

# Advancements in Hardening the Cybersecurity Posture of Nuclear Power Plant Defence-in-Depth Network Architecture

International Conference on Nuclear Security (ICONS) 2020  
10-14 February 2020, Vienna, Austria

C. Neal<sup>1</sup>, D. Trask<sup>2</sup>, K. Thiyagarajan<sup>2</sup>, R. Doucet<sup>2</sup>, P. Adamson<sup>2</sup>,  
M. Daley<sup>2</sup>, J. Fernandez<sup>1</sup>

<sup>1</sup> *Polytechnique Montreal*

<sup>2</sup> *Canadian Nuclear Laboratories*



Canadian Nuclear  
Laboratories

Laboratoires Nucléaires  
Canadiens

**POLYTECHNIQUE  
MONTREAL**

TECHNOLOGICAL  
UNIVERSITY



# Introduction

- Nuclear Power Plants (NPPs) increasingly rely on digital devices
  - Information Technology (IT)
  - Operational Technology (OT)
- Integrated IT/OT environments are complex and are susceptible to having cybersecurity blindspots
- Canadian Nuclear Laboratories (CNL) is continuously developing a Cyber Range to assess the impact of attacks against NPP process controls

# Nuclear Power Plant Cybersecurity

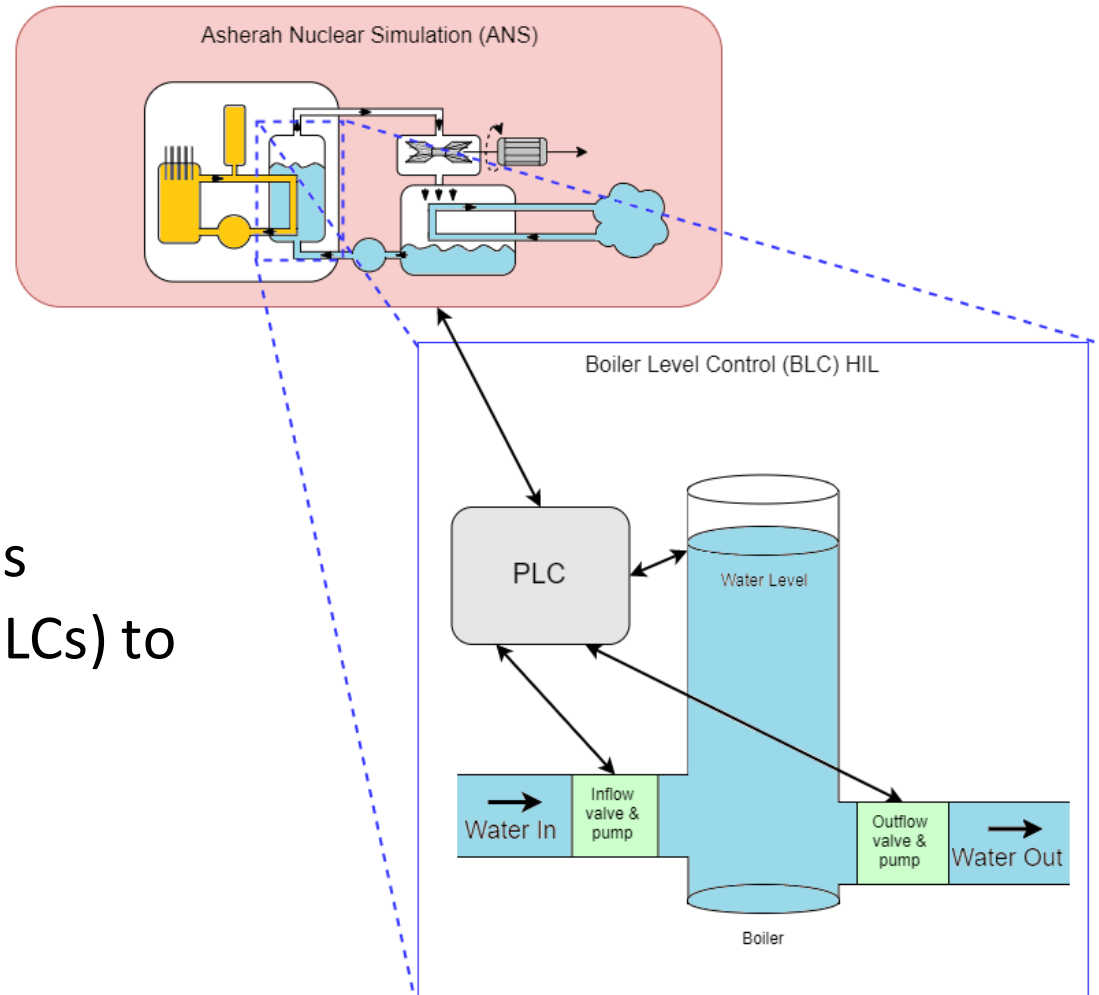
- Defence-in-Depth Architecture

Level 1	Level 2	Level 3	Level 4	Level 5
Reactor Protection Systems	Operational Control Systems	Real Time Supervision Systems	Technical Data Management Systems	Business Supporting Systems

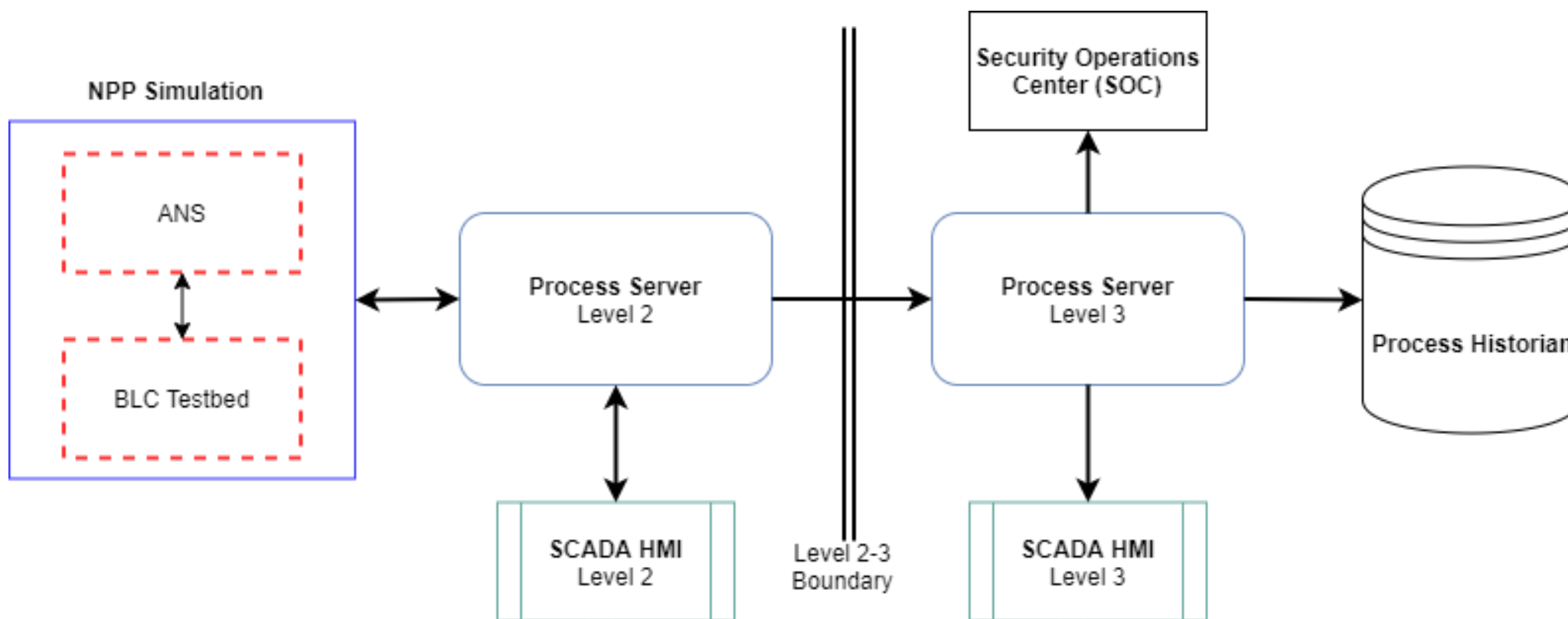
- Threat Model
  - Adversary aims to infiltrate Level 2 and disrupt NPP processes

# Boiler Level Control (BLC) Cyber Range

- Hardware-in-the-Loop (HIL)
  - Matlab simulation of NPP dynamics
  - Programmable Logic Controllers (PLCs) to control a down BLC system



# IT/OT Integrated Cyber Range



# Cyberattack Scenarios

- CNL hosted an IAEA Agency Mission in support of CRP J02008
  - "Enhancing Computer Security Incident Analysis at Nuclear Facilities"
  - 8-12 July 2019
- Conducted attacks against PLCs to interfere with NPP processes
  - Man-in-the-Middle (MITM)
  - Exploits to known vulnerabilities
- Incident response exercise

# Conclusion

- Threat landscape is continually evolving
- CNL Cyber Range is being used to develop and experiment with state-of-the-art defensive technologies and techniques
- Future work
  - Data-driven detection techniques
  - Incident response using IT/OT integrated security tools

Thank you