CELTIC Proposers Day

in Vienna on 30.01.26

- Business Impact Session -

Collective intelligence supported by security aware nodes (CISSAN)

CELTIC-NEXT

Eureka Cluster

Klaus Chmelina, GeoData

www.celticnext.eu

Collective intelligence supported by security aware nodes (CISSAN)

A collectively intelligent security platform consisting of a set of innovative algorithms, technologies, and solutions

Key Facts

Project status: Running
Coordinator: Ilgin Safak, University of Jyväskylä (JYU), Finland
No. of partners: 18
Partner countries: Austria, Finland, Spain, and Sweden
Start date: May 1st, 2023
End date: May 31st, 2026
Supported by: Austrian Research Promotion Agency (FFG), Business Finland, Centre for the Development of Industrial Technology (CDTI), Swedish Agency for Innovation Systems (Vinnova)
Total project budget : ~ EUR 8.5M
Total effort : ~ 74.6 PY

https://www.celticnext.eu/project-cissan
https://www.jyu.fi/en/projects/cissan

Consortium

Summary

Countries: 4
Organizations: 18
Universities: 2
Research inst.: 1
Industry: 6
SMEs: 9

* 1 research inst. in Austria is subcontracted

Partners

Austria

- GeoData

Finland

- Bittium Biosignals
- Bittium Wireless
- University of Jyväskylä (coordinator)
- Mattersoft
- Mint Security
- Netox
- Nodeon
- Scopesensor
- Wirepas

Spain

- Councilbox

Sweden

- Äffarsverken
- Arctos Labs
- Blekinge Tekniska Högskolan
- Blue Science Park
- Clavister
- Savantic
- Techinova

Timeline

Work packages and tasks		GANTT Timing and milestones											
		Year 1				Year 2				Year 3			
		M1-3	M4-6	M7-9	M10-12	M13-15	M16-18	M19-21	M22-24	M25-27	M28-30	M31-33	M34-36
WP0	**Management of the project**												
T0.1	Coordination												
T0.2	Organisation (Project kick-off, Mid-term and Final reviews)	M0.1					M0.3						M0.6
T0.3	Dissemination												
T0.4	Exploitation (Workshops)				M0.2				M0.4				M0.5
WP1	**Continuous follow-up of the related research fields**												
T1.1	Follow-up of the related research fields												
T1.2	Detection and analysis of weak signals				D1.1								D1.2
WP2	**Definition of the system architecture**												
T2.1	Definition of the architecture, system elements, interfaces			D2.1									D2.3
T2.2	Risk, threat and impact analysis				D2.2								
WP3	**Business models**												
T3.1	Recognition and definition of the earning models				D3.1								
T3.2	Business impact analysis of the new earning models						D3.2						
T3.3	Modification and update mechanisms to earning models												D3.3
WP4	**Data security, gathering and quality assessment**												
T4.1	Data quality verification				D4.1						D4.5		
T4.2	Data gathering for distributed algorithms and load balancing				D4.1				D4.3				
T4.3	Distributed network logging systems						D4.2			D4.4			
WP5	**Distributed intelligent security mechanisms**												
T5.1	Distributed intelligent security incident detection						D5.1			D5.2			
T5.2	Collective intelligence algorithms											D5.4	
T5.3	Tools to optimally distribute security functions												D5.5
T5.4	Blockchain-based IoT network security												D5.3
WP6	**Proof of work**												
T6.1	CISSAN platform and solutions of the project use cases												D6.1, D6.3
T6.2	Interfaces to 3rd parties' applications											D6.2	
WP7	**Standardization**												
T7.1	Standardization follow-up and action planning								D7.1				
T7.2	Standardization-related coordination in other WPs										D7.2		

Project Idea

- **Goal (why)**
  Detecting and countering security and operational threats in IoT networks.

- **Content (how)**

  by *Collective Intelligence*

  Devel. of techniques enabling distributed & intelligent
  - *security & operational monitoring*
  - *attack & event detection and*
  - *response*

  in IoT networks.

- **Outcome:**
  A security platform (**CISSAN platform**) consisting of a set of innovative techniques (algorithms, methods, devices)

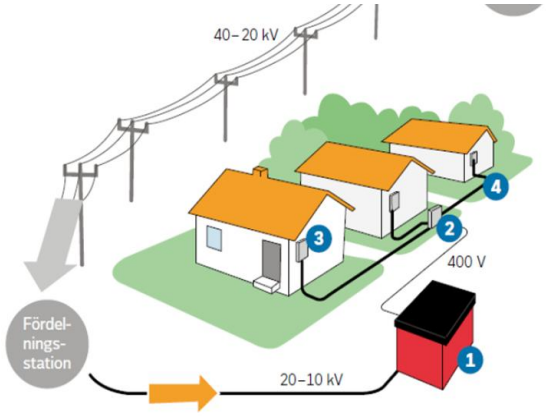
  that collaborate in an orchestrated way to

  protect IoT networks.

Use Cases

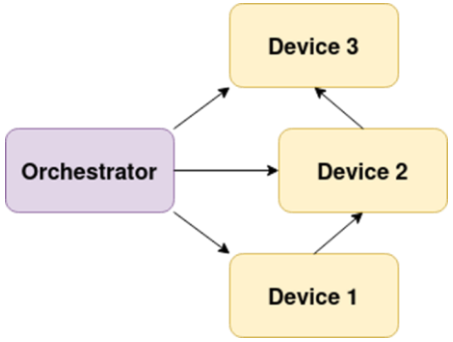
Public Transport
(Mattersoft and Nodeon)

Energy - Smart Grid
(Affärsverken)



Tunnelling
(GeoData)

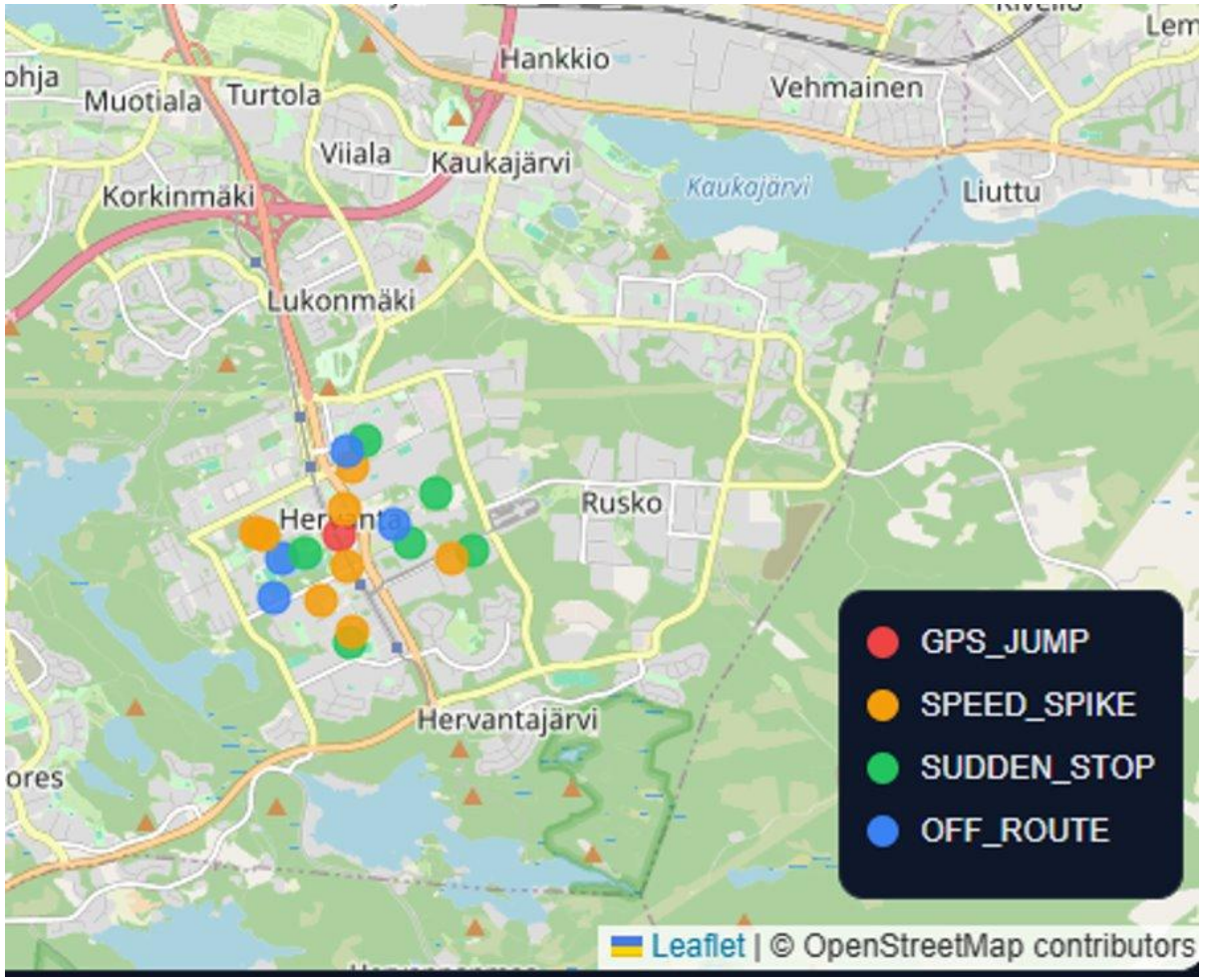
Manufacturing
(Bittium)



Automated Disaster Recovery
(Arctos Labs/JYU)

Use Case Public Transport

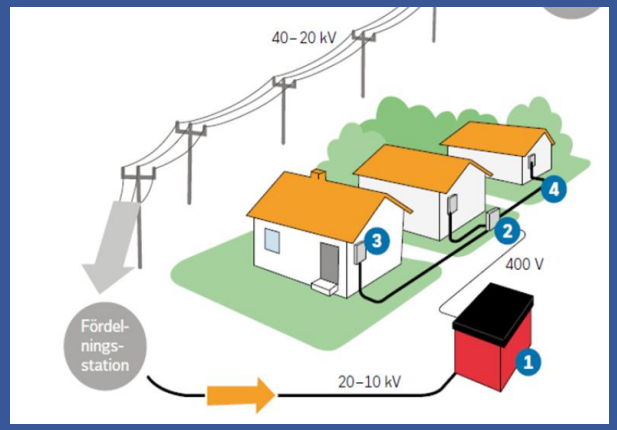
Protecting vehicles from GPS/GNSS signal spoofing by



Detection of **position anomalies** by domain-specific algorithms

Alarming the control center

Initiating **defensive actions** (vehicle isolation,…)



Use Case
Energy - Smart Grid

Protecting Energy Grids from attacks on local control stations (RTUs) by

Detection of **operational anomalies** in RTUs using **ML algorithms**

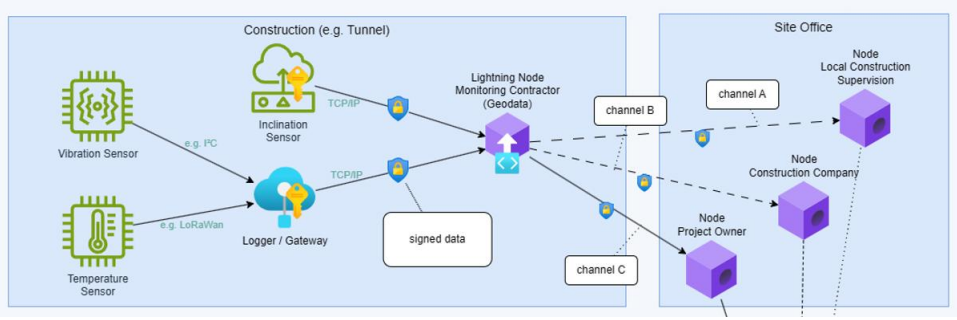
Propagation of **attack information** to other RTUs

Initiating **defensive actions** in the network (blocking of IP,…)

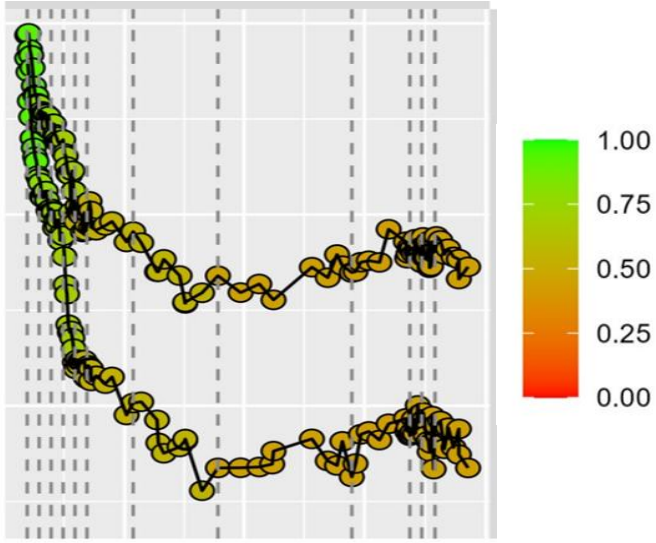
Use Case Tunnelling

Protecting tunnelling processes from data tampering attacks by

Signing sensor data at creation with **Security Chips**



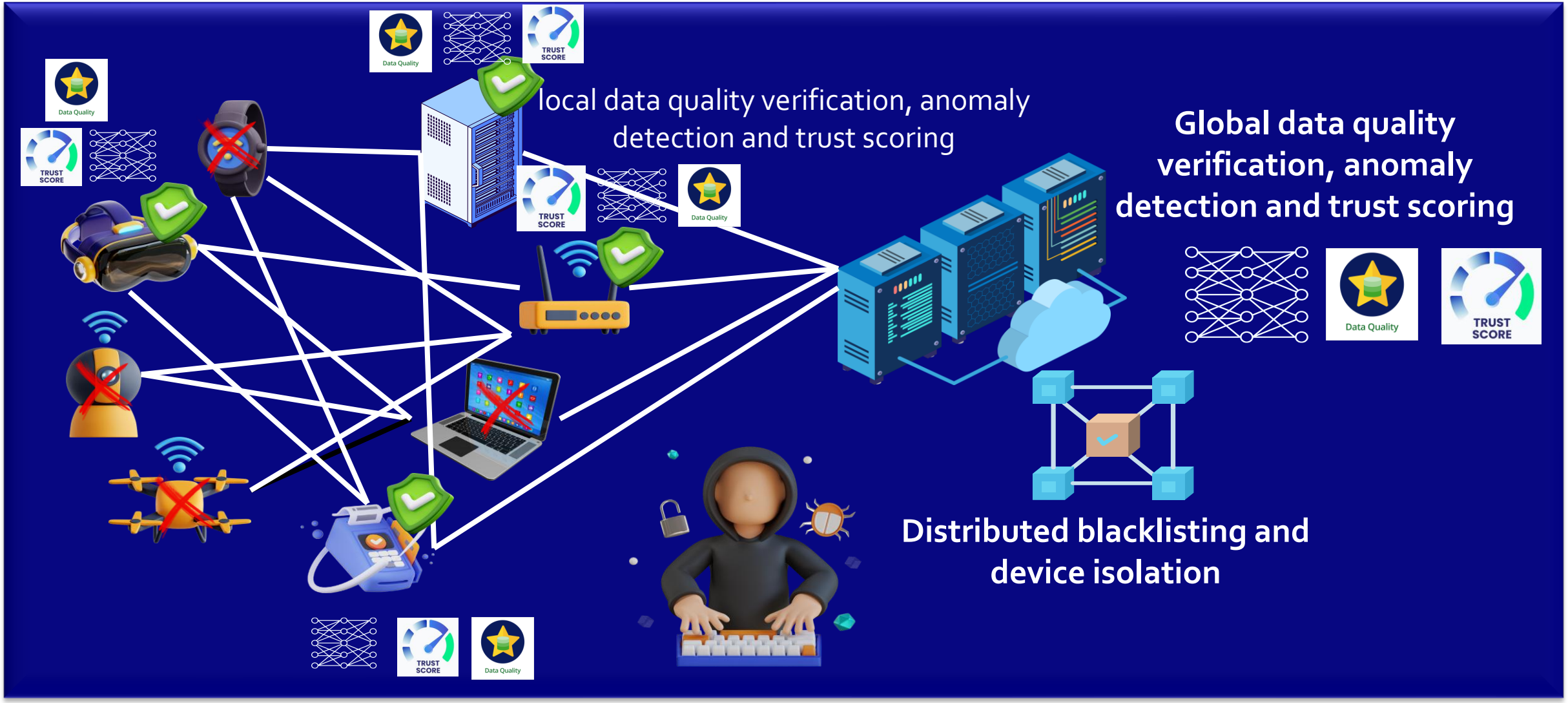
Transferring sensor data applying **Multi-party channel routing** (Blockchain)



Anomaly detection by assessing **Data Believability** using **empirical rules** and **AI**

Initiating **defensive actions** (data isolation,…)

Collective intelligence mechanisms



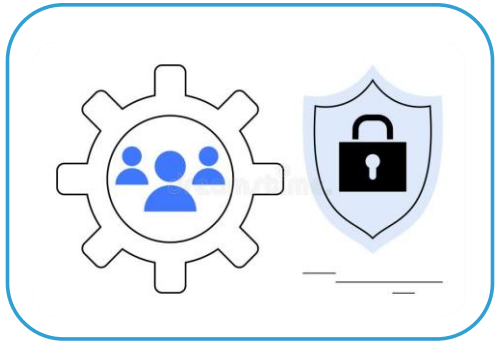
Business Impact

Operational resilience and business continuity

Cost efficiency and improved return on security investments

Better risk management and faster decision-making

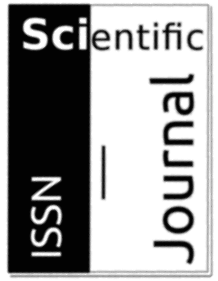
Business enablement and interoperability



Strategic autonomy and ecosystem collaboration

New products and Services: **15**

Dissemination



14 academic publications

4 patent applications filed

16 invited talks / poster presentations

5 websites

CelticNextEurekaCluster

@CelticNext

CELTIC-NEXT Video Channel

MANY THANKS FOR YOUR ATTENTION.

CELTIC-NEXT

Klaus Chmelina, GeoData
klaus.chmelina@geodata.com