CS SESSION - MODERATORS

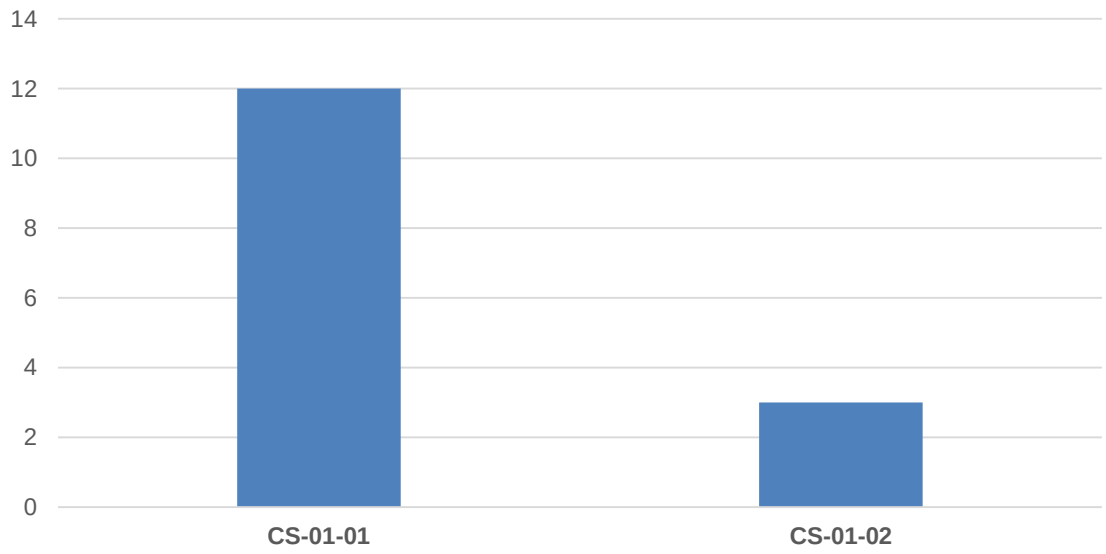
Jeannette Klonk
Jeannette.klonk@ffg.at

Lydia Lindner
Lydia.lindner@ff.at

Cristina Picus
Cristina.picus@ait.ac.at

CS Review Team:

Cristina Picus | Salvatore D'Antonio | Krzysztof Samp | Alberto Bianchi | Jeannette Klonk



CS SESSION - PRESENTATIONS

CS-01-01	1. Pietro Ferrera	pietro.ferrara@unive.it
	2. James Bezamat	james@cetrac.io
	3. Lilian Adkinson	ladkinson@gradiant.org
	4. George Kioumourtzis	gk@ianus-consulting.com
	5. Monica Florea	monica.florea@simavi.ro
	6. Aishvarya Kumar	Aishvarya.Kumar.Jain@emi.fraunhofer.de
	7. Serge Benoliel	serge.benoliel@alstomgroup.com
	8. Benoît Triolo	benoit.triolo@gatewatcher.com
	9. Santiago Macho González	santiago.macho@treetk.com
	10. Armand Puccetti	armand.puccetti@cea.fr
	11. Branka Stojanovic	Branka.Stojanovic@joanneum.at
	12. Ivonne Herrera and Per Meland	Ivonne.Herrera@samforsk.no / Per.H.Meland@sintef.no
CS-01-02	13. Petr Dzurenda	dzurenda@vut.cz
	14. Martin Zuber	martin.zuber@cryptonext-security.com
	15. Jaime Loureiro Acuña	jloureiro@gradiant.org

CS-01-01

Approaches and tools for security in software and hardware development and assessment

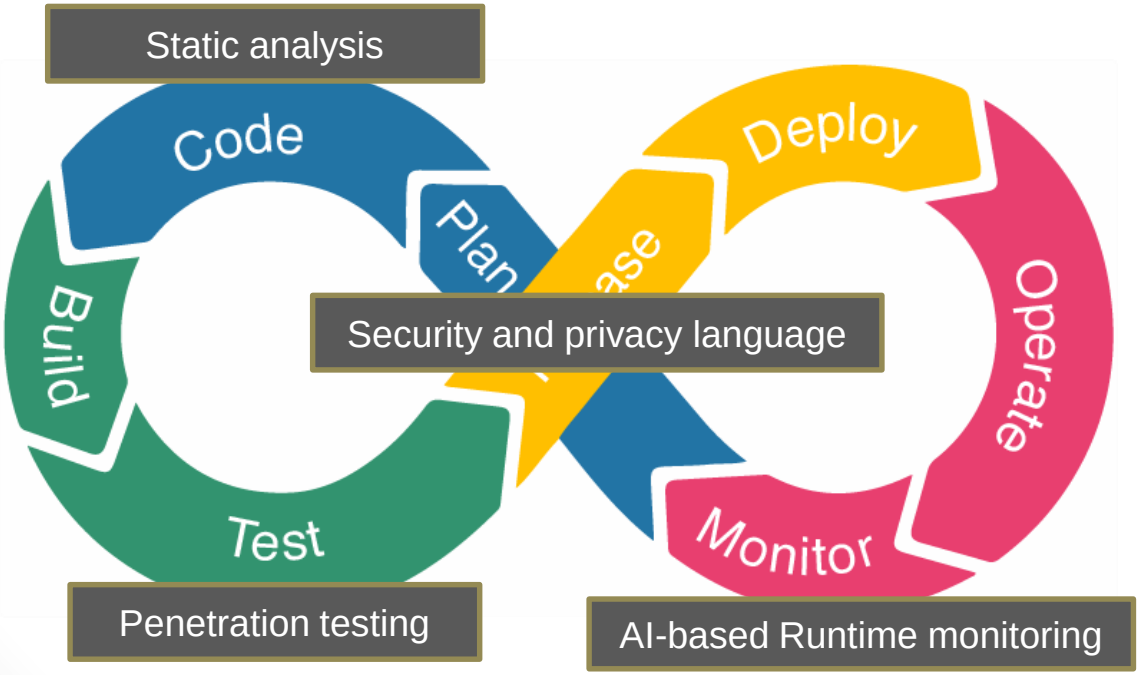
Presenters:

1. Pietro Ferrera
2. James Bezamat
3. Lilian Adkinson
4. George Kioumourtzis
5. Monica Florea
6. Aishvarya Kumar
7. Serge Benoliel
8. Benoît Triolo
9. Santiago Macho González
10. Armand Puccetti & Christophe Gaston
11. Branka Stojanovic
12. Ivonne Herrera and Per Melan

- *Prof. Pietro Ferrara*
- *pietro.ferrara@unive.it*
- *Ca' Foscari University of Venice, Italy*
- Role: *Proposal coordinator, WP leader*
- Topic to be addressed: *HORIZON-CL3-2024-CS-01-01*
  - Approaches and tools for security in software and hardware development and assessment

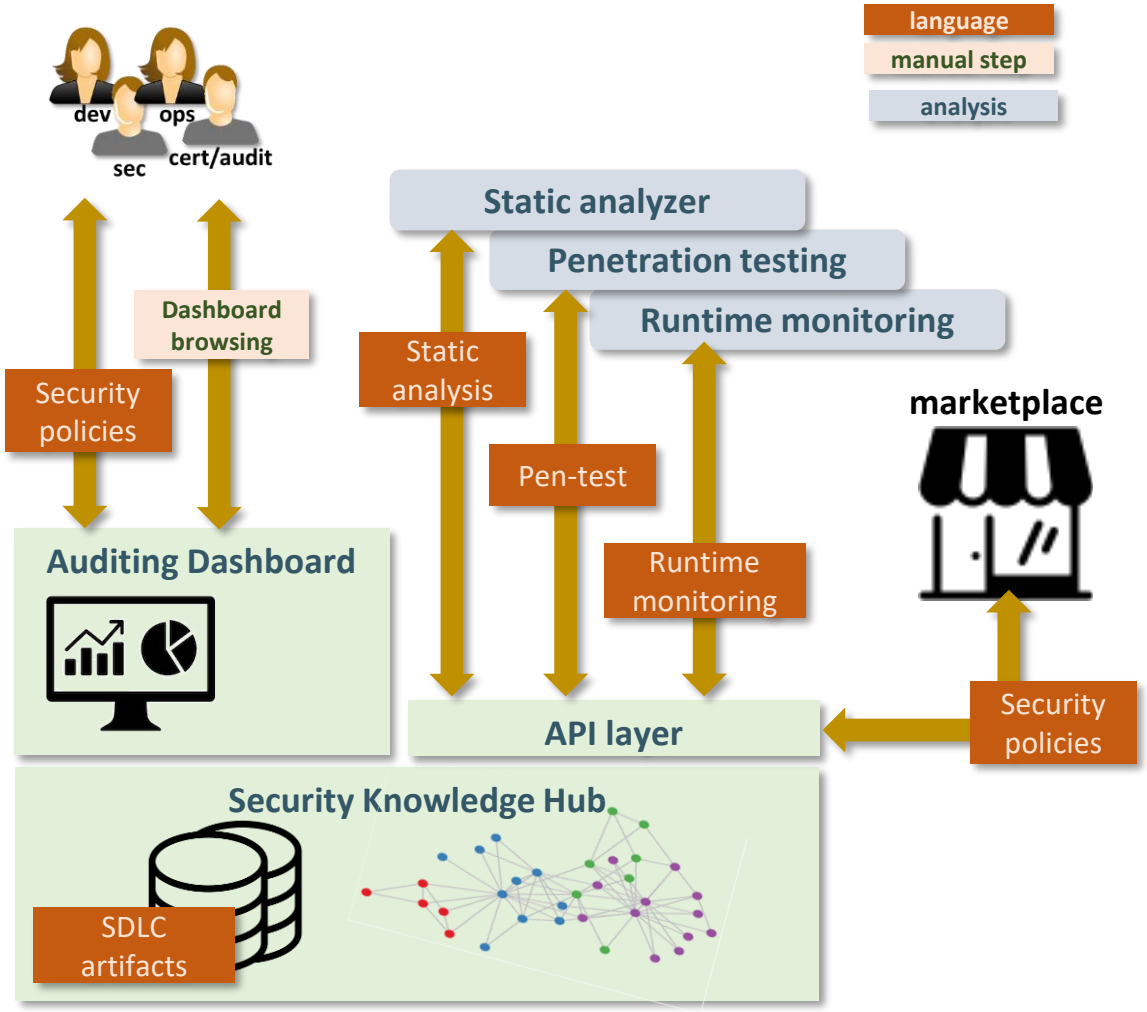
Proposal idea

- *Develop a set of integrated tools into the DevSecOps lifecycle*
- *Cover all the phases through static analysis, testing, monitoring*
- *Involve all the actors of the software development lifecycle*
  - *Developers, project managers, CTOs, auditors, users*



Pietro Ferrara – pietro.ferrara@unive.it

Proposal overview



Pietro Ferrara – pietro.ferrara@unive.it

Project participants

- Existing consortium:
  - Proposed coordinator: *Ca' Foscari?*
  - Partners / Other participants:
    - *University in Norway (empirical software engineering)*
    - *Research center in France (static analysis)*
    - *University in Germany (security analysis)*
- Looking for partners with the following expertise/ technology/ application field:
  - *Case studies/pilots*
  - *Hardware security engineering*
  - *Industrial experts in security engineering*

Pietro Ferrara – pietro.ferrara@unive.it

cyber resilience by design

- *James BEZAMAT*
- *james@cetrac.io*
- *CetraC.io*
- *Role: WP leader, S/T provider*

A disruptive hardware approach serving the cyber resilience of networks

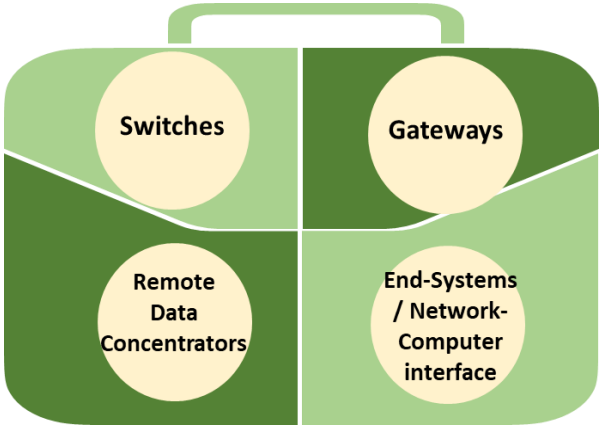
- Destination of interest: CL3-CS (Increased Cybersecurity 2024)

- Horizon-CL3-2024-CS-01-01: *Approaches and tools for security in software and hardware development and assessment*

Proposal idea/content

To improve the security and resilience of critical communication systems through the deployment of an innovative, reliable and cyber resilient solution by design and certifiable by its development process.

To contribute to the security of AI services through a deterministic solution, capable of detecting and processing anomalies in a reliable and safe manner.



James BEZAMAT james@cetrac.io

Project participants

Looking for partners with the following expertise/ technology/ application field:

- Digital infrastructure
- Vulnerability assessment and analysis
- Test tools and methods
- AI based intrusion detection

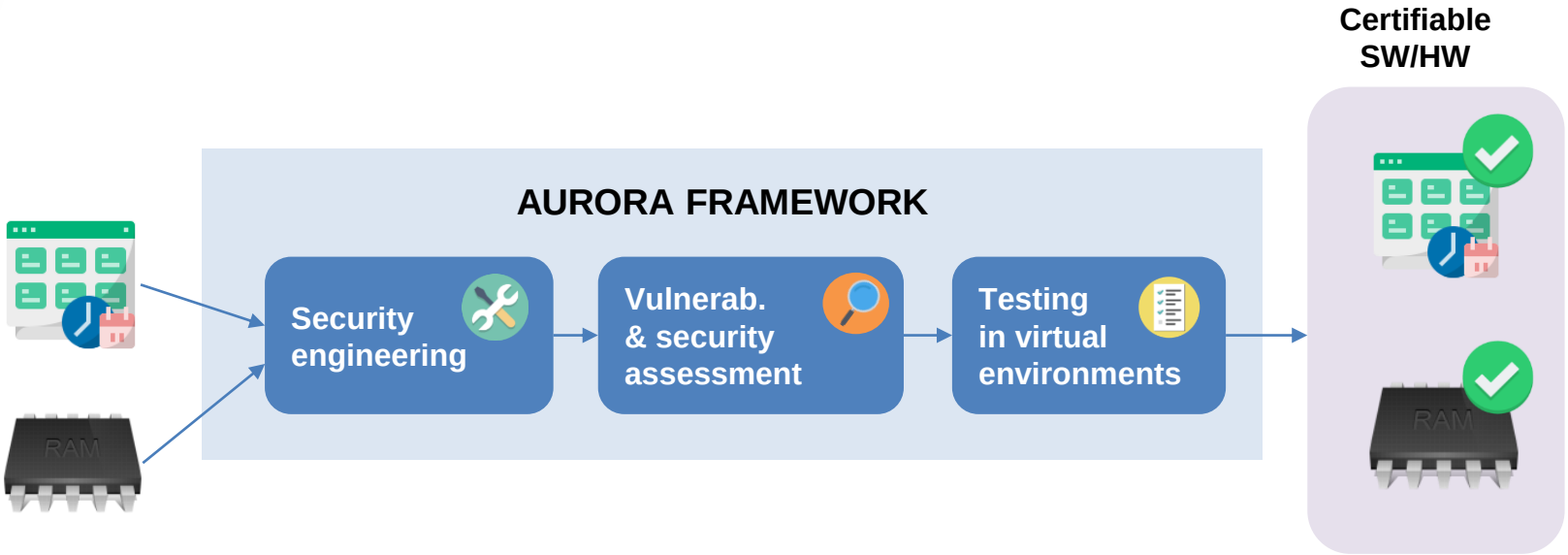
James BEZAMAT james@cetrac.io

AURORA: frAmework for secURity assessment of sOftware and haRdwAre

- *Lilian Adkinson*
- *ladkinson@gradiant.org*
- *Gradiant (RTO, Spain)*
- Role: *WP leader, S/T provider*

- Topic to be addressed: *HORIZON-CL3-2024-CS-01-01: Approaches and tools for security in software and hardware development and assessment*

Proposal idea/content



gradiant
Connectivity · Intelligence · Security
for your business

Lilian Adkinson / ladkinson@gradiant.org

Proposal idea/content

- *The project will deliver a **framework composed by different methodologies and tools** that will allow to perform an assessment on the actual level of security of a hardware or software.*
- *In particular, it will provide:*
  - *A **methodology** to improve **security engineering processes** in hardware and software, taking into account S-SDLC practices, among others.*
  - *A **toolbox** for practical **vulnerability assessment**, including the identification and scoring of the vulnerabilities, which will allow to prioritize their remediation.*
  - *Different **virtual environments for testing** the security properties of the hardware and software under analysis:*
    - *Simulated industrial/IoT environment for the testing and certification of AI-based tools.*
    - *Other (TBD).*
- *The project will also analyse potential regulatory aspects that could affect the platform.*

gradiant
Connectivity · Intelligence · Security
for your business

Lilian Adkinson / ladkinson@gradiant.org

Project participants

- Existing consortium:
  - Proposed coordinator: *TBD*
  - Partners / Other participants:
    - *Gradiant (Spain): virtual environment for the testing of AI-based tools*
- Looking for partners with the following expertise/ technology/ application field:
  - *Security engineering*
  - *Vulnerability assessment*
  - *Software/hardware certification*
  - *Legal experts*

gradiant
Connectivity · Intelligence · Security
for your business

Lilian Adkinson / ladkinson@gradiant.org

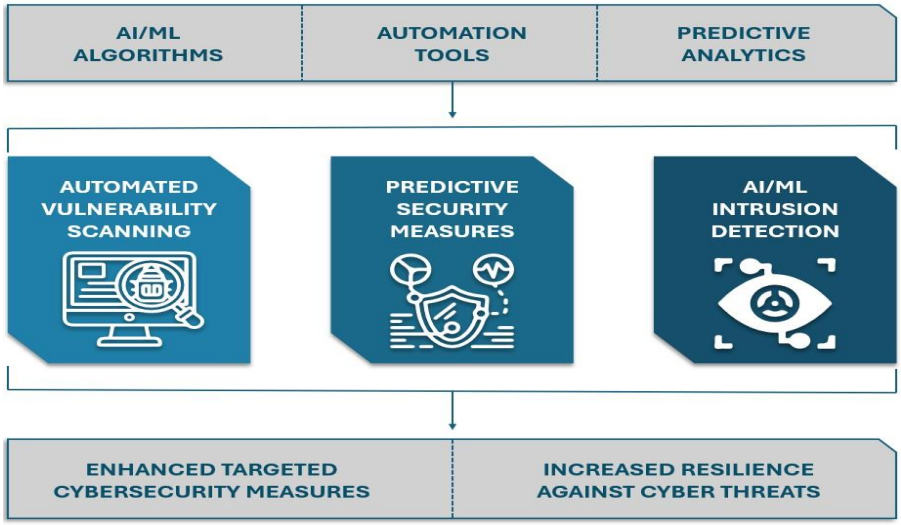
Machine **I**ntelligence for **N**etworked **D**efence and **S**ecurity (**MINDS)**

- *George Kioumourtzis*
- *gk@ianus-consulting.com*
- *IANUS consulting Ltd*
- Role: *Proposal coordinator*

- Topic to be addressed: CL3-2024-CS-01-01

Proposal idea/content

- Project Aim: Enhance cybersecurity defenses using advanced machine learning and AI.
- Core Components:
  - Machine Learning Algorithms: To predict and identify cybersecurity threats in real-time.
  - Network Analysis: Continuous monitoring of network traffic for anomalies and potential breaches.
  - Adaptive Security Protocols: AI-driven adjustments to security measures in response to emerging threats.



Georgios Kioumourtzis - gk@ianus-consulting.com

Project participants

- Existing consortium:
  - Proposed coordinator: *IANUS consulting Ltd*
  - Partners / Other participants:
  - Cybersecurity (Vulnerabilities analyzing and mitigation/ cybersecurity solutions)
  - AI provider
  - End Users (from target sectors e.g. government, finance, healthcare)
- Looking for partners with the following expertise/ technology/ application field:
  - Software engineering (Framework Integration)

Georgios Kioumourtzis - gk@ianus-consulting.com

Increased hardware and software security in Health Tech Applications

- ***Dr. Monica Florea**, Head of Unit European Projects*
- *monica.florea@simavi.ro*
- ***Software Imagination & Vision (SIMAVI), Romania***
  - *SME with strong experience in software development (in fields as Security & Cybersecurity, Energy, Industry 4.0, eHealth, Smart Cities), integration & pilot implementation in Hospitals, Airports & Ports, Financial Institutions, Utility companies, Manufacturing, Telecom, DSOs/TSOs*
  - *Over 70 HORIZON, DEP, EDF & ISF projects*
  - *Coordinator role for 5 security Horizon projects*

- **Role**:
  - *WP-leader, Technical provider/leader, Integrator, Coordinator*
- **Topic to be addressed**:
  - **HORIZON-CL3-2024-CS-01-01**

SIMAVI
Software Imagination & Vision

Proposal idea

SIMAVI
Software Imagination & Vision

The overall goal of the proposal is the development of secure eHealth solutions that will make high-quality health care efficiently accessible for all and thus contributing to good public health.

It will propose a layered cybersecurity model for interconnected medical devices covering built-in device security by considering security and privacy by design from the beginning. This will be achieved by employing diferent technologies based on a software & hardwaresecure elements that serves as a root of trust for several security functions, like:

- **Cross-Layer Anomaly Detection** within a **zero-trust framework,** integrating advanced algorithms (such as predictive, generative AI, and quantum-resistant), to automatically identify and respond to network anomalies and malicious activities in real-time, adaptable across various network infrastructures;
- Simulation of cyber-attack scenarios (including on edge devices), utilizing virtual environments that replicate real-world systems and networks via **Digital Twin**;
- **Collaborative cyber-security** leveraging a **Federated Learning approach** to enable collective intelligence with privacy-preserving machine learning;
- An **AI-driven Security Self-Assessment (SAQ)** tool to guide organizations through cybersecurity defenses and organizational measures, incorporating cost-benefit analysis and awareness of privacy and customized data protection rights;
- Interactive Dashboards for dynamic security monitoring that offer **real-time data visualization, trend analysis, and actionable insights.**

Monica FLOREA ✉ monica.florea@simavi.ro

Project participants

- Existing consortium:
  - Proposed coordinator:
    - *SIMAVI (Security & Cybersecurity R&D References: https://www.simavi.ro/en/rd-projects);*
    - *Open for other coordinator collaboration.*
  - Partners / Other participants:
    - *Pilot infrastructures (from Romania and other EU countries);*
    - *National cyber security and incident response teams*
    - *Security & Cybersecurity SMEs;*
    - *Universities.*

- Looking for partners with the following expertise/ technology/ application field:
  - *R&D organizations / other technology providers specialized in hardware and software security & cybersecurity processes and testing*
  - *Other pilots*

SIMAVI
Software Imagination & Vision

Monica FLOREA ✉ monica.florea@simavi.ro

Automated cybersecurity risk assessment for critical cyber-physical systems

- *Serge BENOLIEL*
- *serge.benoliel@alstomgroup.com*
- *ALSTOM*
- *Proposal Coordinator*

- Topic to be addressed: *CL3-CS-01-01*

Proposal idea/content

Context & Pb to solve

Alstom & Airbus protect have developed a cybersecurity risk assessments methodology for critical industrial cyber-physical systems which is based on the integration of EBIOS RM and IEC 62444.
The creation and management of threat scenarios still poses challenges for complex system, as numerous scenario can be identified, each scenario needing to be created and evaluated by experts, making the process prone to errors, difficult to repeat, and time-consuming.

Innovative proposal / Value proposition

The objective of this project is to automate and enhance reliability and repeatability of cybersecurity risk assessment for critical industrial infrastructure such as railway, through extension of EBIOS RM and IEC 62443.

The main focus of the innovation will be:

- to select relevant cyber-physical system modeling methods able to address the challenges of managing cyber risks
- to specify algorithm to be applied on these models to generate end-to-end attack scenarios, coupled with databases or libraries of attack mechanisms, following the "TTP" protocol (Tactics, Techniques, Procedures).
- to support the processing of these scenarios, using AI technologies, to assist in identifying the most relevant scenarios, to evaluate their likelihood, and to aid in the identification and prioritization of relevant countermeasures.

The approach target to be applicable both to secure system in development and to system already operational. The approach will be validated on real-life use case from the partners.

Serge BENOLIEL – serge.benoliel@alstomgroup.com

Project participants

- Proposed consortium:
  - Coordinator: *Airbus Protect or Alstom (To Be Defined)*
  - Current identified partners:
    - *Airbus Protect*
    - *Alstom*
    - *RATP*
    - *SNCF*
  - Looking for complementary partners such as research institute with the following expertise:
    - *Artificial intelligence, Operational research*
    - *Cybersecurity Risk Assessment,*
    - *Industrial Cybersecurity*

Serge BENOLIEL – serge.benoliel@alstomgroup.com

When Generative AI revolutionises SOC_

- *Benoit Triolo, COO*
- *benoit.triolo@gatewatcher.com*
- *Gatewatcher*
- Role: *WP leader*

- Topic to be addressed: *Horizon-CL3-2024-CS-01-01*

AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks

Proposal idea/content

GATEWATCHER

GATEWATCHER AI ASSISTANT *(GAIA)_*

Technical & Operations

AUGMENTED SOC_
Explain complex alerts
Correlation with AI
Best Practices Advisor

OPERATION ENRICHMENT_
AI Enriched alerts & metadata
Multi source enrichment
OpenCTI integration

ORCHESTRATION & REMEDIATION_
Interaction with EDR/FW/XDR
AD / AZURE AD / O365
Gatewatcher APIs aware

INTERACTIVE ASSISTANT_
Configuration acceleration
Troubleshooting
KB Awareness

_REPORTING ASSISTANT
Alert / Threat Summary
Notifications
Dashboarding

_OPERATIONAL CYBER ASSISTANT
Rule generation by AI
Threat Hunting by AI
Tag / Notes / Triage by AI

When ***Generative AI*** revolutionises SOC_

Benoit Triolo, benoit.triolo@gatewatcher.com

Project participants

- Looking for partners with the following expertise/ technology/ application field:
  - *GEN AI specialist*
  - *Other software editors to build interconnection*
  - *Use case providers*

Benoit Triolo, benoit.triolo@gatewatcher.com

VirtuSEC

- *Santiago Macho González*
- *santiago.macho@treetk.com*
- *Tree Technology (SME)*
  - Spanish SME
  - Field of expertise: Big Data, AI, Cybersecurity
  - >30 EU projects. 11 (EU) ongoing +6 national PPI on cybersecurity
  - 10 projects on H2020-SEC. 3 ongoing: TRUSTaWARE, TeamAware and Nightingale.
  - 3 proposals under HE-CL3 recently approved

- *CL3-CS*
- *Topic: HORIZON-CL3-2024-CS-01-01 - Approaches and tools for security in software and hardware development and assessment*

Proposal idea/content

The objective of the project is to integrate security measures from the ground up into the design and development of both hardware and software across all stages of the system's development lifecycle.

- *Development of a modular framework to integrate security throughout the SW and HW lifecycle.*
- *Research into advanced resilient design techniques to prevent attacks.*
- *Creation of a virtualised platform for secure and customisable HW and SW testing.*
- *Development of AI-based automated security testing tools.*
- *Establishment of a transparent security certification process.*

Santiago Macho González (santiago.macho@treetk.com)

Project participants

- Looking for partners with the following expertise.
  - Final users: HW/SW designers/developers.
  - Virtualised environments (hardware, network, etc.).
  - Anomaly detection, static/dynamic analysis.
  - Systems security certification. Security evaluations.

- Which role do you prefer in a consortium?
  - No preference on being leader or partner
  - AI-powered anomaly and vulnerability detection and prediction. Identification of new vulnerabilities/weaknesses for detection tools (OSINT). Automation of software penetration testing and security measures. AI-driven static and dynamic code analysis.

Santiago Macho González (santiago.macho@treetk.com)

Security of Essential Software and Hardware in Critical Systems through Formal Analyses

- *Armand Puccetti/Christophe Gaston*

{armand.puccetti,christophe.gaston}@cea.fr

- *CEA LIST (*https://www.cea.fr/English)

- Role: Coordinator, Technical leader

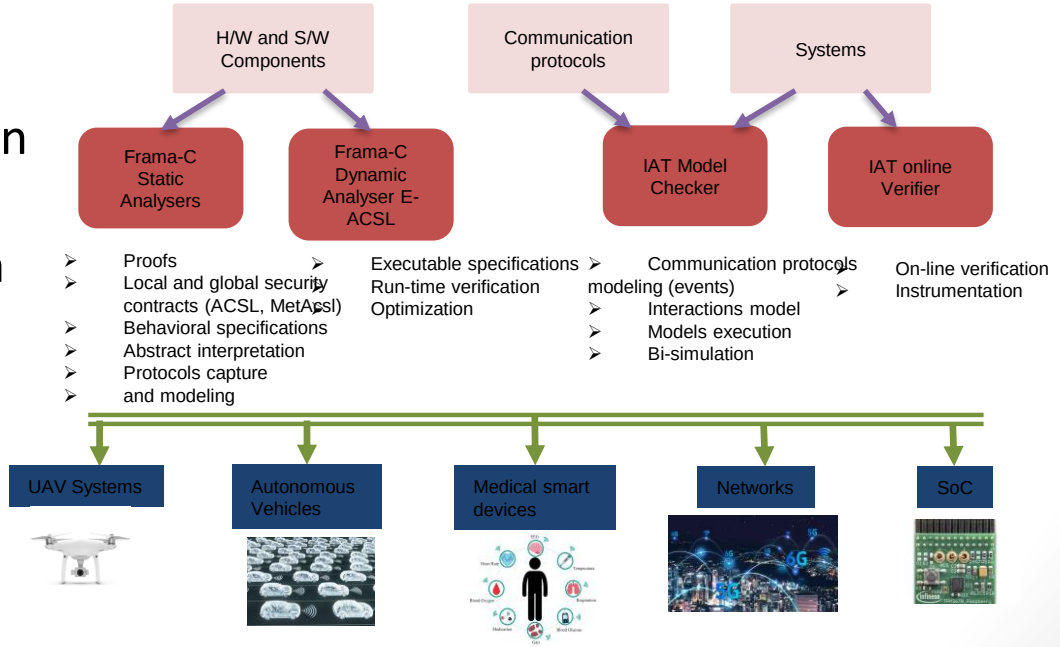
- Destination of interest: HORIZON-CL3-2024-CS-01-01

Proposal idea/content

Improve the cybersecurity and safety of critical systems based on innovative Verification and Validation (V&V) techniques using Formal Methods, and more specifically **Frama-C** and the **Interaction Analysis Tools (IAT)**. FM provide a measure of security and can serve to assess of code vulnerability continuously.

AI is fully integrated into Formal Methods for :

- code evolution prediction
- code correction
- incremental certification
- continuous assessment of code security.



Armand Puccetti/Christophe Gaston {armand.puccetti,christophe.gaston}@cea.fr

Project participants

- Existing consortium:
  - Proposed coordinator: Technikon, Austria.
  - Technical leader: CEA LIST, France
  - Partners/other participants:
    Potential use-case partners and tool partners identified and contacted.

  <you may only disclose number, type and country info of partners, and/or expertise already available, current status (confirmed/tbc partners)>

- Looking for partners with the following expertise/technology/application field:
  - Hardware security
  - Certification
  - Hardware use-cases with software layers (e.g. BIOS, HdS, etc).

Armand Puccetti/Christophe Gaston {armand.puccetti,christophe.gaston}@cea.fr

ARMOR

- *Branka Stojanovic*
- *Branka.Stojanovic@joanneum.at*
- *Joanneum Research Austria*

- Role: *Proposal coordinator, WP leader*

- Topic to be addressed: *CL3-CS-01-01 Approaches and tools for security in software and hardware development and assessment*

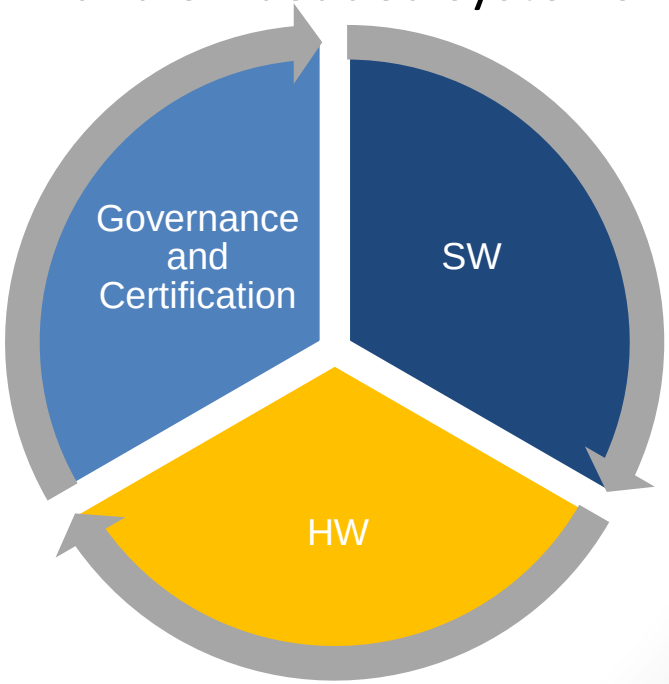
- *Advanced Resilience Measures for Optimal Software and Hardware Security*

ARMOR

- *Advanced Resilience Measures for Optimal Software and Hardware Security*

- Trustworthiness and robustness of AI and embedded systems
  - Automated testing framework
  - Security and safety of AI
  - HW production compliance

- Use-cases
  - Industry 4.0 → 5.0
  - Cyber Physical Systems
  - Edge to cloud continuum



Branka Stojanovic, Branka.Stojanovic@joanneum.at

Project participants

- Existing consortium:
  - Proposed coordinator: *Joanneum Research*
  - Partners / Other participants: *Chip production company (tbc), University (tbc)*

- Looking for partners with the following expertise/ technology/ application field:
  - *Additional use-case partners*
  - *Certification company*
  - *Technology partners*

Branka Stojanovic, Branka.Stojanovic@joanneum.at

- *Per Håkon Meland*
- *SINTEF Digital, Norway*
- *Per.H.Meland@sintef.no*

- Role: *Proposal coordinator (by proxy)*

- Proposal activity: *CL3-CS-01-01*
  Approaches and tools for security in software and hardware development and assessment

Proposal idea/content

1. Improved hardware and software security engineering; resilient design;
   - Security by design, build security in
2. Improved security testing of hardware and software in virtual, closed and secure environments;
3. Systematic study of vulnerabilities, software analysis, vulnerability discovery, and dynamic security assessment;
4. Trustworthy certifiable hardware and software;
5. AI-based security services e.g. predictive security, advanced anomaly and intrusion detection, system health checks.

Per Håkon Meland - Per.H.Meland@sintef.no

Project participants

- Existing consortium:
  - Possible coordinator: *University of Southampton*
  - Partners / Other participants:
    - *SINTEF Digital, Norway*
    - *Red Alert Labs, France*
    - *Visma, Norway*

- Looking for partners with the following expertise/ technology/ application field:
  - *Users with use-cases (Telco, infrastructure, end-users, SME)*
  - *Software development organizations*
  - *Hardware manufacturers*
  - *++*

Per Håkon Meland - Per.H.Meland@sintef.no

Increased Cybersecurity

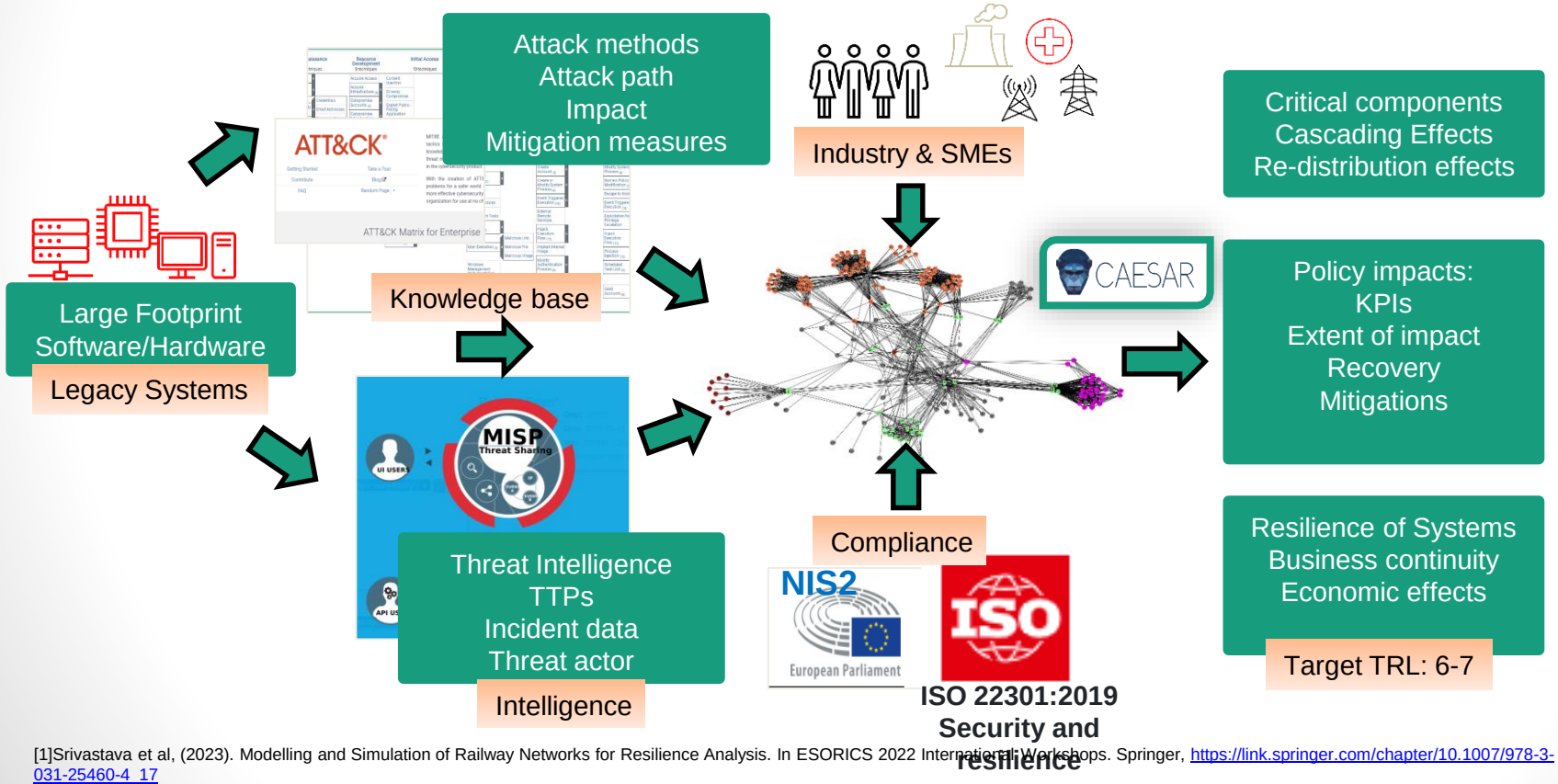
- *Kushal Srivastava, Katja Faist , Dr. Mirjam Fehling-Kaschek*
- *Kushal.Srivastava@emi.Fraunhofer.de, Mirjam.Fehling-Kaschek@emi.fraunhofer.de*
- *Fraunhofer Institute for High-Speed Dynamics, Ernst-Mach-Institute, EMI, 79588 Efringen-Kirchen, Germany*

- **Role**: *Proposal coordinator, Project Coordination (Open)*
- **Topic to be addressed**: *HORIZON-CL3-2024-CS-01-01*

- Supply grids
- ICT systems
- Transport
- Cyber Security

CTI enabled Resilience assessment and monitoring of Cyber-physical systems

- *Integration of AI based methods for vulnerabilities, incident and abnormality detection with agent-based impact simulation to evaluate key threats on target infrastructure.*
- *Derive expert inputs and recommendations based on **ISO 22301:2019** and **NIS2 directives.***
- *Development of **knowledge base** with **standard response and mitigation measures** for threats.*
- *Exploring vulnerabilities of large footprint legacy software/hardware systems using expert knowledge.*



[1]Srivastava et al, (2023). Modelling and Simulation of Railway Networks for Resilience Analysis. In ESORICS 2022 International Workshops. Springer, https://link.springer.com/chapter/10.1007/978-3-031-25460-4_17

[2] Köpke et al, (2020). Impact propagation in Airport Systems. In ESORICS 2020 International Workshops. Springer, https://link.springer.com/chapter/10.1007/978-3-030-69781-5_13

Kushal Srivastava, Kushal.Srivastava@emi.Fraunhofer.de

Project participants

- Existing consortium:
  - Proposed coordinator: *Fraunhofer (Open)*

- Looking for partners with the following expertise/ technology/ application field:
  - *Experts in Legacy hardware/SCADA Systems used in supply chains/healthcare.*
  - *Experts in Legacy/Open-source software Industrial solutions.*
  - *Experts in Malware detection systems.*

Kushal Srivastava, Kushal.Srivastava@emi.Fraunhofer.de

CS-01-02

Post-quantum cryptography transition

Presenters:

1. Petr Dzurenda
2. Martin Zuber
3. Jaime Loureiro Acuña

- *Dr. Petr Dzurenda*
- *dzurenda@vut.cz*
- *Brno University of Technology, Czech Republic*

- Role: *WP leader*

- Topic to be addressed: CL3-CS-01-02: **Post-quantum cryptography transition**

Proposal idea/content

***QuantumShield*: Post-Quantum Cryptography for Privacy, Connectivity, and Trust in the IoT World**

- ***quantum-safe privacy-preserving protocols*:**
  - *I.e., use in modern online services such as e-voting, e-auctions, or cryptocurrencies.*

- ***quantum-safe cryptography for IoT*:**
  - *I.e., implementation problem on computational and memory-restricted microcontrollers.*

- ***hybrid cryptographic solutions*:**
  - *I.e., combining pre- and post-quantum protocols or post-quantum protocols to increase trust and security.*

Dr. Petr Dzurenda, dzurenda@vut.cz

Project participants

- Existing consortium:
  - Proposed coordinator: ***TBD***
  - Partners / Other participants: ***TBD***

- **Cryptographic Protocol Design** and **Applied Cryptography** :
  - PETs (attribute-based credentials, **authentication** protocols),
  - PQC (CRYSTALS-**Dilithium** & **Kyber**, DS2),
  - QC (quantum key distribution - **ID Quantique**),
  - PQC transition mechanisms (KEM combiners),
  - Apps for **smart cards**, wearables, MCU, **FPGA**.
- **We are part of** :

SPARTA

CHESS

REWIRE
CYBERSECURITY SKILLS ALLIANCE

EULiST

Digital4Security
Shaping Europe's cyber future

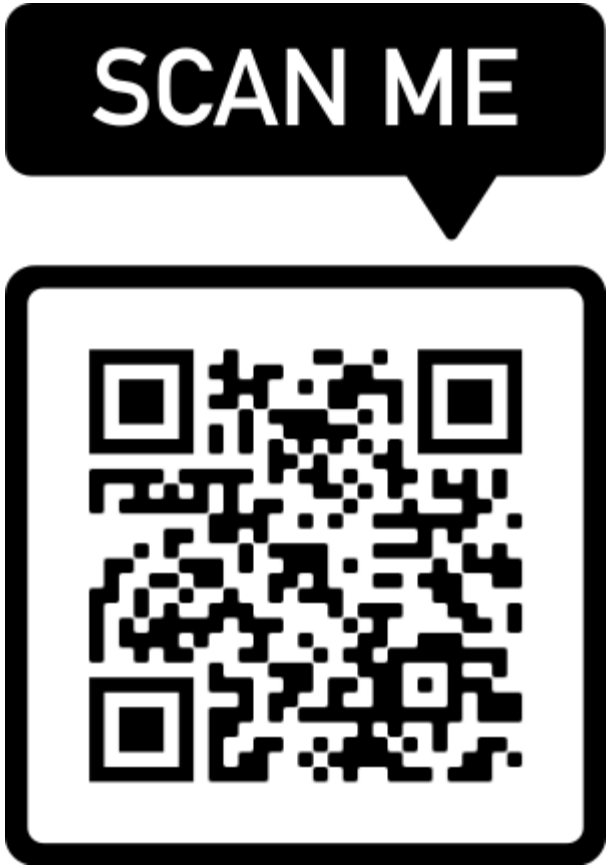
Dr. Petr Dzurenda, dzurenda@vut.cz

Contact us!

- **Dr. Petr Dzurenda**
- **Email**: dzurenda@vut.cz

- **Brno University of Technology**
- Academic institution
- Czech Republic

- Websites: https://axe.vut.cz/



Call on the PQC transition

- *Martin Zuber*
- *martin.zuber@cryptonext-security.com*
- *CryptoNext Security*

- Role: *WP leader or S/T provider*

- Topic to be addressed: *HORIZON-CL3-2024-CS-01-02 (Post-quantum cryptography transition)*

Potential projects

The use cases:

- *Code signing / firmware update / SOTA*
- *PQC implementation for critical or embedded systems.*
- *PQC migration tools, hybrid and crypto-agile protocols (TLS, IPSEC, X3DH, Matrix…)*
- *Crypto-Inventory in the context of PQC migration.*

For one or several verticals:

- *Payment systems and financial infrastructures.*
- *Automotive*
- *Telco*
- *Industrial IoT*
- *IT security & networks infrastructures*

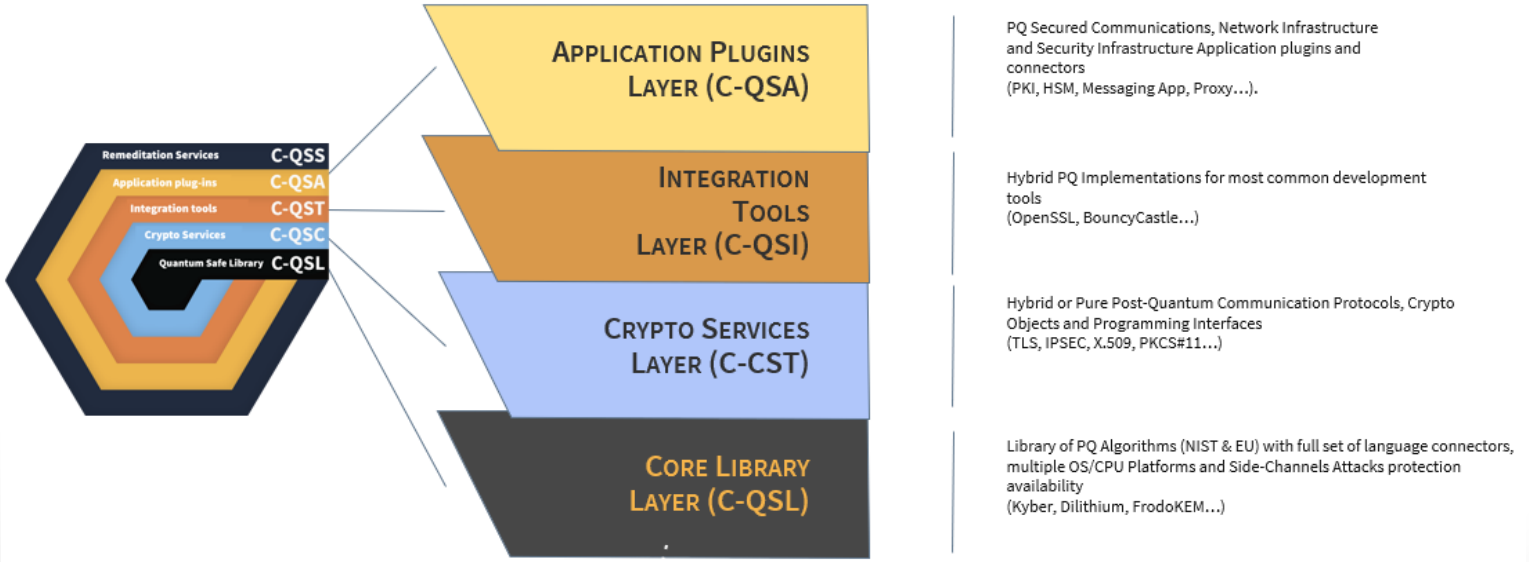
Martin Zuber - martin.zuber@cryptonext-security.com

Our contribution

CryptoNext's business: Development of PQC software solutions to support organizations in the migration of their IT/OT infrastructures to quantum safe.

CryptoNext's contributions to the project would include:

- *Participation to the standardization bodies and PQC WG (IETF, NCCoE, MITRE PQC Coalition…).*
- *Set of tools to make the migration easier*
- *Optimized PQC implementations with side-channel counter-measures.*



Martin Zuber - martin.zuber@cryptonext-security.com

Project participants

- Consortium to build.
- Looking for partners with the following expertise/ technology/ application field:
  - Use-case providers / “end consumers” of cryptography / large accounts.
  - Security systems vendors / Equipment, hardware Manufacturers & software providers…
  - Academics / public research.

Martin Zuber - martin.zuber@cryptonext-security.com

QBeCAS

- *Jaime Loureiro Acuña*
- *jloureiro@gradiant.org*
- *GRADIANT (RTO, Spain)*
- Role: *WP leader, S/T provider*

- Topic to be addressed: **HORIZON-CL3-2024-CS-01-02: Post-quantum cryptography transition**

Proposal idea

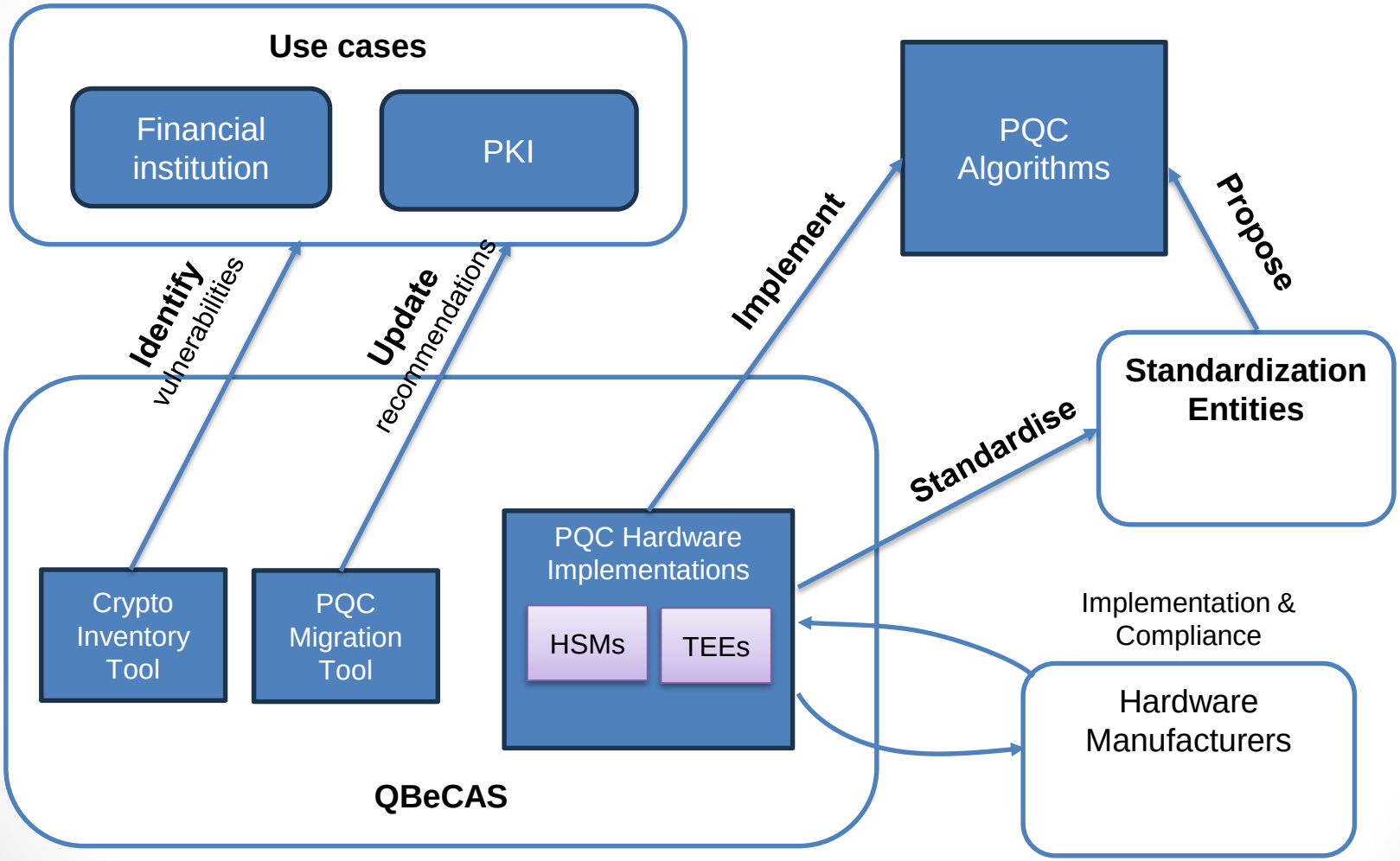
- ***Objectives***
  - To ease the transition from the pre-quantum era to the post-quantum one
  - To provide recommendations on how to implement PQ
  - To contribute to standardization and regulatory activities for PQC

- ***Expected outcomes***
  - to develop a tool that allows to automatically identify and assess the security of cryptographic material used by applications
  - to develop a set of tools that ease the transition of applications to post-quantum cryptography
  - to validate the research and implementations across several use case pilots

- ***Use cases***
  - *PKI*
  - *Financial institution*

Jaime Loureiro Acuña / jloureiro@gradiant.org

Proposal concept



Jaime Loureiro Acuña / jloureiro@gradiant.org

Project participants

- ***Existing consortium:***
  - **CERICT** (UNI, Italy): Coordinator
  - **Gradiant** (RTO, Spain): Focuses on research and implementation in PQC and crypto-agile
  - **Infocert** (LE, Italy): Involved in the PKI use case.
  - **Poste Italiane** (Italy): Involved in the Financial use case.
- ***To be confirmed***
  - **Kleuven** (UNI, Belgium): Specializes in PQC research (TBC)
  - **PQShield** (SME, Netherlands): Specializes in PQC implementation and crypto-agile (TBC)
  - **Thales** (LE, France): HSM manufacture (TBC)
  - **DIN** (Germany): Standardization body
- ***Looking for partners:***
  - PQC cryptography research and development
  - Standardization bodies
  - HSMs Manufactures
  - Legal expertise on data protection
  - Exploration of other use cases

Jaime Loureiro Acuña / jloureiro@gradiant.org