

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

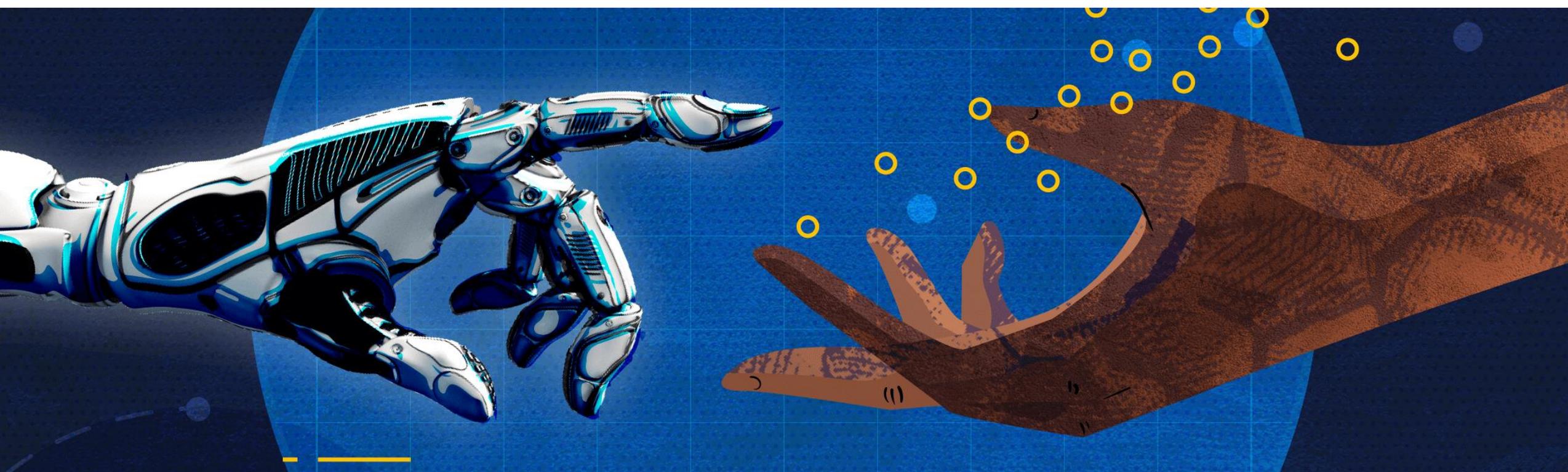
References

- 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](#)).

6G security challenges

introduction to cybersec landscape & few messages

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

emmanuel.dotaro@thalesgroup.com





Trust in Me

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

Tech Disruptions as common (Digital) scope

Assuming transformation is ongoing...

Going Digital
B2C, B2B, B2G

Id
AAA
ABAC

Data
Centric
Crypto
Tech
*FHE, MPC, ZKP,
Ledgers, ...*

AI
*Smart
Autonomous
systems,
OSINT, ...*

Coms &
Sensing,
ICT+OT
*ThZ, NTN, NPN,
D2D, ...*

Q
*Beyond PostQ
crypto or QKD:
→ Sensors &
QCI*

CIP & other Security applications

Industry

Transport

Health

Blue light

Military

Energy

.....

OPEN

THALES

002

in whole or in
parts reserved.

Arch & Biz Disruptions as a companion

Tech as game changer

Going Digital
B2C, B2B, B2G

Id
AAA
ABAC

Data
Centric
Crypto
Tech
FHE, MPC, ZKP
Ledgers,

AI
Smart
Autonomous

Coms &
Sensing,
ICT+OT
5G, 6G, NPN,

Q
Beyond PostQ
crypto or QKD:
→ Sensors &
QCI

6G

as main recipient:
μSBA,
SecaaS w/ QoSec,
(far) Edge/slicing,
3D,
SecOps,
...

CIP & other Security applications

Industry

Transport

Health

Blue light

Military

Energy

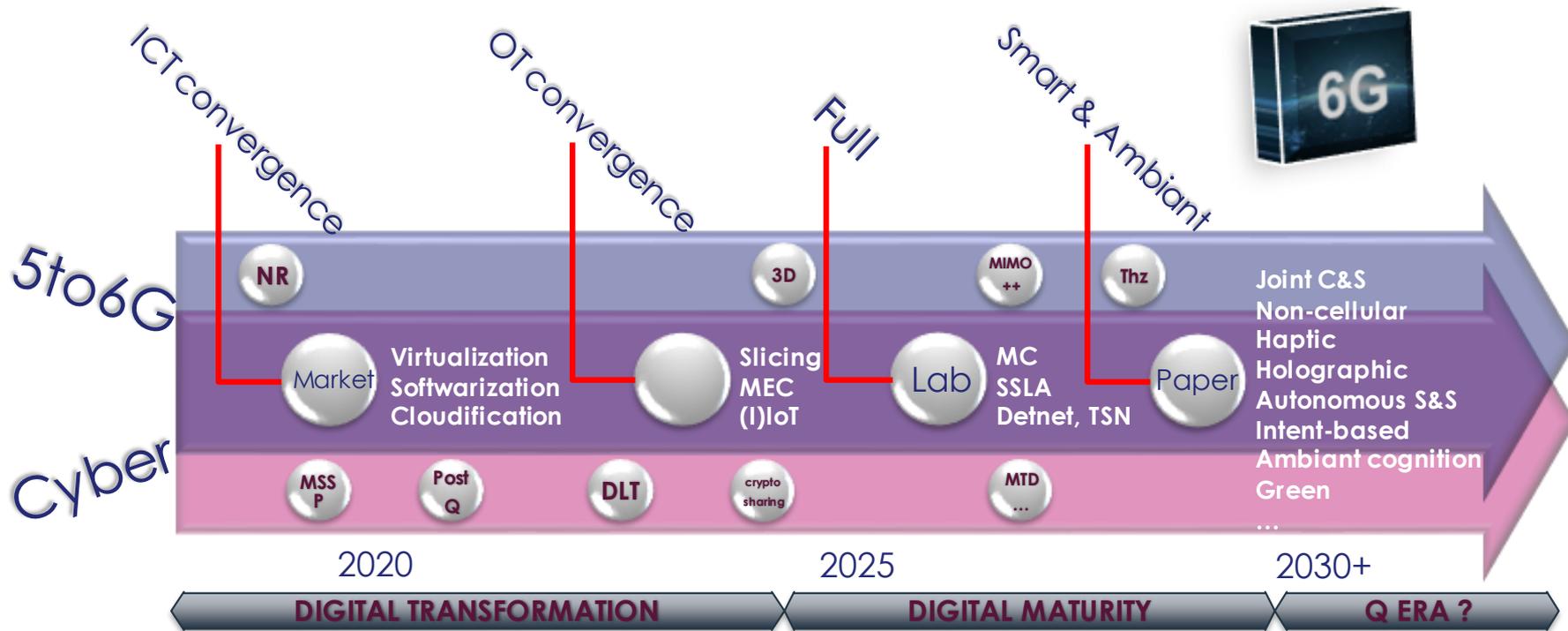
.....

THALES

xG & Cyber a common path

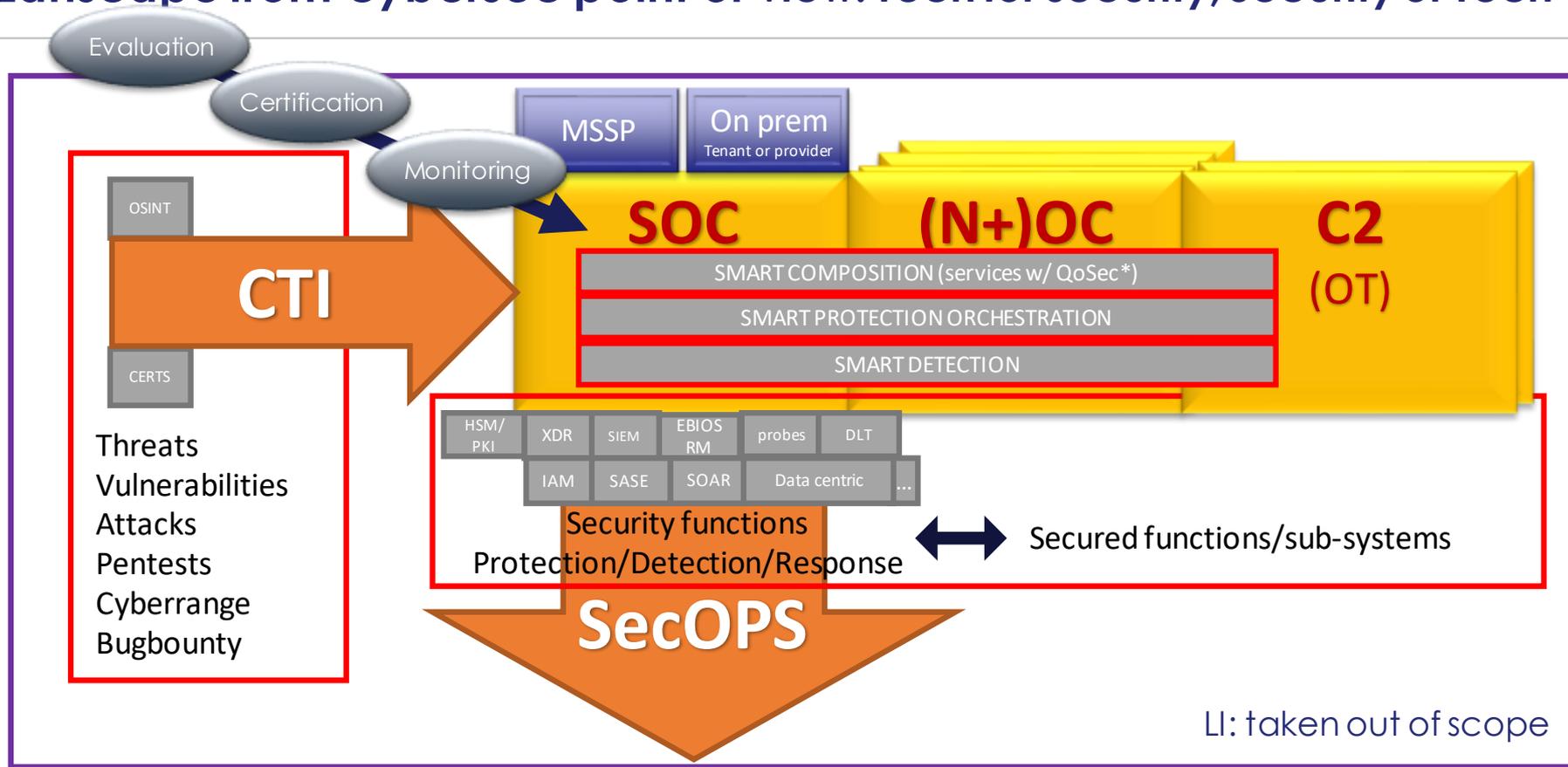
Problem space: Static perimeter → herogeneous → fragmented/polymorphic → metamorphic
 Solution space: perimetric → by Design (really ?) → sticking systems and services fundamentals

dynamics,
 Smart
 autonomous
 Highly distributed
 ...



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part, or disclosed to a third party without the prior written consent of Thales - ©Thales 2015 All rights reserved.

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



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - ©Thales 2015 All rights reserved.

*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

Ref number- date

Name of the company/ Template : 87204467-DOC-GRP-EN-002

Landscape 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:

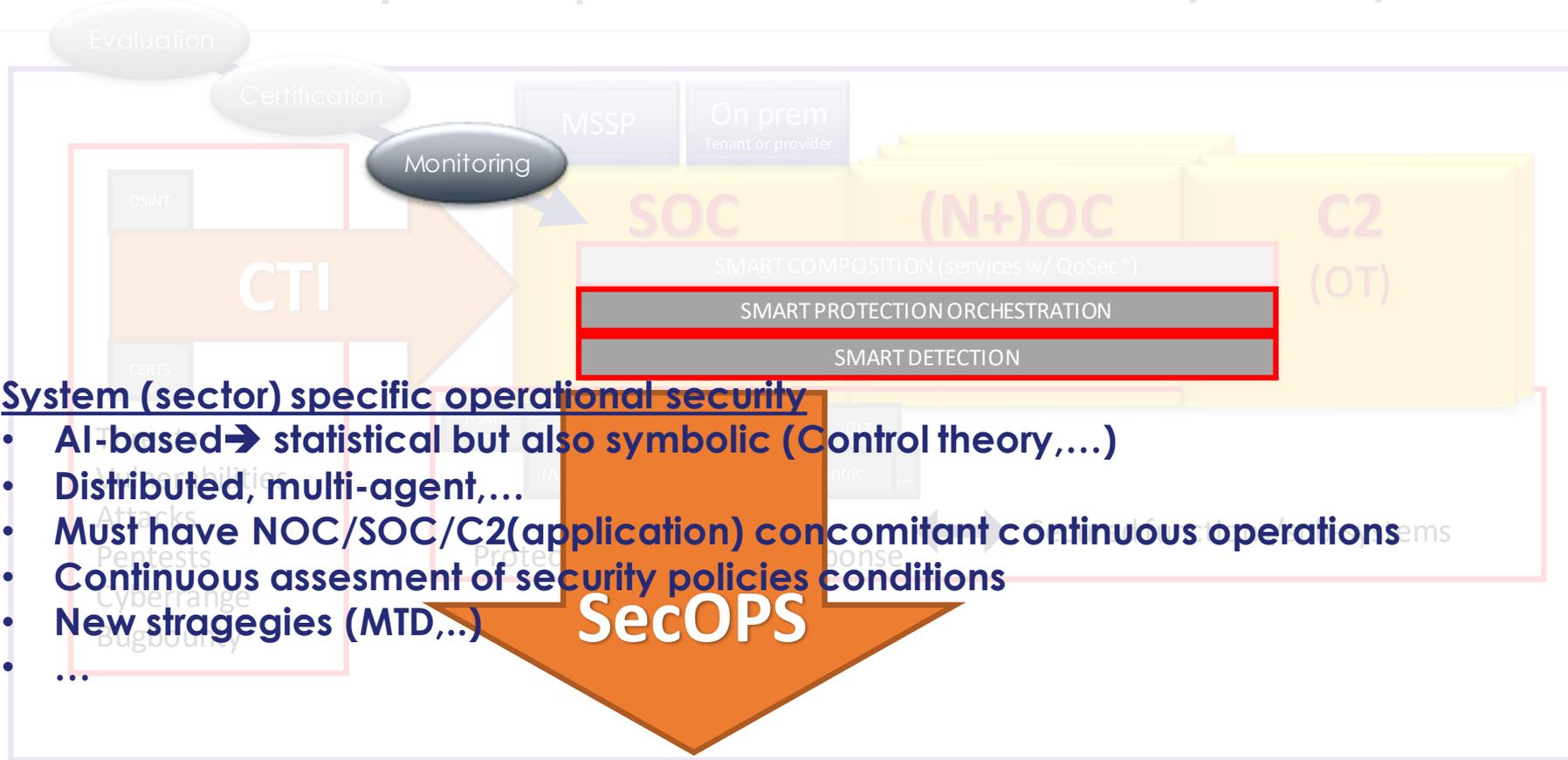
- safe code....along life cycle
- hyperware,
- control please check your AI engines & security (CIA) of Protocol exchanges
 - Integrate SOTA data centric techs (FHE, MPC, DLT, ZKP,...)
- Management please check your AI engines & security (CIA) of Protocol exchanges

Check relevant CTI !

- Should be mandatory as basic « by design »

Secured functions/sub-systems

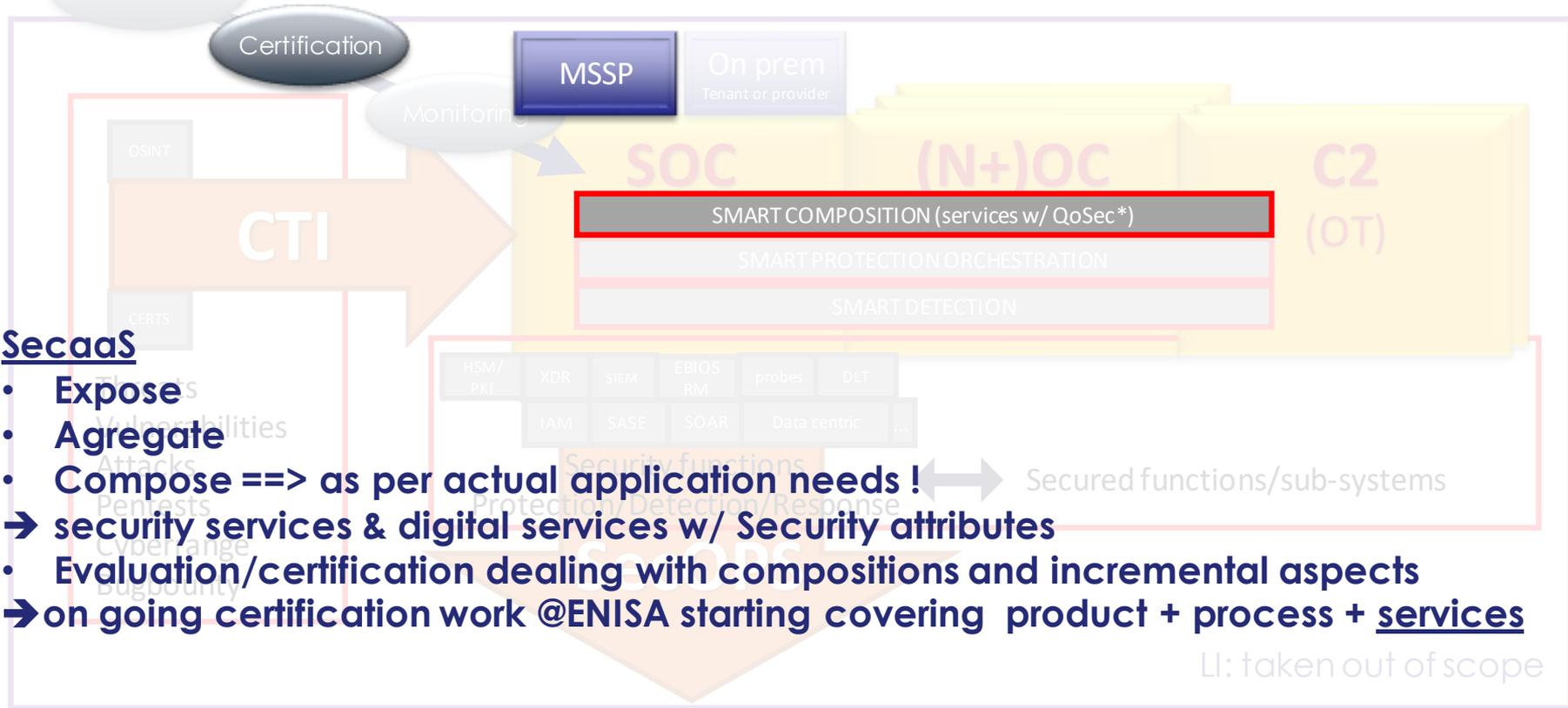
Landscape from cybersec point of view: Tech for security, Security of Tech



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,...)
- ...

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



SecaaS

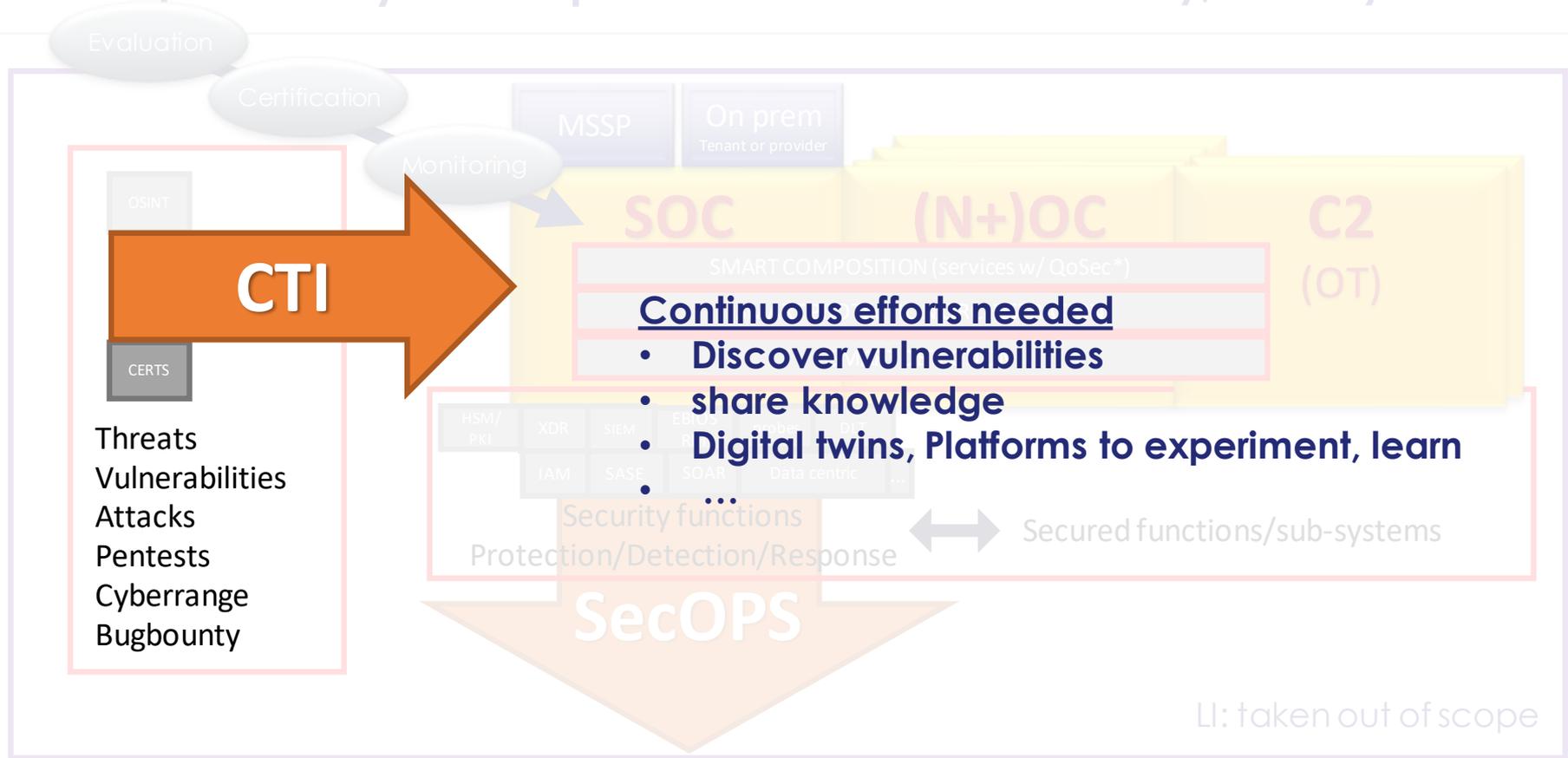
- **Expose**
- **Agregate**
- **Compose ==> as per actual application needs !**
- ➔ **security services & digital services w/ Security attributes**
- **Evaluation/certification dealing with compositions and incremental aspects**
- ➔ **on going certification work @ENISA starting covering product + process + services**

LI: taken out of scope

*ECSO w hite paper

OPEN

Landscape 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

Ref number- date

Name of the company/ Template : 87204467-DOC-GRP-EN-002

Special notice



THALES



THANKS !

www.thalesgroup.com

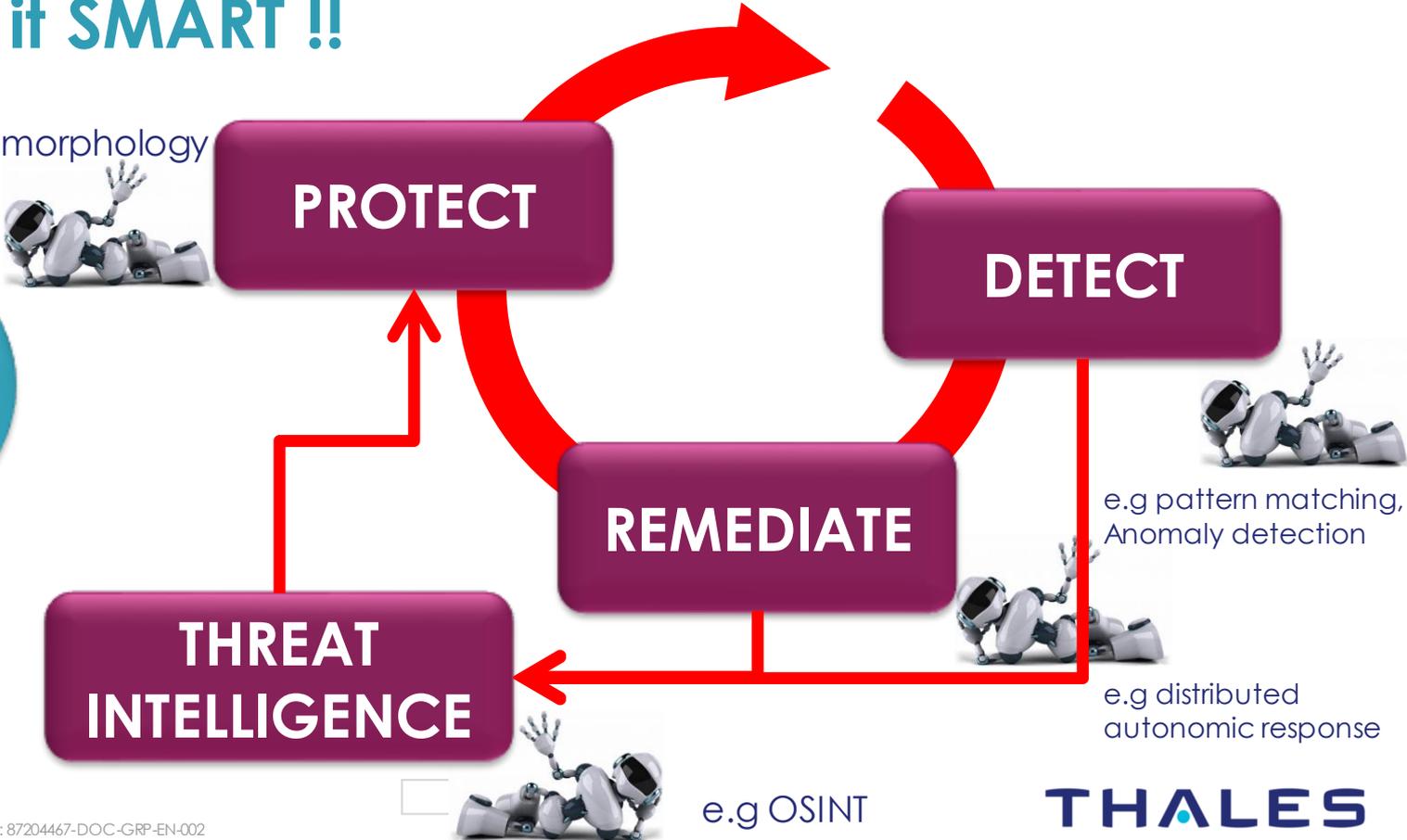
OPEN



Smart Software Defined Security in all phases

Make it SMART !!

e.g Source Code morphology



This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - ©Thales 2015 All rights reserved.

This document may not be reproduced, modified, adapted, published, translated, in any way, in whole or in part or disclosed to a third party without the prior written consent of Thales - ©Thales 2015 All rights reserved.

Table of Contents

1. Introduction	7
1.1 Global Megatrends – Societal Challenges	7
1.1.1 Trends related to the natural environment	8
1.1.2 Trends related to the political system	9
1.1.3 Trends related to the education system	10
1.1.4 Trends related to the economic system	10
1.1.5 Trends related to the media-based and culture-based public system	11
1.2 Strong Contribution to the European Economy	12
1.3 Smart Networks Vision	13
2. Policy Frameworks and Key Performance and Value Indicators towards 2030	17
2.1 Policy Objectives	17
2.1.1 Global view UN Sustainable Development Goals	17
2.1.2 The Green Deal	18
2.1.3 Full industrial digitization and support of vertical industries	19
2.2 Societal, Economical and Business Drivers for 6G	20
2.2.1 Integrate new technologies and support emerging applications	25
2.3 Mapping of the UN SDGs to ICT development	25
2.4 Key Performance Indicators (Access, Network, Management)	30
• Runtime Service Scheduling efficiency increase compared to overprovisioning (for a service requiring 99.999% or higher success rates and under typical traffic arrival conditions)	33
• Time required for runtime conflict resolution when applying resource efficiency methods, that is the increase in multiplexing desired when compared to independent exclusive allocations and the time that is required to settle all the conflicts that may exist	33
• In terms of network-resources collection (network garbage collection), in the sense of recovering resources that are not being used anymore, we expect:	34
• Features of the pervasive resource control, in terms of autonomic functions	34
• In terms of network-suitable AI, we expect	34
2.5 Technical Standard Areas	35
2.6 Key Value Indicators	36
3. Human Centric and Vertical Services	39
3.1 Emerging applications and use cases	39
3.2 Digital Service Transformation	45
3.3 From Software-Centric to Human-Centric Internet Services	47
3.4 Services Everywhere, Infrastructure No Limits	49
3.5 Network-Unaware Vertical Services	50
3.6 Extreme Automation and Real-Time Zero-Touch Service Orchestration	51
3.7 Service Injection Loop	53

Page 2
Draft Version for Public Consultation 1.1

4. System Architecture	55
4.1 Evolution of Networks and Services	55
4.2 System Architecture Vision: Towards Smart Green Systems	57
4.3 Virtualised Network Control for Increased Flexibility	59
4.3.1 Programmability in Control	59
4.3.2 Separation of control/controlability	60
4.3.3 Multi-Tenancy and Ownership	61
4.3.4 Known Unknowns	61
4.3.5 Self-Preservation	62
4.3.6 Research Challenges	62
4.4 Re-Thinking the Data & Forwarding Planes	62
4.4.1 Design Considerations for an Evolved Data & Forwarding Plane	62
4.4.2 Key Research Questions	65
4.4.3 Recommendations for Actions	66
4.5 Efficiency and Resource Management	67
4.5.1 Network Slicing versus Network Capacity Planning	67
4.5.2 Slicing Requires Conflict Resolution	68
4.5.3 Elasticity: Slicing Efficiency Requires Runtime Scheduling	68
4.5.4 Towards Green ICT	69
4.5.5 Research Challenges	70
4.6 AI/ML-based System Evolution	70
4.6.1 Proliferation of AI/ML in Network Operations	71
4.6.2 AIaaS Proliferation in Service Provisioning	72
4.6.3 Related Research Challenges	72
4.6.4 Recommendations for Future Actions	73
4.7 Deep Edge, Terminal and IoT Device Integration	74
5. Edge Computing and Meta-data	78
5.1 Introduction	78
5.2 ETSI MEC evolution	81
5.3 Activities on MEC in other Standardization Bodies	82
5.4 NFV, SDN, orchestration	82
5.5 Computing platform technologies	83
5.6 Containers and container orchestration	85
5.7 Distributed services	85
5.8 Edge, Mobile Edge Computing and Processing	86
5.9 Edge AI	87
6. Radio Technology and Signal Processing	89
6.1 Spectrum Re-farming and Reutilisation	89
6.2 Millimetre Wave System	91
6.3 Optical Wireless Communication	92
6.4 Terahertz Communication	94
6.5 Massive and Ultra-Massive MIMO	97
6.6 Waveform, Multiple Access and Full-Duplex	100
6.7 Coding and Modulation	102

Page 3
Draft Version for Public Consultation 1.1

6.8 Positioning and Sensing	103
6.9 Massive Random Access	104
6.10 Wireless Edge Caching	106
7. Optical networks	108
7.1 Sustainable capacity scaling	109
7.2 New switching paradigms	110
7.3 Deterministic networking	111
7.4 Optical wireless integration	112
7.5 Optical network automation	114
7.6 Security for mission critical services	116
7.7 Ultra-high energy efficiency	117
7.8 Optical integration 2.0	117
8. Network and Service Security	119
8.1 Rationales for Security Transformation	119
8.1.1 Change in system nature	119
8.1.2 Disruptive Technologies integration	122
8.1.3 Change in Security grade expectation	124
8.1.4 Change in scope	125
8.2 System-wide Security challenges	126
8.2.1 Further Security challenges in phases	126
8.2.2 Specific challenges as per 5G/6G architecture	127
8.3 Operational Security Research directions for System & Services	130
8.3.1 Security quantification	131
8.3.2 Green Security	131
8.3.3 Security as a Service	132
8.3.4 Security orchestration	132
8.3.5 Disruptive Security Strategies	132
8.3.6 Distributed Logic/ Technologies	133
8.3.7 Artificial Intelligence	134
9. Satellite Communications Technologies	136
9.1 Introduction	136
9.2 System architectures	136
9.2.1 Expected impact	138
9.3 Evolution of Networking Architectures	138
9.3.1 Expected impact	140
9.4 Hybrid Infrastructures: Broadcast/Multicast/Unicast/Storage – EDGECASTING	140
9.4.1 Expected impact	141
9.5 Smart Satellite Networking	142
9.5.1 Expected impact	142
9.6 Optical based Satellite Communications	143
9.6.1 Expected impact	144
9.7 Software Defined Payloads	144
9.7.1 Expected impact	144
9.8 Radio Access Network beyond 5G and 6G	145

Page 4
Draft Version for Public Consultation 1.1

10.4 Antenna and Packages	160
10.4.1 On-chip antennas, lens-integrated antennas, antenna MIMO arrays	160
10.4.2 Metamaterials and metasurfaces	161
10.5 High-speed Transceivers, Wireline and Optical	162
10.5.1 Radio-over-fiber communication, sub-systems and components for B5G and 6G networks	162
10.5.2 Terahertz capable opto-electronic transceivers	162
10.5.3 Ultra low-cool and low-power coherent THz transceivers	164
10.5.4 Optically assisted wireless subsystems	165
10.6 Baseband Modems	165
10.7 Processors for Cloud-AI, Edge AI and on-device-AI	166
10.8 Memories	168
10.8.1 Memory technologies towards 2030	168
10.8.2 Compute-in-Memory	170
10.9 Hardware for Security	171
10.10 Opportunities for IoT Components and Devices	172
10.10.1 Approach for components	173
10.10.2 Approach for devices	174
10.10.3 Requirements for IoT devices	174
11. Emerging Technologies and Challenging Trends	176
11.1 The Physical Stratum: Communication and Computing Resources	179
11.1.1 Nano- and Bio-Nano Things	179
11.1.2 Quantum Networking	181
11.1.3 AI/ML for the Physical Layer	184

Page 5
Draft Version for Public Consultation 1.1



May 2020

Strategic Research and Innovation Agenda 2021-27

European Technology Platform NetWorld2020

“Smart Networks in the context of NGI”

2020

Page 1

Draft Version for Public Consultation 1.1

OPEN



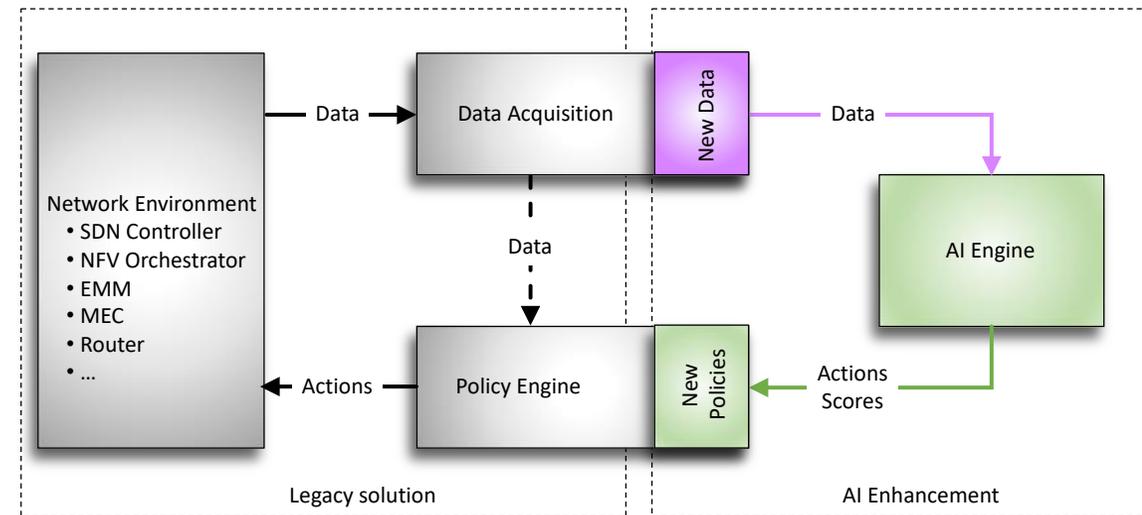
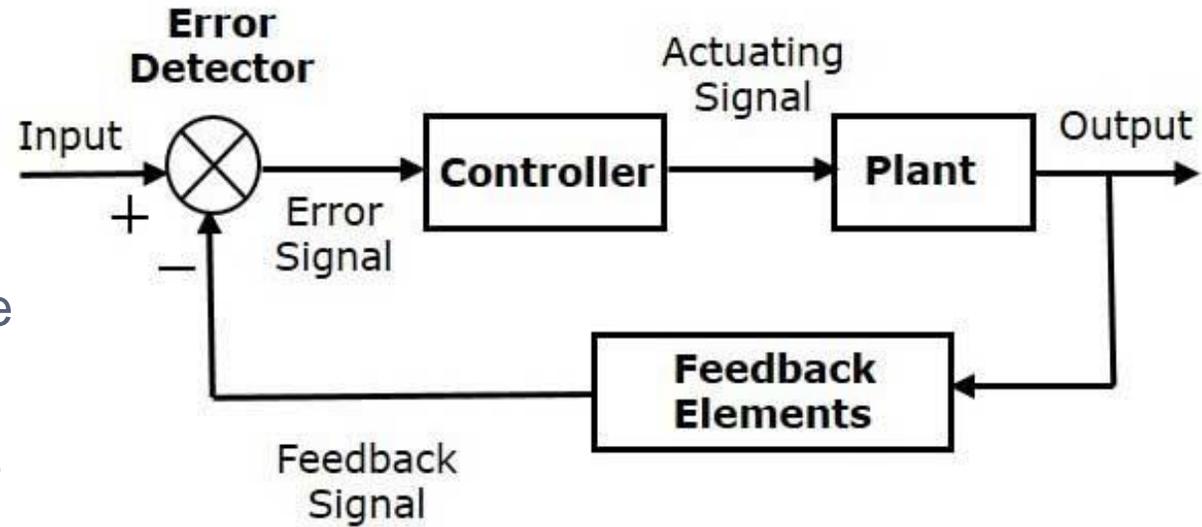


Closing the Closed Loops



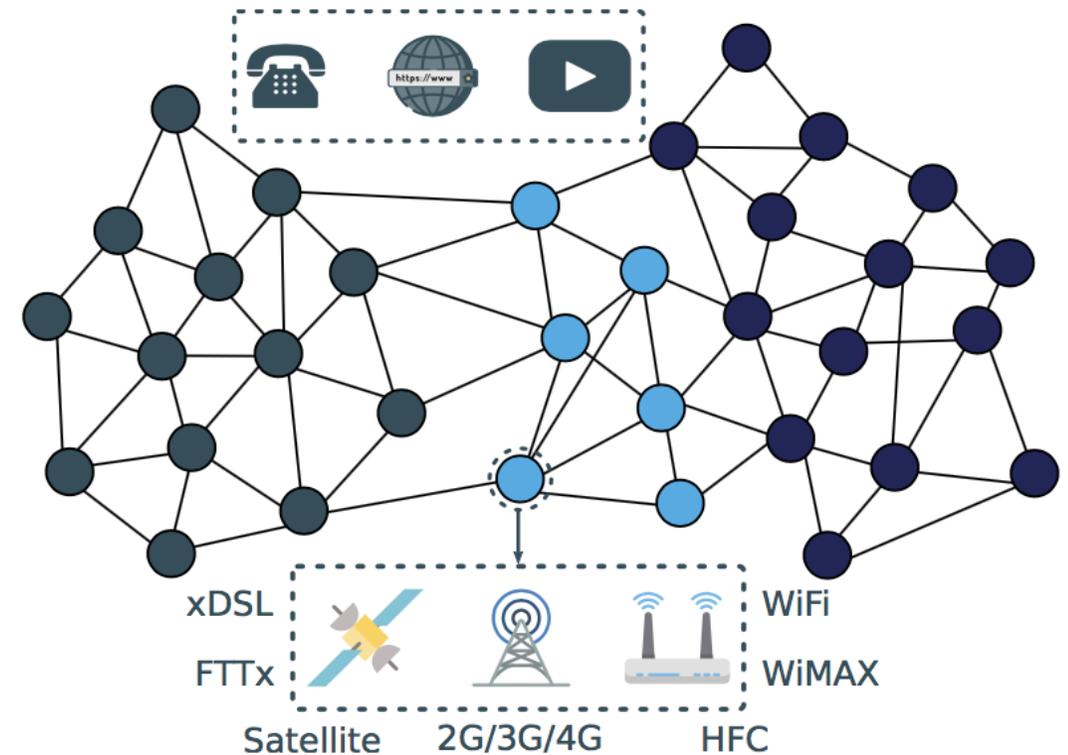
Network Closed Loops

- 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



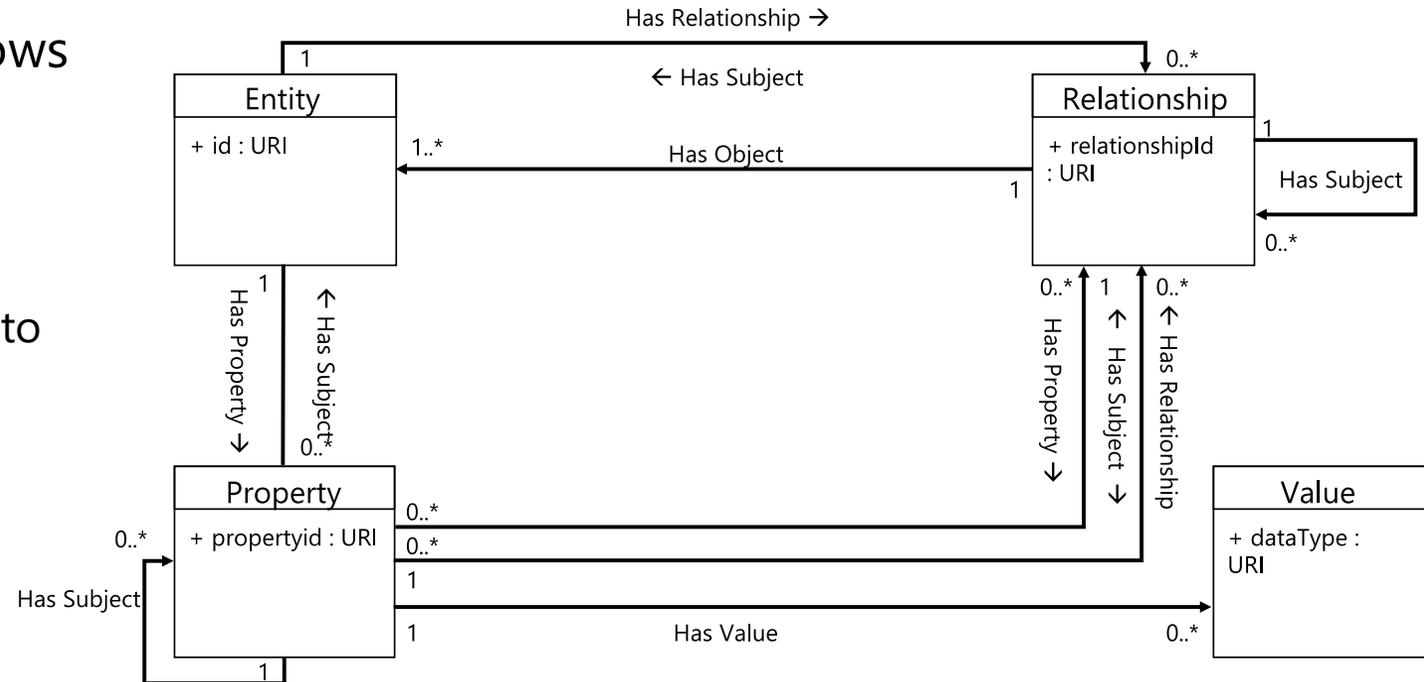
The Aggregation Scenario

- 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

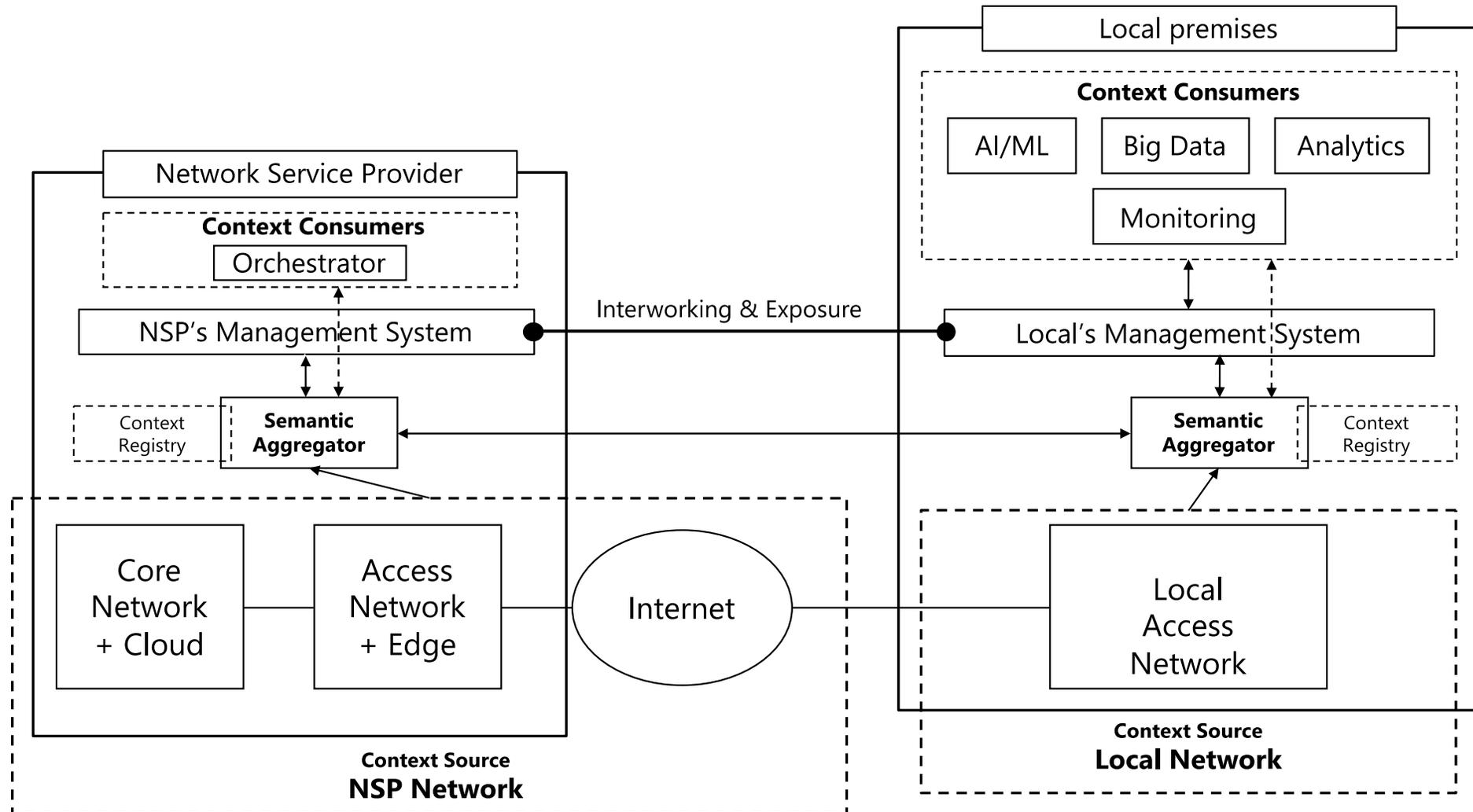


Applying a Semantic Model

- 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.

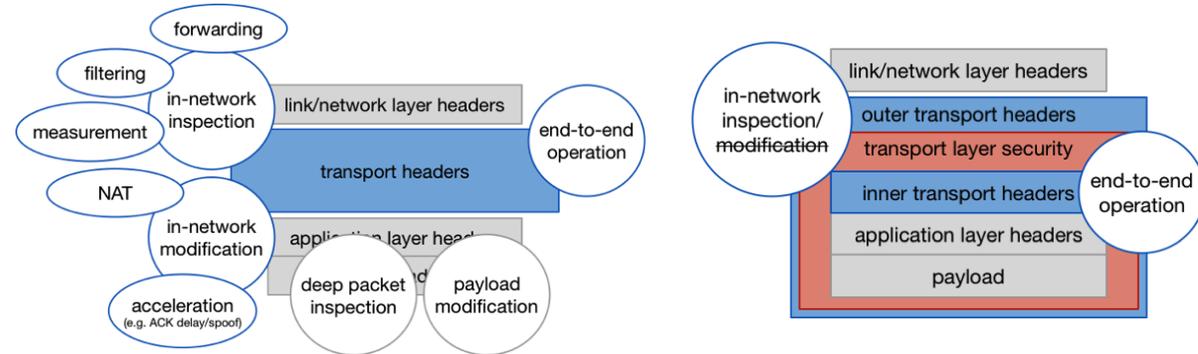
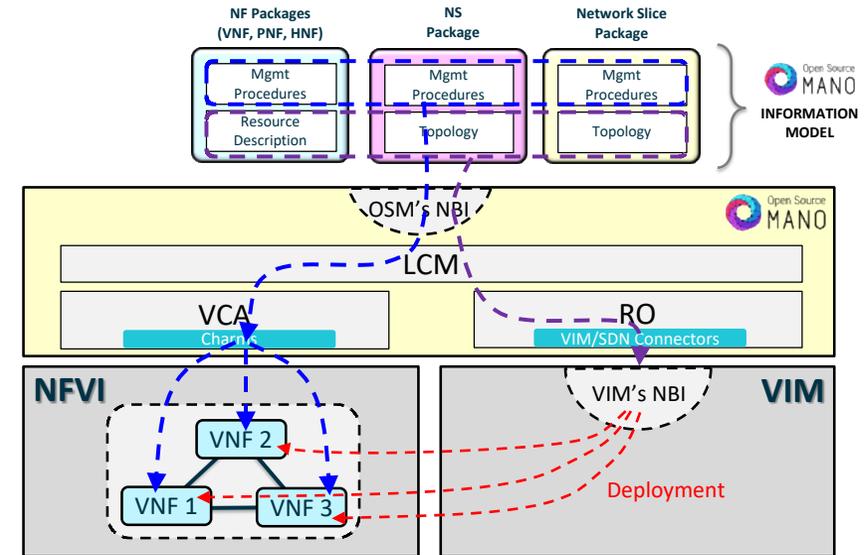


Supporting Federated Models



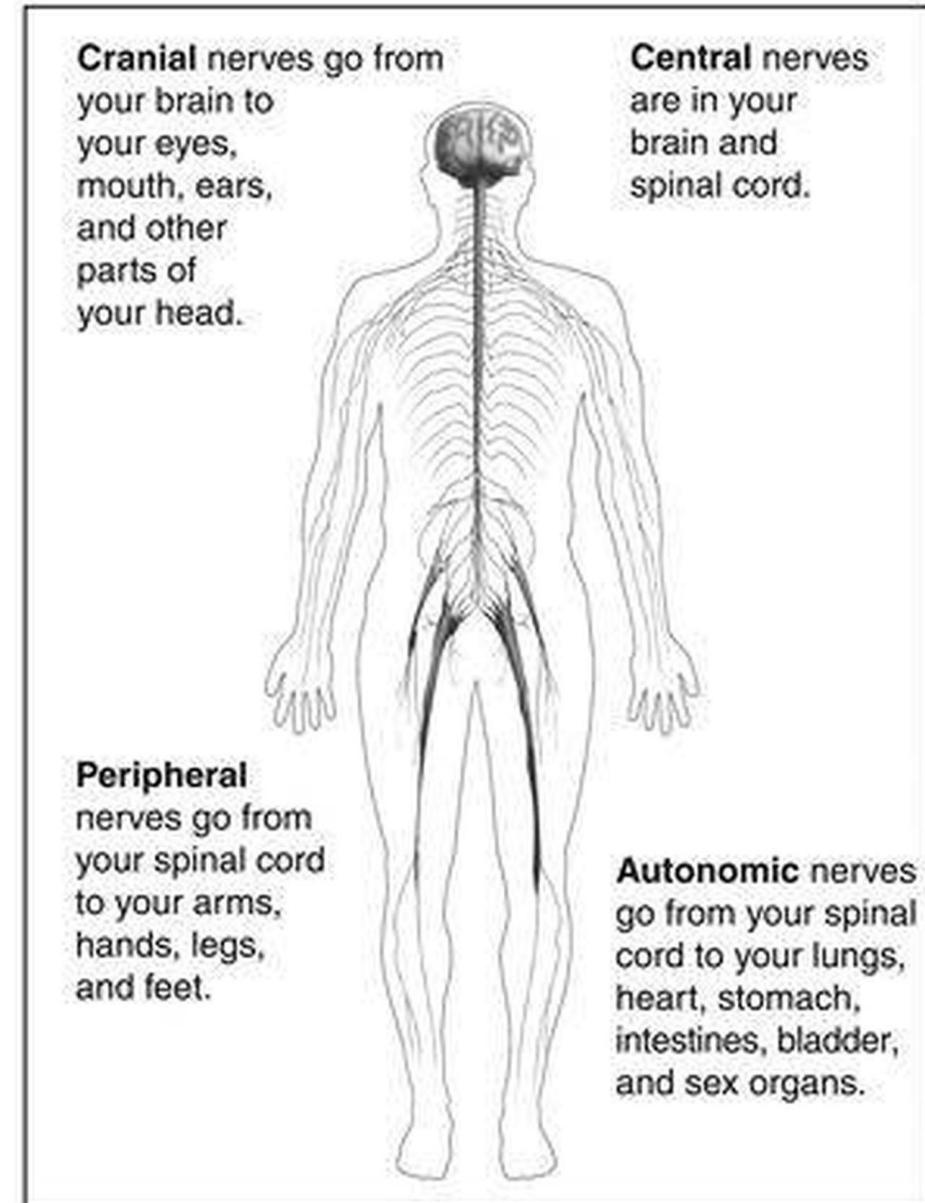
The Actuating (Control) Stream

- 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



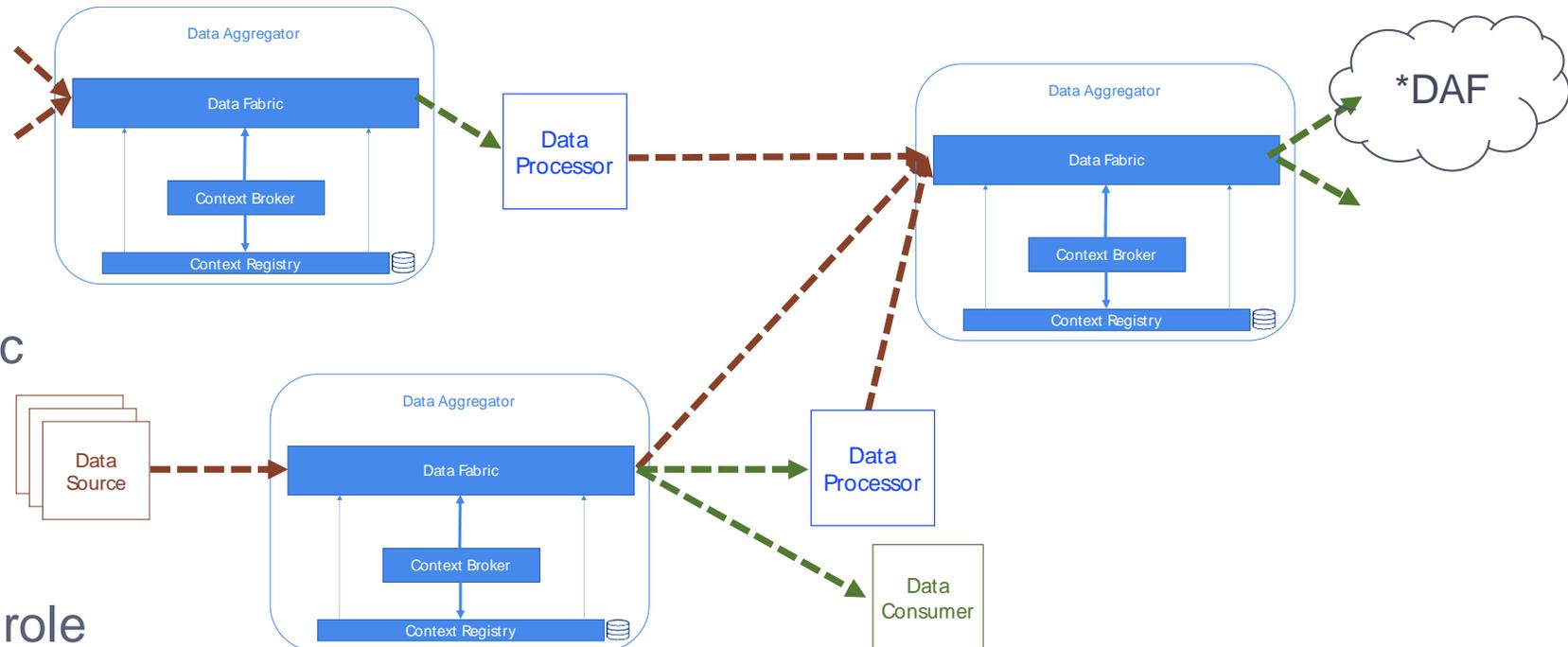
The Nervous System Paradigm

- 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



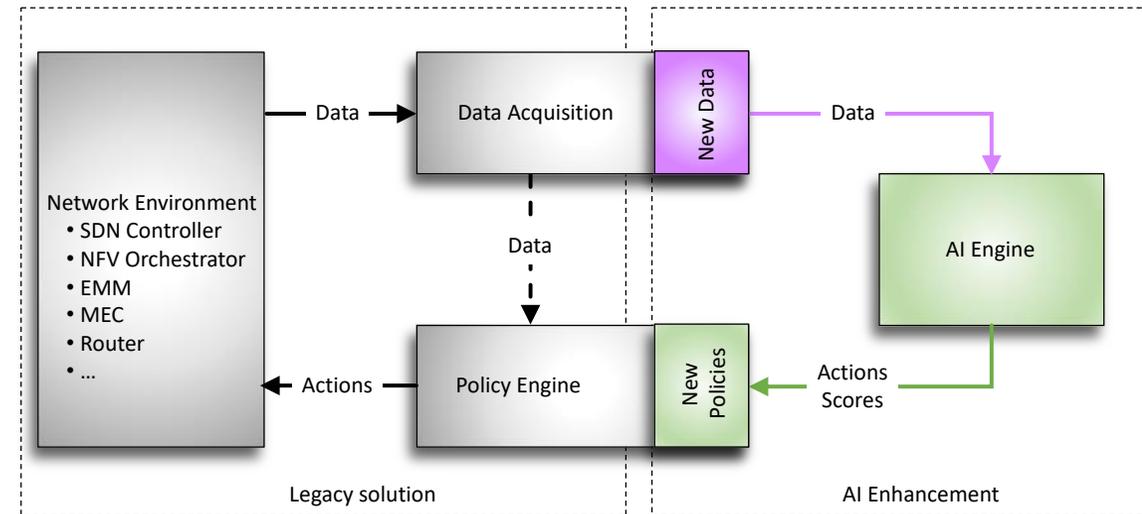
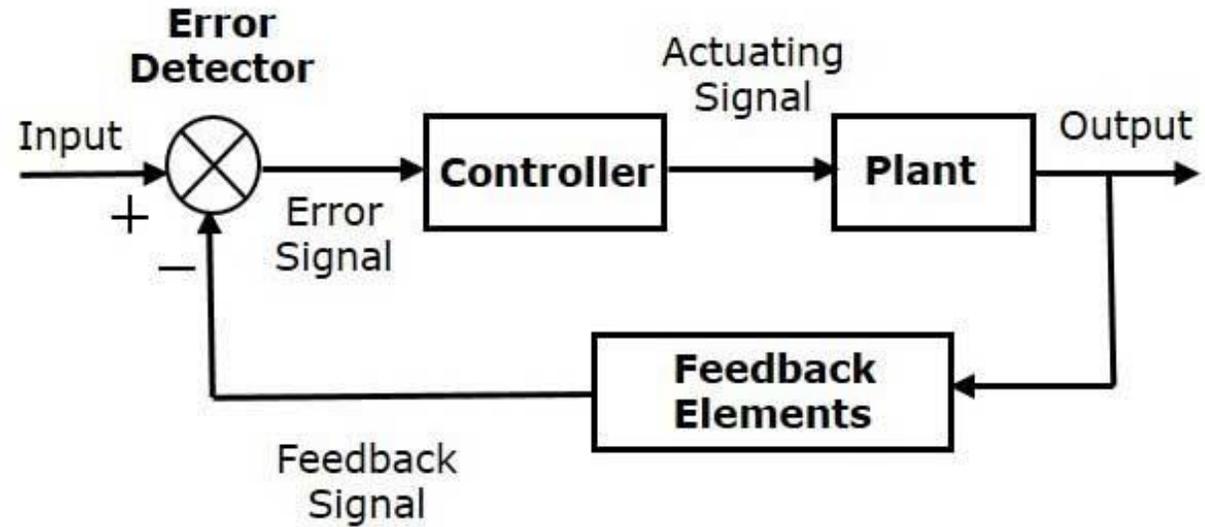
Building the Nervous Data Infrastructure

- 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



Secure and Trustworthy Open Networks

Raul Muñoz, PhD

Research Director

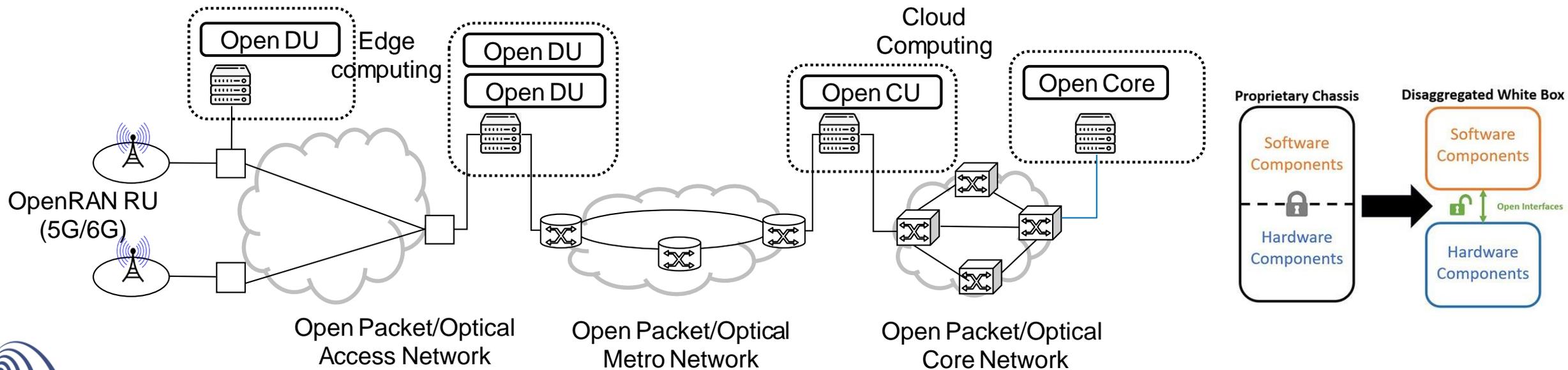
Head of Optical Networks and Systems Department

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

