JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

AI at the Core of Cyber-Physical Systems

Niko Mäkitalo
UNIVERSITY OF JYVÄSKYLÄ
12.09.2024

Topics

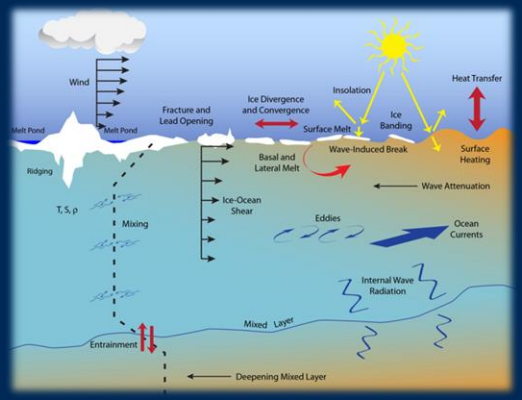
1. What are cyber-physical systems?
2. Current and future trends in cyber-physical systems
3. My research related to cyber-physical systems

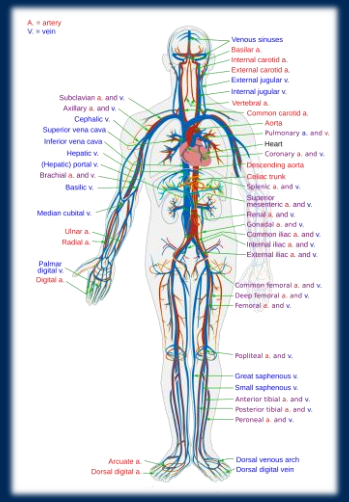
JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

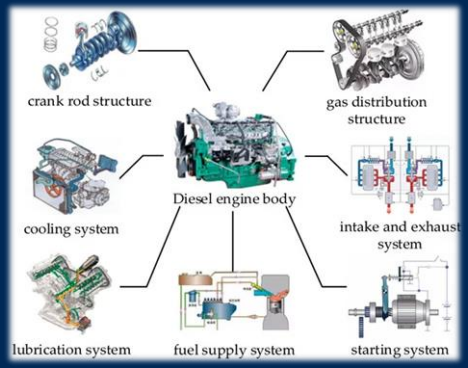
What are Cyber-Physical Systems?

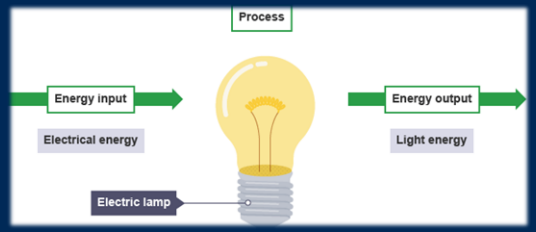
JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Physical World – And Its Infinite Number of Processes









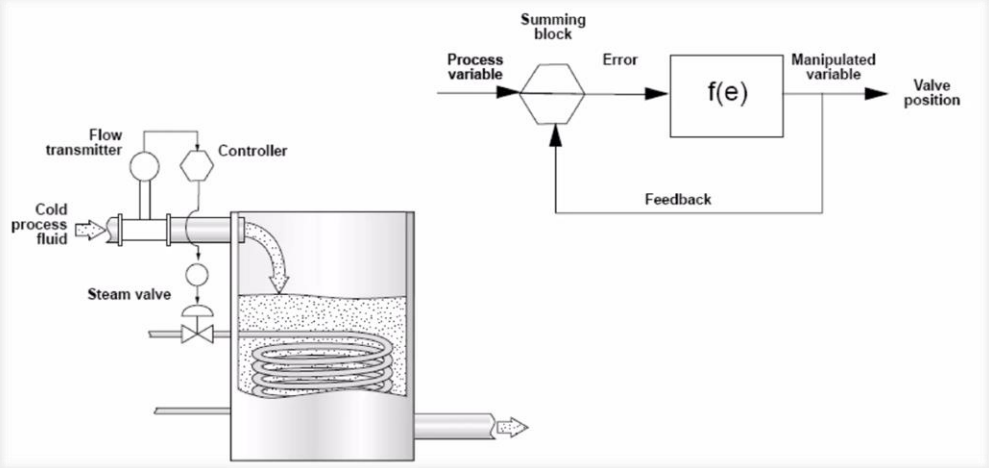
- Thinking world via processes
- The physical world consists of an infinite number of processes
  - Processes on very different scales
  - Processes can be highly complex
  - Processes can be nested
  - Processes are often linked to each others
  - Processes can have side effects

[1] Frederick, J. M., et al. (2016). The Arctic coastal erosion problem (No. SAND2016-9762). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).
[2] Wikipedia: https://en.wikipedia.org/wiki/Circulatory_system
[3] Liu Z, Zhang C, Dong E, Wang R, Li S, Han Y. Research Progress and Development Trend of Prognostics and Health Management Key Technologies for Equipment Diesel Engine. *Processes*. 2023; 11(7):1972. https://doi.org/10.3390/pr11071972
[4] BBC UK: https://www.bbc.co.uk/bitesize/guides/znr8nrd/revision/1

Harnessing the Processes

- **Process control:** In physics, the processes are analyzed and controlled via measures and variables

- **Process automation:**
  - The concept of CPS is broader and heavily more IT-oriented
  - Focus is not only on industrial processes
  - On the other hand, an automated industrial process is a CPS



An illustration of physics and control systems

Process Control Basics, Chapter 5. Online. https://www.slideshare.net/slideshow/process-controlpdf-254001923/254001923

The Concept of Cyber-Physical System

Concept of CPS

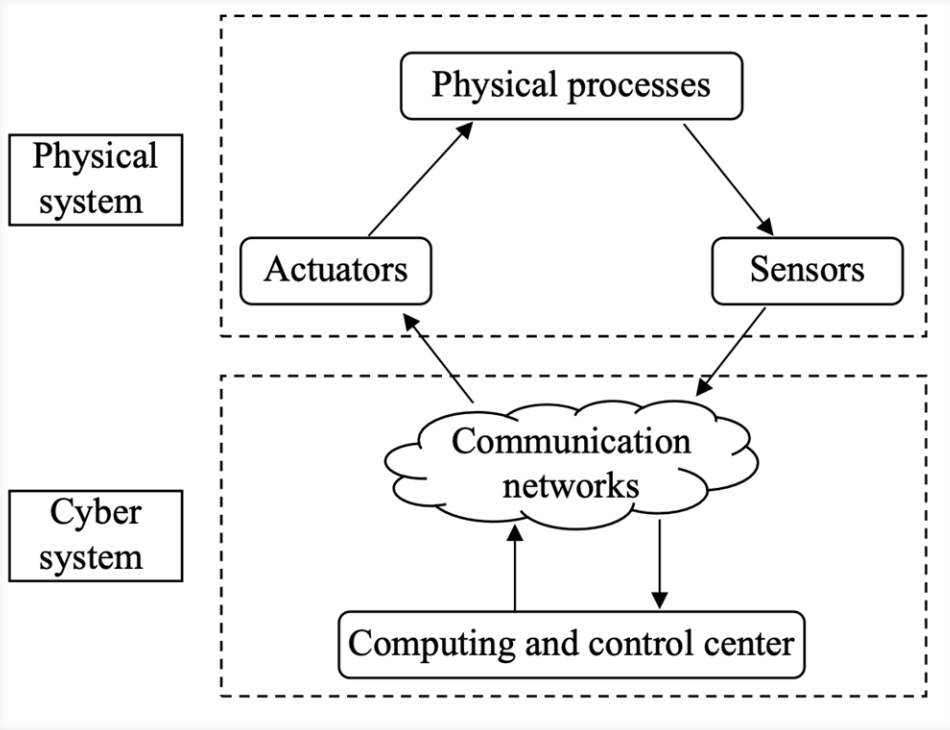
Cyber-Physical Systems (CPS) are interconnected systems that bridge the gap between physical elements and digital technologies. They enable real-time monitoring, control, and automation of physical processes through integrated computing systems.

Interactions in CPS

CPS involve the seamless integration of physical components with computational and network systems. This integration allows for real-time data exchange, decision-making, and control mechanisms to optimize operations.

Synergy of Cyber and Physical

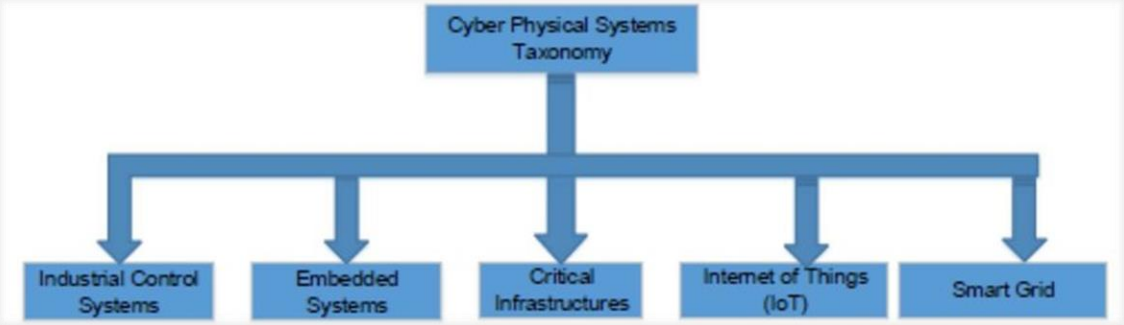
The integration of cyber and physical elements in CPS enables adaptive, responsive systems capable of autonomous functioning and intelligent decision-making, leading to enhanced performance and operational efficiency.



W. L. Duo, M. C. Zhou, and A. Abusorrah, "A survey of cyber attacks on cyber physical systems: Recent advances and challenges," IEEE/CAA J. Autom. Sinica, vol. 9, no. 5, pp. 784–800, May 2022.

Cyber-Physical Systems vs. the Internet of Things

- What is the difference between the Internet of Things and Cyber-Physical Systems?
  - Both are concepts names
    - It's about mental images!
  - CPS can be IoT system, and IoT system can be CPS
    - IoT is the main building block for a CPS
  - IoT: "Connecting physical objects to the Internet"



Yeboah-Ofori, Abel & Abdulai, Jamal-Deen & Katsriku, Ferdinand. (2018). Cybercrime and Risks for Cyber Physical Systems: A Review. 10.20944/preprints201804.0066.v1.

Cyber-Physical System: "An interface between physical world's processes and digital worlds processes"

Building Blocks of Cyber-Physical Systems

- **1. Physical Components**
  - **Sensors**: Measure physical quantities such as temperature, pressure, light, motion, etc. Sensors collect information from the environment or devices.
  - **Actuators**: Device components that perform physical actions, such as motors, valves, heaters, and other mechanisms that respond to changes measured by sensors.
  - **Computing**: CPS use digital processors and computers to analyze data, perform calculations, and make decisions in real-time. This can range from simple microprocessors to advanced cloud services.
- **2. Digital Components**
  - **Software**: Software enables implementing features to control, monitor, and manage the interactions between physical and digital components. This includes embedded software, real-time operating systems, and advanced algorithms for decision-making and control.
  - **Artificial Intelligence and Machine Learning**: These are used for data analysis, creating predictive models, and optimizing decision-making. AI can, for example, optimize processes and predict failures in systems.
- **3. Communication**
  - **Networking**: Physical and digital components are connected via data transfer protocols and networks. This includes connections between IoT (Internet of Things) devices, wireless networks, 5G connectivity, or industrial Ethernet networks.
  - **Communication Protocols:** CPS use communication protocols to enable reliable and secure data exchange between devices, sensors, networks, and other systems, ensuring coordinated operation and real-time response across distributed components.
- **4. Control Systems**
  - **Human-in-the-loop**: These regulate the operation of physical components based on information received from digital components. This can include feedback loops that ensure the system operates as intended.
  - **Autonomous Systems**: In more complex cyber-physical systems, control systems can be fully autonomous, making decisions and executing actions without human intervention.
- **5. Human-Machine Interfaces**
  - **Human-Machine Interfaces**: These allow users to interact with the cyber-physical system, monitor its operation, and make necessary adjustments. An HMI can be a graphical interface, a mobile application, or another interface that connects humans and machines.
- **6. Security and Privacy**
  - **Security Components**: These are necessary to protect systems from cyber threats. In cyber-physical systems that impact the physical world, security is particularly critical.
  - **Privacy Protection**: Data collection and processing may involve sensitive information that must be adequately protected.

Real-world Application Domains of Cyber-Physical Systems

Smart Grids

Smart grids leverage CPS to optimize energy distribution, monitor power usage, and enhance grid resilience. By integrating digital sensors and analytics, smart grids enable efficient energy management and support renewable energy integration.

Health Monitoring Systems

In healthcare, CPS applications include remote patient monitoring, wearable health devices, and personalized healthcare systems. These systems collect real-time health data, enabling predictive analytics and personalized treatment strategies.

Autonomous Vehicles and Machines

Autonomous vehicles utilize CPS technologies for navigation, communication, and decision-making processes. By integrating sensors, AI algorithms, and connectivity, autonomous vehicles enhance road safety, traffic efficiency, and passenger experience.

Smart Manufacturing

In the industrial sector, smart manufacturing systems optimize production processes, automate assembly lines, and improve quality control through CPS integration. These systems enhance productivity, reduce downtime, and enable real-time monitoring of manufacturing operations.

Future Trends and Innovation in CPS

Emerging Technologies

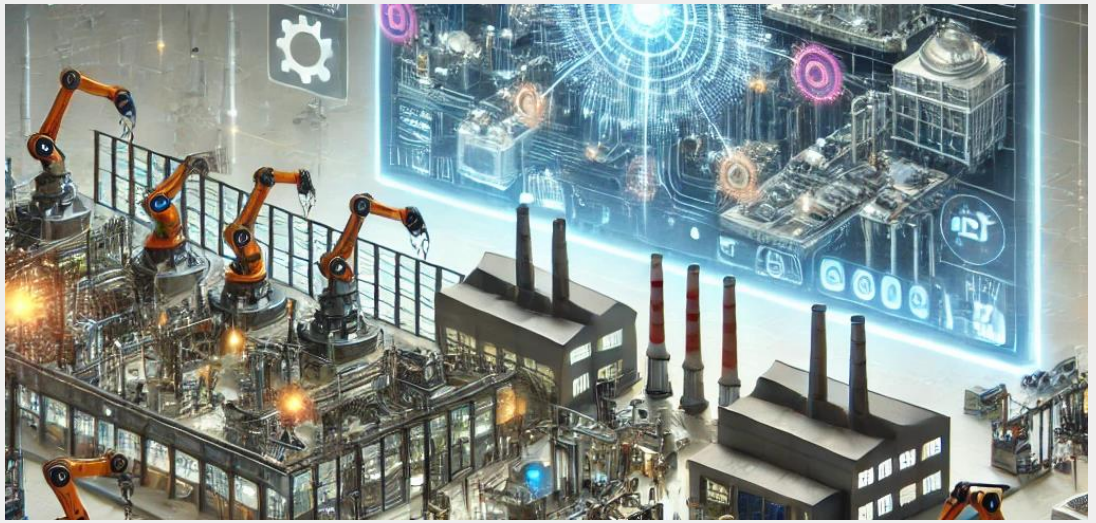
The future of CPS is shaped by emerging technologies such as AI, IoT, blockchain, and edge computing. These technologies advance the capabilities of cyber-physical systems, enabling autonomous decision-making, real-time analytics, and enhanced connectivity.

Industry 4.0 and 5.0 Revolutions

Industry 4.0 focuses on integrating CPS, automation, and data exchange to enhance productivity, customization, and sustainability in manufacturing. Industry 5.0 builds on this by emphasizing human involvement, where human creativity is complemented by AI, robotics, and automation.

Digital Twin Technology

Digital twin technology creates virtual replicas of physical assets, enabling real-time simulations, predictive maintenance, and data-driven insights. Together with AI, digital twins enhance operational efficiency, optimize resource utilization, and facilitate innovation in product development.



JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Challenges and Risks in CPS Deployment

Security

The deployment of CPS introduces cybersecurity vulnerabilities, including the risk of data breaches, system manipulation, and unauthorized access. Securing interconnected systems is essential to safeguard critical infrastructure and sensitive information. Addressing these challenges requires robust cybersecurity practices, standards, and continuous monitoring.

Operational Challenges

Challenges in CPS deployment include system complexity, interoperability issues, and ensuring resilience against contingencies. Addressing these challenges requires truly intelligent solutions that can help the systems to self-adapt.

Regulatory Compliance

Compliance with data protection regulations, industry standards, and cybersecurity best practices is crucial for mitigating risks in CPS deployment. Organizations must navigate regulatory frameworks to ensure ethical and secure implementation of cyber-physical systems.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Research Activities

My research on Cyber-Physical Systems

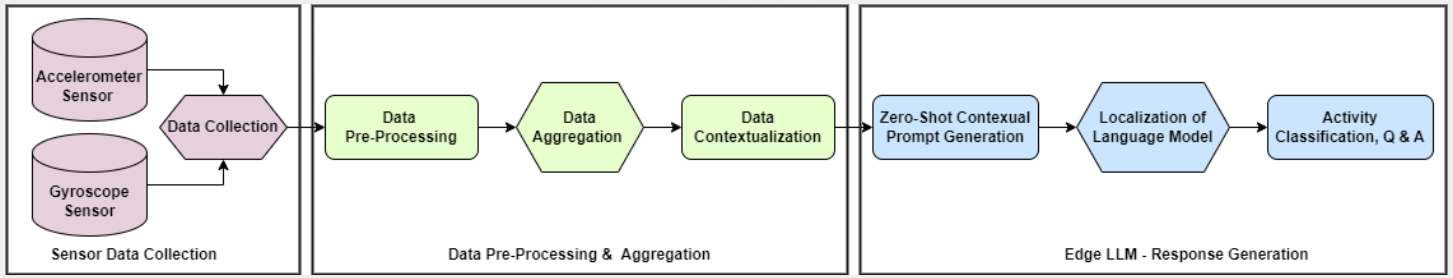
- History in cyber-physical systems research:
  - 2009 Nokia collaboration: How physical devices can share content and sensor information for easier access?
  - 2012 Social devices: How to make interactions with cyber-physical systems more natural for human?
  - 2016 PhD dissertation: How to program interactions with CPS?
  - 2017 Collective Execution: How physical objects around humans can collectively execute the same software instance?
  - 2020 Creative robotics: How heterogenous robots could creatively and autonomously collaborate?
  - 2021 Platform economy for robots: What kind of platform is required by companies implementing cyber-physical systems to make business?
  - 2023 Tenure track: AI-powered cyber-physical systems

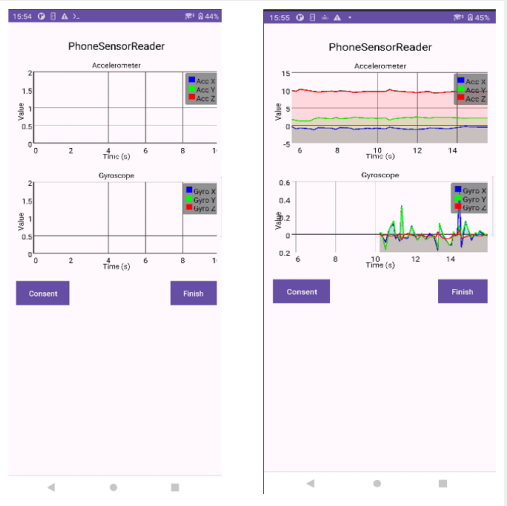
6G Software Project

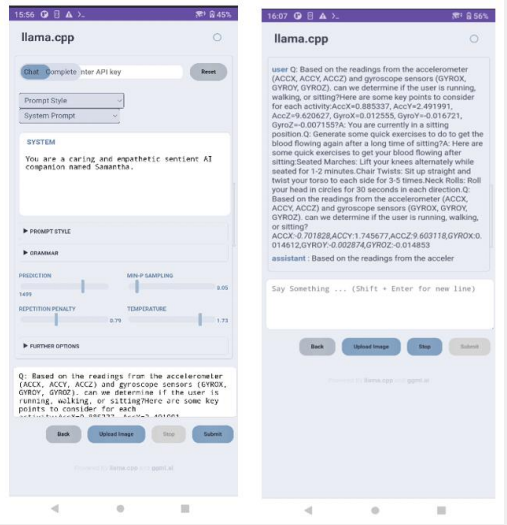
- **PROJECT:** 6G software for extremely distributed and heterogeneous massive networks of connected devices
- **COLLABORATORS:**
  - University of Oulu, LUT University, Tampere University and University of Jyväskylä
  - Bittium, Aidon, and Wirepas
- **GOALS:**
  - Study what future software means
  - AI in the core of the applications
  - Understand the what kind of infrastructure is required

Exploring LLMs at the Edge of the Network

- Exploring the LLMs at the edge with Android devices
- Prototype of sensor data processing
  - Detecting user's current activity
  - Current model Phi3 mini (SLM – "small language model")
  - Experimenting with different prompting techniques
- Early prototype
  - Currently under peer-review
- Work continues
  - Towards more advanced features and various multimodal LLMs
  - Truly decentralized approach – Running LLMs are offloaded within the network







JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Liquid AI project

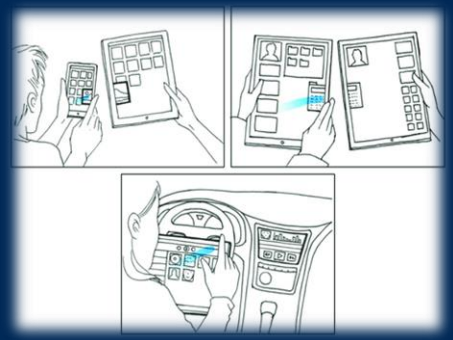
PROJECT: Liquid AI for 6G software

COLLABORATORS:

- Tampere University and University of Jyväskylä
- Nokia Bell Labs, Sitowise, Silo AI

GOALS:

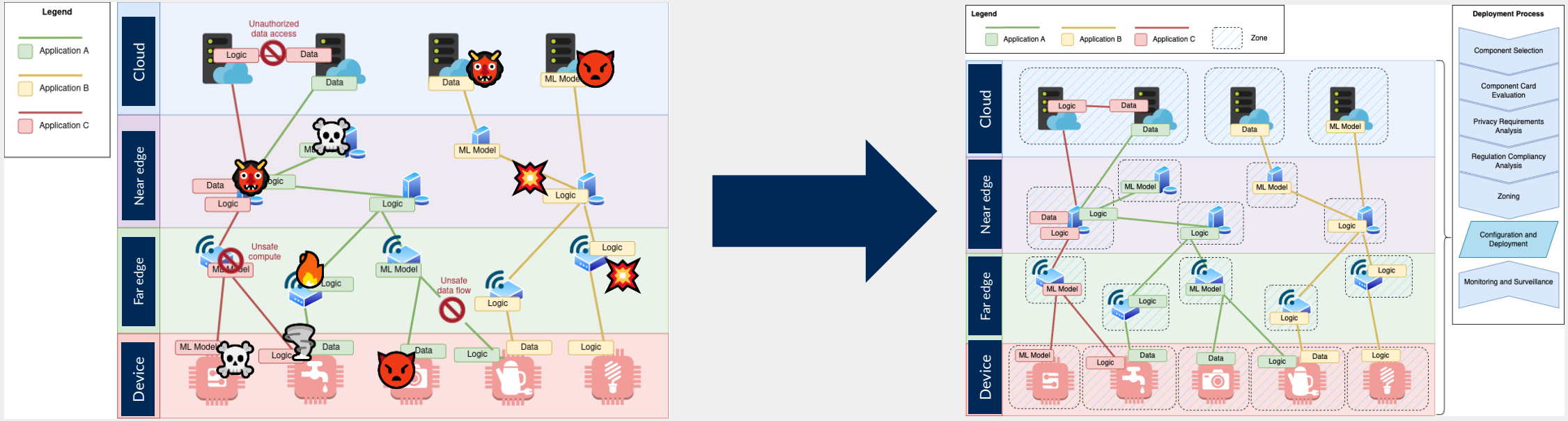
- Study portable ML models in the context of IoT by proposing “liquid” IoT architectures.
- Portability enables deploying applications closer where the data is, improving security, privacy, as well as performance.



Typical example of liquid software

[1] Taivalsaari, A., & Mikkonen, T. (2015). From apps to liquid multi-device software. *Procedia Computer Science*, *56*, 34-40.

The Programmable World and Its Emerging Privacy Nightmare!



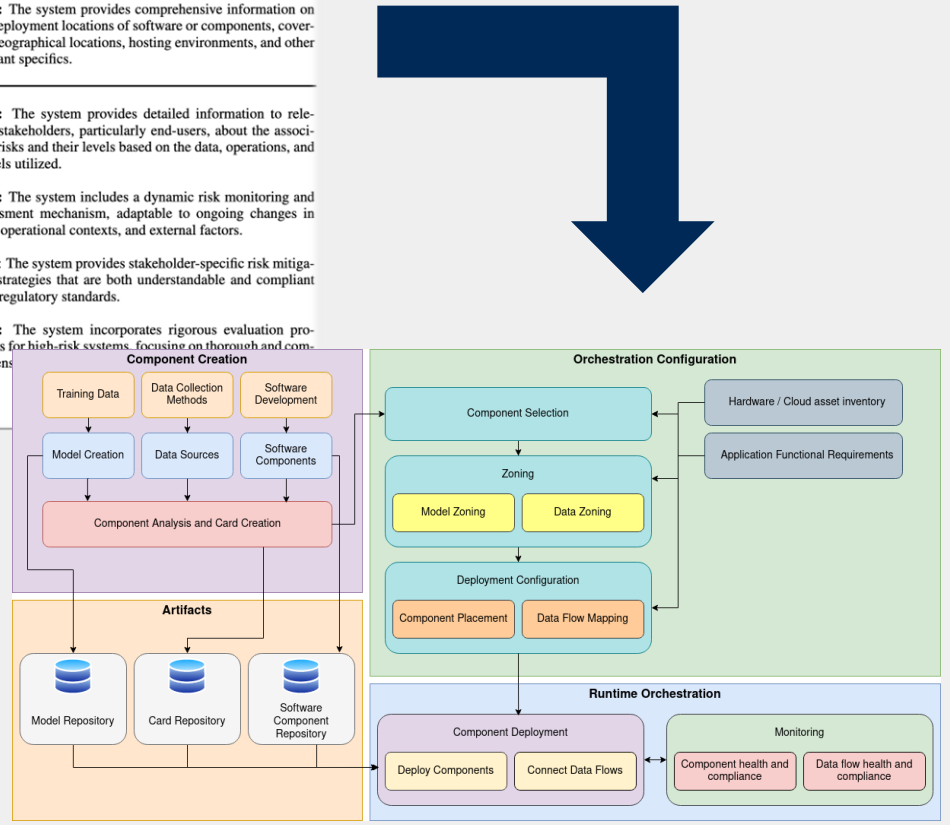
[1] Pyry, K., Ali, M., Tommi, M., & Niko, M. (2024). The Programmable World and Its Emerging Privacy Nightmare. In *Lecture Notes in Computer Science*. Springer Nature Switzerland.

[2] Agbese, M., Mäkitalo, N., Waseem, M., Mohanani, R., Abrahamsson, P., & Mikkonen, T. (2023, November). Examining privacy and trust issues at the edge of isomorphic IoT architectures: case liquid AI. In *Proceedings of the 13th International Conference on the Internet of Things* (pp. 245-252).

From Regulation to Requirements and Automated AI Deployments

- Analyzing the current regulations related to AI and data
- Based on the analysis, drafted seven principles for ethical orchestration:
  - *Principle 1: Comprehensive transparency in*
  - *Deployments*
  - *Principle 2: Support for risk assessment*
  - *Principle 3: Empowered monitoring and*
  - *control of data access*
  - *Principle 4: Enhanced explainability and*
  - *traceability of data*
  - *Principle 5: Oversight and reporting support*
  - *Principle 6: Active bias mitigation and*
  - *discrimination prevention*
  - *Principle 7: Seamless interoperability and*
  - *portability*
- Requirements for automated orchestration architecture

Principle	Motivation (GDPR, EU AI Act)	Requirements
Principle 1: Comprehensive transparency in deployments **Description:** The ethical orchestration system needs to make it transparent for the end-user, developer, authorities, and any other stakeholder to understand how the services are deployed and what these services include (code, models, and data).	• **Transparency Obligations**: AI systems intended to interact with humans, those used to detect emotions or determine association with social categories, and deep fakes, need to be clearly labeled. • **One-Stop-Shop Mechanism (GDPR)**: The responsibilities of GDPR should be handled by a single regulatory authority even for cross-border data processing activities.	• **R1.1:** The system descriptions ensure transparent disclosure of all deployed software, including details about their functionalities and operational scopes. • **R1.2:** The system clearly communicates information about the deployed and operational AI models, including their purposes and data sources. • **R1.3:** The system provides comprehensive information on the deployment locations of software or components, covering geographical locations, hosting environments, and other relevant specifics.
Principle 2: Support for risk assessment **Description:** The ethical orchestration system must actively support and guide comprehensive risk assessments, focusing on identifying and evaluating risks related to its deployment and functionality. It involves analyzing risks from various data types and system contexts, proactively flagging issues like data privacy and security vulnerabilities, and offering strategies for risk mitigation.	• **Risk-based Approach:** AI Act uses four risk levels (Unacceptable Risk, High-Risk, Limited Risk, and Minimal or No Risk) to assess the potential harm the system may cause. • **Governance and Accountability:** Providers of high-risk AI systems must establish post-market monitoring, ensuring that any issues that arise after the system is deployed are addressed. • **Conformity Assessments:** High-risk AI systems must undergo a conformity assessment before being placed on the market. • **Data Protection Impact Assessments (GDPR):** The solution should support impact assessment required for organizations with data processing operations that are likely to result in high risks to individuals' rights and freedoms.	• **R2.1:** The system provides detailed information to relevant stakeholders, particularly end-users, about the associated risks and their levels based on the data, operations, and models utilized. • **R2.2:** The system includes a dynamic risk monitoring and assessment mechanism, adaptable to ongoing changes in data, operational contexts, and external factors. • **R2.3**: The system provides stakeholder-specific risk mitigation strategies that are both understandable and compliant with regulatory standards. • **R2.4:** The system incorporates rigorous evaluation processes for high-risk systems, focusing on thorough and comprehens



JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Thank You!
Questions?

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Thank You!
Questions?