NetWare 2024 & SocSys 2024

PANEL #1

Navigating the Challenges in Security and Safety of Cyber-Physical Systems

Panel #1

NICE
FALL 2024

Moderator

Salvatore Vella, CEO Toogood Ventures Inc. & doctoral student, Toronto Metropolitan University, Canada

Panelists

Prof. Dr. Annabelle Mercier, University Grenoble Alpes - Laboratoire LCIS, France
Prof. Dr. Hiroki Takakura, National Institute of Informatics, Japan
Prof. Dr. Alexander Lawall, IU International University of Applied Science, Deutschland
Assoc Prof. Dr. Livinus Obiora Nweke, Noroff University College - Oslo, Norway
Dr. Svetlana Boudko, Norwegian Computing Center in Oslo, Norway

Chair Introduction

NICE
FALL 2024

Salvatore Vella
Toronto Metropolitan University

Cyber-Physical Systems, such as autonomous vehicles, smart grids, and industrial control systems, integrate physical components with cyber technologies, making them increasingly critical to modern society. However, the interconnected nature of CPS poses significant challenges to security and safety, as vulnerabilities in either the cyber or physical domain can impact the overall system. This panel session will bring together experts to discuss emerging threats, safety concerns, and the complexities of securing CPS in an evolving technological landscape.

Chair Introduction

NICE
FALL 2024

Salvatore Vella
Toronto Metropolitan University

Challenges

- Heterogeneity and Complexity
- Lack of Security by Design
- Cyber-Physical Nature of Threats
- Real-Time Requirements
- Uncoordinated Changes
- Infrastructure Security Threats
- Information Security Threats
- And many others …

Chair Introduction

NICE
FALL 2024

Salvatore Vella
Toronto Metropolitan University

Requirements for Securing CPS

- Infrastructure Security
- Information Security
- Personnel Security
- Monitoring and Control
- Real-time adjustments and precision
- Robustness and reliability
- Utilization of feedback loops
- Safety-critical applications
- Standards and Regulations
- And many others …

Panelist Position

NICE
FALL 2024

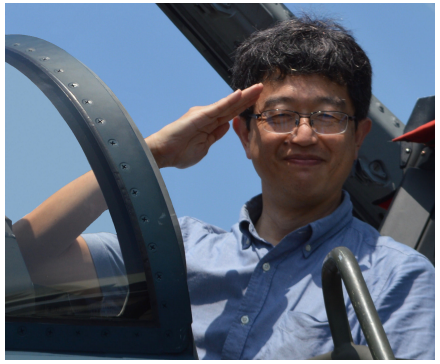
Annabelle Mercier

Université
Grenoble Alpes
LCIS Laboratory

- **Monitoring security for CPS seen as decentralized system**
  - **Open environment**
    - Devices can connect and disconnect freely
  - **Autonomy**
    - Local rules and behavior -> Emerging global behavior
  - **Architecture for monitoring communications**
    - Monitoring for detecting attacks
    - Distributed networks context
  - **Physical inputs of embedded systems**
    - Resources like battery level
    - Signal quality

Panelist Position

NICE
FALL 2024



Hiroki Takakura

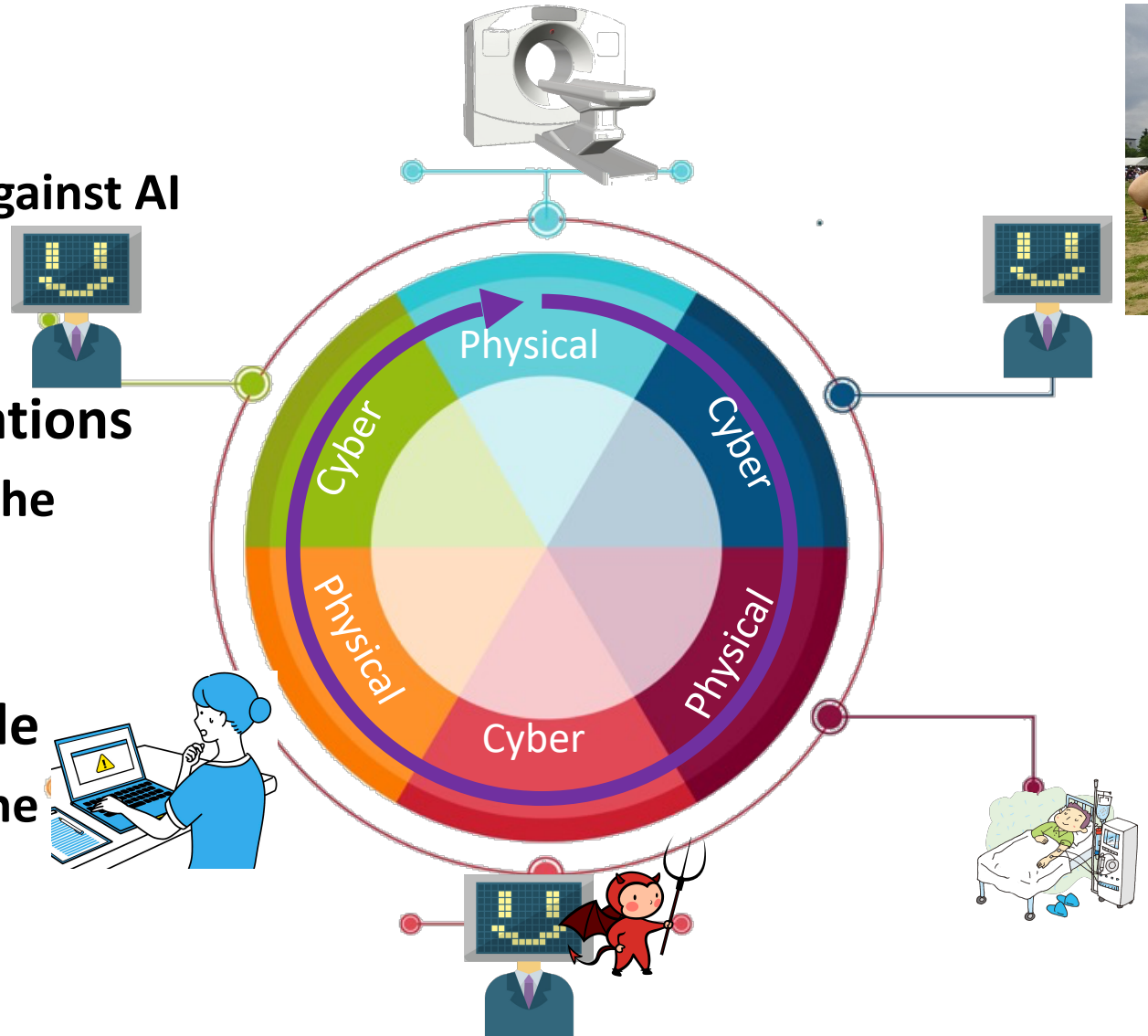
National Institute of Informatics

- A typical example of Cyber-Physical Systems…Medical
  - Sensors monitor your vital sign
  - Programs, including AI, investigate the monitored data
  - Programs judge the treatment for you
  - Medical devices are controlled based on the judgment
  - Effects, including side effects, are monitored by sensors

Panelist Position

NICE
FALL 2024

- Cyber attacks
  - Influencing Operations Against AI
  - Bugs
    - They affect recursively
- Detecting conflicting situations
  - Cross-checking is one of the countermeasures.
  - By AI and humans
- Breaking the negative cycle
  - Methods for mitigating the impact



Hiroki Takakura

National Institute of Informatics

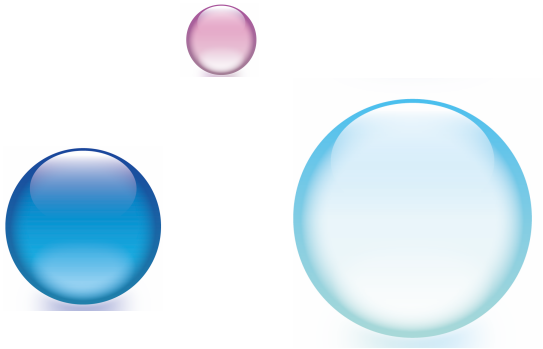
Panelist Position

NICE
FALL 2024

Hiroki Takakura

National Institute of Informatics

- Even if it is a rare case of disease, AI can teach you if there are documents related.
- AI cannot say, “I don't know.”
  - It's easy to answer the closest one
    - even if it is a cluster far away



- Collaboration with AI
  - We should understand AI’s limitation
  - AI is a good friend but not an omniscient master.

Panelist Position

NICE
FALL 2024

1. Cybersecurity in Cyber-Physical Systems (CPS)

Alexander Lawall

IU International University of Applied Science

- **Challenges**
  - **High vulnerability to cyberattacks in critical areas (e.g., healthcare, energy, autonomous vehicles)**
  - **Lack of universal security standards for CPS communication and data processing**
- **Focus on**
  - **Development of robust, attack-resistant security architectures**
  - **Real-time protection mechanisms with minimal system interference**
  - **AI-driven, self-learning cybersecurity systems for adaptive threat response**
  - **Enhanced resilience through autonomous, proactive security**

Panelist Position

NICE
FALL 2024

2. Real-Time Requirements and Reliable Decision-Making (with AI)

Alexander Lawall

IU International University of Applied Science

- **Challenges (i.e. Industry 5.0 with AI)**
  - Real-time response demands in autonomous vehicles, industrial machines, etc.
  - High computational requirements for rapid data processing and low latency
  - Good data quality for AI & Machine Learning for enhanced CPS performance and autonomy
- **Focus on**
  - Focus on deep learning & reinforcement learning applications
  - Faster, more accurate decision-making within CPS
  - Dynamic processing distribution with combined edge and fog computing
  - Multi-agent systems for reliable, autonomous decision-making in CPS

3. Interoperability and Standardization in CPS

Alexander Lawall

IU International University of Applied Science

- **Challenges**
  - **Complexity in integrating devices from multiple manufacturers**
  - **Inconsistent communication protocols across CPS environments (e.g., industrial, smart cities)**
- **Focus on**
  - **Security guidelines and standards (e.g., CRA, NIS2, ISO 27001, IoT Security, Cloud Security)**
  - **Development of open standards and protocols (e.g., OPC UA, MQTT)**
  - **Cross-manufacturer communication solutions for seamless integration**
  - **Authentication and Authorization between CPS**
  - **Self-organizing networks for automatic device adaptation and communication**

Panelist #1

Livinus Obiora Nweke
Noroff University College, Norway

- Associate Professor
  - Risk Assessment and Management
  - Interdisciplinary Collaboration and Workforce Training
  - Resilience and Recovery
  - Preparing for Future Trends: AI and Quantum Computing Impacts

Panelist Position

NICE
FALL 2024

Svetlana Boudko
Norwegian Computing Center

- Cyber-Physical Systems (CPS) in healthcare, such as remote monitoring systems, robotic surgery, and wearable health devices, are revolutionizing medical care
  - integrate computation, networking, and physical processes
  - provide efficient and personalized medical solutions
  - raise significant security and safety challenges

Key challenges in the security and safety of CPS in healthcare

- Data Privacy and Security
  - sensitive personal information and health records
  - secure data at rest, in use, and in transit
  - use robust encryption methods
  - implement secure authentication mechanisms
- Device and Network Security
  - devices (e.g. pacemakers or insulin pumps) can be hacked
  - ensure secure communication channels
  - regular software updates
  - vulnerability assessments
  - pen testing
- System Reliability and Availability
- Integration and Interoperability Issues
- Regulatory and Compliance Challenges
- Insider Threats
- Ethical and Social Implications

created by Copilot