New paradigm for privacy in 6G and beyond

Enrico DEL RE

University of Florence and CNIT

Italy

User data protection and privacy

- Recent and repeated violations of sensitive personal data made it clear even to the majority of ordinary Internet users that privacy protection is a mandatory issue for NGI
- To make users confident with the new technologies (5/6G, AI and IoT) we must assure that the concrete violation of the fundamental human rights of personal data protection and privacy is eliminated as far as possible
- Otherwise, we shall be faced with the probable risk of generalized rejection of the new technologies and their benefits

Inadequacy of present privacy normative rules

- The EU GDPR is the more advanced regulation of normative rules for the user data protection and privacy in NGI
- Personal data protection is entrusted to third parties as service providers or network operators
- This is not adequate to guarantee the ultimate user privacy rights for two main reasons
  - First, we must rely on the correct behavior of a not always reliable third party
  - Second, future technologies (6G, AI, IoT) may acquire human sensitive information without the awareness of the interested subjects, e.g. automatic profiling, automatic facial recognition and individual pheromones, that are very difficult or even impossible to be ruled by the GDPR

What we need

- We must fully comply with the stated EU principle "*Individuals shall remain in control of their personal data generated or processed*"
- Not only *a posteriori* (as potentially provided by a Distributed Ledger Technology, like Blockchain)
- Definitive solution of personal data control must be implemented *a priori*
- We need the **human-centric privacy new paradigm** of *"individual a priori data usage control"*

New scientific paradigm
"individual a priori data usage control"

- Defined as: *"except in cases of force majeure or emergency, any use in any form and for any purpose of personal data must be authorized in advance and explicitly by its owner, correctly informed of the purpose of use"*.
- To meet this highly challenging objective, we need synergize innovative and revolutionary normative rules (as GDPR) and very innovative efficient scientific and technological tools specifically dealing with the direct and *a priori* control by the user of her/his data.

What to do

- Currently, some international research projects are ongoing on this subject. In the literature, they appear with different names: "*User-centric security and privacy*“, "*Information-centric cybersecurity*", "*Usage control cybersecurity*“ [see references]
- Absolute necessity of a continuing disruptive research to arrive in reasonable time frames at effective tools, simple enough to be affordable by the ordinary Internet user
- The International Scientific Community (within EU in particular) has the challenging and primary task to strongly ask for sufficient funding to sustain scientific and technical initiatives on the subject of the *definitive a priori* user-controlled personal data protection and privacy
- To be pursued in spite of the likely resistances by major actors and absolutely mandatory to guarantee the fundamental individual rights to all people in the future human digital society

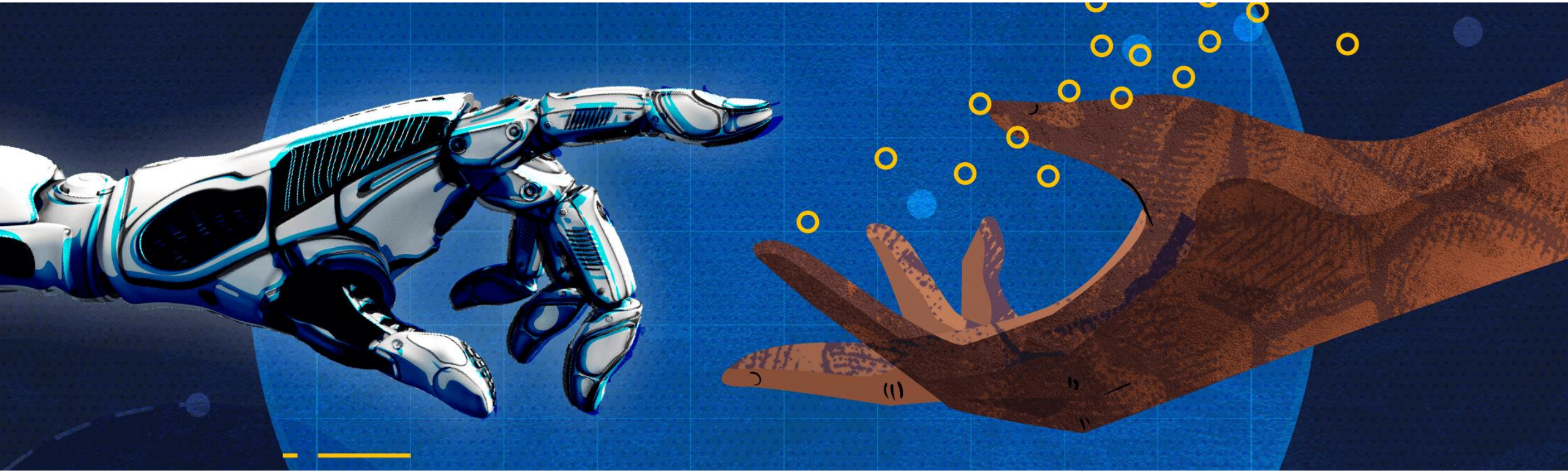
References

- E. Del Re, "Which future strategy and policies for privacy in 5G and beyond?“, 2020 IEEE 3rd 5G World Forum (5GWF), Bangalore, India, Sept. 2020, pp. 235-238, doi: 10.1109/5GWF49715.2020.9221371.
- R. Chow, et al., *Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control,* in *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, ser. CCSW ’09. New York, NY, USA: ACM, 2009, pp. 85–90 http://doi.acm.org/10.1145/1655008.1655020 .
- R.B Lee*, Rethinking computers for cybersecurity,* IEEE Computer, 2015.
- *IEEE Communications Mag.,* Jan. 2017.
- A. Lazouski, F. Martinelli, P. Mori, *Usage control in computer security: A survey*, Computer Science Review, vol. 4, no. 2, pp. 81–99, May 2010 http://dx.doi.org/10.1016/j.cosrev.2010.02.002 .
- E. Carniani, D. D’Arenzo, A. Lazouski, F. Martinelli, P. Mori, *Usage Control on Cloud systems,* Future Generation Computer Systems, vol. 63, pp. 37 – 55, 2016, Modeling and Management for Big Data Analytics and Visualization http://www.sciencedirect.com/science/article/pii/S0167739X16300875 .
- J.L. Hernandez Ramos, A. Skarmeta, (Eds), *Security and Privacy in Internet of Things - Challenges and Solutions,* within the series: *Ambient Intelligence and Smart Environments,* (*Introduction* by E. Del Re), IOS Press, 2020.

Human in the Loop

Arianna Schuler Scott

arianna@safenetics.co.uk

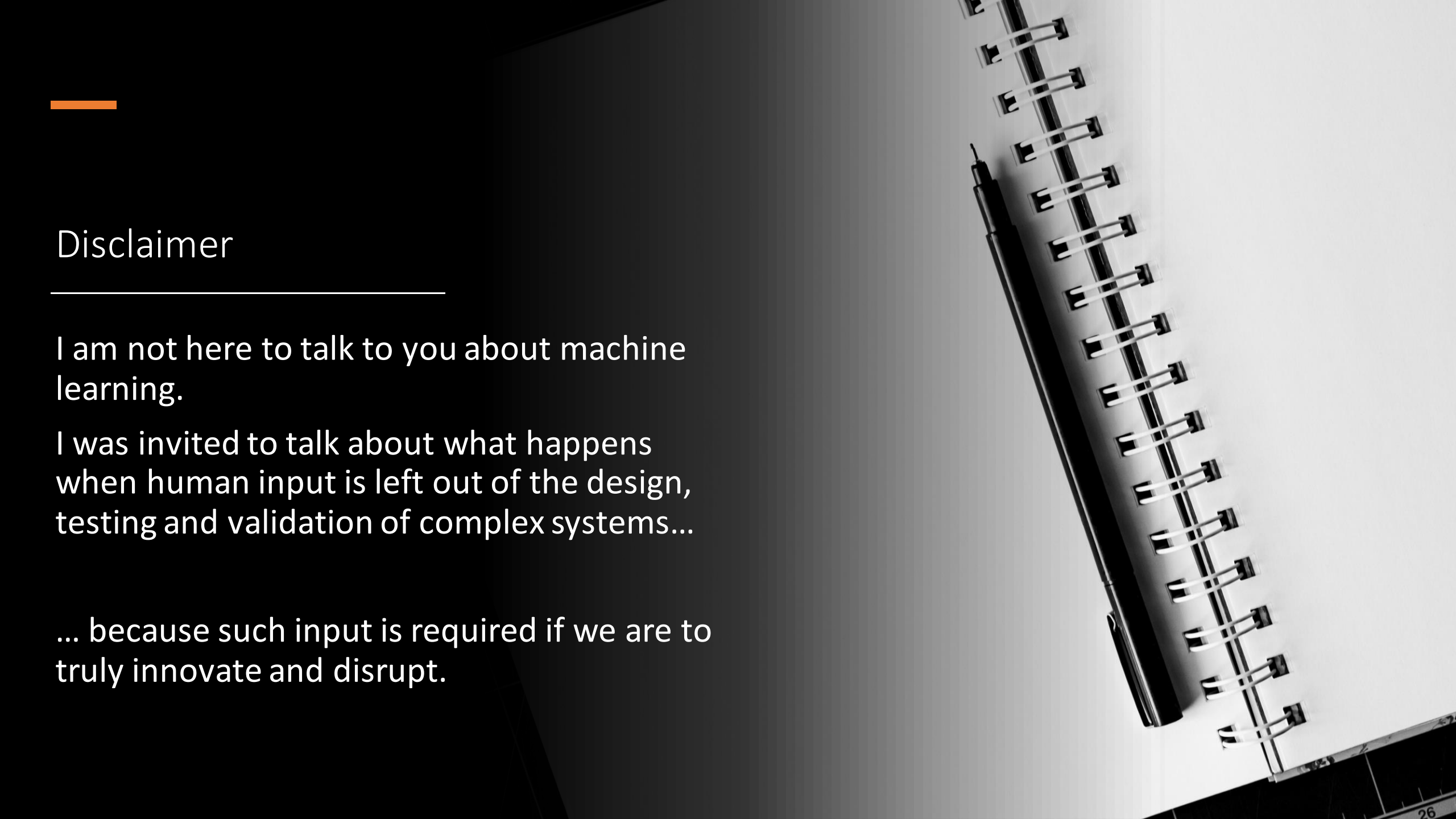


Disclaimer

I am not here to talk to you about machine learning.

I was invited to talk about what happens when human input is left out of the design, testing and validation of complex systems…

… because such input is required if we are to truly innovate and disrupt.



H in the L: a development approach

Automation: selective inclusion of human participation (rather than the removal of human involvement in a task)[1].

Design principles

- Harness human agency.
- Reduce complexity, without over-simplifying.
- Interfaces should extend (e.g., capability, understanding…).

Benefits

- **Human judgment: enabled**
  - Value lies in agency and being able to exercise preference, as well as efficiency and correctness.
- **Imperfection: acceptable**
  - "Correct" behaviour can be developed over time as the technology will ultimately be guided by human/s.
- **Transparency++**
  - As we design human-readable/understandable interfaces, and the process being automated becomes less obscure.
- **Power++**
  - Equipping a human with relevant information and supporting the decision-making process may show that a "hybrid" approach (not entirely automated or manual) improves performance.

How could we do this?

This is a room of network people who do not work with users.

BUT novel ideas → testbeds → wider use → standard practice.

We have been talking about a need to design interfaces.

Of future networks, we could ask:

- In what ways could humans become part of this loop?
- Where might human judgement and preferences improve effectiveness?
- How could we accept human feedback (and what can that be used for)?
- What might an interaction models or user interfaces look like?

How might we measure this?

- Future networks are going to need to accommodate technical, economical and social conditions.
- In this complex space we are going to need to demonstrate value.
- Performance indicators may be helpful (we know a lot about these).
- Value indicators may be helpful (we are not used to working with these).
- Let us take a Human in the Loop smart factory system as an example:
  - The Loop: asset tracking, security cameras, environment sensors feed data into a monitoring platform. Information from safety-critical systems is prioritised.
  - The Human: digital twin specialist, using XR tech to monitor production.
  - KPI: overall equipment effectiveness, cycle time, customer satisfaction (surveys).
  - KVI: employee privacy, customer trust, employer responsibility.

Summary

- At this summit, we are thinking about:
  - How to identify relevant technologies for future research.
  - Specifically, research directions for the communications field.
- Currently, there is a lack of:
  - Humans in the Loop.
  - Consideration of societal impact.
  - Interfacing (i.e., communication, from one layer to another and vice versa).
- There is significant focus on the building smarter, faster, "better", but **who** benefits from massively fast, super-low latency cat videos in 4k?
- I would like to add to the conversations we have had so far:
  - Real change requires significant re-thinking of how we build with (and for) humans.
  - E.g., an excellent and exciting look into the work ahead… Tactile Internet with Human-in-the-Loop[2].

References

Title image: Bisen (2020). “What is human in the Loop Machine Learning, Why & How Used in AI” (url).

[1] Wang (2019). “Humans in the Loop: The Design of Interactive AI Systems” (url).

[2] Fitzek, Li, Speidel & Strufe (2021). Tactile Internet with Human-in-the-Loop: New frontiers of transdisciplinary research. In Tactile Internet (pp. 1-19). Academic Press (url).

THALES

6G security challenges

introduction to cybersec landscape & few messages

Emmanuel Dotaro
Head of ICT&Security labs, Thales/SIX/CTO

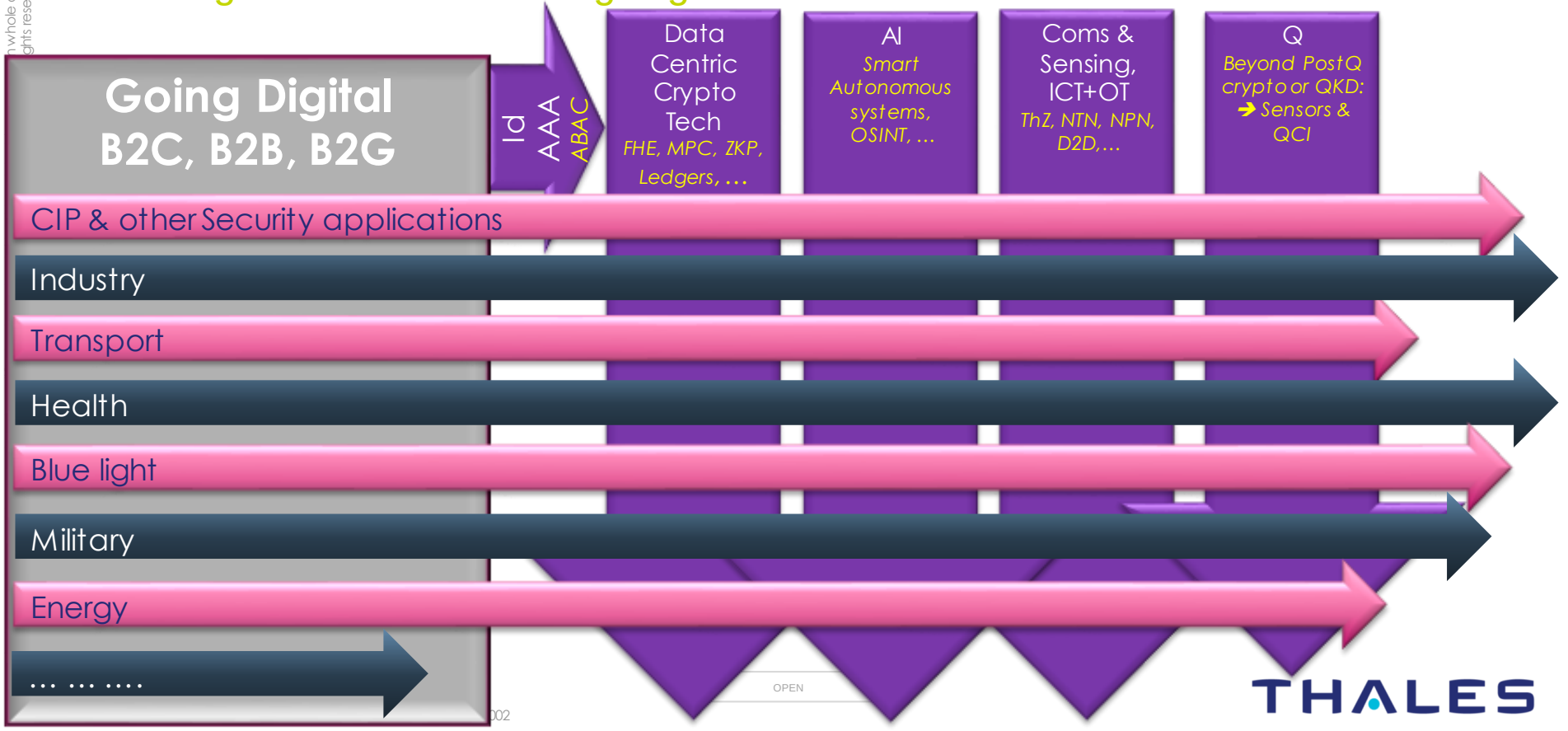
emmanuel.dotaro@thalesgroup.com

TrXst in Me

…at least, not just for your eyes…tell me why !

Tech Disruptions as common (Digital) scope

Assuming transformation is ongoing…

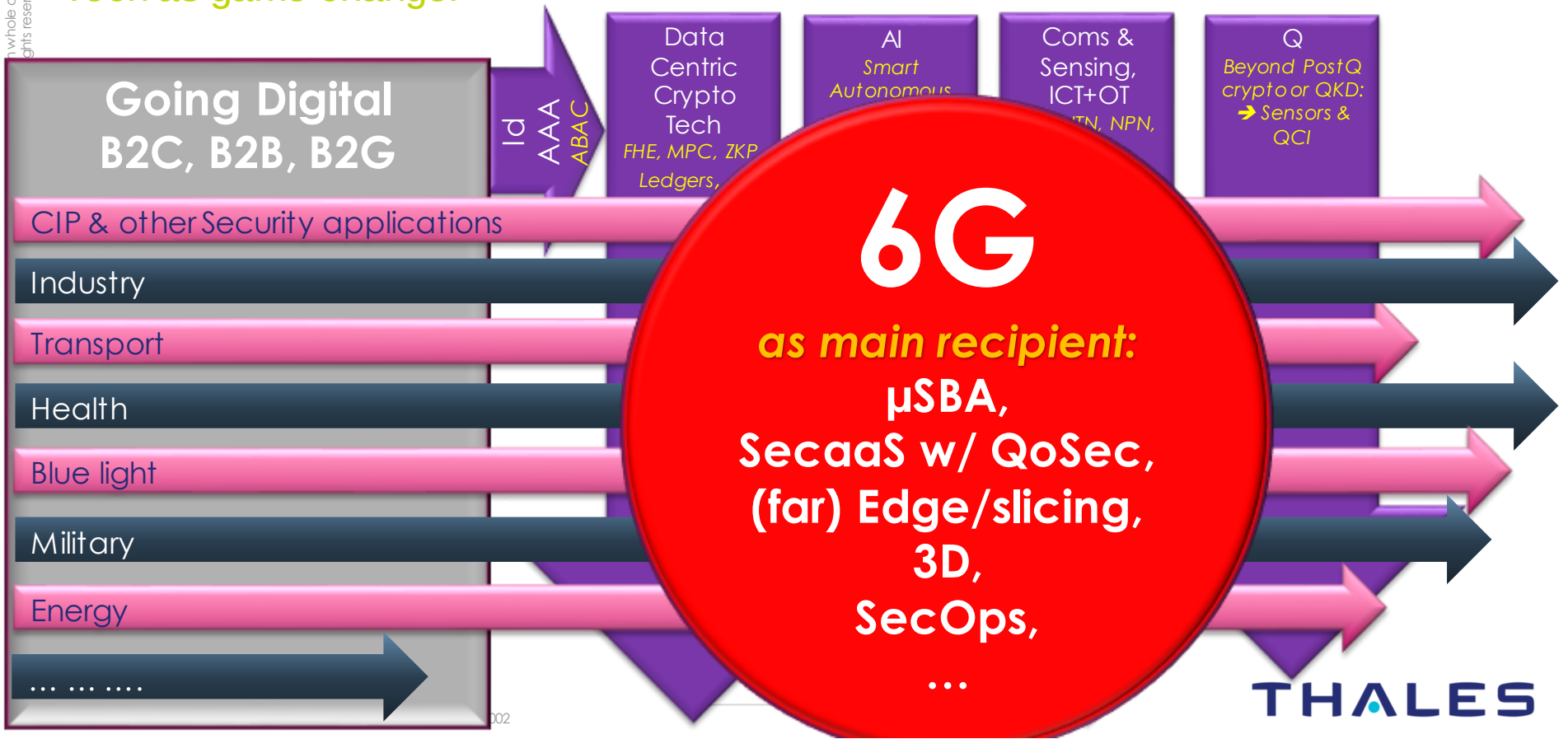


OPEN

THALES

Arch & Biz Disruptions as a companion

Tech as game changer

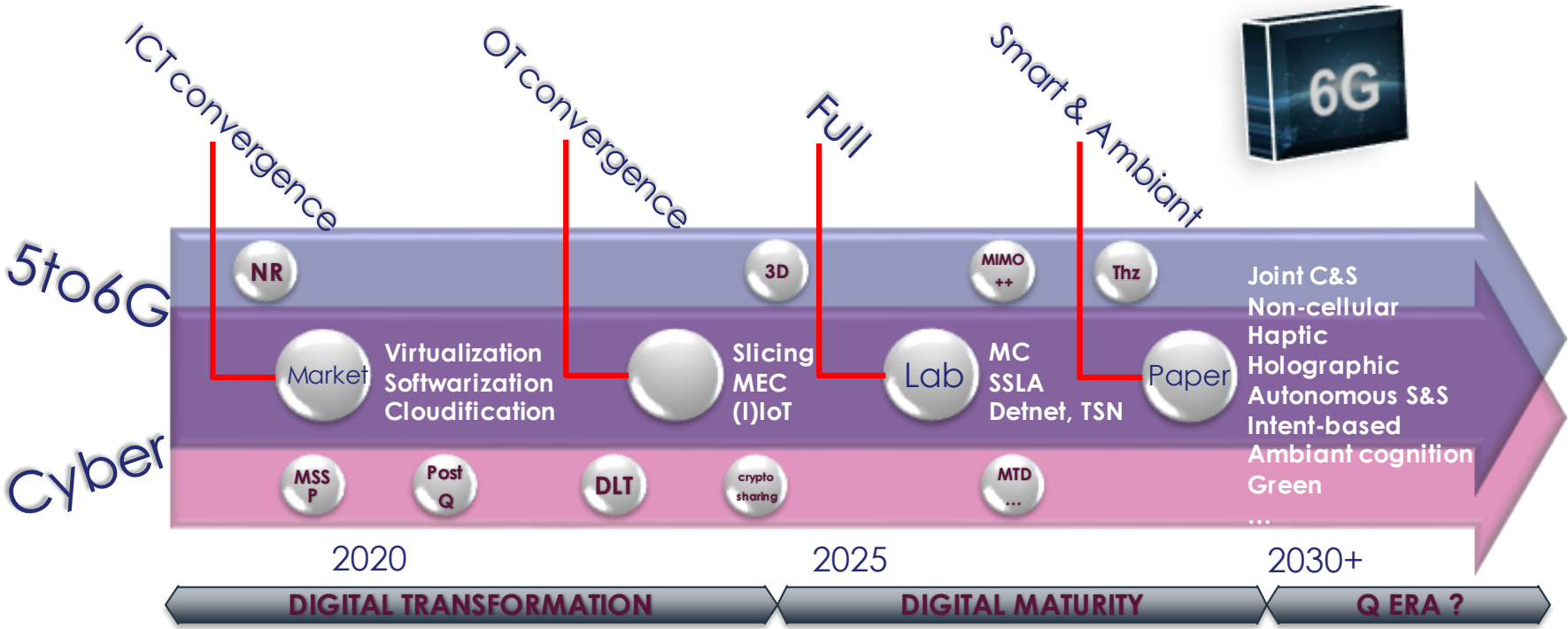


THALES

xG & Cyber a common path

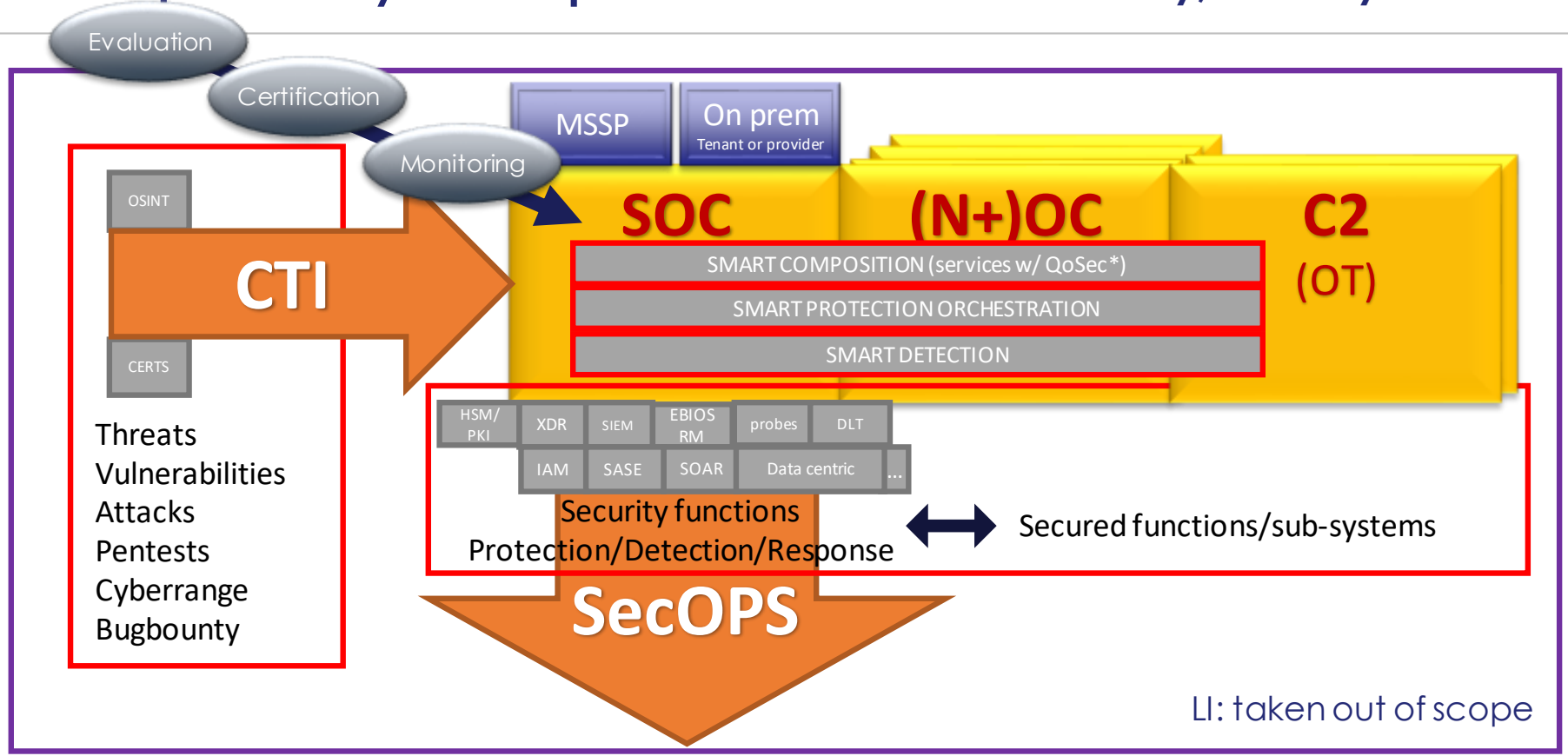
dynamics,
Smart
autonomous
Highly distributed
…

Problem space: Static perimeter➔herogeneous➔fragmented/polymorphic➔metamorphic
Solution space: perimetric ➔by Design (really ?)➔ sticking systems and services fundamentals



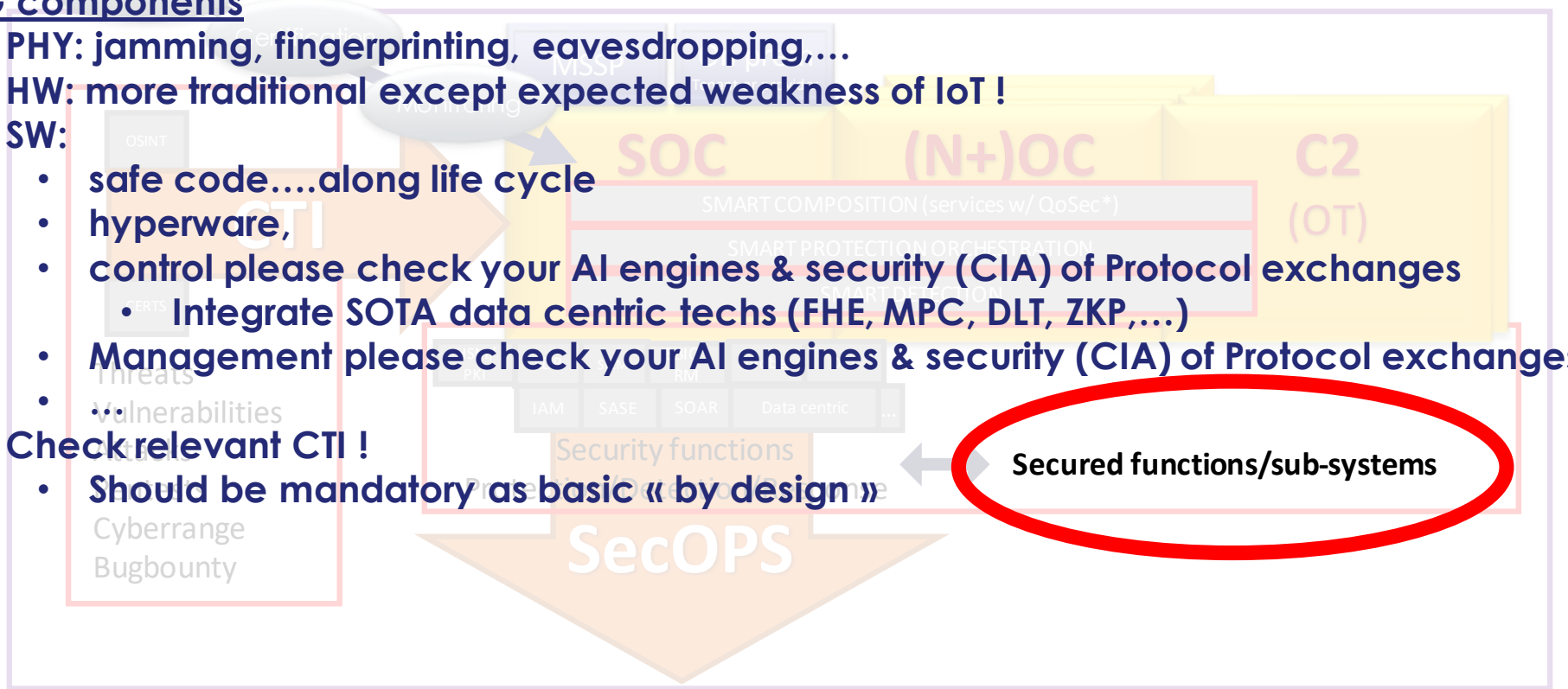
THALES

Lanscape from cybersec point of view: Tech for security, Security of Tech



*Invited Keynote, IEEE Conference on Communications and Network Security, 2020,
Quality of Security: the mandatory service attributes? – Evaluation, exposure, composition, monitoring of QoSec for SecSLA in 5G & beyond developments

Lanscape from cybersec point of view: Tech for security, Security of Tech

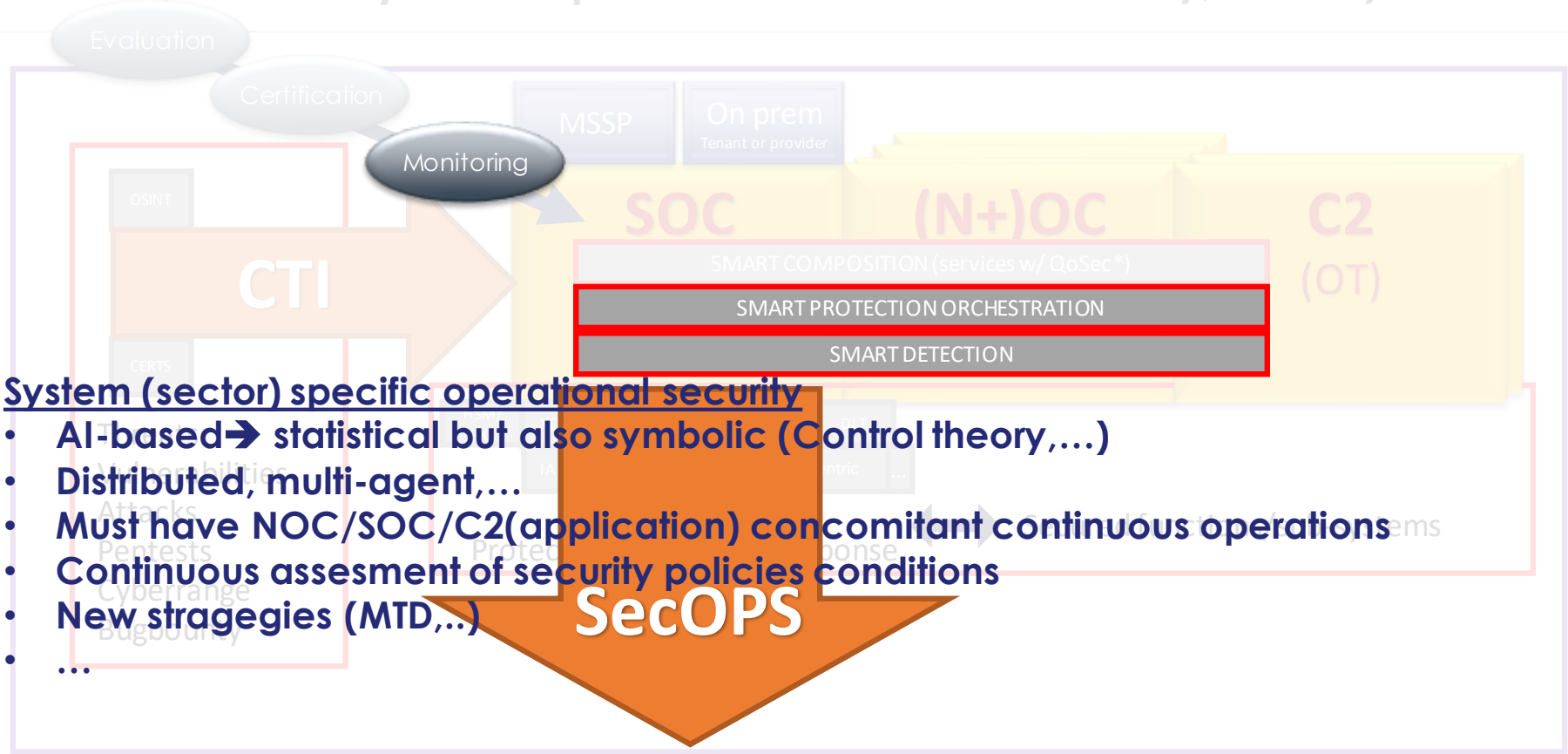


6G components

- PHY: jamming, fingerprinting, eavesdropping,…
- HW: more traditional except expected weakness of IoT !
- SW:
  - safe code….along life cycle
  - hyperware,
  - control please check your AI engines & security (CIA) of Protocol exchanges
    - Integrate SOTA data centric techs (FHE, MPC, DLT, ZKP,…)
  - Management please check your AI engines & security (CIA) of Protocol exchanges
  - …
- Check relevant CTI !
  - Should be mandatory as basic « by design »

Secured functions/sub-systems

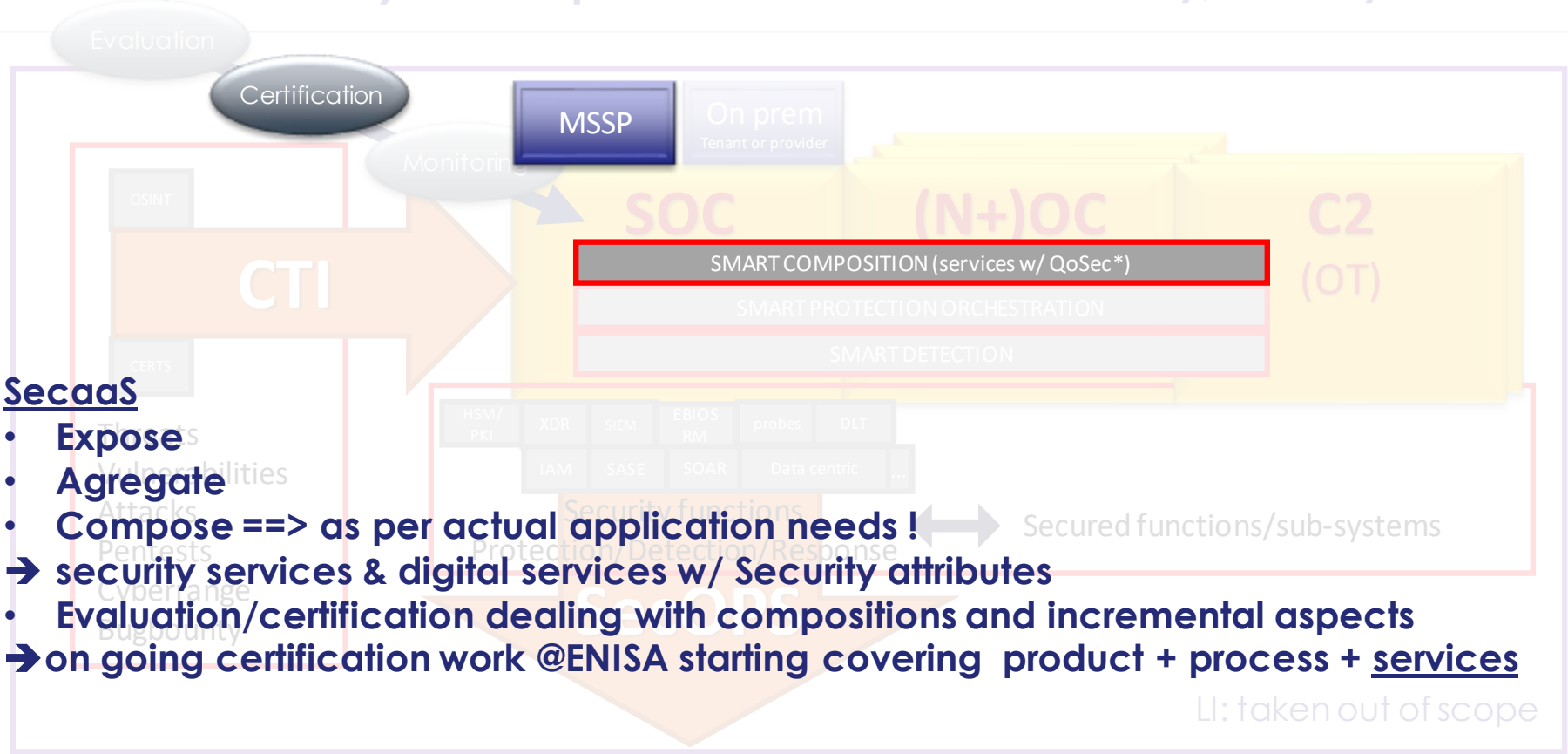
Lanscape from cybersec point of view: Tech for security, Security of Tech



System (sector) specific operational security

- AI-based➔ statistical but also symbolic (Control theory,…)
- Distributed, multi-agent,…
- Must have NOC/SOC/C2(application) concomitant continuous operations
- Continuous assesment of security policies conditions
- New stragegies (MTD,..)
- …

Lanscape from cybersec point of view: Tech for security, Security of Tech



SecaaS

- **Expose**
- **Agregate**
- **Compose ==> as per actual application needs !**

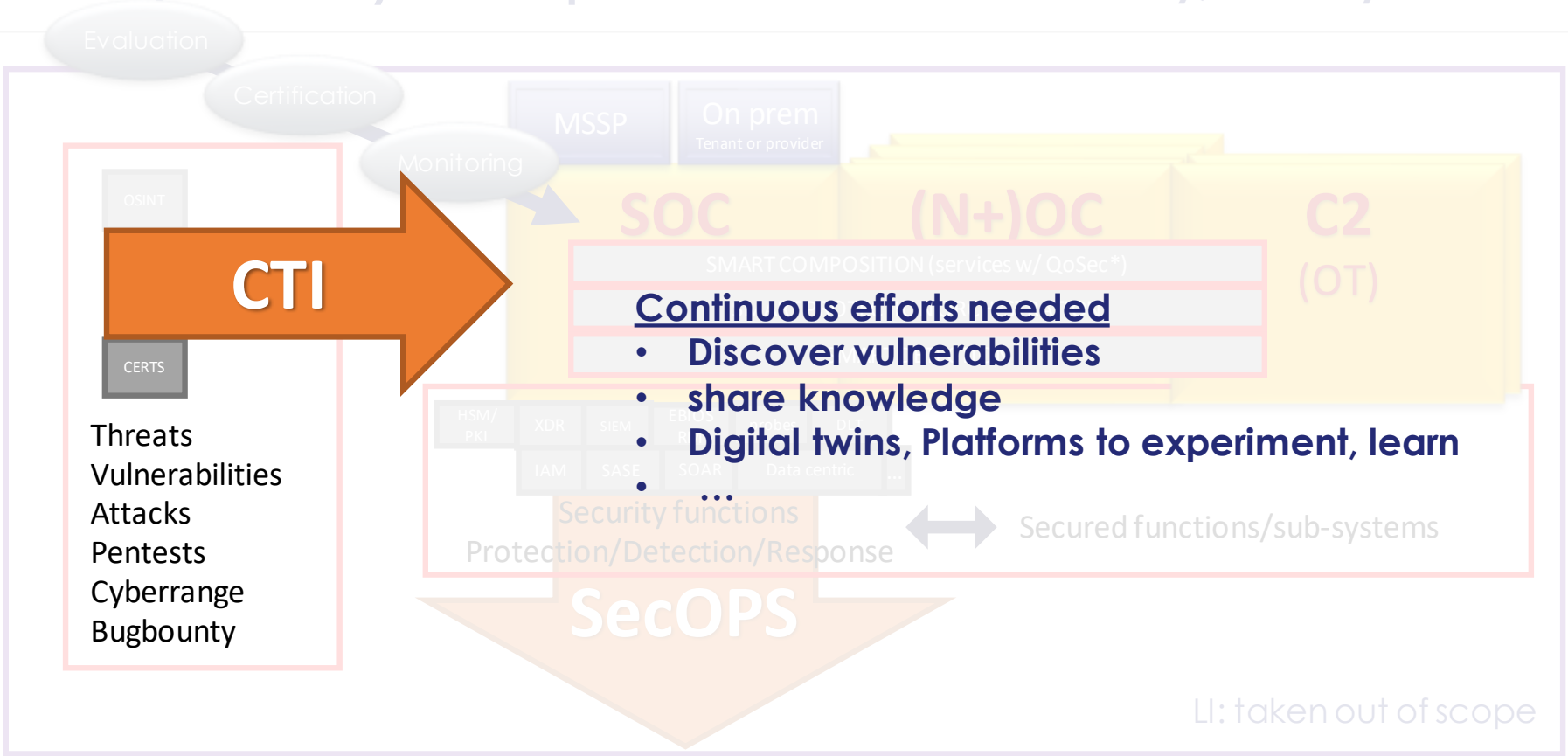
➔ **security services & digital services w/ Security attributes**

- **Evaluation/certification dealing with compositions and incremental aspects**

➔ **on going certification work @ENISA starting covering product + process + services**

*ECSO w hite paper

Lanscape from cybersec point of view: Tech for security, Security of Tech



*Invited Keynote, IEEE Conference on Communications and Network Security, 2020,
Quality of Security: the mandatory service attributes? – Evaluation, exposure, composition, monitoring of QoSec for SecSLA in 5G & beyond developments

Special notice

THALES

THANKS !

www.thalesgroup.com

Smart Software Defined Security in all phases

Make it SMART !!

e.g Source Code morphology

SDsec

PROTECT

DETECT

REMEDIATE

THREAT INTELLIGENCE

e.g pattern matching, Anomaly detection

e.g distributed autonomic response

e.g OSINT

NetWorld

May 2020

Strategic Research and Innovation Agenda 2021-27

European Technology Platform NetWorld2020

"Smart Networks in the context of NGI"

2020

Table of Contents

OPEN

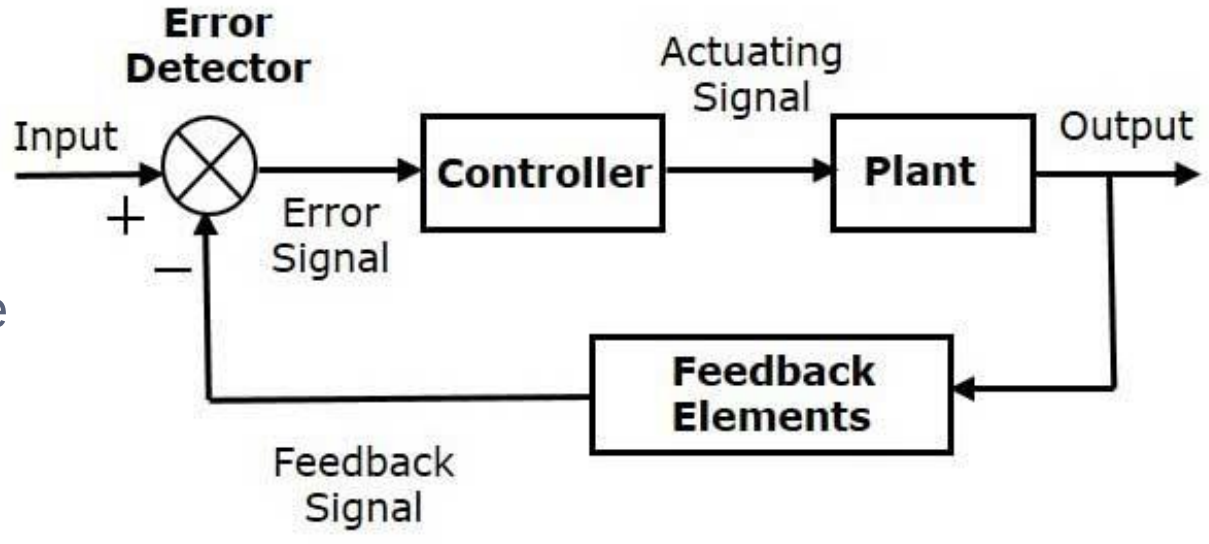
THALES

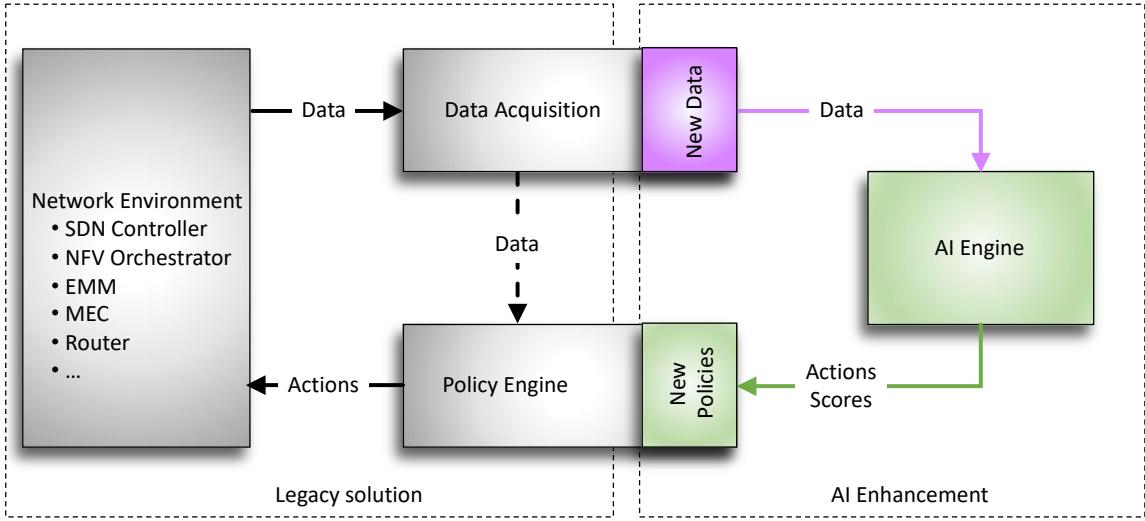
Telefónica

Closing the Closed Loops

Network Closed Loops

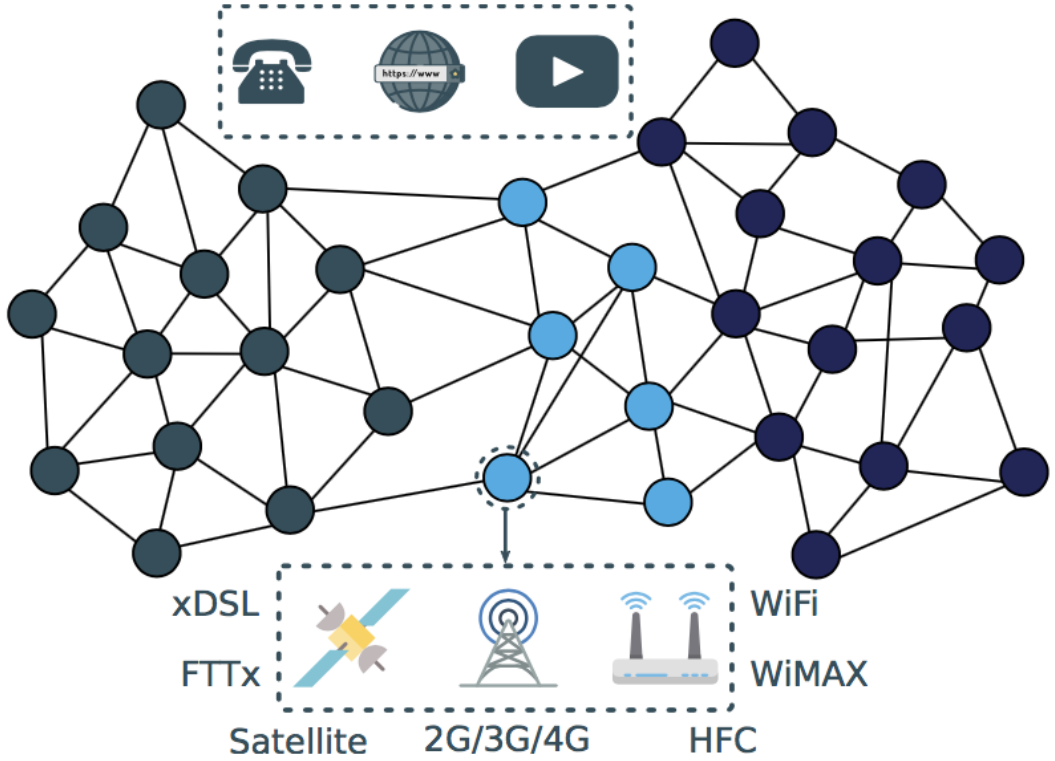
- The use of closed loops do not imply such a radical change
  - Automatics have been around for a long time
  - An essential aspect of industrial processes
- Not such a radical change: Smarter closed loops
  - Tools to derive further insights from data and improve policies
- Extended capabilities, but do not expect Skynet
- Software network technologies have become an essential enabler
  - Look, there is a *controller*!
- Essential abstractions at all elements
  - Feedback, input, detection, actuation





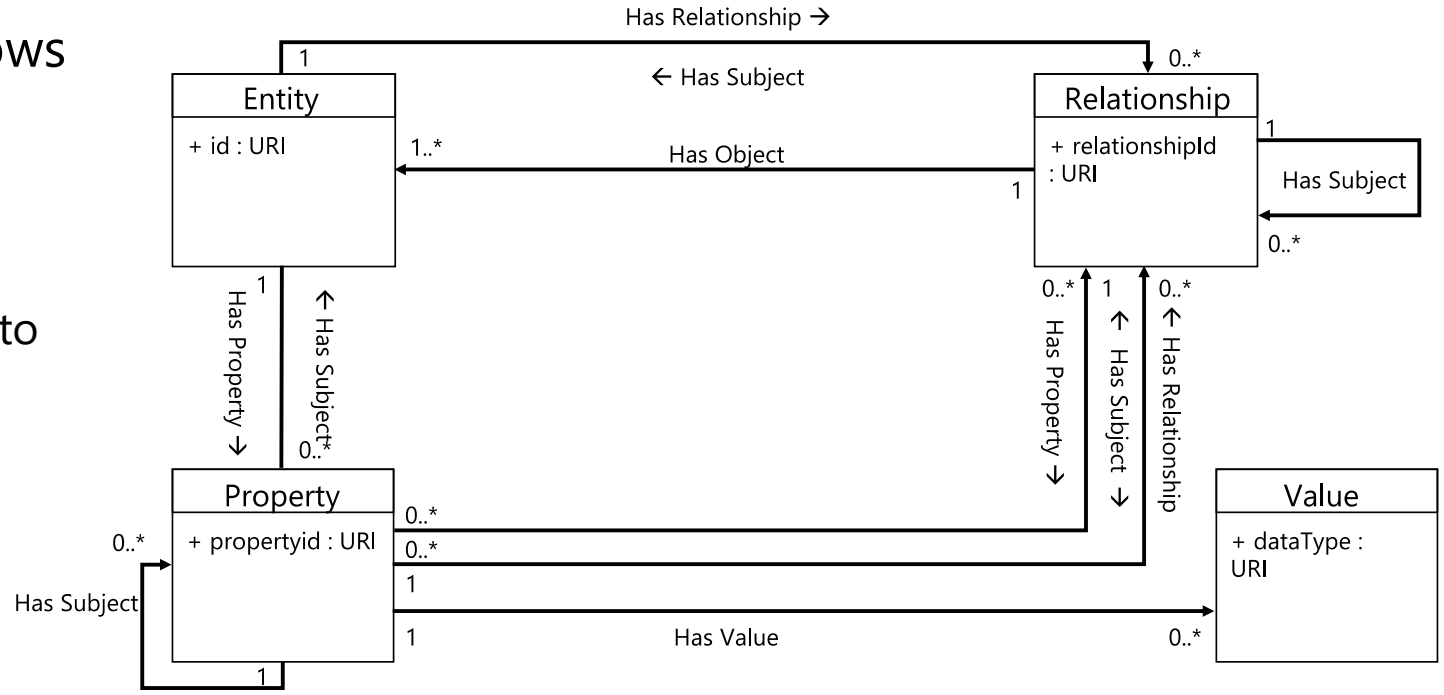
The Aggregation Scenario

- Support the integration of different data flows
  - Open
  - Automated
  - Secure
  - Scalable
- Deal with heterogeneity at all levels
  - Data sources
  - Data consumers
  - Data models
  - Deployment styles
  - Supporting infrastructures
- Not just data
  - Metadata becomes essential, including semantic mappings
  - What seems to claim for a data stream ontology
  - Not that far away: data modeling is a first step

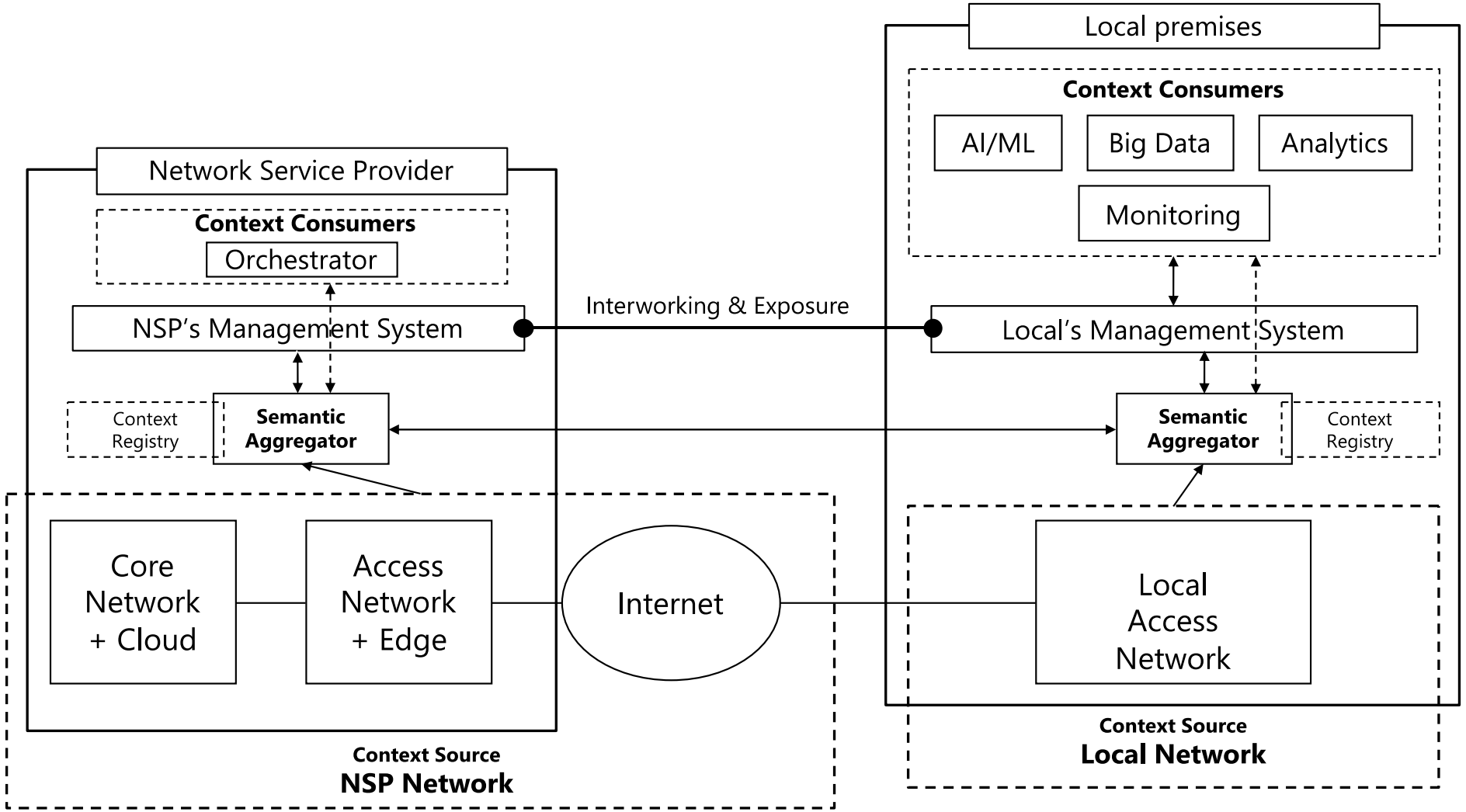


Applying a Semantic Model

- Use the model to describe data flows
  - Sources
  - Consumers
  - Elements in the flow
- And including
  - The identification of the relationships to the flow data model
  - Provenance metadata
  - Security
- Note we are not talking about modeling the whole systems
  - Only the data they provide and/or consume
  - Usable to analyze and normalize flows
  - Without the need of explicit standard alignment
- Extend descriptors
  - Include a protocol for registration, announcements, discovery, etc.

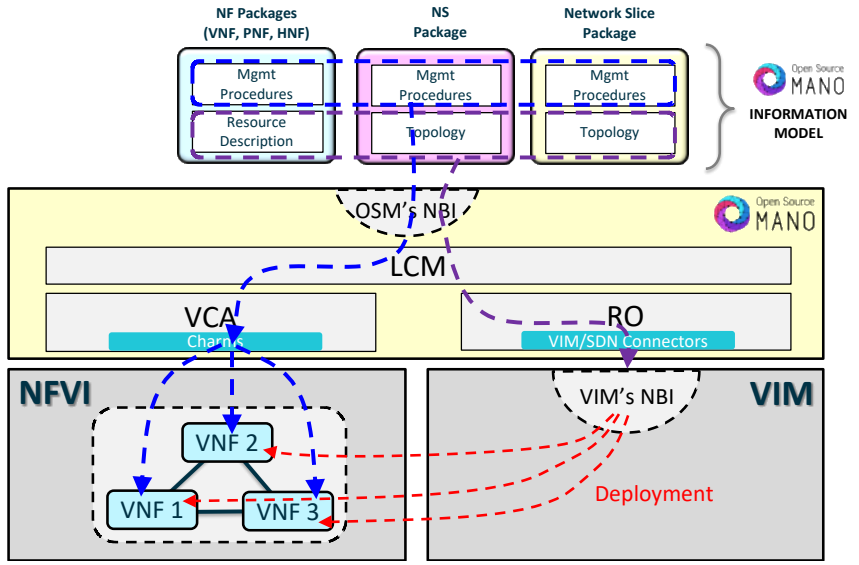


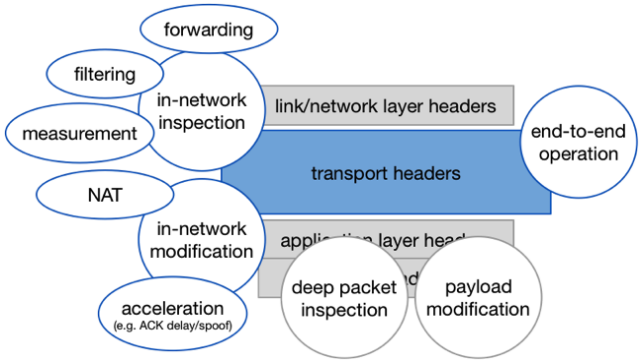
Supporting Federated Models

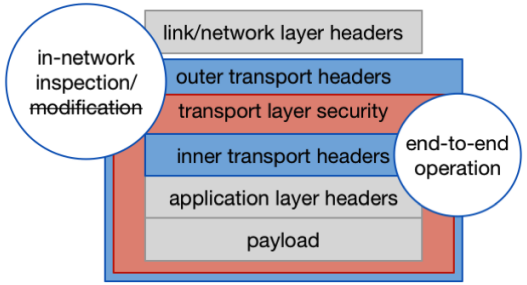


The Actuating (Control) Stream

- OAM actions at a wide variety of different domains
  - Challenging, given the current state-of-the-art
- Initial strategies
  - Domain specific
  - Recommendation systems
  - Autonomic protocols
- SBA approaches and capability models
  - Reusable functionality description
  - Abstractions of network element functionalities usable as building blocks
  - Combined to provide more powerful features
  - Registration mechanisms to support CI/CD
  - Inter-domain collaboration for E2E management

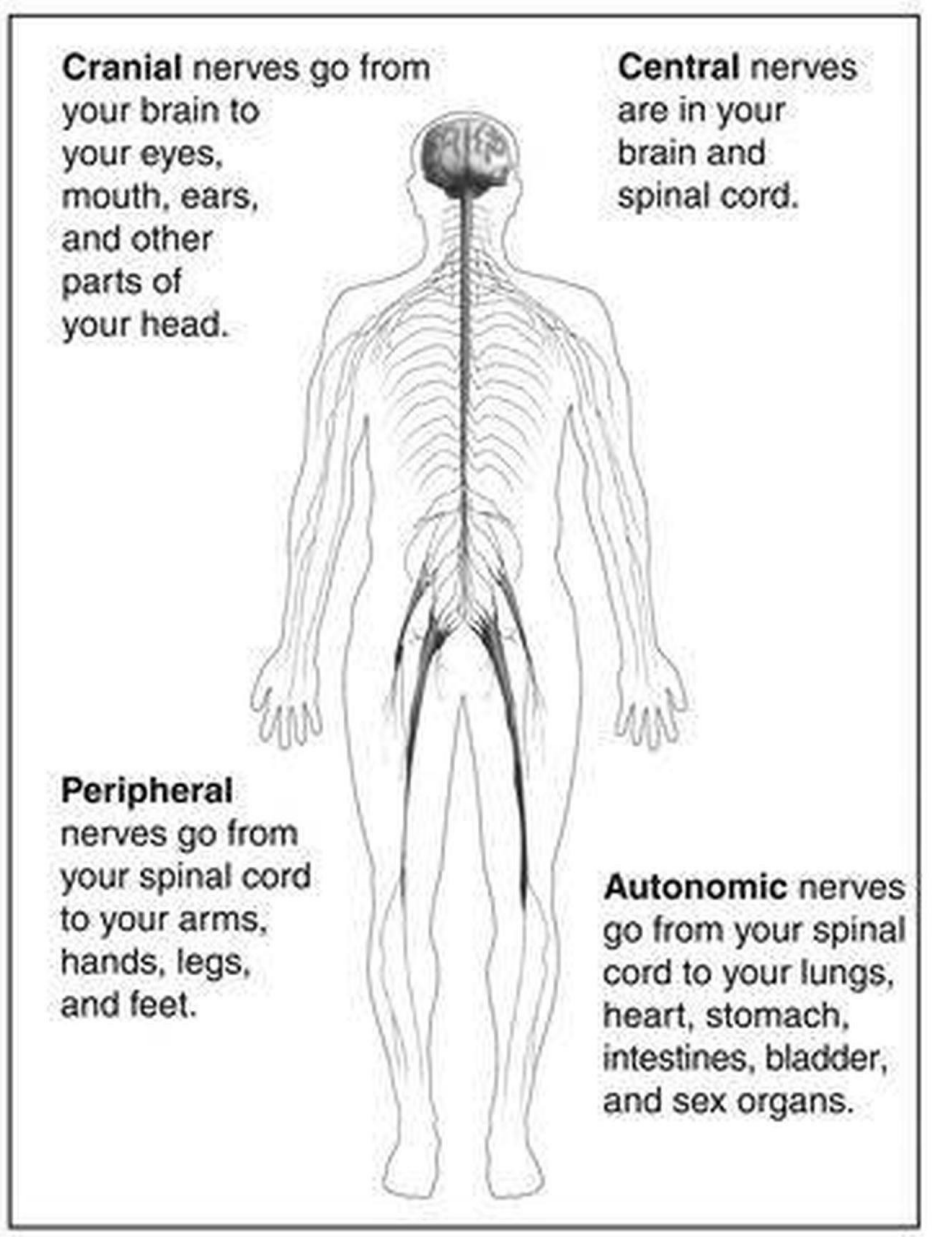






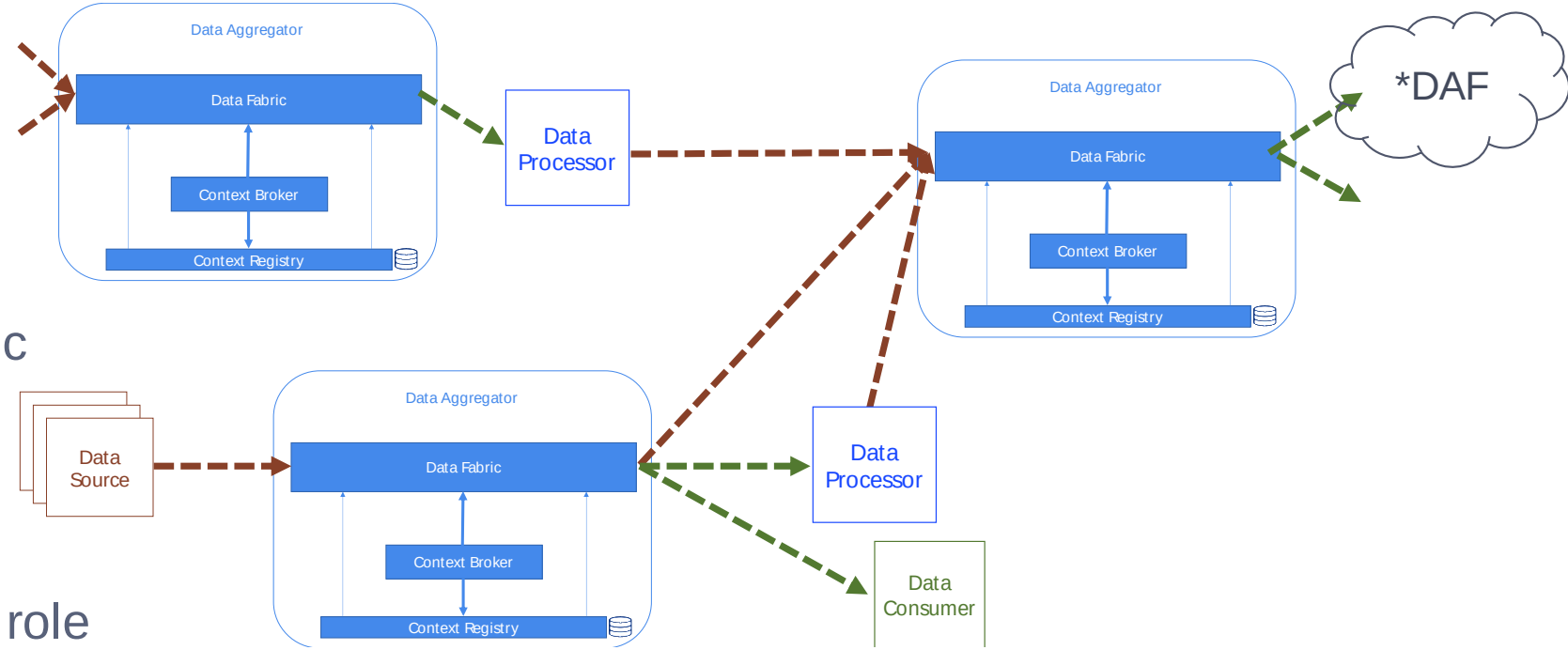
The Nervous System Paradigm

- Combine distributed architectures and holistic approaches
- Local loops
  - Detailed analysis
  - Fast response
  - Dynamic deployment
- Central loop(s)
  - Cumulated analysis
  - Integral view
  - Explicability
  - Local loop orchestration
- All using a common impulse for all kind of interactions
  - Central elements receive and process aggregate information
  - A common data infrastructure for forwarding and aggregation



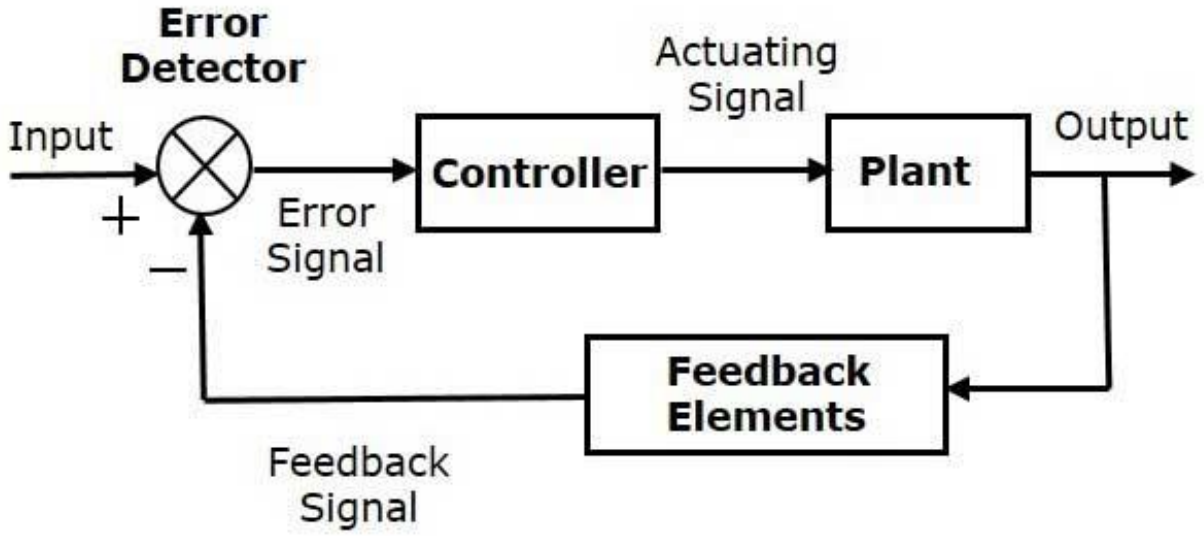
Building the Nervous Data Infrastructure

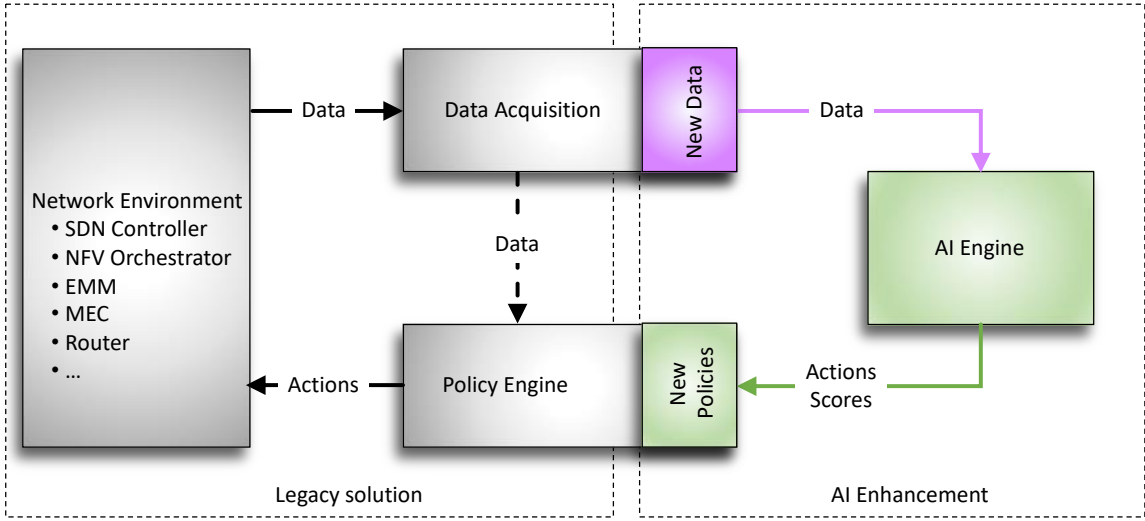
- Rely on aggregation nodes
  - Sources feed data
  - Consumers receive them
  - Aggregators map and integrate
- Based on metadata
  - Dynamic composition
  - Transport protocol agnostic
  - Telemetry data models
  - Knowledge ontologies
- Compositional patterns
  - Any element can play any role
  - AI / ML supported anywhere



Closing the Closed Loops

- The use of closed loops is common everywhere
  - Automatics have been around for a long time
  - An essential aspect of industrial processes
- Not only about offering network data
  - An integral monitoring data substrate
  - Generalization of network DAFs
  - DLT generalized services
- Well-defined data flow semantics
  - Data models for sources and consumers
  - Registry, discovery and dynamic orchestration
  - Full data sovereignty
- Going beyond
  - KVI distillation
  - Network-hosted AI and learning mechanisms
  - Support for serverless in-network computing





This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 856709.

Secure and Trustworthy Open Networks

Raul Muñoz, PhD

Research Director

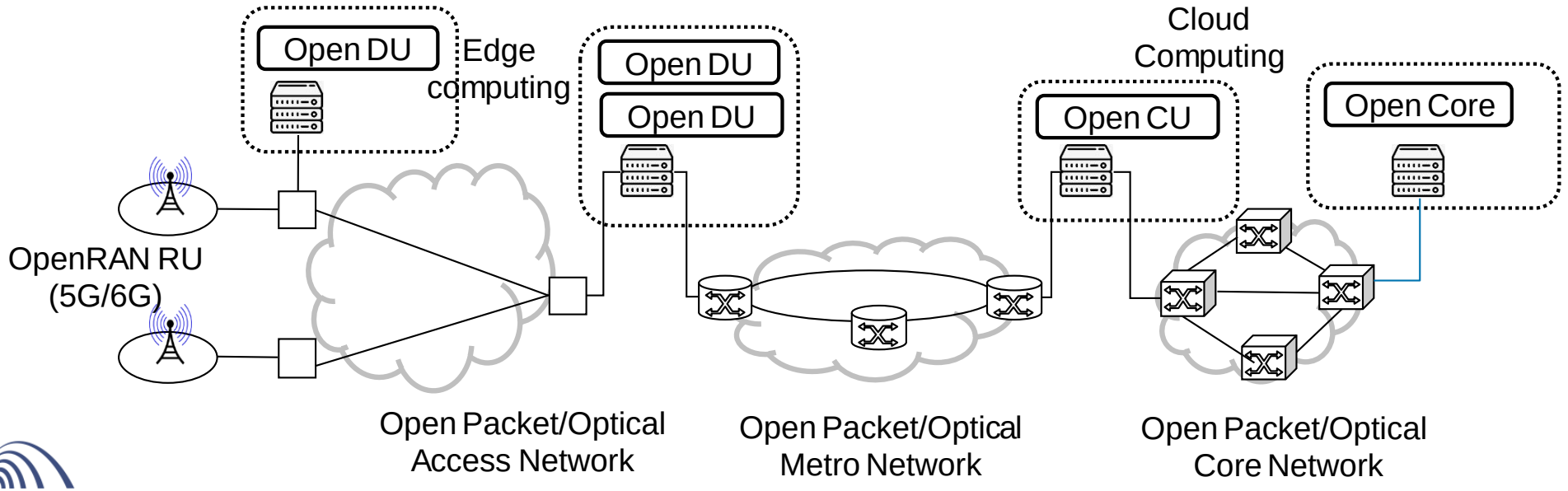
Head of Optical Networks and Systems Department

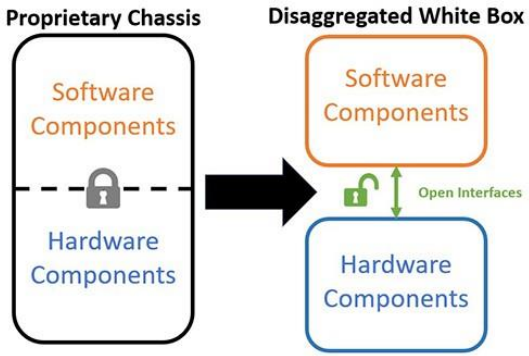
Centre Tecnològic de Telecomunicacions de Catalunya (CTTC)

Third Visions for Future Communications Summit, Lisbon, November 24-25 2021

Future trends in 6G networks: multi-vendor challenge

- Traditionally, telecom equipment is based on proprietary integrated software and hardware solutions provided by a few vendors, generating the well-known vendor islands in the telecom networks.
- In the last years, there is an emerging trend to replace the closed systems at the different network segments (RAN, aggregation, transport, and core) by open white boxes deployed on COTS –based hardware with open interfaces to support any software vendor.
- Some examples of industry-lead initiatives are O-RAN Alliance (ORAN) and Telecom Infra Project (TIP)





Future trends in 6G networks: multi-operator challenge

- Traditionally, telecom operators deploy and manage their own network from end-to-end (RAN, fixed access, metro and aggregation, transport)
- The more frequent deployment of new technologies at the different network segments (4G, 5G, GPON, XG-PON, 400Gb/s backbone, etc.) together with the pressure to keep the prices low, make this situation difficult to keep in the future.
- In the future it would be required multiple telecom operators, each one deploying and managing different network segments that will collaborate to deploy an end-to-end network infrastructure that will be shared among them to reduce the capital (CAPEX) and operational (OPEX) expenditures.
- Network slicing will be become an essential tool to provide end-to-end services across a shared infrastructure.

Security management in multi-vendor and multi-operator 6G networks

- Telecom operators are used to rely on the vendor's proprietary complete solutions (e.g., user authentication, end-to-end encryption, intrusion detection, access control) for security management.
- 6G open networks will offer a unique opportunity to telecom operators, for the first time, to take advantage of the programmability and flexibility of the open technologies to directly manage the security of their networks, rather than relying on a vendor's proprietary solution.
- 6G operators must deploy **smart and secured network slice management with security policies** using software defined security.
- This will allow operating network security proactively, deploying security probes and functions where necessary, using predictive and prescriptive analytics that can detect and anticipate security issues (e.g. attacks, threats, intrusion detection) and proposing corrective actions to mitigate.
- Network slices's security policies must be enforced at the design time, but also redefined at the runtime to cope with unanticipated security requirements

Trust management in multi-vendor and multi-operator 6G networks

- Trust is a complicated concept with regard to the confidence, belief, and expectation on the reliability, security, integrity, dependability, ability, and other features of an entity.
- Reputation is a measure used to assess the level of trust put into an entity. In closed telecom vendors, with few vendors in play, trust management was based on the reputation of the vendors.
- 6G operators need a **trustworthy platform where trust can be measured and evaluated**, providing evidence of the reputation:
  - Distributed ledger technology (DLT) will play a key role to create a new basis of trust for telecom services in multi-provider multi-operator scenarios. Blockchain is a distributed database with many advantages such as decentralization, non-tampering, openness and transparency, consistent data, and verifiability.
  - DLT will enable a radical approach to network management, replacing centralized multi-domain management (where each domain is provided by one vendor), to a distributed multi-provider model of infrastructure (i.e., hardware) and network services (i.e., software), allowing different providers to advertise, negotiate and acquire, in real time, resources and services.

Key management in in multi-vendor and multi-operator 6G networks

- In a multi-vendor environment, **identifying and designing suitable cryptographic systems and methods**, taking into account the impact on the telecommunications infrastructure, are of paramount importance.
- The security of current and future networks is threatened by the advance of the quantum computing.
- It is particularly relevant to consider quantum technologies and quantum secure communications in preparation for the radical technological advance envisioned for future networks:
  - Quantum key distribution (QKD) represent a key technology for long-term security of 6G networks.
  - Integration of QKD technologies with post quantum cryptography (PQC) and an appropriate key management system enable hybrid quantum networks with the required security functionalities and enhanced performance.
  - PQC can also be used for the authentication of the classical channels to support to support a public key infrastructure (PKI)
  - Software-defined networking (SDN) facilitates and ease the integration of key management with conventional systems in 6G networks enabling hybrid quantum secure communications.

Thank you! Questions?

Raul Muñoz

Raul.munoz@cttc.es