Trust model for verticals over 5G

Speaker: Claire Loiseaux

November 17, 2020 – ICCC20

Joint work

- 6 Authors from Internet of Trust and Orange
  - Mohamad Hajj, Claire Loiseaux,
  - Chrystel Gaber, Jean-Luc Grimault, Marc Lacoste, Jean-Philippe Wary

- Involved in
  - System and use-case based evaluation methodology in ODSI project (1)
  - 5G core Network security requirements definition for FFT
  - Open RAN security requirements definition for O-RAN Alliance (2)
  - 5G risk analysis for 3 verticals (confidential document)
  - Liabilities topic investigation in INSPIRE-5GPlus project (3)

(1) ODSI is a CelticPlus project (ID: C2014/2-12)

(2) Support of Orange, co-chair of O-RAN Security Working group

(3) Work partly funded by the European Union's Horizon 2020 research and innovation program under grant agreement no 871808 (5G PPP project INSPIRE-5Gplus). The paper reflects only the authors' views. The Commission is not responsible for any use that may be made of the information it contains.

Agenda

- Context & challenges
- Related work & Available tools
- Complexity illustration
- Our dream
- First stones to pave the way towards an operational 5G Trust model
- Conclusion

Context

- Multiple stakeholders
  - Operators, Vendors, Verticals, Governments

- Lack of
  - Harmonized requirements for baseline security
  - Specific-vertical risk assessments are not available

- A wide variety of security requirements and robustness levels
  - Specific needs for Mainstream/Sensitive/Critical Uses cases,
  - European requirements: NIS directive, EECC, GDPR, ePRIVACY, SEVESO,…
  - National requirements: equipment authorization (L34-11), Lawful interception (R226), …
  - Heterogenous vertical requirements: low latency, safety, high availability, confidentiality, compliance to dedicated business regulation, that are potentially conflicting and/or interdependent e.g. Safety vs Security

Cartography of Available Tools

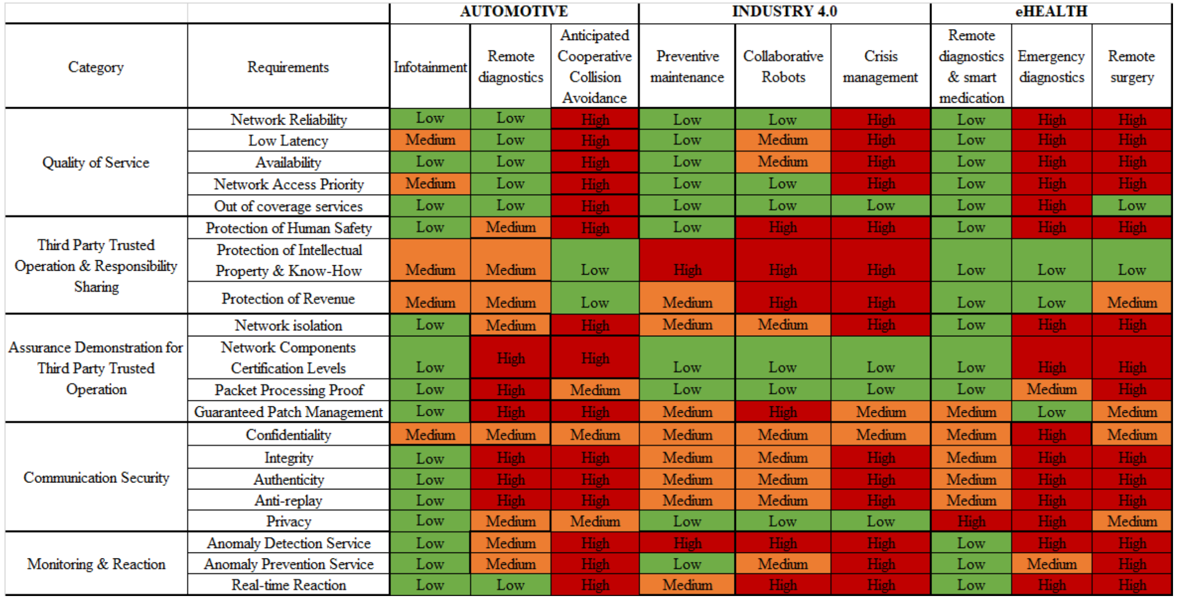
- Existing/emerging schemes
  - Product certification schemes such as **EUCC** which includes composition, security by design, secure update, vulnerability handling
  - Composition and **mutual recognition** defined in certification schemes, CC, GP, EMVCo,…
  - **5G EU Security Toolbox** (NIS Cooperation Group)
  - Under discussion: Coverage of AI and software update in Product Liability directive 85374-EEC

- At research level
  - **SLA languages** that are still fragmented and not yet mature to be integrated in certification schemes (see SuperCloud project whitepaper)
  - Risk analysis and **On demand security** (developed in ODSI project), focus on the need
  - Smart supervision, **trust and liability chain** in 5G ecosystem (developed in Inspire 5G+ project)
  - Security as a service **SECaaS**
  - Abstract interpretation…

Challenges for a certification scheme: Intrinsic complexity

- Massive number components
  - 50-100K radio equipment for a single telco operator per country ;
  - 500 k-1M distribution equipment for energy per country;
- Components
  - are diverse: HW and SW products : TPM, PKI, HSM, routers, hypervisors, but also Cloud, …
  - come from third parties, may include open source, have multiple versions;
- Integration is dynamic and resources are shared
  - Suppliers push for CI/CD processes
  - Components are configured and composed dynamically, and 5G slices themselves are subject to near real time re-orchestration;

Security requirements diversity in sensitive verticals with critical uses cases.

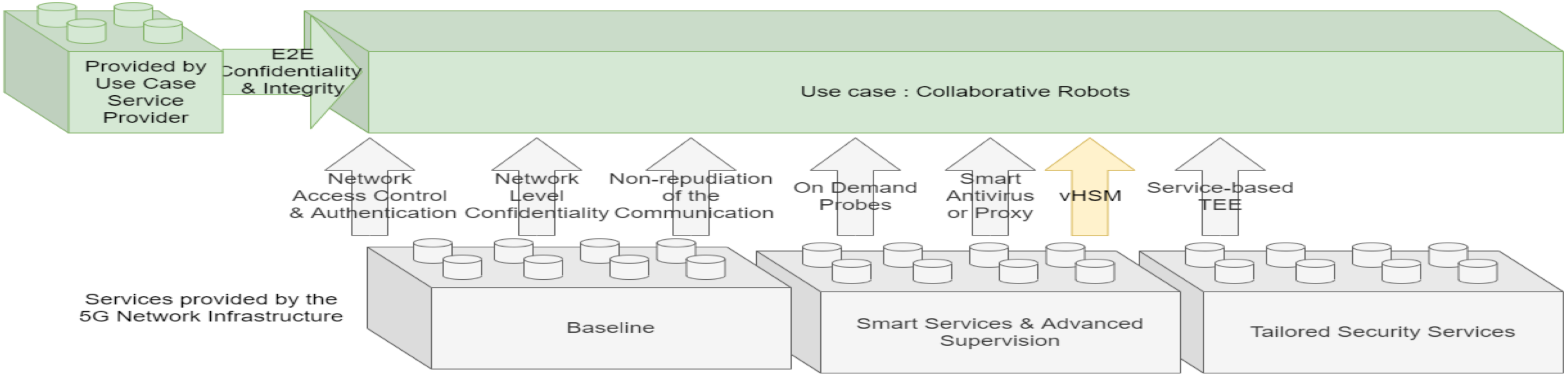


		AUTOMOTIVE			INDUSTRY 4.0			eHEALTH		
Category	Requirements	Infotainment	Remote diagnostics	Anticipated Cooperative Collision Avoidance	Preventive maintenance	Collaborative Robots	Crisis management	Remote diagnostics & smart medication	Emergency diagnostics	Remote surgery
Quality of Service	Network Reliability	Low	Low	High	Low	Low	High	Low	High	High
	Low Latency	Medium	Low	High	Low	Medium	High	Low	High	High
	Availability	Low	Low	High	Low	Medium	High	Low	High	High
	Network Access Priority	Medium	Low	High	Low	Low	High	Low	High	High
	Out of coverage services	Low	Low	High	Low	Low	Low	Low	High	Low
Third Party Trusted Operation & Responsibility Sharing	Protection of Human Safety	Low	Medium	High	Low	High	High	Low	High	High
	Protection of Intellectual Property & Know-How	Medium	Medium	Low	High	High	High	Low	Low	Low
	Protection of Revenue	Medium	Medium	Low	Medium	High	High	Low	Low	Medium
Assurance Demonstration for Third Party Trusted Operation	Network isolation	Low	Medium	High	Medium	Medium	High	Low	High	High
	Network Components Certification Levels	Low	High	High	Low	Low	Low	Low	High	High
	Packet Processing Proof	Low	High	Medium	Low	Low	Low	Low	Medium	High
	Guaranteed Patch Management	Low	High	High	Medium	High	Medium	Medium	Low	Medium
Communication Security	Confidentiality	Medium	Medium	Medium	Medium	Medium	Medium	Medium	High	Medium
	Integrity	Low	High	High	Medium	Medium	High	Medium	High	High
	Authenticity	Low	High	High	Medium	Medium	High	Medium	High	High
	Anti-replay	Low	High	High	Medium	Medium	High	Medium	High	High
	Privacy	Low	Medium	Medium	Low	Low	Low	High	High	Medium
Monitoring & Reaction	Anomaly Detection Service	Low	Medium	High	High	High	High	Low	High	High
	Anomaly Prevention Service	Low	Medium	High	Low	Medium	High	Low	Medium	High
	Real-time Reaction	Low	Low	High	Medium	High	High	Low	High	High

Offer the highest security levels for all services? **NOT an option !!!**

- Critical and sensitive use-cases represent less than 20% of the total usages on 5G infrastructures.
- Mainstream use-cases may not be ready to pay for highest security levels.
- Some security requirements may be incompatible.

On demand security features: use case driven



Provided by Use Case Service Provider

E2E Confidentiality & Integrity

Use case : Collaborative Robots

Network Access Control & Authentication

Network Level Confidentiality

Non-repudiation of the Communication

On Demand Probes

Smart Antivirus or Proxy

vHSM

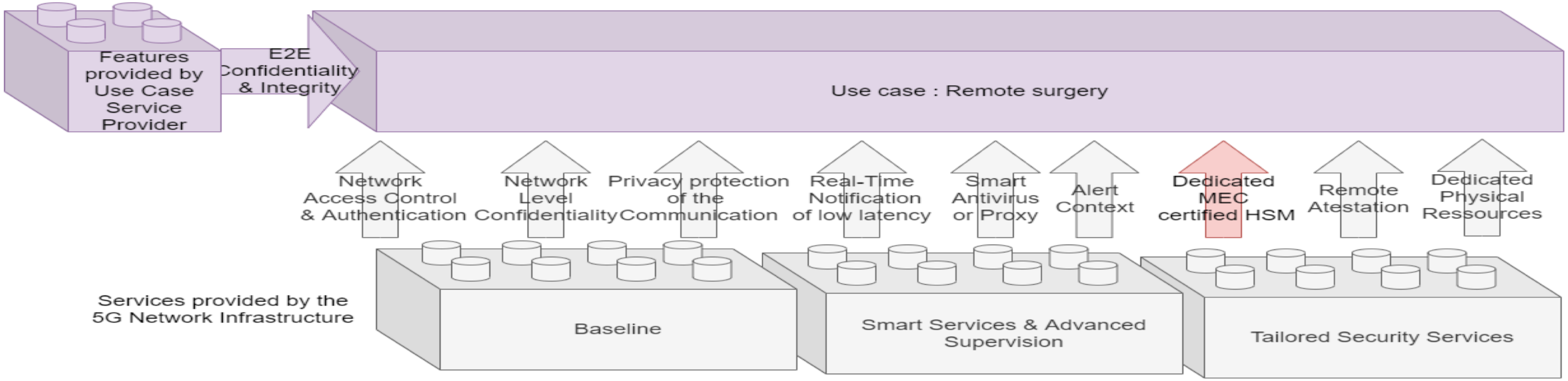
Service-based TEE

Services provided by the 5G Network Infrastructure

Baseline

Smart Services & Advanced Supervision

Tailored Security Services



Features provided by Use Case Service Provider

E2E Confidentiality & Integrity

Use case : Remote surgery

Network Access Control & Authentication

Network Level Confidentiality

Privacy protection of the Communication

Real-Time Notification of low latency

Smart Antivirus or Proxy

Alert Context

Dedicated MEC certified HSM

Remote Atestation

Dedicated Physical Ressources

Services provided by the 5G Network Infrastructure

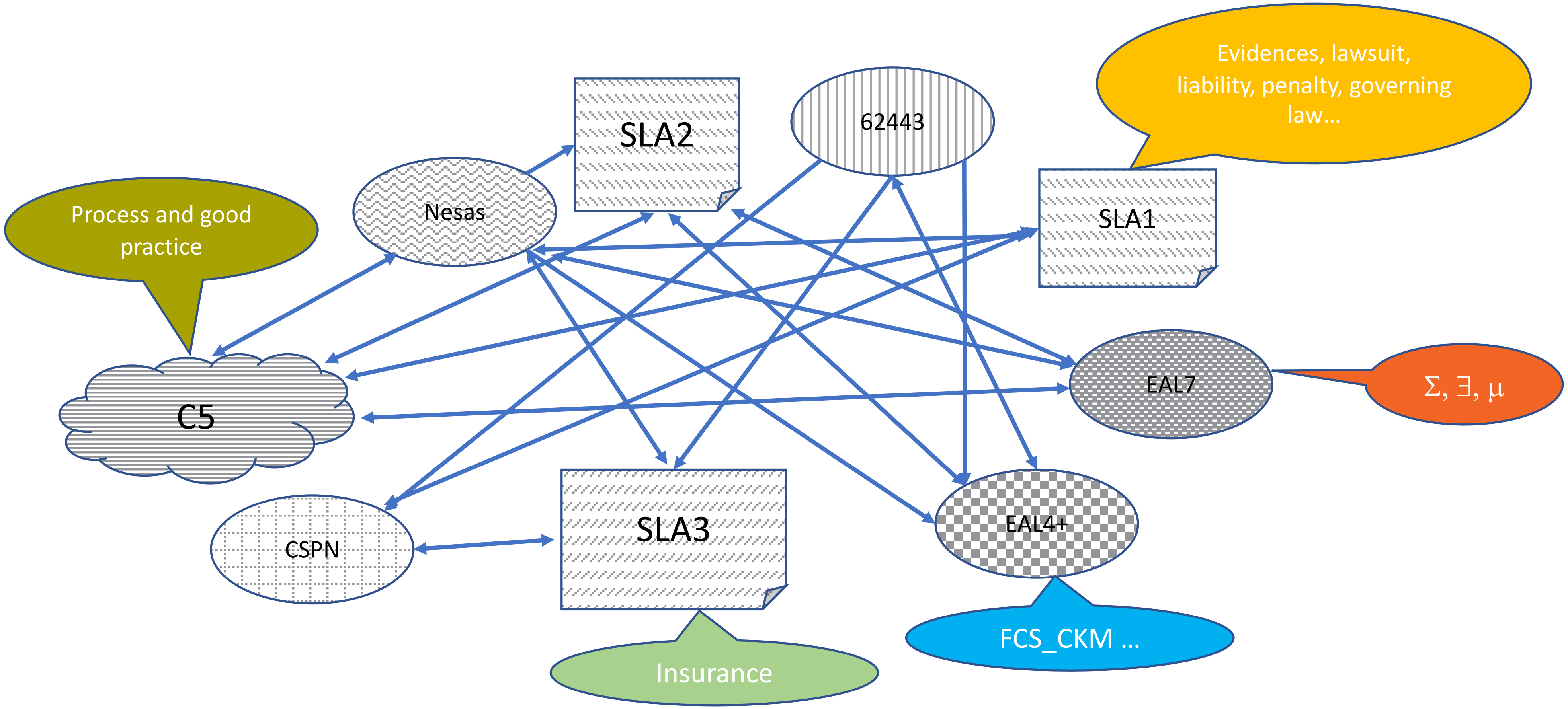
Baseline

Smart Services & Advanced Supervision

Tailored Security Services

Dynamic system of systems

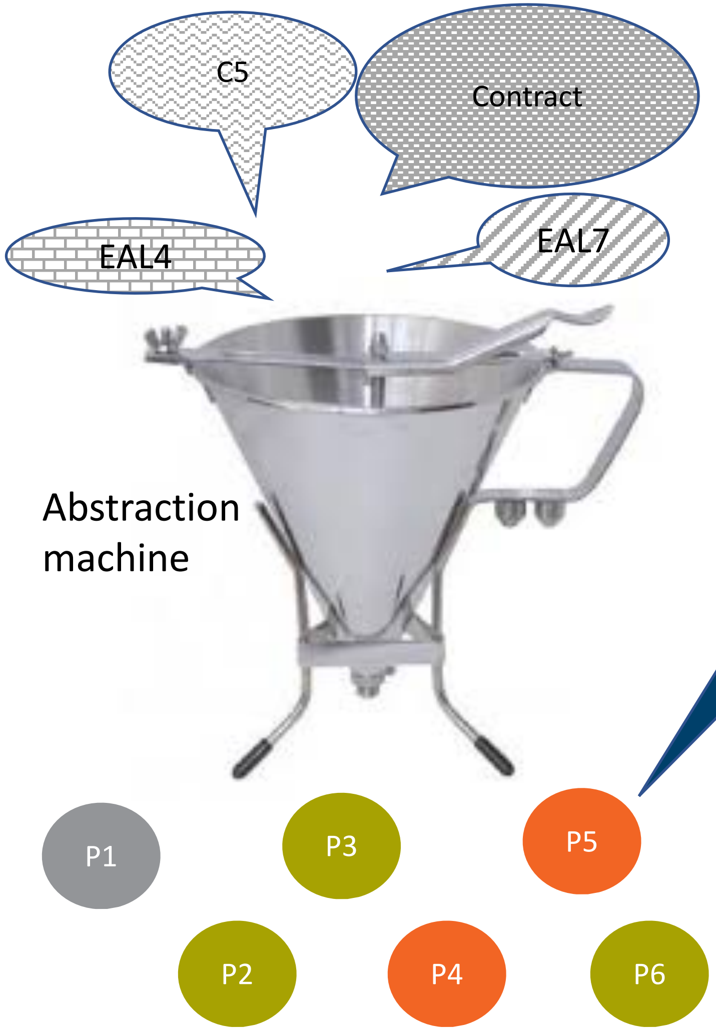
Multiple dependencies and heterogeneous languages



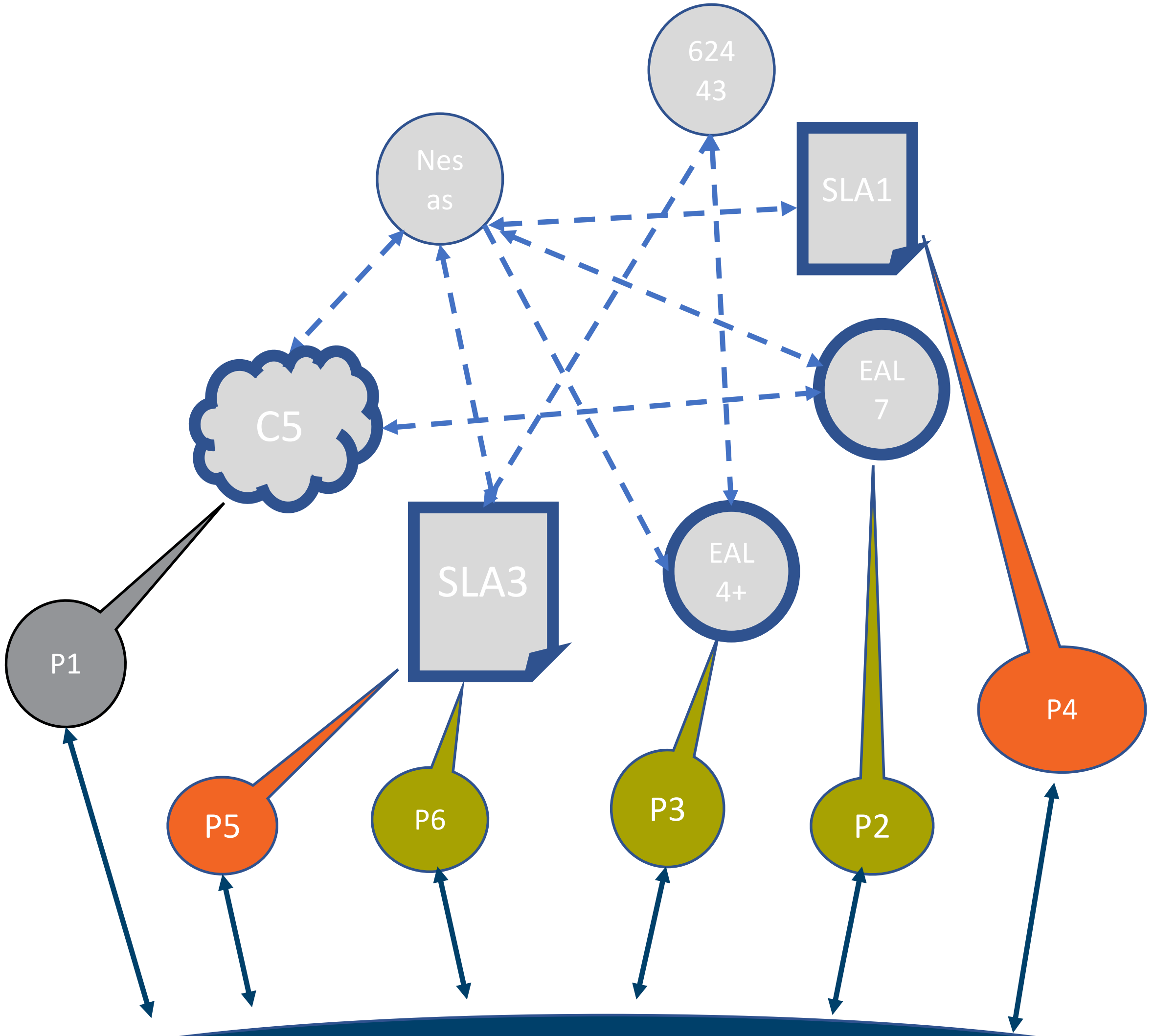
Evidences, lawsuit, liability, penalty, governing law…
SLA2
62443
Nesas
Process and good practice
SLA1
C5
EAL7
Σ, ∃, μ
CSPN
SLA3
EAL4+
FCS_CKM …
Insurance

How to break down complexity?

We have a dream ...



3 levels for cybersecurity properties according to the use case criticality



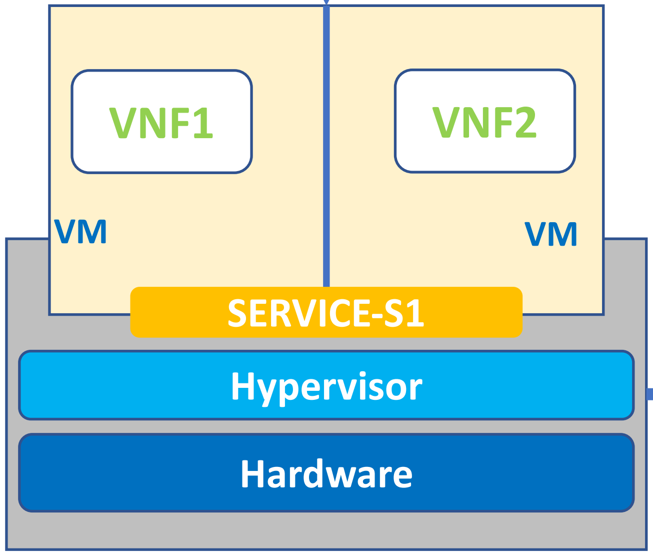
Language to combine cybersecurity properties to meet the e2e use case requirements.

3 abstract levels for cybersecurity properties

Abstract level	Applicable schemes, standards, regulations, etc. (for illustration)	Measures (for illustration)	Liability up to (for illustration)
Level 1	Self-assessment, GSMA-NESAS, CSPN(Fr), EU-CSA basic to substantial – EUCC (VAN.1 or 2), EECC (e.g. R226(Fr)) CSA-Star Level 2	Supplier update database Activity log (post mortem investigation) OWASP10 for web service	10K€
Level 2	**Level 1** + EU-CSA Substantial to High EUCC (Moderate attack potential Van.3) CSA-Star Level3	Best effort obligation Enforced operational security - Operational responsiveness 'On Demand' Monitoring, root-cause analysis Communication monitoring on demand (Licensed and free spectrum monitoring) Contextualization and smart supervision (ML and AI)	100K€
Level 3	**Level 2** + EUCC High on technical domains (VAN.4 and VAN.5), Private schemes (EMVCo,…)	Tailored security services and resources Result obligation or dedicated means Hardware grounded features Attestation, Proof of transit, proof of elapsed time, … Strong Isolation (5G-Slice, VM or Containers) Tailor made security	1000k€

Insurance company another kind of certification body?

The SERVICE-S1 offers controlled data sharing between containers (confidentiality and integrity) by authorized Users only



Contract between Service User – Service Provider

*Service-**Security Objectives and SLA-***

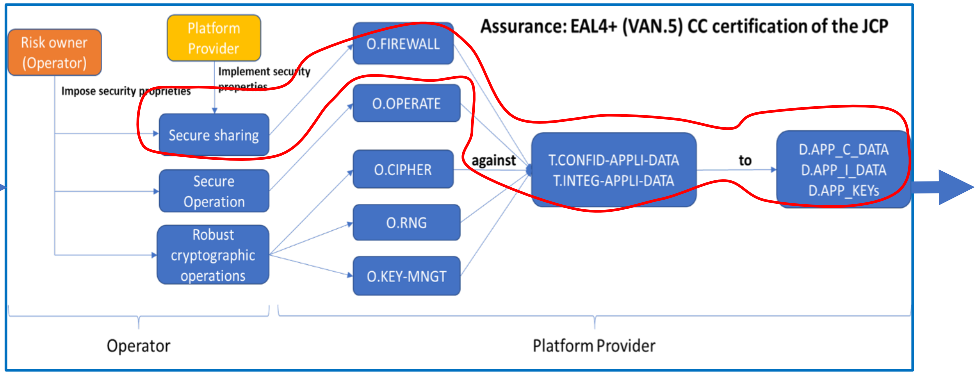
maximum liability amount

Operated through/warranted by the Insurance Company

The Insurance Company delivers Insurance Certificates

Insurance Liability up to :

Level 1	(10k€)
Level 2	(100k€)
Level 3	(1M€)

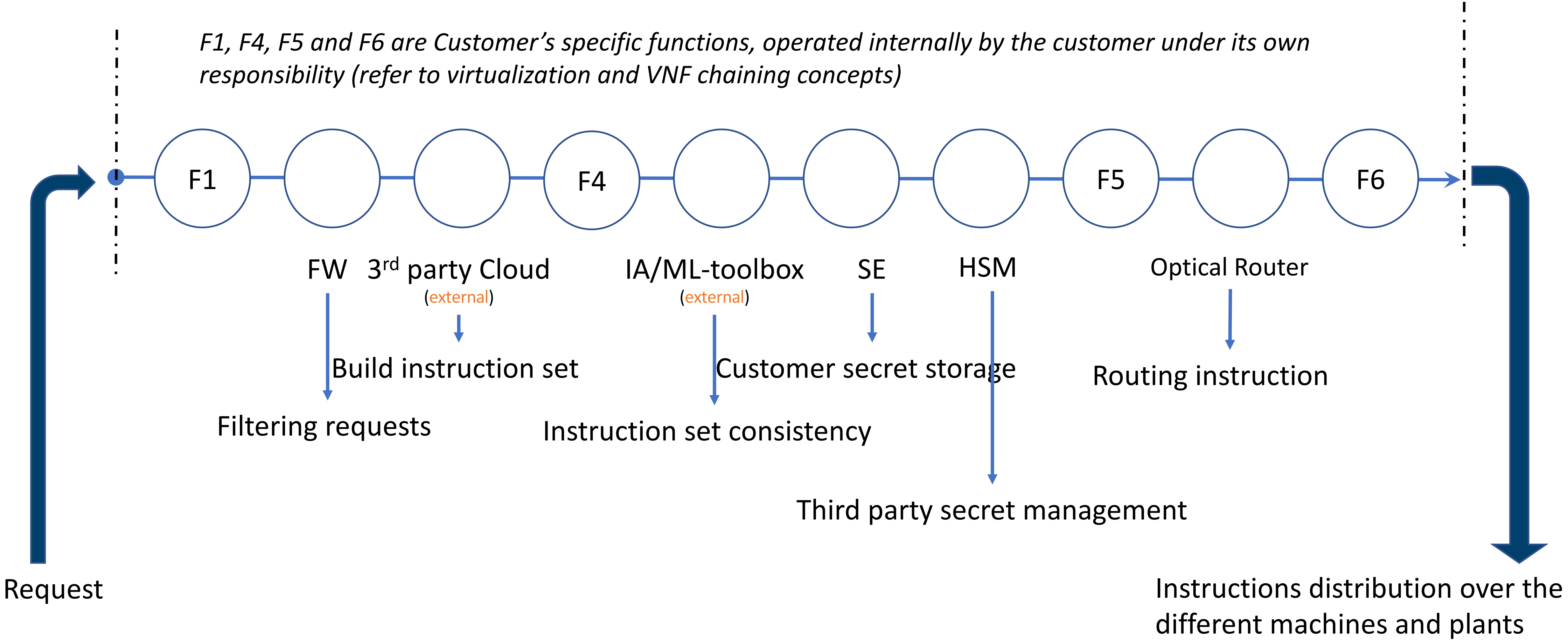


The Insurance Company performs

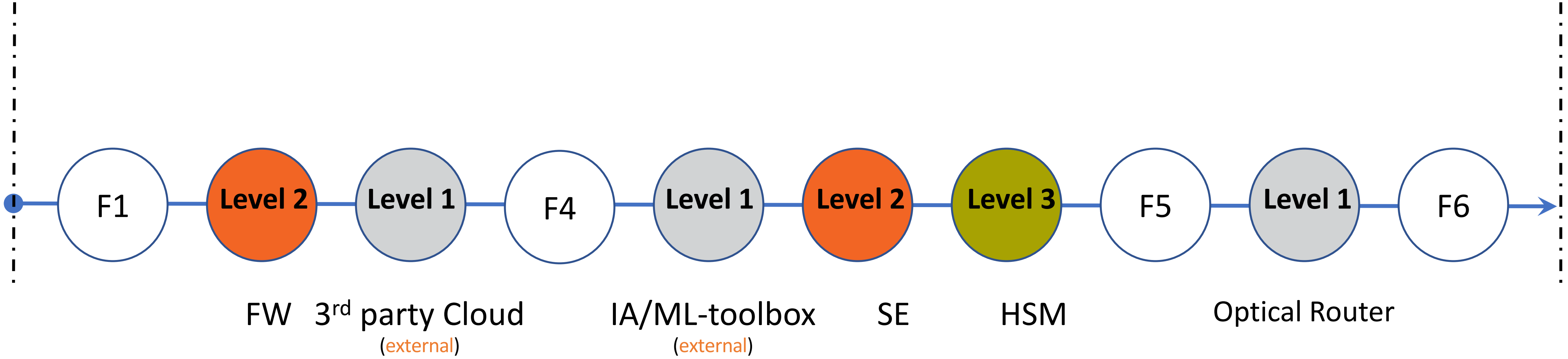
Audit, Pentest and whatever technics relevant for the use case.

Pilot and supervise Industrial plants

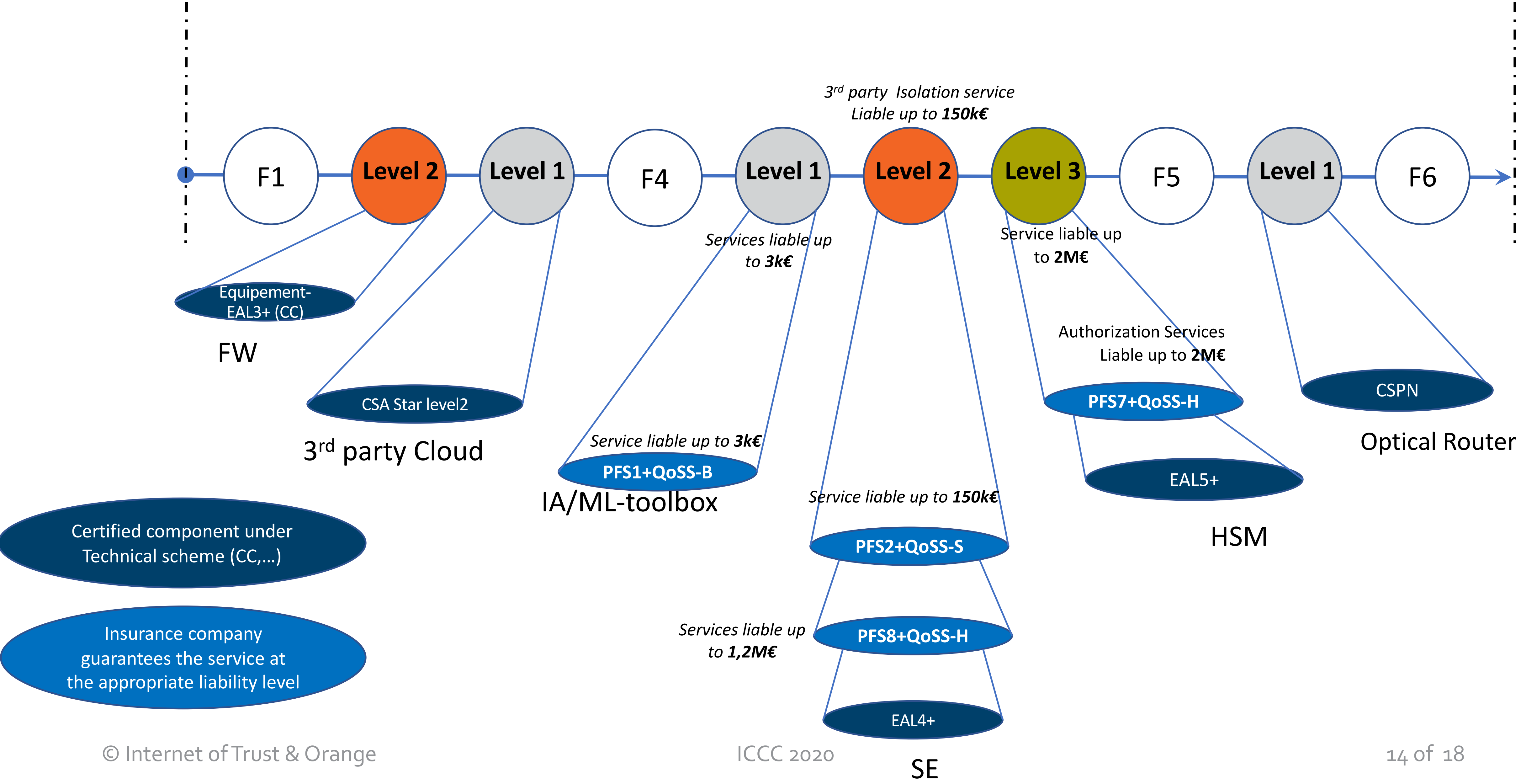
F1, F4, F5 and F6 are Customer's specific functions, operated internally by the customer under its own responsibility (refer to virtualization and VNF chaining concepts)



Determine the E2E security strategy



Get appropriate assurances



F1

Level 2

Level 1

F4

Level 1

Level 2

Level 3

F5

Level 1

F6

Equipement-EAL3+ (CC)

FW

CSA Star level2

3rd party Cloud

*Services liable up to **3k€***

*Service liable up to **3k€***

PFS1+QoSS-B

IA/ML-toolbox

*3rd party Isolation service Liable up to **150k€***

*Service liable up to **150k€***

PFS2+QoSS-S

*Services liable up to **1,2M€***

PFS8+QoSS-H

EAL4+

SE

Service liable up to **2M€**

Authorization Services Liable up to **2M€**

PFS7+QoSS-H

EAL5+

HSM

CSPN

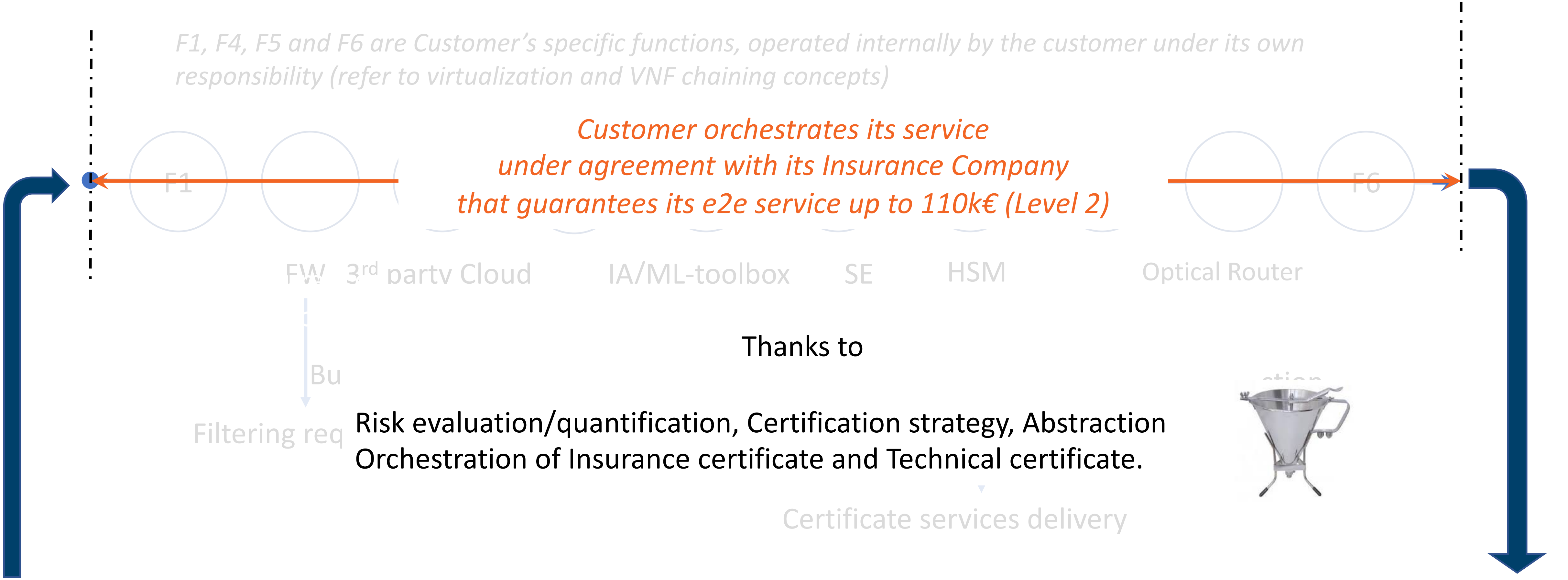
Optical Router

Certified component under Technical scheme (CC,…)

Insurance company guarantees the service at the appropriate liability level

E2E customer service guarantied

F1, F4, F5 and F6 are Customer's specific functions, operated internally by the customer under its own responsibility (refer to virtualization and VNF chaining concepts)



Customer orchestrates its service
under agreement with its Insurance Company
that guarantees its e2e service up to 110k€ (Level 2)

Thanks to

Risk evaluation/quantification, Certification strategy, Abstraction
Orchestration of Insurance certificate and Technical certificate.

Request

Instructions distribution over the different machines and plants

Conclusion

Trust model for verticals over 5G?

Our answer:

- an abstract interpretation approach reduces the whole complexity of 5G-ecosystem and is fully compatible with the EU CSA.
- our Trust model involves Insurance liability scheme to combine certified platform and non certified services
- our Trust model integrates risk management.

- Open challenges
  - Build an "Abstraction machine" that selects only relevant information from certified product, system and contractual obligations
  - Tailor the abstraction levels according to each use case
  - Reuse as much as possible existing schemes (technical, organizational and contractual)
  - Combine insurance and product certificates, orchestration and abstraction machines

Questions ?