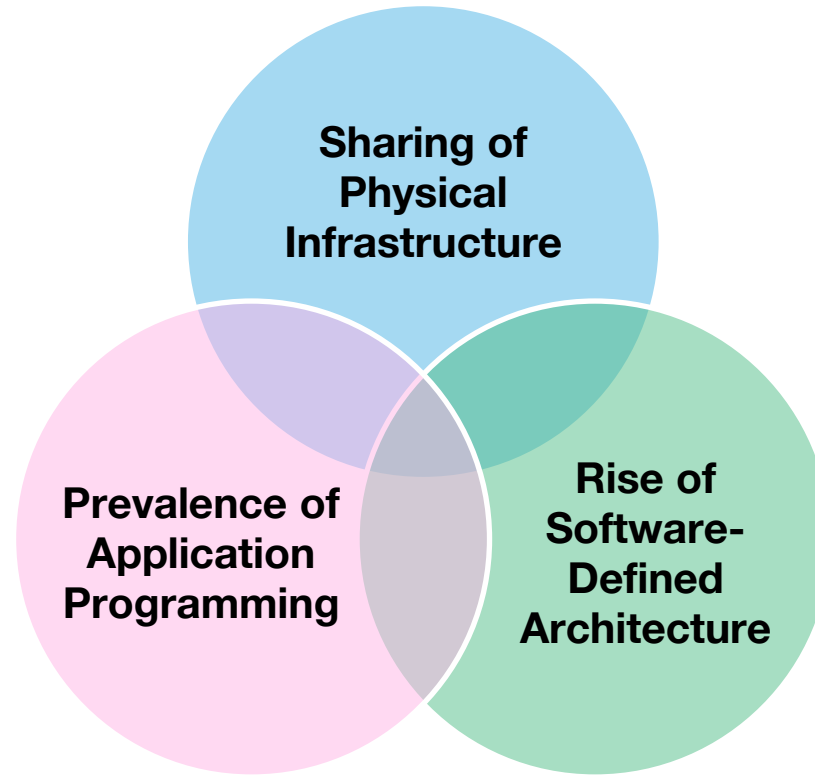


Software-Defined IOT

Chrystel Gaber,
RIOT summit
15th September 2020



SD-IOT : what ?



1-Software-defined internet of things for smart urban sensing. J.Liu, Y.Li, M.Dong, D.Jin, IEEE communications magazine, 2015)



SD-IOT : why ?

IOT

Everything connects from everywhere

Virtualisation & orchestration

Potential solution

Safety

Safety requirements on IoT systems may have an impact on network security requirements



Data

Large volumes of data produced

Network infrastructure

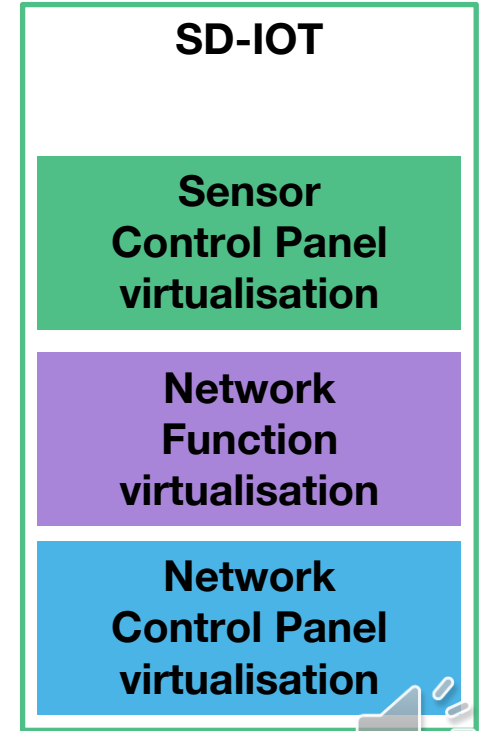
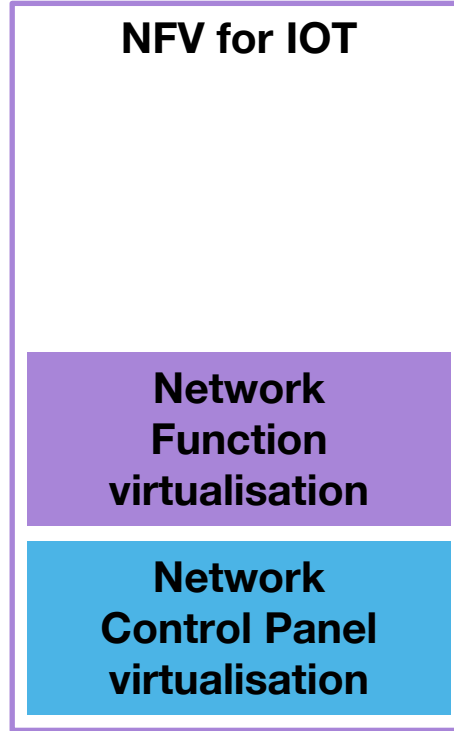
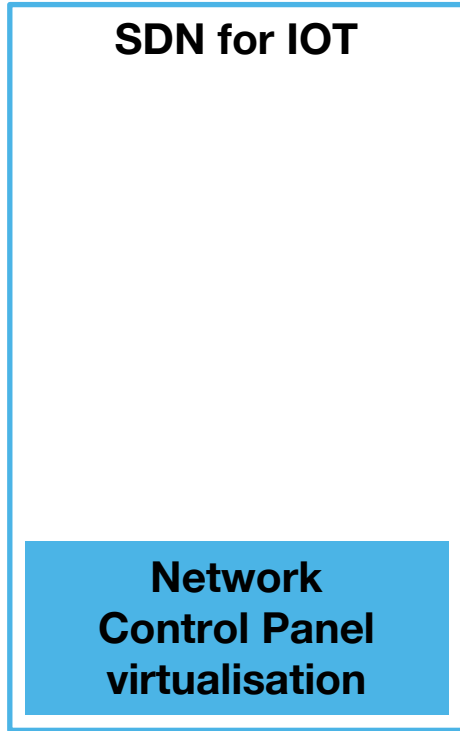
Increased need to install network & core devices

Efficient management

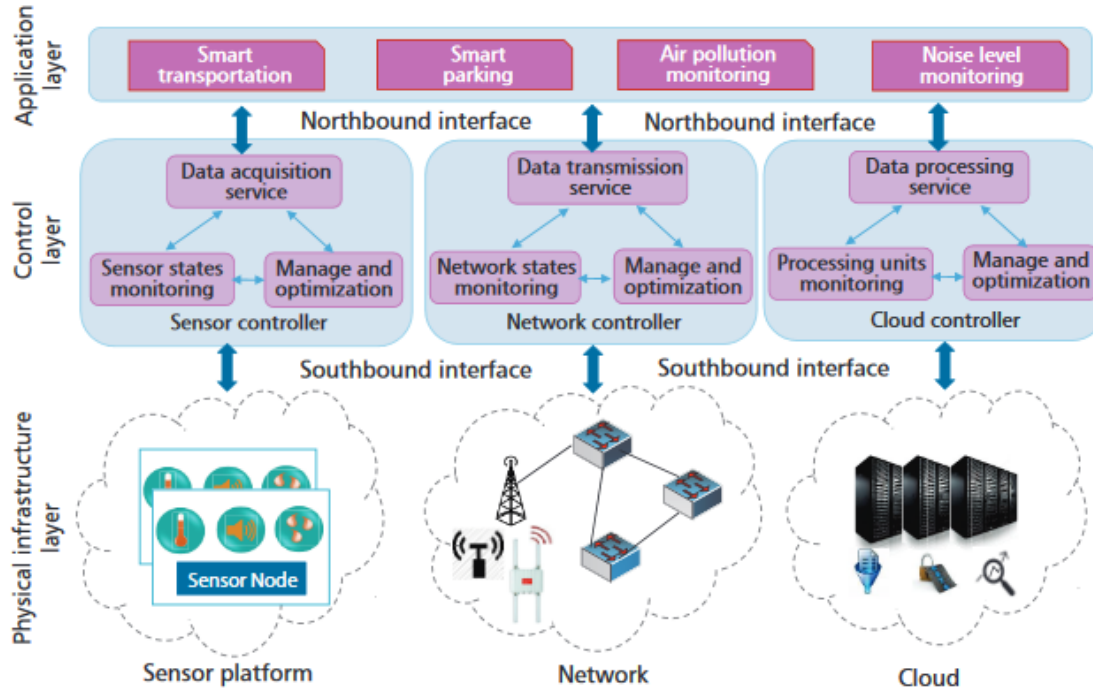
QoS & Costs need to be optimized



SD-IOT : 3 types of architectures



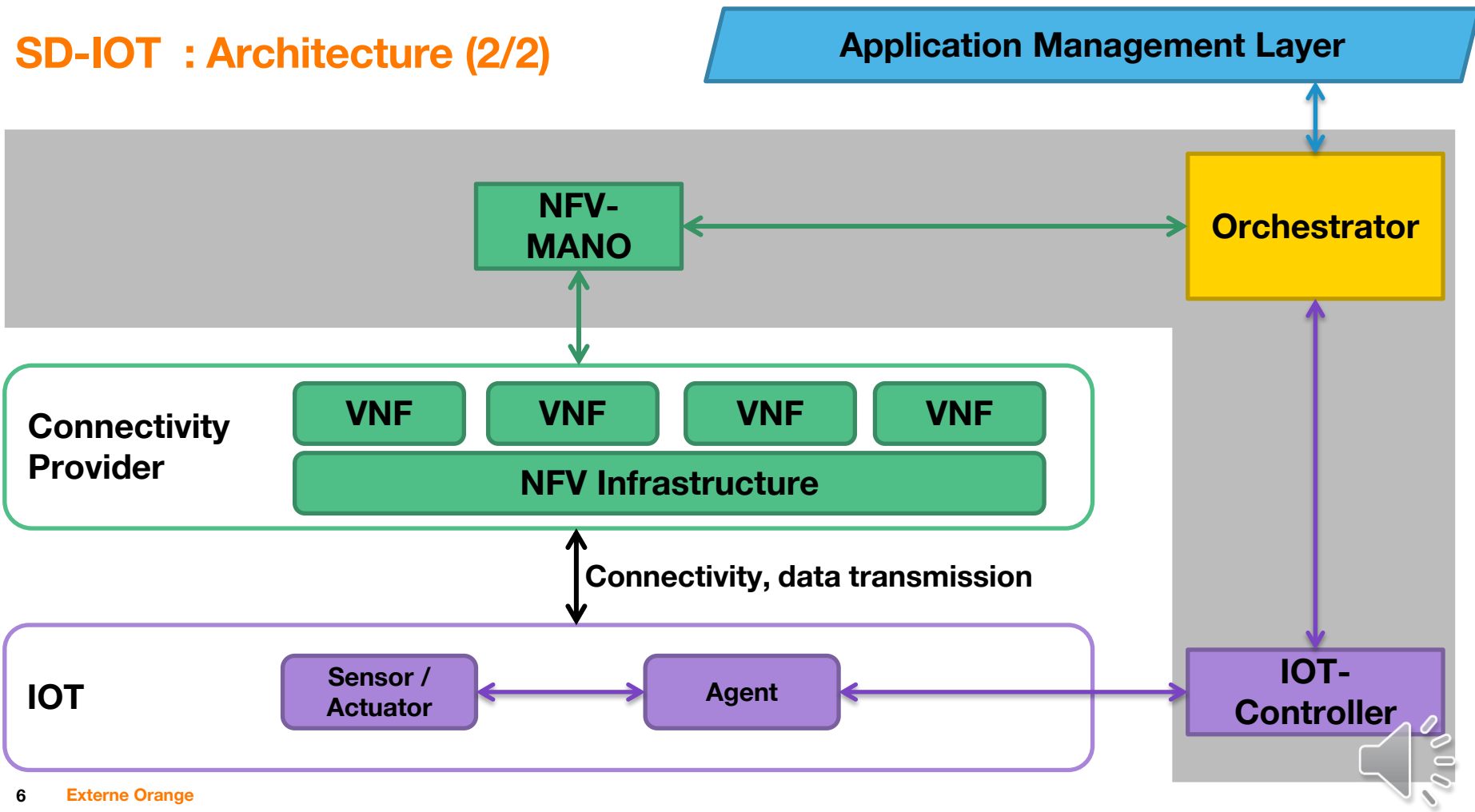
SD-IOT : Architecture (1/2)



1-Software-defined internet of things for smart urban sensing. J.Liu, Y.Li, M.Dong, D.Jin, IEEE communications magazine, 2015)



SD-IOT : Architecture (2/2)



SD-IOT : Possibilities

- **Configure network**
- **Deploy VNF for on-demand QoS, security or storage**
- **Manage IoT device e.g. update**
- **Share & manage access to IoT device**

[link](https://www.cio-online.com/actualites/lire-orange-va-deployer-un-dispositif-iot-pour-monitorer-ses-poteaux-telephoniques-12297.html) : <https://www.cio-online.com/actualites/lire-orange-va-deployer-un-dispositif-iot-pour-monitorer-ses-poteaux-telephoniques-12297.html>



SD-IOT : Use case 1 – Serenity at Home

20 Feb 2019 | 14:56 GMT

Japan to Probe IoT Devices and Then Prod Users to Smarten Up

A government project begins testing millions of Internet-connected devices to see how safe they are from cyberattacks

By John Boyd



Illustration: iStockphoto

- **Service Provider takes responsibility for fully securing your IoT devices at home**
 - Manage passwords & updates
 - Control the access to IoT devices to authorized users (family, neighbours, tenants)
 - Enrich IoT security services with edge & fog on-demand virtual functions
 - Isolate sensitive / malicious IoT devices in dedicated subnetworks

[link](https://spectrum.ieee.org/tech-talk/telecom/internet/japan-aims-to-probe-unsecured-iot-devices-and-then-prod-users-to-smarten-up) : <https://spectrum.ieee.org/tech-talk/telecom/internet/japan-aims-to-probe-unsecured-iot-devices-and-then-prod-users-to-smarten-up>



SD-IOT : Use case 2 – 5G Infrastructure Management

 Hello Future

 Augmented Planet / Networks

Monitored telephone poles with IoT

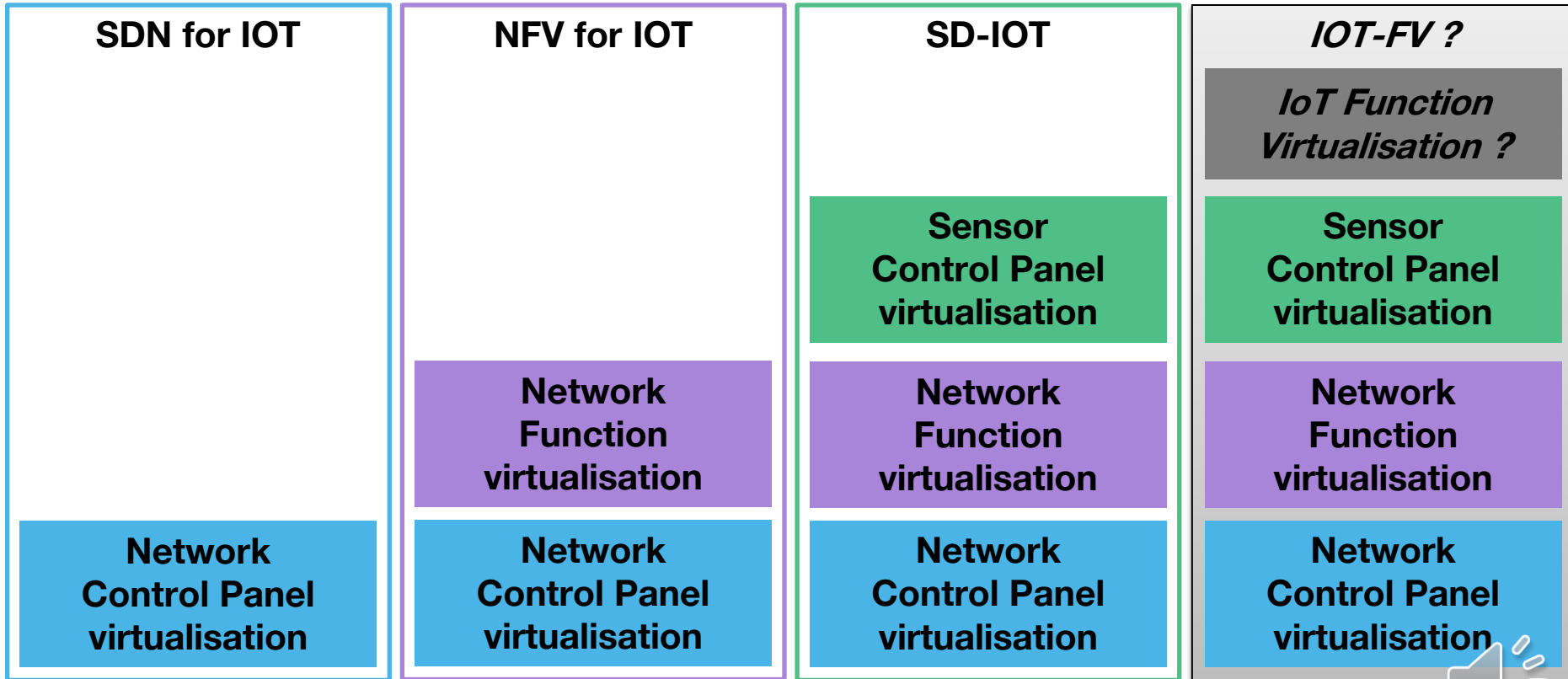


- Operators deploys IoT devices to monitor 5G antennas ([link](#))
- Verify trustworthiness of sensed data to avoid disruption of service
- Full visibility of vulnerability of 5G infrastructure

[link](https://hellofuture.orange.com/en/monitored-telephone-poles-with-iot/) : <https://hellofuture.orange.com/en/monitored-telephone-poles-with-iot/>

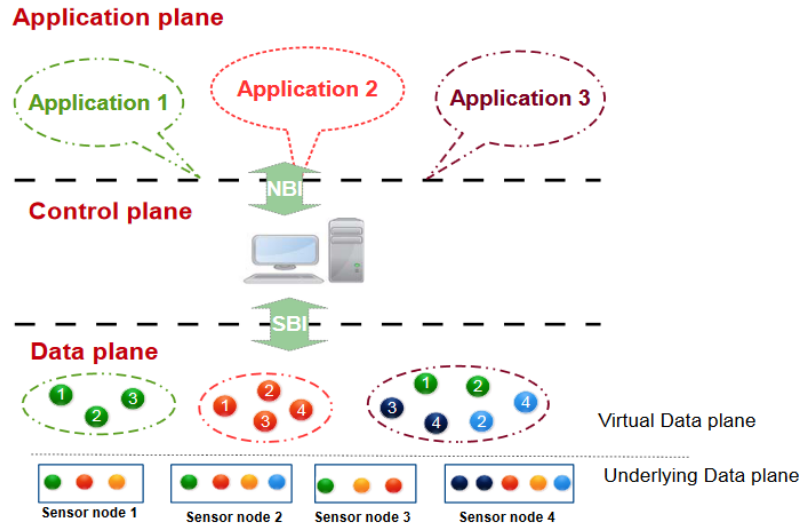


What is up next?



Reprogrammability of IoT devices

- IOT- virtualisation through the use of twins
 - Decorrelate instructions from physical devices, e.g. virtualSensors¹



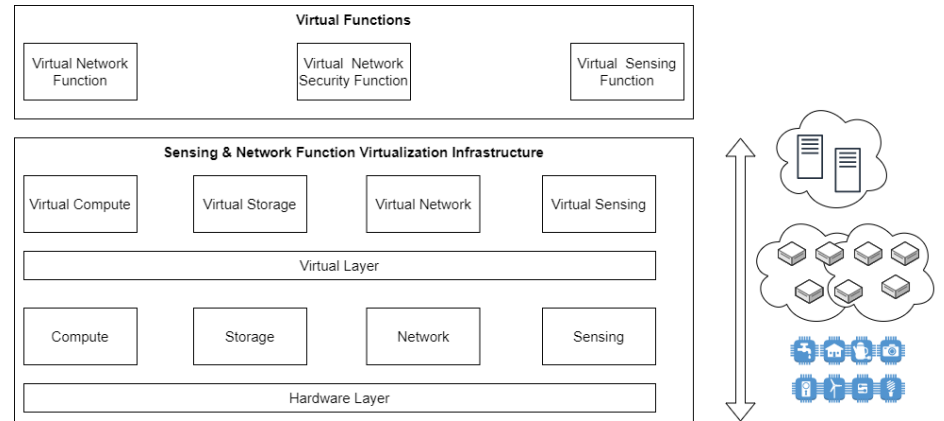
1-Toward a Programmable Software-Defined IoT architecture for Sensor Service Provision On Demand, T. M. C. Nguyen, Doan, B. Hoang, T. D. Dang, 2017 27th International Telecommunication Networks and Applications Conference (ITNAC)



Reprogrammability of IoT devices

- **Use case : Cloud-IoT convergence**¹
 - from centralized to decentralized model (e.g. Fog computing)
 - from homogeneous to specialized & heterogeneous (e.g. FaaS)

- **Containers for continuum Cloud / Edge / IOT**
 - OTA scripting containers²
 - Avoid large code with exhaustive conditions
 - Update application logic without rebooting
 - Privacy processing on far-edge devices



1-Next-Generation Cloud Architectures, K.M. Giannoutakis, M. Spanopoulos-Karalexidis, C.K.F Papadopoulos and D. Tzovaras, Book, The Cloud-to-Thing continuum – Opportunities and Challenges, Fog and Edge Computing, Chapter 2, pp23-39

2- Scripting-over-the-air: Towards containers on low-end devices in the Internet of Things, E. Baccelli, J. Doerr, S. Kikuchi, F.A. Padilla, K. Schleiser & I. Thomas, 2018 IEEE International Conference on Pervasive Computing and Communications Workshops



Challenges for SD-IOT & IOT-FV



- **Need to develop liability-aware security mechanisms**
 - Gartner Sept 2020 : 75% of CEOs **personally liable** for **cyber-physical incidents** by 2024¹
 - Complex architectures & liability / torts management
 - Manifests for IoT & VNF capture liabilities from the supply & deployment chain
→ liability-aware security management ²
- **Virtualisation- or container-like technology for constrained devices**
 - security & isolation properties for constrained devices
- **Orchestrator for IoT & NFV : compatibility ?**

1- [link](https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl) : <https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl>

2- Liability-Aware Security Management, Chrystel Gaber and José Sanchez Vilchez, Gürkan Gür, Morgan Chopin, Nancy Perrot, Jean-Luc Grimault and Jean-Philippe Wary, IEEE 5G World Forum – Workshop on 5G Security: Current Trends, Challenges and New Enablers, 2020



Conclusion

IOT
Everything connects from everywhere

Virtualisation & orchestration
Potential solution

Safety
Safety requirements on IoT systems may have an impact on network security requirements

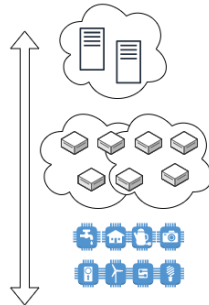
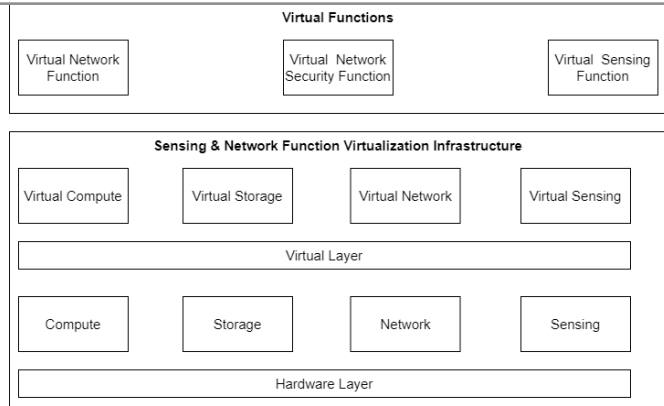
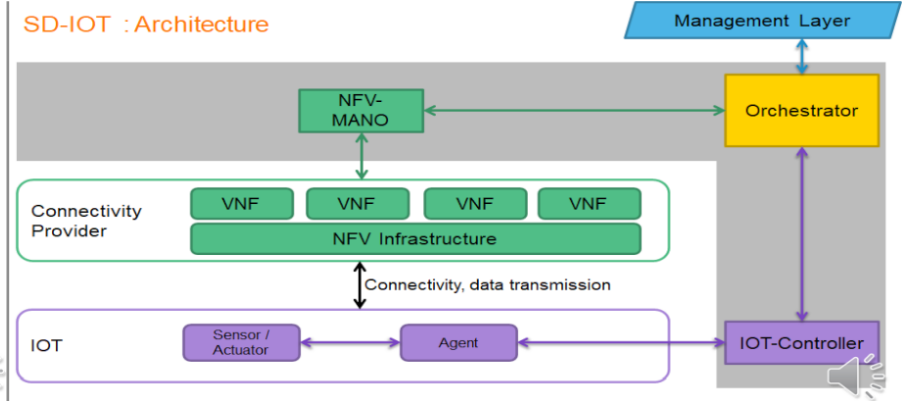


Data
Large volumes of data produced

Network infrastructure
Increased need to install network & core devices

Efficient management
QoS & Costs need to be optimized

SD-IOT : Architecture



Merci Thank you

Contact : chrystel.gaber@orange.com

