Advanced real-time data analysis used for infrastructure resilience

HORIZON-CL3-2024-INFRA-01-03

Call Assessment

Roy Pennings

Rules of the EU grant game

How a Horizon Europe Call grant works (1)

- **Competitive** Call: anywhere between 2-100 consortium applications. Notification after 5 months. 1 project will be funded. Project **duration**: 3-4 years; €5 Million total budget.
- If successful, all partners sign the **grant agreement**; each partner is only responsible for its own share.
- **Collaborative** project: mix of industry + academia; we jointly deliver step-change improvement.
- Deliverables are **contractual obligations**, but grant = effort-based, not result-based.
- **Work-load** consists of: technical work, reporting of results, consortium meetings, EC-reviews, dissemination/exploitation activities + cost administration.
- Funding: in RIA projects all direct project costs (hours, materials, equipment, consumables, travel) for ALL partners is funded 100% (but only real costs, no markup!). Total: €4M direct cost + €1M overhead cost.
- Call = lump-sum scheme: budget only evaluated at submission. No timesheets, no justifications other than deliverables. Also: no extra money, if costs prove to be higher!
- Funding **schedule**: 50% at project start, max 25% at 1st review, 20% at 2nd review, 5% at final project close.

How a Horizon Europe Call grant works (2)

- **Competitive** Call = beauty contest. Highest value for money + best credible proposition wins. **EC = our client!** They look for a solution to a political problem. We present the solution!
- Project needs to be **positioned** as: unique, timely, meeting urgent need, addressing all scope elements (and beyond), present tangible (expected) results, have exploitation strategy.
- Grant proposal =/= tender; text must still be rooted in **scientific approach**.
- End-stage TRL5-6: prototype demonstration in relevant environments. Not product development!
- Evaluators will read proposals within 1 hour: **to-the-point, tables, graphs & pictures**. Numbers!
- Consortium must be **scientifically** credible & top-level, industrial use cases must be able to credibly **build/influence future market uptake** at European scale.
- Proposal should show **spread** in content (e.g. application and transferability potential) , but also in consortium composition.

Responding to EC political need

In line with the EC Strategic Plan: to contribute to the **"resilience and autonomy of physical and digital infrastructures and vital societal functions"**, notably through:

- Resilience of large-scale interconnected systems infrastructures and the entities that operate them in in case of complex attacks (…)
- Resilience of operators and protection of critical infrastructure to enable rapid, effective, safe and secure response and without substantial human intervention (…)
- Within the limits of EU legal framework and working with public oversight & enforcement authorities.

To remind us of our Call…

Expected Call Outcomes

- Improved capabilities for risk and faulty events identification in infrastructure networks and smart cities through real-time analysis by public and private actors where the collaboration follows clear legal and political frameworks.
- Tools and processes to identify, analyse, assess and continuously monitor risks and boost adaptive capacity to unexpected event risks in advance by allowing for the analysis of various data sources.
- Fast and continuous real-time identification, classification and tracking of hazardous agents, contaminants or anomalies in infrastructure networks and supply-chains.
- Interoperable interfaces and improved collaboration between infrastructure operation detection and response systems, national/EU risk management/coordination centres and first responder equipment.
- Increased cyber-resilience of industrial xG networks and cloud data covering specific infrastructure domains.
- Improved ability to map in real-time the source(s) of risk factors that could endanger the networked infrastructure supported by Earth Observation and geolocation data.

Not just a technical solution, but a solution that holds in court. Also address user acceptance / inertia.

Include mechanisms for collaboration with public oversight bodies.

Future-tech oriented solution.

Assess PNT aspects (and risks!) as well.

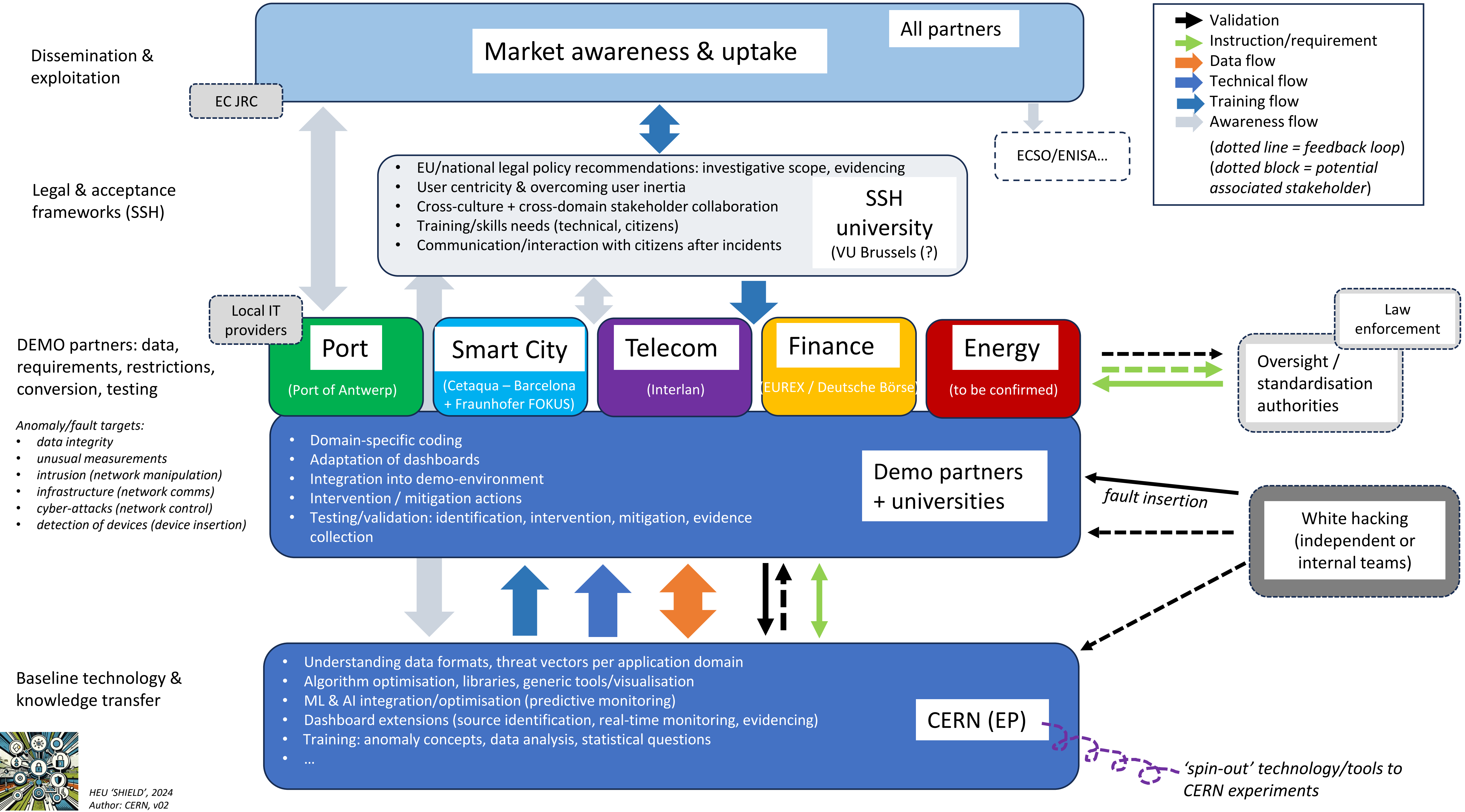
Scope of the Call

Scope Overview:

- Fast and resilient analytical tools (incl. visualisations) to filter information to identify data that are relevant as indicators for risks and allow prioritisation of risk-levels.
- Risk anticipation through context and source awareness.
- Intrusion capture (incl. source), recording & storage that can be used in case of prosecution.
- Provide quick counter-response, but also inform and involve citizens and avoid damage. Integrate with the systems public authorities use to notify citizens.
- Cooperation between different actors to ensure a common understanding and interpretation of data + decision support.

Key Proposal Components

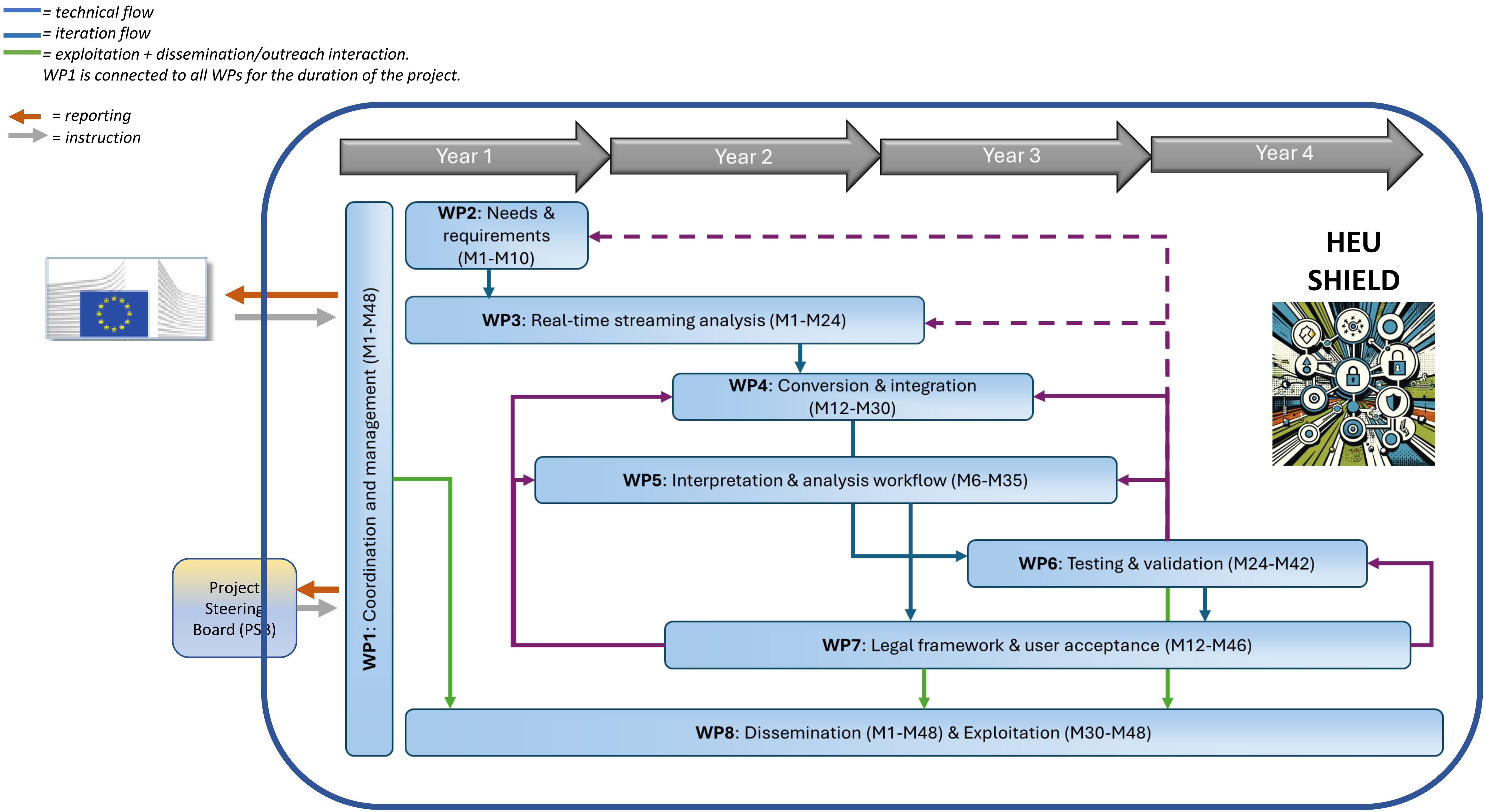
- Single underlying tool for risk identification, able to cope with large data flows and multiple sources.
- Application on Use Cases that constitute interconnected nodes.
- Use of multiple data source types.
- Single but flexible user-dashboard, able to collect, flag, record, prioritise and store in line with (future) EU law. AI-driven?
- Interface with public response systems.
- Pathway for transfer to other application areas, incl. training module.
- Support or indirect involvement from oversight/regulators (advisory board, endorsement of results).
- Demonstrate coordination with ‘Community for European Research and Innovation for Security’ (CERIS) activities.
- Clear pathway for upscaling and product development (post-project).



Dissemination & exploitation
Market awareness & uptake
All partners
EC JRC
ECSO/ENISA…
Validation
Instruction/requirement
Data flow
Technical flow
Training flow
Awareness flow
(dotted line = feedback loop)
(dotted block = potential associated stakeholder)
Legal & acceptance frameworks (SSH)
EU/national legal policy recommendations: investigative scope, evidencing
User centricity & overcoming user inertia
Cross-culture + cross-domain stakeholder collaboration
Training/skills needs (technical, citizens)
Communication/interaction with citizens after incidents
SSH university
(VU Brussels (?)
Local IT providers
DEMO partners: data, requirements, restrictions, conversion, testing
Port
(Port of Antwerp)
Smart City
(Cetaqua – Barcelona + Fraunhofer FOKUS)
Telecom
(Interlan)
Finance
(EUREX / Deutsche Börse)
Energy
(to be confirmed)
Law enforcement
Oversight / standardisation authorities
Anomaly/fault targets:
data integrity
unusual measurements
intrusion (network manipulation)
infrastructure (network comms)
cyber-attacks (network control)
detection of devices (device insertion)
Domain-specific coding
Adaptation of dashboards
Integration into demo-environment
Intervention / mitigation actions
Testing/validation: identification, intervention, mitigation, evidence collection
Demo partners + universities
fault insertion
White hacking (independent or internal teams)
Baseline technology & knowledge transfer
Understanding data formats, threat vectors per application domain
Algorithm optimisation, libraries, generic tools/visualisation
ML & AI integration/optimisation (predictive monitoring)
Dashboard extensions (source identification, real-time monitoring, evidencing)
Training: anomaly concepts, data analysis, statistical questions
…
CERN (EP)
'spin-out' technology/tools to CERN experiments
HEU 'SHIELD', 2024
Author: CERN, v02

Reserve slide

(*initial suggestion for WP structure and timing*)


= technical flow
= iteration flow
= exploitation + dissemination/outreach interaction.
WP1 is connected to all WPs for the duration of the project.
= reporting
= instruction
Year 1
Year 2
Year 3
Year 4
HEU SHIELD
Project Steering Board (PSB)
WP1: Coordination and management (M1-M48)
WP2: Needs & requirements (M1-M10)
WP3: Real-time streaming analysis (M1-M24)
WP4: Conversion & integration (M12-M30)
WP5: Interpretation & analysis workflow (M6-M35)
WP6: Testing & validation (M24-M42)
WP7: Legal framework & user acceptance (M12-M46)
WP8: Dissemination (M1-M48) & Exploitation (M30-M48)