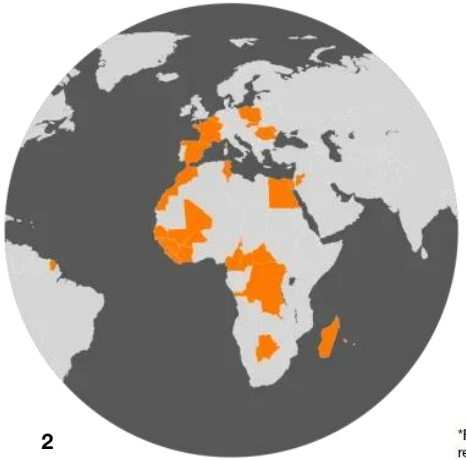
New security directions and challenges for Infrastructures Operators in an evolving EU Landscape

Jean-Philippe Wary
Head of Systems & Products Security research program
Orange Research Chatillon - France

Orange Research in a nutshell

Orange operators

- 36 countries
- 127k employees
- 291M customers
- 40,3Mds €



Research and Intellectual Property in a few figures

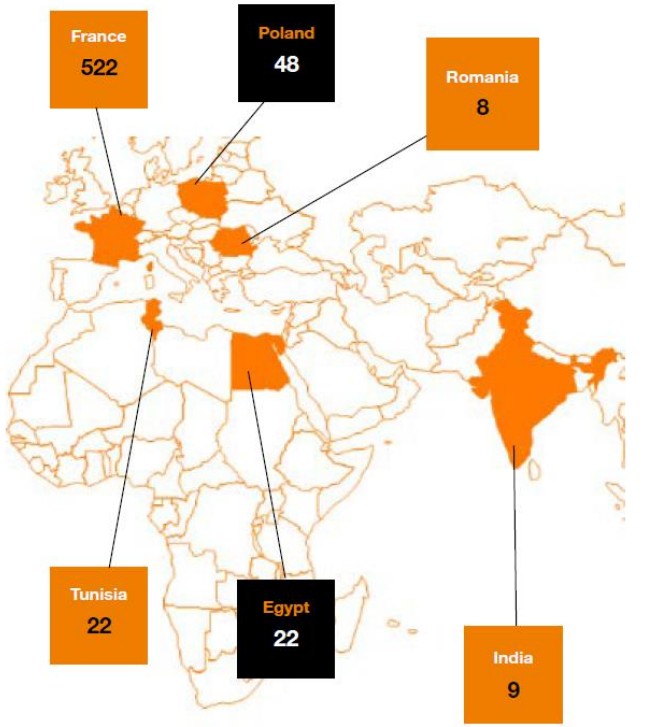
200 new inventions protected by patent on average each year	**115** doctoral and post-doctoral researchers	**+ 110** publications in international conferences or scientific journals, Research Papers
11th in the overall INPI 2024 ranking and 1st European operator	**23** Patent pools in which Orange is engaged	**+ 50** software projects analyzed for their market value
+ 150 partners (laboratories, universities, industries...)	**730*** researchers in France and internationally	**42 %** of Senior Experts contribute to Research
+ 11000 patents and patent applications in our portfolio by the end of 2024	**+ 2000** industries worldwide have licensed our patents	**10** Awards et recognitions

*FTE evaluated based on the total number of person-days reported by Orange Group employees in research projects.

International Research

Number of FTE (Full-Time Equivalent) by country

Here is the distribution of researchers in France and internationally, noting that there are about a hundred more at OAB, Sofrecom, etc. :



EU cybersecurity regulation landscape

EU Legislative Texts: Constraints & Future Challenges for Infrastructure Providers

NIS2 Directive

Constraints:

- Implement comprehensive risk management and security measures.
- Mandatory incident reporting within 24 hours.
- Increased oversight and compliance obligations.

Future Challenges:

- Ensuring continuous compliance across diverse sectors.
- Enhancing incident detection and response capabilities.
- Managing evolving cyber threats and supply chain risks.

AI Act

Constraints:

- Conduct risk assessments for high-risk AI systems.
- Implement transparency and human oversight measures.
- Comply with documentation and testing requirements.

Future Challenges:

- Developing trustworthy AI that balances innovation and safety.
- Ensuring compliance across diverse AI applications.
- Addressing ethical and societal implications of AI deployment.

Cyber Resilience Act

Constraints:

- Incorporate security-by-design in ICT products and services.
- Conduct vulnerability assessments and document security measures.
- Ensure transparency and traceability of security features.

Future Challenges:

- Integrating security requirements into rapid product development cycles.
- Managing vulnerabilities in complex supply chains.
- Adapting to emerging cyber threats targeting ICT products.

DORA (Digital Operational Resilience Act)

Constraints:

- Establish comprehensive ICT risk management frameworks.
- Regular testing and incident reporting.
- Oversight of third-party ICT service providers.

Future Challenges:

- Managing complex third-party dependencies.
- Enhancing resilience against sophisticated cyber-attacks.
- Maintaining operational continuity amid evolving ICT risks.

Other current & future EU legislative texts : scope, application, constraints and challenges for infrastructure providers in relation to NIS2 & CRA

CER Directive on the Resilience of Critical Entities

Scope: Enhances resilience, security, and contingency planning for critical infrastructure sectors (energy, transport, health, etc.).
Applicability: Applies to critical entities operating within the EU, with future expansions to include more sectors and stricter requirements.
Constraints/Challenges: Compliance costs, operational disruptions, and data sharing complexities for infrastructure providers.
Link to NIS2 & CRA: Reinforces cybersecurity measures and resilience standards aligned with NIS2 and the Cyber Resilience Act.

EU Chip Act

Scope: Promotes secure, resilient, and innovative semiconductor supply chains within the EU, supporting technological sovereignty.
Applicability: Targets chip manufacturers, designers, and supply chain stakeholders, with future initiatives to expand manufacturing capacity and R&D.
Constraints/Challenges: High investment costs, supply chain dependencies, and geopolitical risks for infrastructure reliant on chips.
Link to NIS2 & CRA: Secures critical hardware supply chains, essential for maintaining cybersecurity and operational resilience.

EU eIDAS2

Scope: Modernizes electronic identification and trust services for secure digital transactions across the EU.
Applicability: Applies to digital identity and trust service providers, and users, with future updates to enhance interoperability and security.
Constraints/Challenges: Integration costs, interoperability issues, and ensuring security of digital identities for infrastructure providers.
Link to NIS2 & CRA: Strengthens digital trust and secure communication channels critical for infrastructure cybersecurity.

Other current & future EU legislative texts : scope, application, constraints and challenges for infrastructure providers in relation to NIS2 & CRA

EU Cyber Solidarity Act

Scope: Facilitates coordinated EU responses to large-scale cyber incidents and crises, promoting mutual assistance.
Applicability: Applies to EU member states and relevant cybersecurity authorities, with potential inclusion of private sector cooperation.
Constraints/Challenges: Coordination complexities, resource allocation, and legal jurisdiction issues during crises for infrastructure providers.
Link to NIS2 & CRA: Enhances collective cybersecurity resilience, directly supporting infrastructure security and incident response.

EU DMA, DSA

Scope: Regulates digital market fairness (DMA) and online content moderation (DSA) to ensure a safe and competitive digital environment.
Applicability: Applies to large digital platforms and online service providers operating within the EU, with ongoing updates to address emerging digital challenges.
Constraints/Challenges: Compliance costs, operational adjustments, and potential restrictions on platform operations for infrastructure-dependent services.
Link to NIS2 & CRA: Improves cybersecurity posture and operational resilience of digital platforms, aligning with broader EU digital security objectives.

Other current & future EU legislative texts : scope, application, constraints and challenges for infrastructure providers in relation to NIS2 & CRA

EU DNA (not yet on the table – expected Q4 25)

Scope: Focuses on digital network architecture, data management, and interoperability standards for secure digital infrastructure.
Applicability: Targets digital infrastructure providers, data operators, and network service providers, with future developments to improve security and interoperability.
Constraints/Challenges: Standardization costs, legacy system integration, and ensuring security across diverse infrastructure components.
Link to NIS2 & CRA: Provides foundational standards that support cybersecurity and operational resilience of digital infrastructure.

EU AI Liability (on table for withdrawal by the EC)

Scope: Establishes liability rules for AI systems to ensure safety, accountability, and transparency across sectors.

We have only addressed MNOs related regulations,
Sectorial industries related regulations are not investigated.

Implication for a telecom infrastructure operator

Complex situation, but manageable, we will comply !!

Some Challenges :

- Some Regulation are not consistent and diverge in their requirements
- Some Regulation will be dependant of National transposition, generating complexity for international organisation
- How to industrially rationalize international organisation ? Optimize cost and processus for conformity ?

Implication of NIS2 Directive

150.000 industries or entities may be subject to NIS2 conformity evaluation

EU : 28 countries / certification every 2 years / 200 working days per year

➔14 entities or industries to be certified NIS2 per day per National Cybersecurity Certification Authorities (NCCAs) ….

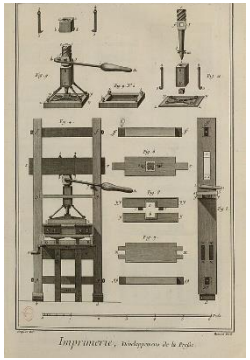
Implication of NIS2 Directive

150.000 industries or entities may be subject to NIS2 conformity evaluation

EU : 28 countries / certification every 2 years / 200 working days per year

➔14 entities or industries to be certified NIS2 per day per National Cybersecurity Certification Authorities (NCCAs) ….

‘manual/paper based’ (descriptive) certification + Pentest



Source : https://gallica.bnf.fr/ark:/12148/bpt6k323141z/f69.item#

Implication of NIS2 Directive

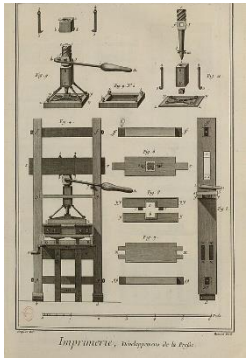
150.000 industries or entities may be subject to NIS2 conformity evaluation

EU : 28 countries / certification every 2 years / 200 working days per year

➔14 entities or industries to be certified NIS2 per day per National Cybersecurity Certification Authorities (NCCAs) ….

How to evolve from ‘paper’ to ‘AI’ ?

‘manual/paper based’ (descriptive) certification + Pentest



‘automatized’ (evidences based) certification

- **Knowledge Base per system**
- **Structured data exchange**
- **Attestations/evidences enforceable**
- **AI Data mining**
- **Continuous evaluation**
- **replicability**

Source : https://gallica.bnf.fr/ark:/12148/bpt6k323141z/f69.item#

New EU certification schemes

EU certification schemes :

- EUCC already published
- EUCS, EU5G, EUDIW under development

EU to recognize the use of EUCC certification(1) to demonstrate conformity with the CRA in a seamless way.

EU5G potentially splits in two parts,

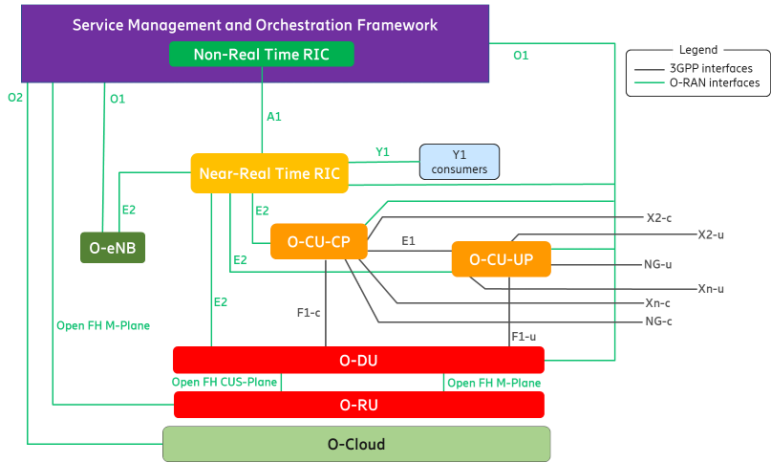
- one dedicated to critical Network Functions and Equipment (level **High** under EU CSA),
- the second focusing on equipment certified at level **Substantial** under EU CSA, that may be delegated to an assimilated GSMA NESAS(2) scheme (similar to CRA conformity, and directly managed by Network equipment suppliers)

(1) : EUCC has to evolve for this equivalence
(2) : see https://www.gsma.com/solutions-and-impact/industry-services/assurance-services/network-equipment-security-assurance-scheme-nesas/

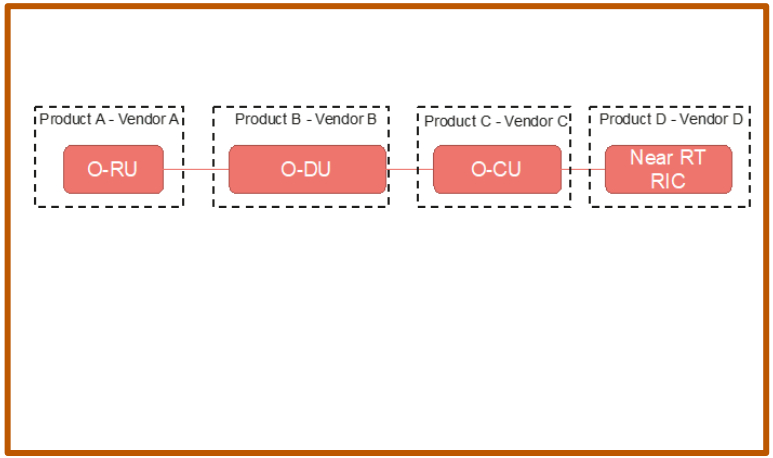
Practical use case with O-RAN

Under ENISA Risks Analysis, O-RAN network elements will have to be certified at level High under EU-CSA.

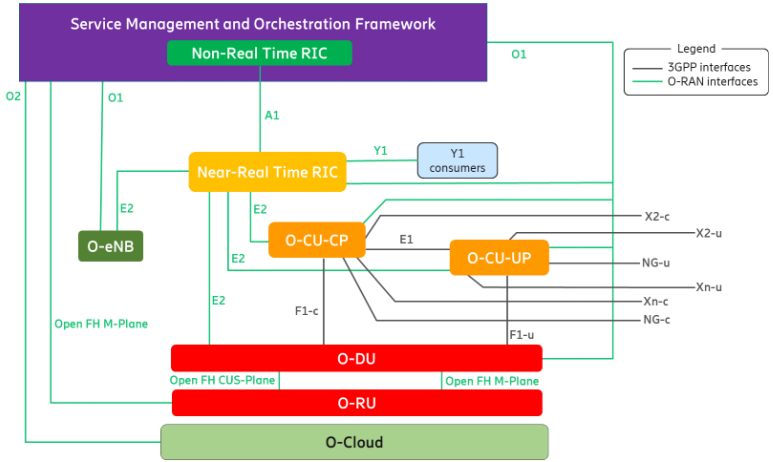
➔Problem position : software certification under EU-CSA at High level or EUCC at least at EAL4 or AVA-VAN3 ?



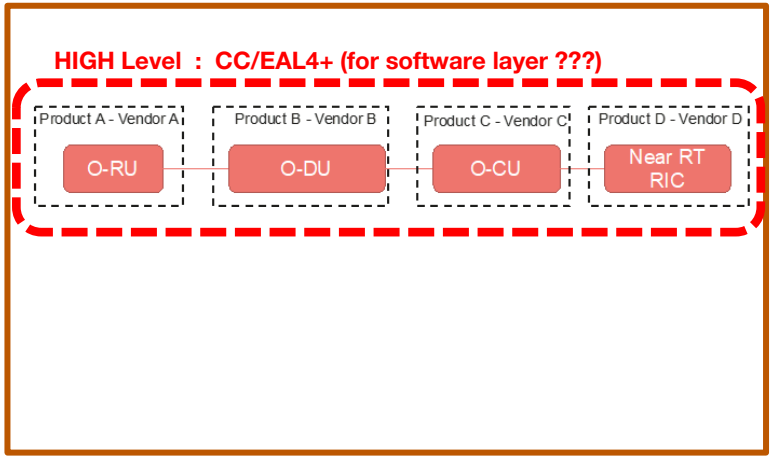
O-RAN system view (Source: O-RAN alliance)



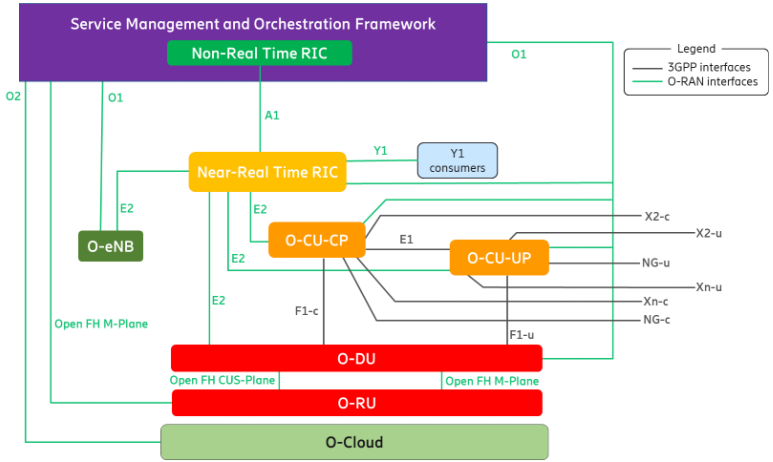
O-RAN components certification ?



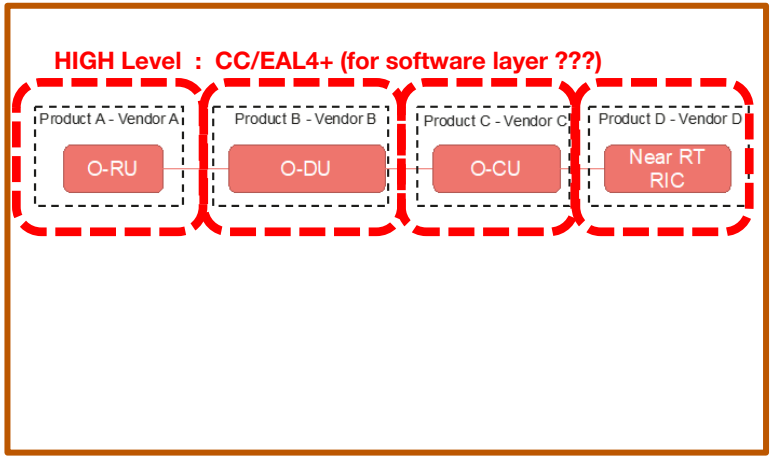
O-RAN system view (Source: O-RAN alliance)



O-RAN components certification ?



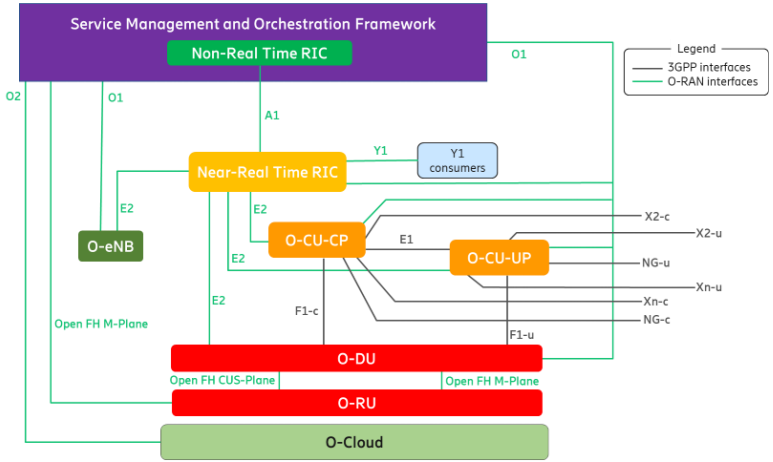
O-RAN system view (Source: O-RAN alliance)



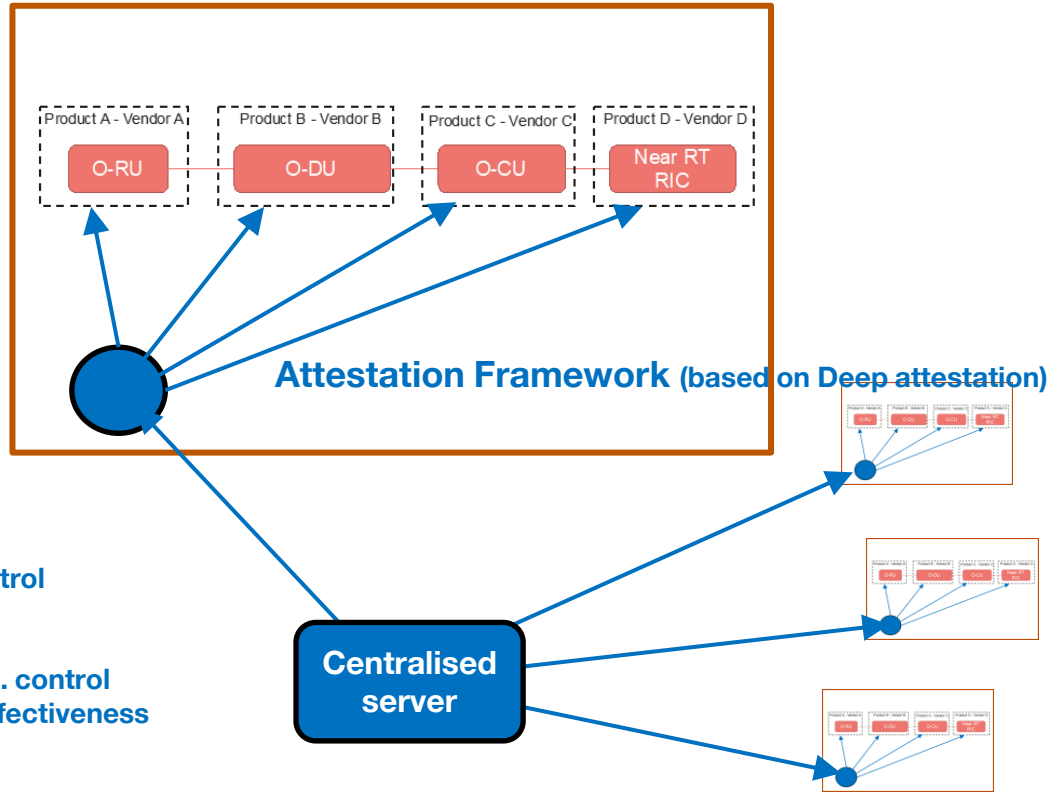
Proposition :

Escape from impossibility of software certification at High level by referring to an external element serving as a trusted anchor for the provision of proofs/evidences.

O-RAN components certification : based on continuous monitoring ?



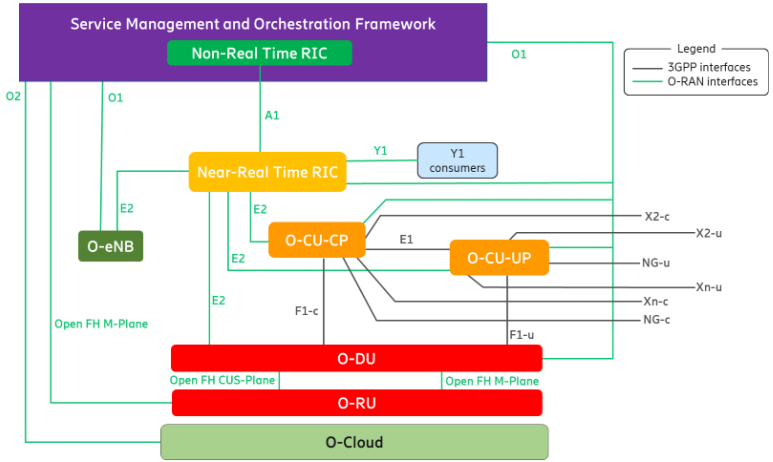
O-RAN system view (Source: O-RAN alliance)



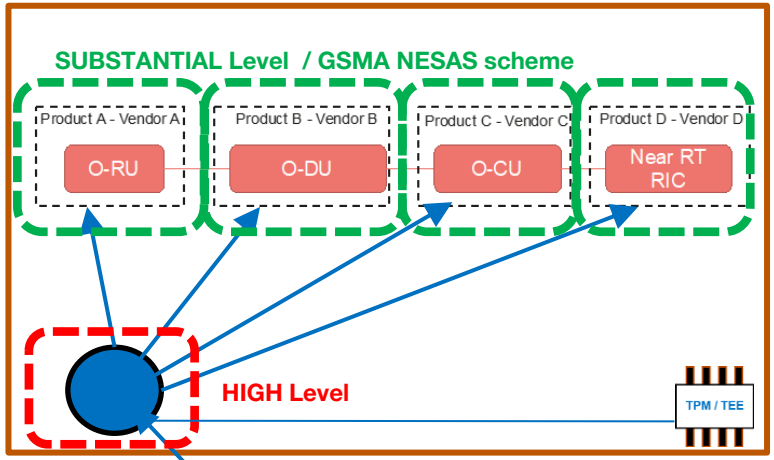
Attestation Agent

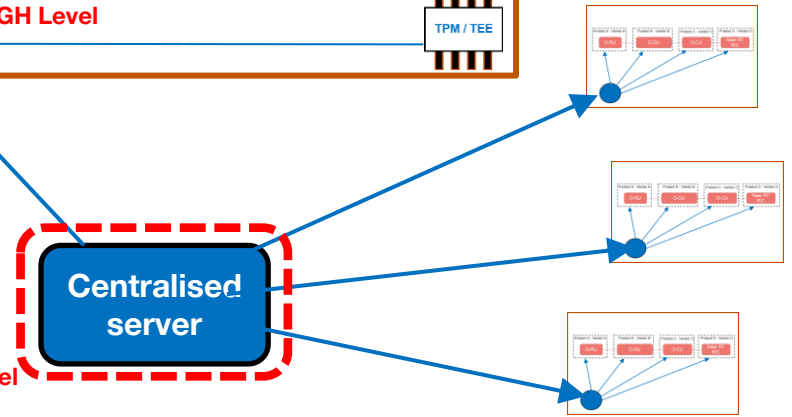
- Component Integrity Control
- Proof of Origin
- Parameters control
- Inter Components Comm. control
- OS / Patchs : Control / Effectiveness
- .....

“Continuous certification” for O-RAN certification ?



O-RAN system view (Source: O-RAN alliance)





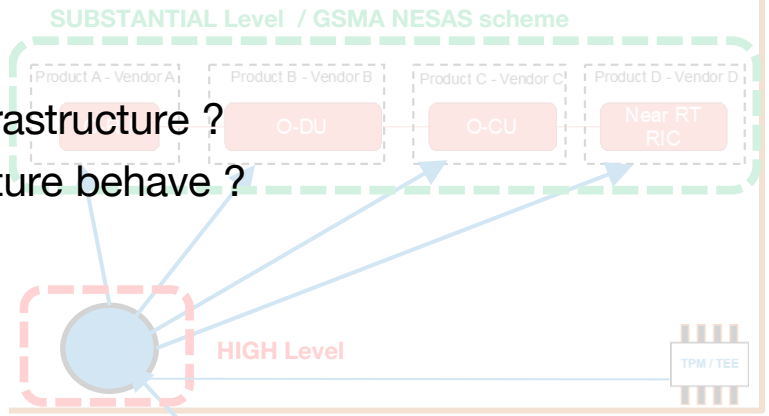
Attestation Agent

- Component Integrity Control
- Proof of Origin
- Parameters control
- Inter Components Comm. control
- OS / Patchs : Control / Effectiveness
- …..

“Continuous certification” for complex infrastructures ?

Could we generalize this approach, in order to be in capacity to commit on some properties ?

- To achieved which measures in the infrastructure ?
- To deliver which KPIs on the infrastructure behave ?



For which business ?
A capacity to sell SLAs ?

Could we demonstrate security ‘equivalence’ with CSA level High for specific security objectives ?

Attestation Agent

- Component Integrity Control
- Proof of Origin
- Parameters control
- Inter Components Comm. control
- OS / Patchs : Control / Effectiveness
- .....

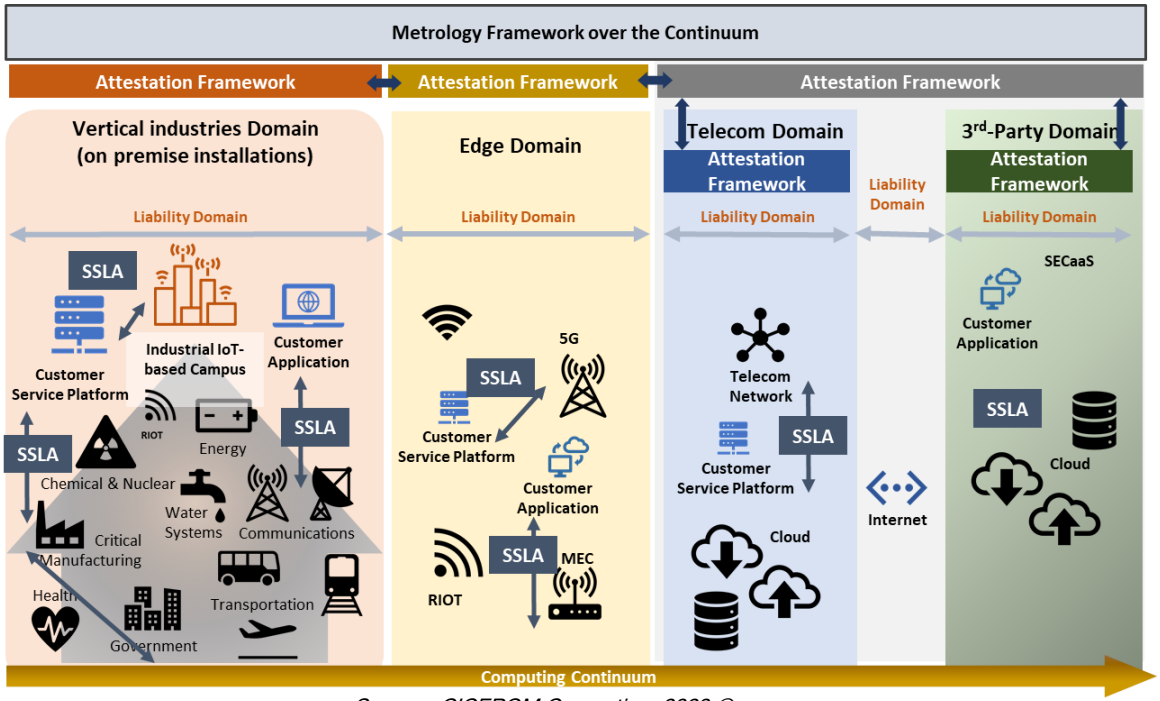
“Continuous certification” for complex infrastructures ? Some “native” Metrology framework ?

Could we generalize this approach, in order to be in capacity to commit on some properties ?

- To achieved which measure in the infrastructure ?
- To deliver which KPIs on the infrastructure behave ?

For which business ?
A capacity to sell SLAs ?

Could we demonstrate security ‘equivalence’ with CSA level High or specific usage for EUCS ?



Source : CICEROM Consortium 2023 ©

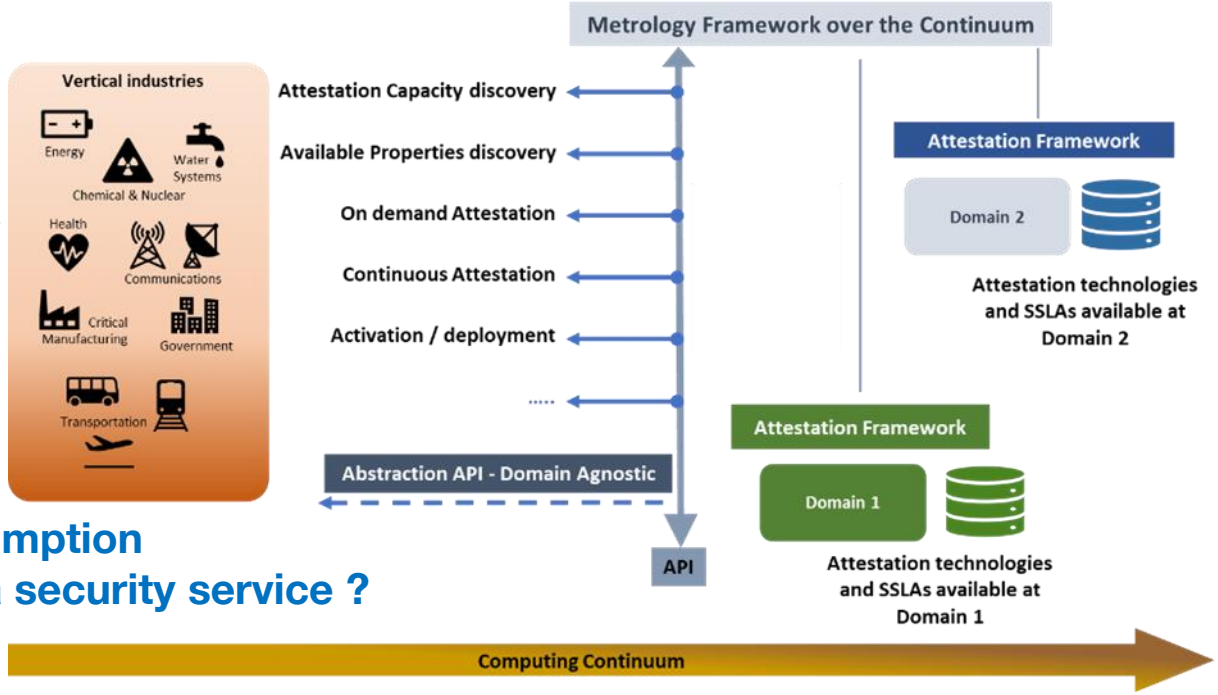
“Continuous certification” for complex infrastructures ? Some native Metrology framework ?

Could we generalize this approach, in order to be in capacity to commit on some properties ?

- To achieved which measure in the infrastructure ?
- To deliver which KPIs on the infrastructure behave ?

For which business ?
A capacity to sell SLAs ?

A capacity to control some assumption of compliance or realization of a security service ?



Source : CICEROM Consortium 2023 ©

How to pave the way to Delegation of security (services) ?

Flexible delegation of security- related responsibilities while optimizing costs and complexity

➔Dynamic control capabilities

Management of on-demand SSLA responsibilities and dynamic achievement demonstration

➔Ability to allocate / redistribute responsabilities

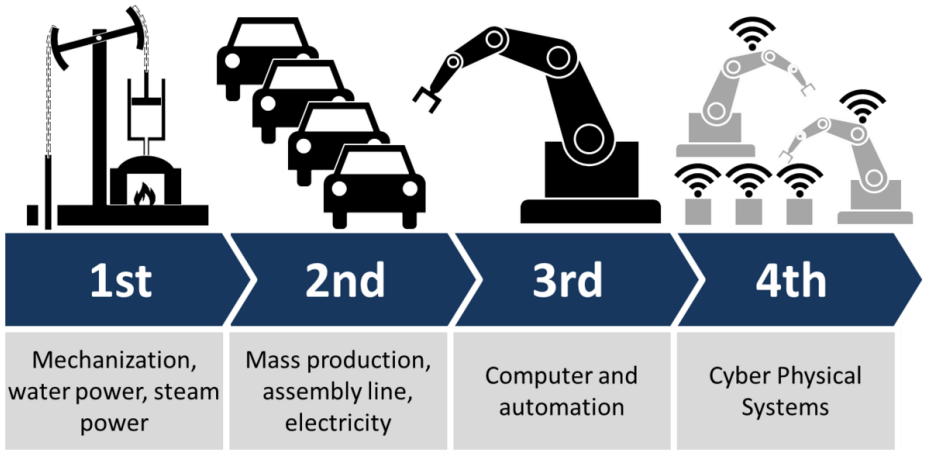
Challenge : How to contract and/or control a SLA in a multi-parties / multi-layers or evolving structure or platform ?

How to address Industry needs with On Demand-security ?

Industries cyber threats exposure

Industries attack surface is extended by the integration of :

- cyber-physical systems,
- Industrial Internet of Things (IIoT),
- cloud-connected platforms



Source : https://commons.wikimedia.org/wiki/File:Industry_4.0.png

Safety and Cybersecurity can no longer be treated as separate disciplines(1).

- Functional safety focuses on ensuring that systems perform their intended functions without leading to hazardous situations(2).
- Cybersecurity addresses intentional threats that target system vulnerabilities(3).

Challenges consideration of Safety and Cybersecurity

A cybersecurity breach can now directly compromise safety functions[4].

The deeper we analyze industrial infrastructure cybersecurity risks, the more underlying safety challenges we uncover.

➔no safety without cybersecurity.

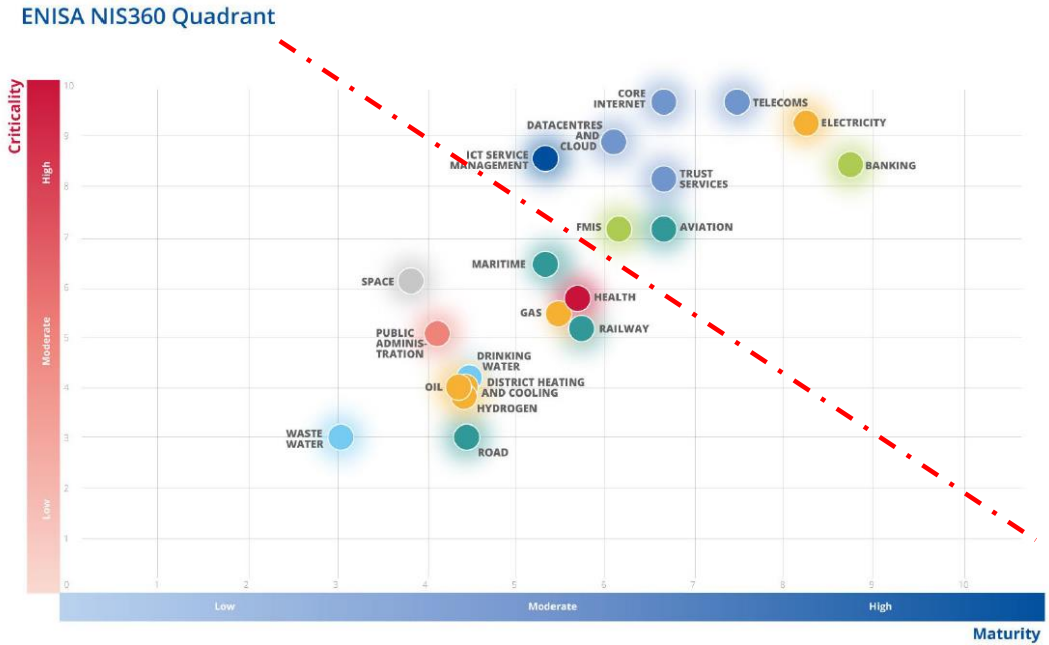
➔Safety and Security requirements should be jointly investigated[5].

Safety and Cybersecurity are commonly built on risk-based and risks reduction approaches.

See Technical report IEC TR 63069 (guidance document for integrating functional safety and cybersecurity in Industrial Automation and Control Systems (IACS))

Business Contraints

Could « Critical Industry » constraints (regulation) become security means obligation ?



Business Contraints

Could « Critical Industry » constraints (regulation) become security means obligation ?

Safety requirements / objectives → **Security requirements / objectives**

Industries → Operators

Evolution : 2/3/4G (Best Effort) → 5/6G with specific security & safety means obligation ?

Business Contraints

Could « Critical Industry » constraints (regulation) become security means obligation ?

Safety requirements / objectives
Industries

→

Security requirements / objectives
Operators

Evolution : 2/3/4G (Best Effort)

→

5/6G with specific security & safety means obligation ?

« 5G trusted network »

→ **?**

« 5G trustable network »

towards an industrial use of the Attestation/Metrology Framework

source : H2020 INSPIRE5G+ (2022)

Demonstration of a first prototype to operate an obligation of 'result' of security property (through SLA) for critical industry verticals (NIS2 & CSA)

- SLA : "*Your applications only share physical resources (over a Cloud or virtualized infrastructure like 5G/MEC) with applications with levels of criticality equivalent or greater*"

- Placement optimization under constraints for criticality and latency (over K8S)

Which set of SLAs ?

- isolation under constraints : criticality, latency, energy efficiency & cost
- authentication of chain of components or of the underlying system (OS, VM, containers, applications)
- effective availability of allocated resources (CPU, memory, TPM, TEE, bandwidth) on physical servers and / or the chain of components
- Only ‘qualified’ or agreed components are put in production to serve Customers.
- composition and insertion of additional services are effective
- authentication at boot-time and at run-time of critical components of the Customer
- critical segments of the Customer are only operated in a protected environment (TEE / HSM).
- software / data zoning : critical components of the Customer are only available and/or executable on identifiable target zones
- data security (integrity and confidentiality) during processing
- ……

➔Potentiality of commercial scheme, based on legal agreement “Convention of Proof” to commit parties on On-demand Security.

How to reuse it to ease NIS2 certification ?

SLA under convention of proof could be continuously monitored, with continuous collect of attestations/evidences enforceable.

➔Vertical could potentially delegate some of their security objectives to third parties

➔National Security Agencies may be in capacity to continuously monitor specific SLAs delivered for a Vertical operated over the infrastructure

How to demonstrate those equivalences between SLAs and Security needs of certification schemes ?

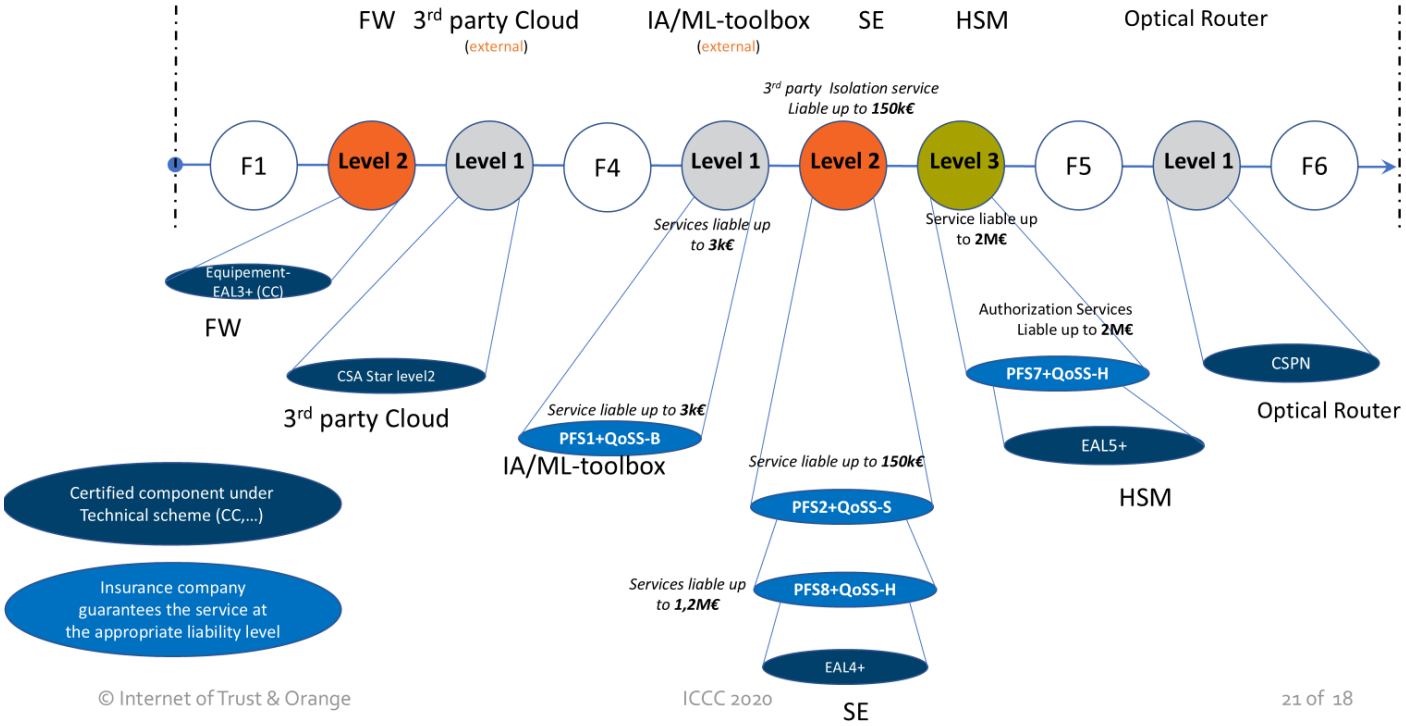
- establish an equivalence between sets of SLAs, which are assessed through the attestations, that are dynamic, and sets of security objectives, dealt with in certification schemes, but in a static manner.

How to reuse it to ease NIS2 certification ?

How to shift from a **static evaluation / certification** of a service/platform before production to a **continuous monitoring**, thank to certified attestation framework ?

- a potential framework to **adapt dynamically an E2E robustness level** to allow continuity of critical activities upon the detection of incidents.
- **a hybrid approach combining security objectives and SLAs** to identify necessary conditions to dynamically change the robustness level for the dedicated infrastructure in the computing continuum.
- **a new composition scheme** between a set of Security Objectives and SLAs with associated evidence collection, (combining SSLA measures and the Metrology Framework for attestation)

Get appropriate assurances



Source : ICCC 2020, Claire Loiseaux, "Trust model for verticals over 5G"

➔how to allow an E2E robustness level evaluation for a dedicated service over a multi-parties infrastructure in the computing continuum ?.

Future challenges to achieved a composable NIS2 certification of infrastructure

Today under Common Criteria and EUCC scheme we know how to certifiy a system composed of multiple components already certified (see eUICC certification at High level, managed by GSMA).

But this composition of components is dedicated to a close environment (the TOE Target of Evaluation under CC/EUCC) and rely on environmental hypothesis (not really structured).

- How to define the composition of components (‘Lego(1)‘ approach) in an open system (a cloud infrastructure or 5G core infrastructure) ?
- Do we have to constraints some ‘EUCC compatibility’ regarding environmental hypothesis of each of those ‘Lego bricks’.
- Which tools and data structures will have to be define ? Do we have to reconsider the CC/EUCC Protection Profil (PP) concept and declined it for a specific platform, in a way we can use automatic tooling to perfom those ‘additions’ between components ?

(1) Lego™

Future challenges to achieved a composable NIS2 certification of infrastructure

Today, there is no real technological nor theorical lock identified that may prevent to consider or propose a Platform oriented PP/Lego(1) Bricks composition framework.

An Hybrid framework combining commercial / liability SLAs delegation, certified Attestation framework with Security Objectives and PP/TOE (CC / EUCC) per platform.

Some additional challenges and investigations :

- Usage of xxBOM(2) structures for CRA compliance and vulnerabilities qualification ?
- Usage of attack paths for CRA or NIS2 compliance ?
- Automatic generation of Knowledge-Base per platform to ease CRA and NIS2 compliance ?

- How to take into account in the proposed Hybrid scheme new On-Demand-Security based on Moving Target Defense (MTD) technology ?
- How to certify at the upper EU CSA level an MTD offer ?

(1) Lego™ (2) See : https://cyclonedx.org/

Thanks