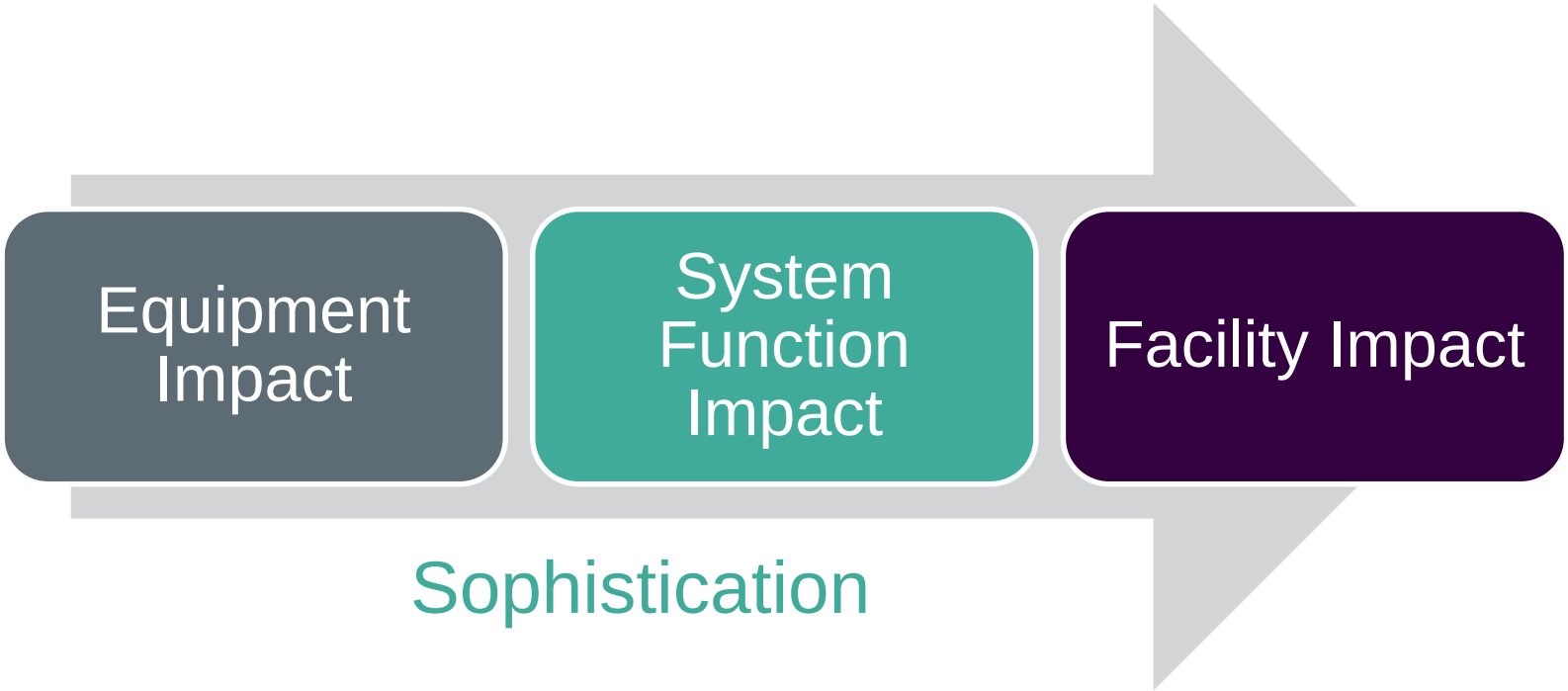
- An **evidential network** is a graph structure for knowledge representation and inference
- Nodes in the graph represent **variables**, e.g.:
  - Control system state
  - HIDS and NIDS alarms
- Variables have a **frame** that defines their mutually exclusive values
- Relations between variables are given as **mass functions** that describe beliefs
- **Dempster Shafer (DS) theory** allows relation implication rules with uncertainty measures
- Inference within the evidential network is achieved by two operators, called **combination** and **marginalisation**

P. P. Shenoy, A valuation-based language for expert systems, International Journal of Approximate Reasoning, Vol. 3, pp. 383–411, 1989.

EXAMPLE THREAT SCENARIO



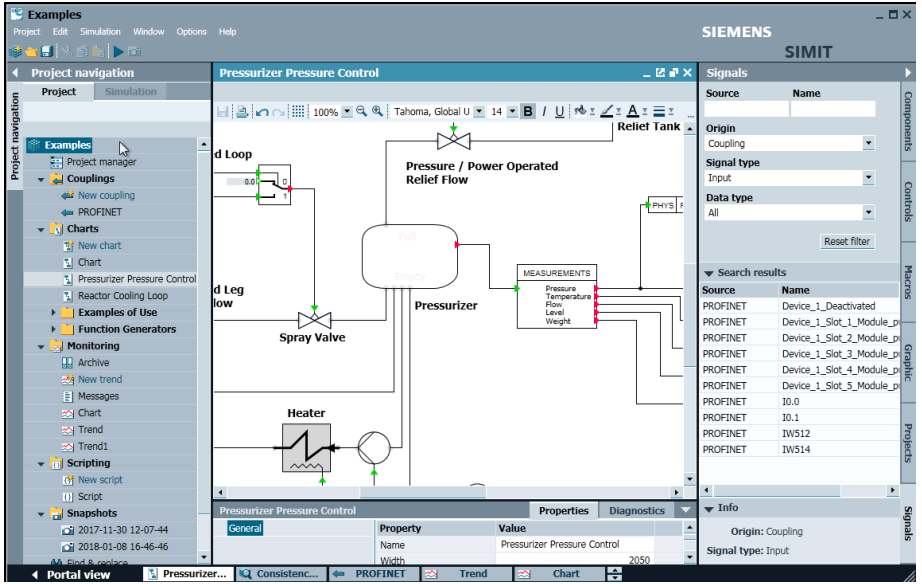
CYBER-ATTACK EFFECTS



ANALYSING SYSTEM FUNCTION IMPACT ON THE CASTLE CYBER RANGE

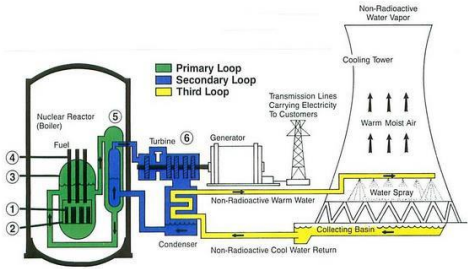
AUSTRIAN INSTITUTE OF TECHNOLOGY

- Developing a hardware-in-the-loop simulation of a pressurizer, part of the primary cooling loop
- Siemens S7 400 PLC interfacing with the Siemens SIMIT simulation framework



TOWARDS FACILITY IMPACT ANALYSIS: THE ASHERAH NUCLEAR FACILITY MODEL

- Develop a model of a hypothetical **Pressurized Water Reactor** (called Asherah), to allow for research testing of the effects of cyber-attacks
- This model will support the **Primary, Secondary, and Tertiary** (Third) cooling loops of a technology neutral facility
- **Real control equipment** (Siemens, ABB, Rockwell) can be interfaced with the model to determine the consequences of sabotage resulting from the exploitation vulnerabilities resulting in loss of Confidentiality, Integrity, and Availability (CIA)
- Informs the development of computer security measures to prevent and protect against cyber-attacks on this equipment and systems (PWR cooling loops)



CONCLUSION AND NEXT STEPS

- Cyber-attacks are increasingly targeting critical infrastructures, such as nuclear facilities, with the aim of causing operational consequences
  - Operators need to perform incident response, including detecting and analysing the consequences of cyber-attacks
  - IAEA CRP J02008 and The SIREN project are investigating technologies and processes to support operators perform incident response in facilities
- To evaluate new technologies and processes, representative scenarios need to be developed that can show system and facility level effects
  - Cyber range technology, which include hardware-in-the-loop simulations, can be used to analyse these effects
  - Ongoing work in the CRP is developing models of the Asherah facility model and interfacing it with hardware

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!