NEUROPULS

http:// www.neuropuls.eu

Neuropuls

Linkedin

COORDINATOR
Fabio PAVANELLO (CNRS)
fabio.pavanello@cnrs.fr

The NEUROPULS project aims to **revolutionize the future of computing** by developing next-generation low-power and secure edge-computing systems. By leveraging the power of novel **photonic computing architectures,** augmented silicon photonics, and advanced machine learning algorithms, NEUROPULS seeks to achieve significant advancements in energy efficiency, processing speed, and security of lightweight accelerators. The project's main objectives include the development of a CMOS-compatible platform integrating silicon photonics with emerging materials, the creation of low-power and secure RISC-V interfaced neuromorphic accelerators, and the establishment of a comprehensive system-level simulation platform. NEUROPULS endeavors to support critical applications such as autonomous driving, network security, and GNSS anti-jamming will pave the way for energy-efficient, and highly secure computing environments.

8 countries

8 M€

2023-2026

15 partners

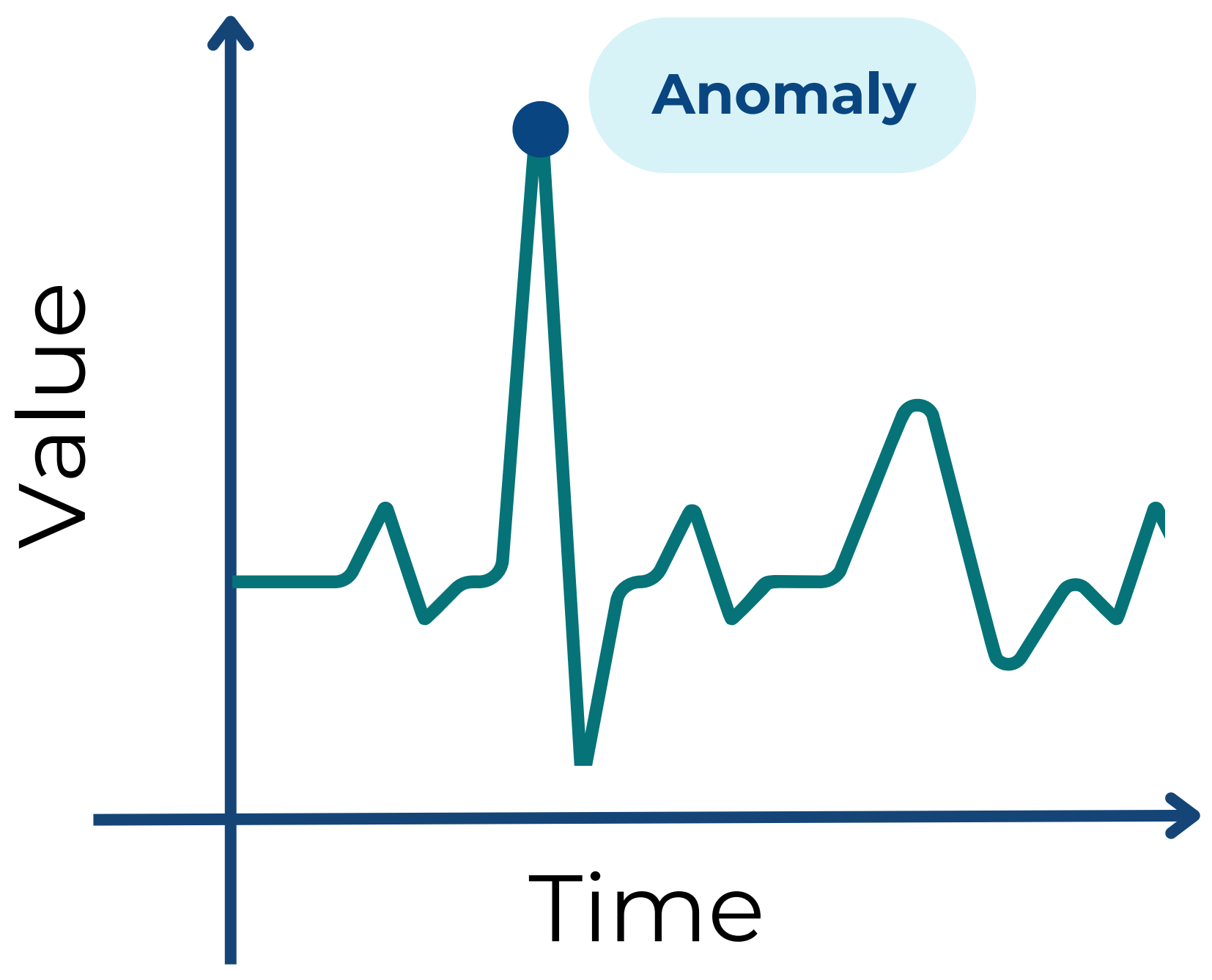
INITIAL PROBLEM

AUTONOMOUS DRIVING

- **Vast sensor-generated data** poses a significant processing challenge.
- Real-time data processing is critical for ensuring safety.
- Delays or errors can **compromise the safety** of autonomous vehicles and passengers.

Studies indicate **processing delays increase accident risk**, highlighting the need for local and energy-efficient processing with lightweight accelerators.

ANOMALY DETECTION



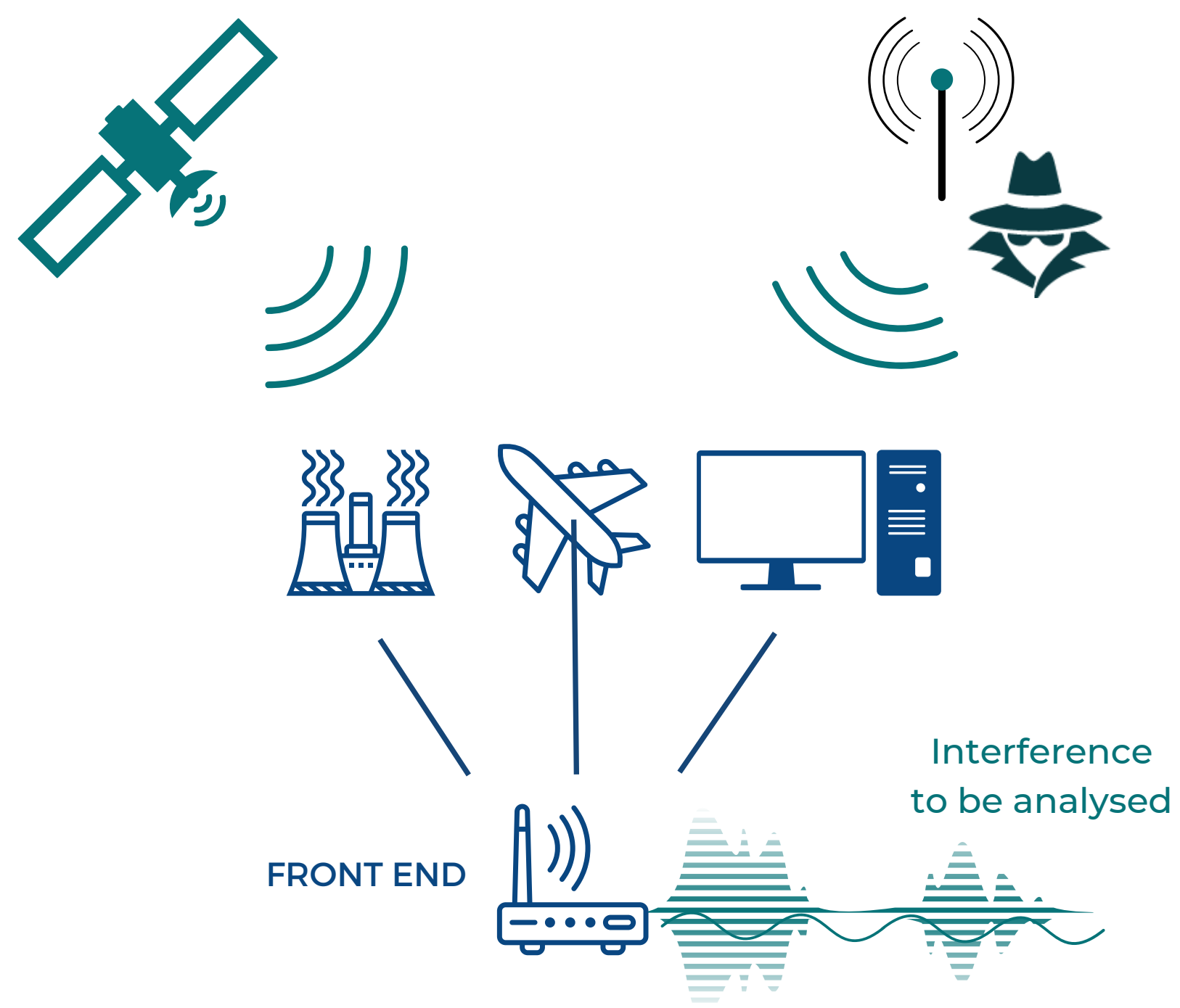
- **Proliferation of IoT devices** creates significant cybersecurity challenge.
- **High volume** of devices and data exchange increases **vulnerability** to attacks.
- Detecting anomalies is crucial for safeguarding against **malicious activities.**

Industry reports show a **300% increase in cyberattacks on IoT devices,** emphasizing the need for robust anomaly detection solutions in neuromorphic accelerators' security layers.

GNSS ANTI-JAMMING

- GNSS is the **primary positioning solution** for civilian, security, and defense applications.
- Growing dependence on GNSS in critical infrastructures raises concerns.
- Potential **disruption of GNSS signals** due to intentional interference poses a significant challenge.
- Protecting GNSS against **jamming** threats is crucial to prevent catastrophic consequences and economic impact.

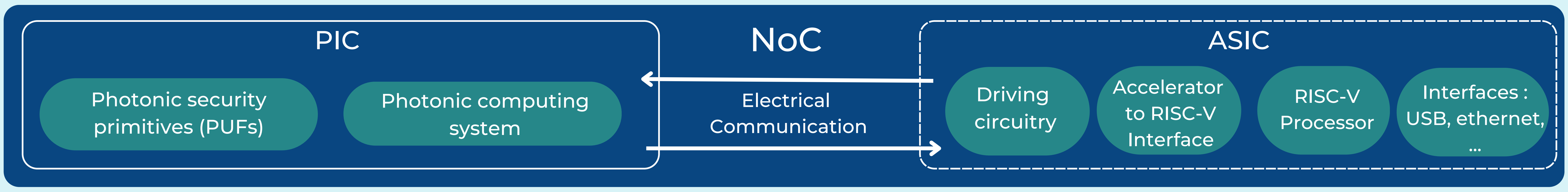
Studies show a **20% annual increase in intentional jamming of GNSS signals,** highlighting the urgent need for effective countermeasures.



SOLUTION

At the core of the NEUROPULS solution, **a state-of-the-art network on chip (NoC)** for edge computing applications, seamlessly integrating on a printed circuit board a **photonic integrated circuit (PIC)** and **an application specific integrated circuit (ASIC)**. This cutting-edge amalgamation unleashes the potential for efficient data processing and analysis delivering unparalleled speed and accuracy.

Leveraging the power of augmented **silicon photonics**, NEUROPULS harnesses the unique properties of this technology to enable swift and dependable **data processing and analysis**. Furthermore, NEUROPULS incorporates **advanced machine learning algorithms**, including neural networks, to discern patterns, identify anomalies, and proactively detect potential threats, amplifying the overall effectiveness and reliability of the solution.



PIC

Photonic security primitives (PUFs)

Photonic computing system

NoC

Electrical Communication

ASIC

Driving circuitry

Accelerator to RISC-V Interface

RISC-V Processor

Interfaces : USB, ethernet, ...

- Anomaly detection for obstacle identification
- Efficient processing of sensor data
- Advanced machine learning to recognize obstacles

- Anomaly detection in real-time for network security
- Optical processors for real-time analysis of network data
- Machine learning algorithms to detect network deviations

- Neural network-based interference detection
- Advanced neural networks
- Reliable gnss protection by detecting and alerting against jamming threats

IMPACT

Reduction in accident rates and near-miss incidents

Decreased response time in **obstacle detection**

Improved reliability of **obstacle identification**

Increased public trust in **autonomous driving technology**

Cost savings in accident-related expenses

AUTONOMOUS DRIVING

Reduction in successful cyberattacks and data breaches

Decreased response time in **detecting and mitigating security incidents**

Minimized financial losses due to cybersecurity incidents

Enhanced user trust and confidence in IoT networks and services

Cost savings in incident response and remediation efforts

ANOMALY DETECTION

Reduced instances of successful GNSS signal jamming incidents

Early detection and alerts for potential jamming threats

Improved reliability and accuracy of GNSS-based services

Mitigated economic losses due to disrupted operations

Enhanced resilience and security in critical applications reliant on GNSS

GNSS ANTI-JAMMING

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.