THALES

Cyber security challenges and requirements for future 5G-enabled PPDR organisations

PSCE CONFERENCE, LANCASTER, 2019 JUNE THE 6TH

Edith Félix

PPDR organisations rely on mission critical systems

5G to support verticals such as public safety organisations

- 5G is intended to support mission critical applications (large crisis, rescue with private data…)

MC requires well defined Quality of Service

- Resilience, security, performance, etc.

Insuring QoS over a public or shared infrastructure requires rules

- For example, pre-emption of the bandwidth over regular traffic for MC applications (cf : FirstNet for First Responder Network Authority in USA)
- Best effort is insufficient

Réalisé par Alexandre DUBUS

Operational technology vs Information technology

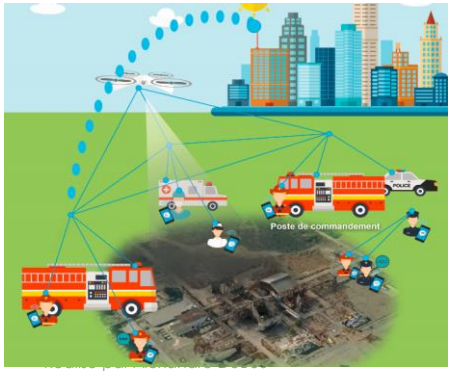
Operational technology (OT)

- is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events.

Information technology (IT) :

- Technologies for information management and processing, including software, hardware, communications technologies and related services.

PPDR organisations tend to use more and more integrated services



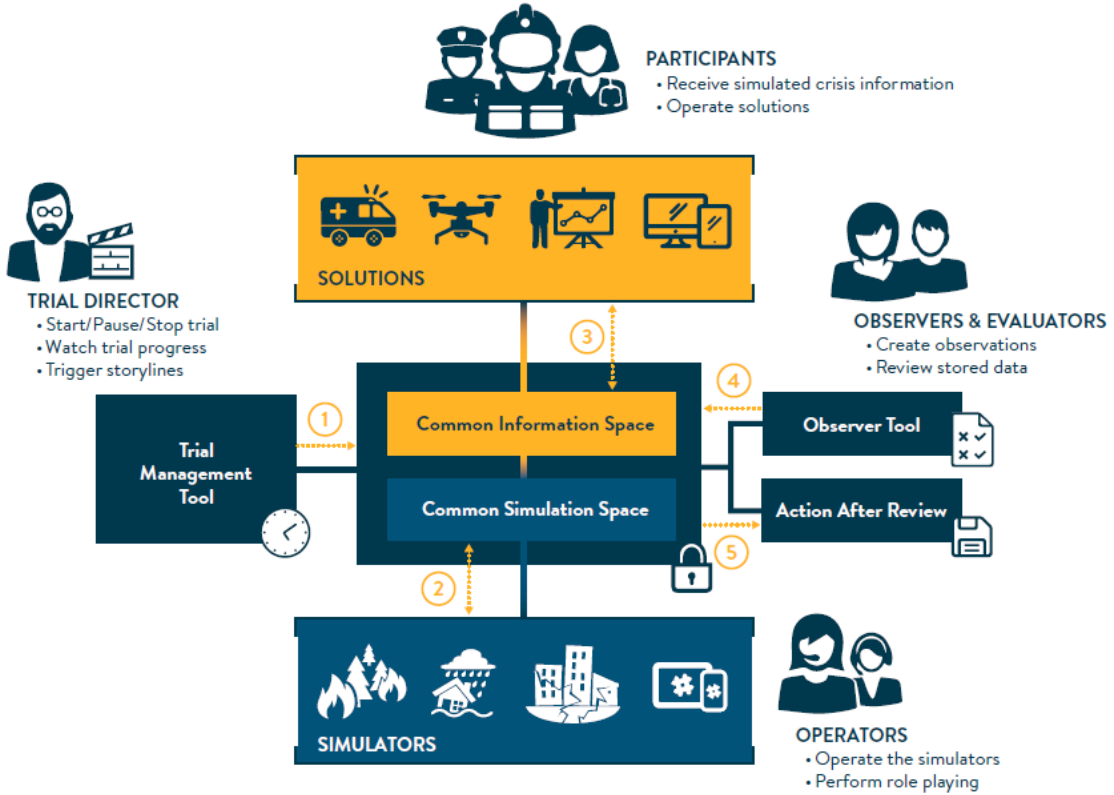
Ex: French FUI AAP20 PODIUM
Plateforme pour déchargement sécurisé dans le cloud mobile

- Ad-hoc deployment of a resilient and autonomous system
- Multimedia Group communication (upload of field data and download for the command chain)
- Rapid mapping from sensors and Common Operational picture with geo-localised data from the connected first responders

THALES

FP7 DRIVER+ example: a secured pan-European testbed to drive innovation in Crisis Management

- CM trials run through solutions connected to the CIS
- Inputs to the scenario are simulated by simulators over the CSS
- Both CIS and CSS run Apache Kafka publish/subscribe which organises the exchange of data through topics.
- Access to topics are authorised through a lightened version of Thales' AuthZforce XAML Open Source Software



OPEN

THALES

Cybersecurity is key to 5G

5G attack surface is broader than in previous generations because

- Major digital architectural patterns of Smart Networks and Services such as:
  - service-dominant/cloud-based ecosystems,
  - Internet of Things (IoT),
  - Cyber-Physical Systems (CPS),
  - Edge Computing,
  - 5G slices, etc.
- more or less disruptive technology trends such as:
  - Artificial Intelligence (AI),
  - Distributed ledgers/blockchain,
  - Virtualisation,
  - Softwarisation,
  - Cloudification,

Threats are targeting States, strategic operators, etc.

- **Strategic sovereignty** (D. Trump bans Huawei) vs **Strategic autonomy** (COMMISSION RECOMMENDATION of 26.3.2019 - Cybersecurity of 5G networks)
- EOS POSITION PAPER - EU **DIGITAL AUTONOMY**: Challenges & Recommendations for the Future of European Digital Transformation

Réalisé par Alexandre DUBUS

THALES

What is the European framework for strategic/digital autonomy ? (some pinpoints)

GDPR has set a first step towards digital autonomy, imposing a European regulation for data privacy

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Cybersecurity Act, adopted in December 2018

- European Commission, Proposal for a Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification. COM/2017/0477 final
- https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

> Reinforces the mandate for the EU Cybersecurity Agency, ENISA

> Announcing a new European cybersecurity certification framework

Réalisé par Alexandre DUBUS

ENISA and other European certification frameworks (2017)

European Agency for Network and Information Security gets more tasks to assist Member States in dealing with cyber attacks:

- A strong mandate
- A permanent status
- Adequate resources

ENISA resources	Now	Future
Staff	84 people	125 people
Budget	€11 million	€23 million
	gradual increase: starting with +5 million 1st year and fully achieved 4 years after entry into force.	

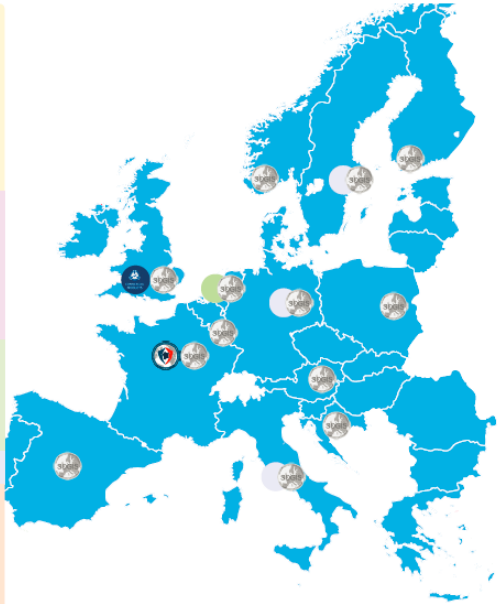
The **Commercial Product Assurance** (CPA) developed in the UK applies to commercial off-the-shelf products that are awarded certifications which prove good commercial security practice and certify that a product is suitable for lower threat environments. However, there is no mutual recognition agreement for CPA, which means that products tested in the UK will not normally be accepted as certified products in other markets.

Certification Sécuritaire de Premier Niveau (CSPN) is an IT security certification scheme established by the National Cybersecurity Agency of France (ANSSI). Similarly to the CPA, there is no mutual recognition for CSPN, which means that products tested in France will normally not be accepted in other markets.

The **Dutch Baseline Security Product Assessment** (BSPA) provides information on the suitability of IT security products for use in the "sensitive but unclassified" domain. The BSPA scheme has been in pilot phase since 2015 and is expected to be operational by the end of 2017.

Other emerging initiatives

SOG-IS MRA includes 12 Member States plus Norway and has developed a few protection profiles on digital products e.g. digital signature, digital tachograph and smart cards. Members can participate in a mutual recognition agreement as certificate consumers and producers.



ENISA Fact sheet - CYBERSECURITY : EU AGENCY AND CERTIFICATION FRAMEWORK - State of the Union in 2017
https://ec.europa.eu/digital-single-market/en/news/cybersecurity-eu-cybersecurity-agency-and-eu-framework-cybersecurity-certification

Réalisé par Alexandre DuBus

Member States responsibility. Lifecycle certification.

COMMISSION RECOMMENDATION of 26.3.2019 - Cybersecurity of 5G networks

- This Recommendation addresses cybersecurity risks in 5G networks by **setting out guidance on appropriate risk analysis and management measures at national level**, on developing a coordinated European risk assessment and on establishing a process to develop a common toolbox of best risk management measures.
- In the absence of harmonised Union law, **Member States may specify** by means of national technical regulations, adopted in compliance with Union law, **that a European cybersecurity certification scheme should be mandatory**. Member States also have recourse to European cybersecurity certification schemes **in the context of public procurement** and of Directive 2014/24/EU[13] and could support the development of assistance mechanisms – such as an assistance hub – for the purchase of cybersecurity solutions by public buyers.
- Important aspects to consider should be the need **to protect the networks across their entire lifecycle** and the need **to cover all relevant equipment, including in the design, development, procurement, deployment, operation and maintenance phases of 5G networks.**

Réalisé par Alexandre DUBUS

EOS POSITION PAPER - EU DIGITAL AUTONOMY: Challenges & Recommendations for the Future of European Digital Transformation

EOS position paper preparing future work

- examining the key risks and opportunities for EU digital autonomy, across five distinct digital products and services
  - **Sourcing and Sharing Cyber Threat Intelligence in Europe**
  - **The Internet of Things (IOT) & Cyber-Physical Security**
  - **Secure Data Lifecycle: A Cryptography Challenge**
  - **Artificial Intelligence (AI)**
  - **Cyber Security as a Service**

Réalisé par Alexandre DUBUS

Digital autonomy

EOS POSITION PAPER - EU **DIGITAL AUTONOMY**: Challenges & Recommendations for the Future of European Digital Transformation

KEY TAKEWAYS

- ❑ **Europe's economy is dependent on digital infrastructures and services**
- ❑ **The cyber-security of these underlying elements must be ensured across complex value chains**
- ❑ **Sourcing critical elements in Europe is the only solution to guarantee compliance to European values, protection of IPRs and continuity of operational capabilities**
- ❑ **EOS recommends developing digital autonomy "enablers" ranging from skills to cyber-threats detection and response mechanisms**

THALES

Further work

The need for evaluation/certification framework

Not enough covered as far: to warranty a continuous assessment for secured operation through the whole lifecycle including

- Hardware, Software,
- Systems and composition of services
- The whole lifecycle (design, development, procurement, deployment, operation and maintenance phases)
- Dynamic reconfiguration of virtualized networks

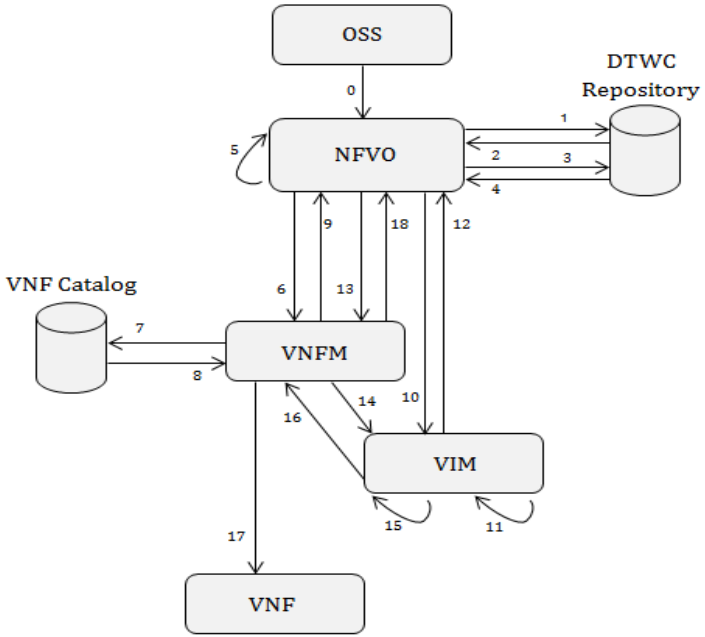
SENDATE Example: Towards evaluating VNF trustworthiness attributes

VNF Certification Enabler

- A tool to evaluate trustworthiness attributes of a VNF implementation by using a digital trustworthiness certificate (with a lightweight certification process).

How to use this Enabler ?

- Automatically by a NFV Orchestrator with a predefined set of attributes.
- Manually by an operator interacting with the NFV Orchestrator.



- Implementation through 3 EU projects (FP7 OPTET, H2020 5GPP 5GENSURE, Celtic+ SENDATE) (2013 -> 2018)

Réalisé par Alexandre DUBUS

THALES

SU-ICT-02-2020 Building blocks for resilience in evolving ICT systems

Specific challenge

- Algorithms, software and hardware systems must be designed having security, privacy, data protection and accountability in mind from their design phase in a measurable manner. Relevant challenges include: (a) to develop mechanisms that measure the performance of ICT systems with regards to cybersecurity and privacy and (b) to enhance control and trust of the consumer of digital products and services with innovative tools aiming to ensure the accountability of the security and privacy levels in the algorithms, in the software, and ultimately in the ICT systems, products and services across the supply chain.

Sub-topics

- a) Cybersecurity/privacy audit, certification and standardisation
- b) Trusted supply chains of ICT systems
- c) Designing and developing privacy-friendly and secure software and hardware