Smart5Grid

Demonstration of **5G** solutions for
SMART energy **GRID**s of the future

5G PPP
The 5G Infrastructure Public Private Partnership

This project has received funding from the European Union's *Horizon 2020 research and innovation programme* under grant agreement n° 101016912

Daniele Porcu

Project Coordinator

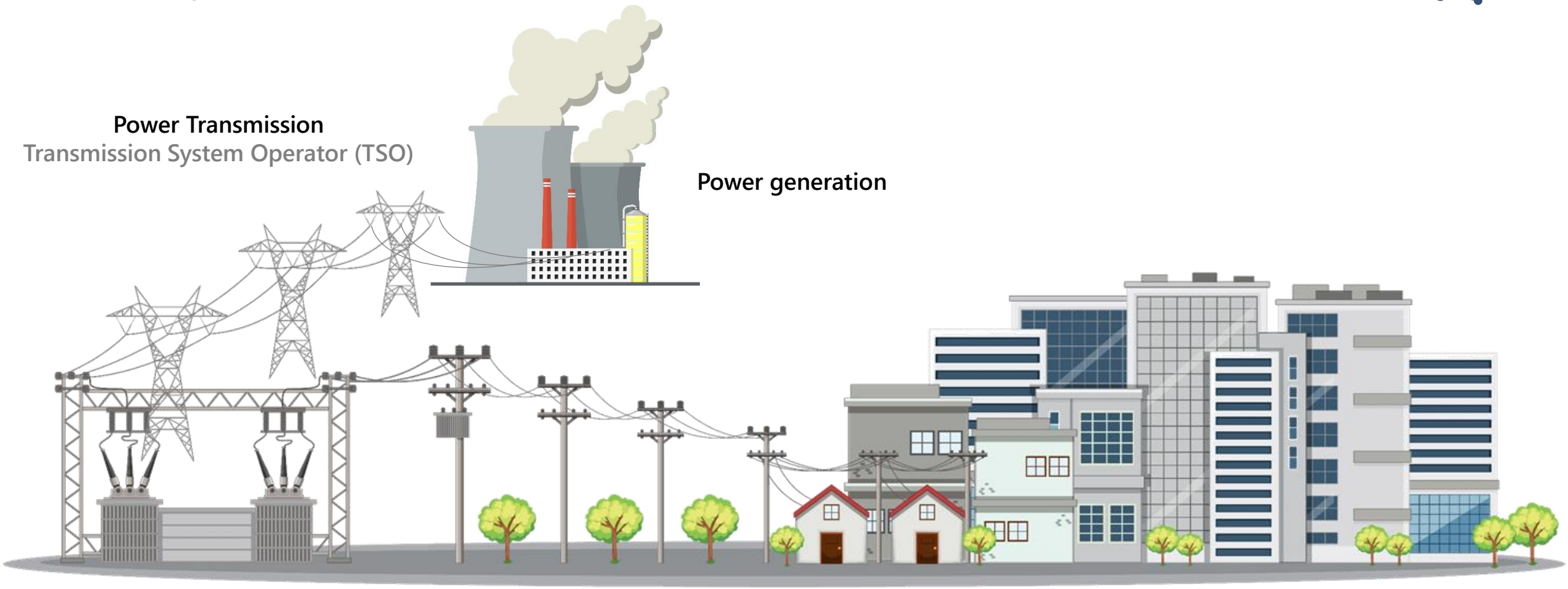
daniele.porcu@enel.com

Energy Vertical

Traditional grid

Power Transmission
Transmission System Operator (TSO)

Power generation

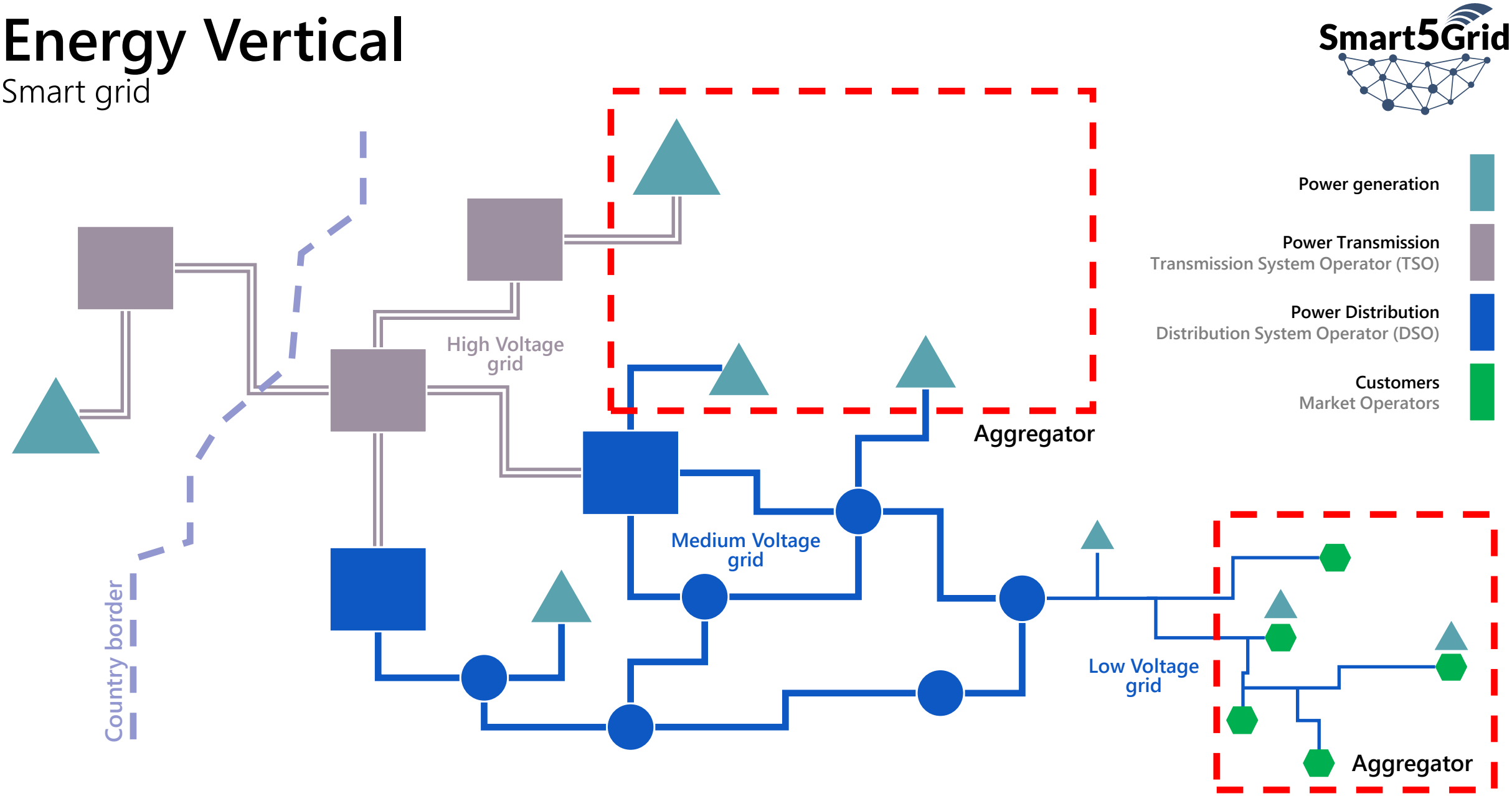


Power Distribution
Distribution System Operator (DSO)

Customers
Market Operators

Energy Vertical

Smart grid



Why 5G?

Advantages and opportunities for the industry

If compared to Optical Fiber

- Lower implementation costs
- Faster implementation
- Higher flexibility

If compared to 4G/LTE

- Lower latency (similar to Optical Fiber)
- Highest stability
- Virtually dedicated bandwidth (Slicing)

Major peculiarities

- Virtual Edge computing, strengthening the system resiliency

What we test in the project

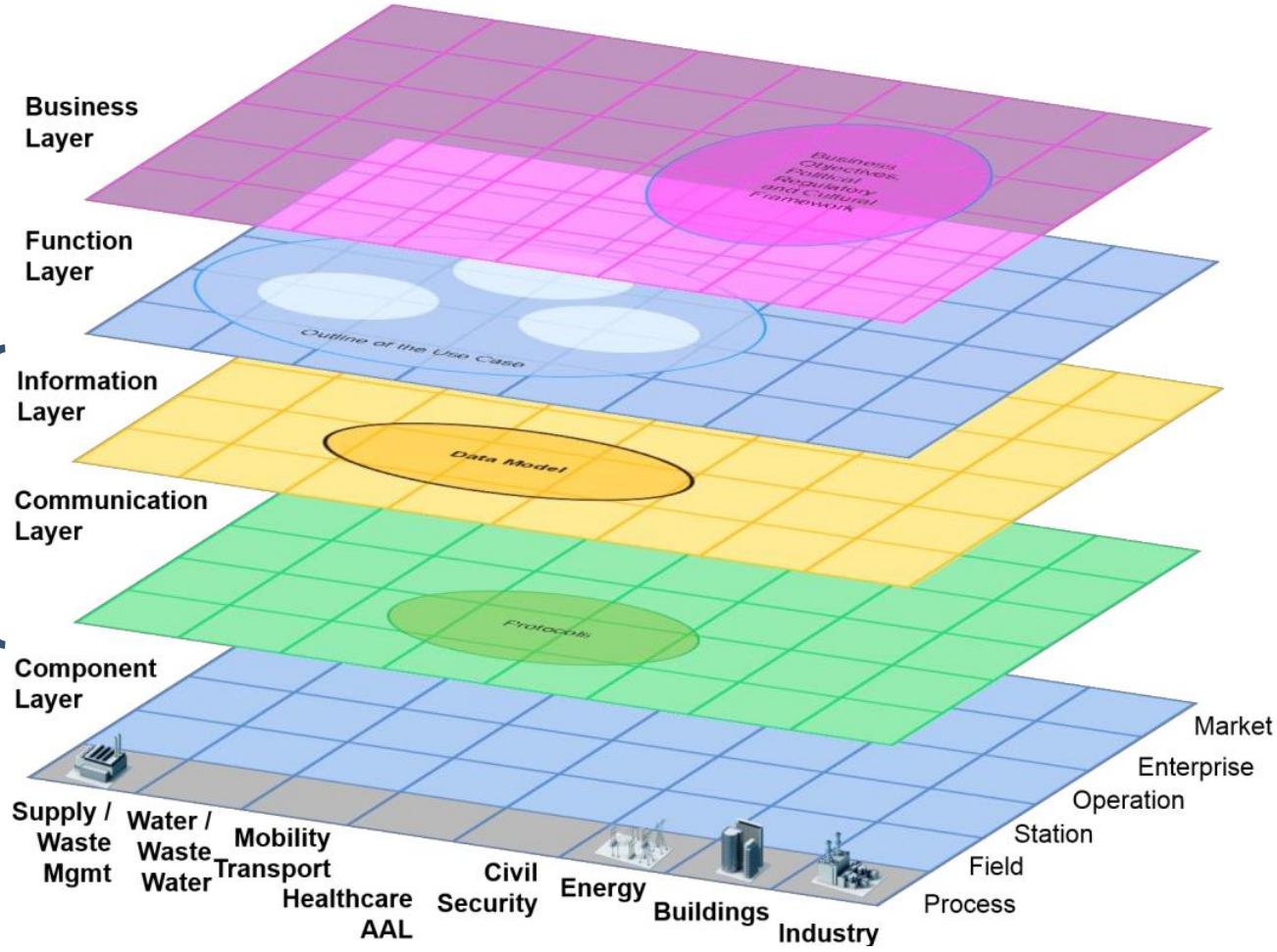
- **NetApp**: an extension of the Network Virtualization Functionality that provides an **abstraction of the 5G complexity** to allow the development of data-network functionalities to a broader group of people. EC aims to create a market segment for NetApps, to support the penetration of 5G technology and foster the digitalization

SGAM

Smart grid architecture model

To successfully cope with the new challenges, all intermediate layers needs to be optimized: in other words, a full digitalization is the key!

Virtualization simplifies the Component layer, offering a more dynamic and flexible approach



Many attacks on energy industry, various methods, serious consequences
(Selection)

DHS published notification that a foreign government conducted a multi-stage intrusion campaign that staged malware, conducted spear phishing, and gained remote access into energy sector networks. **After obtaining access, the foreign government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS).** (2018)

Senior engineers at the Electricity Supply Board in Ireland were sent **phishing emails with malicious software intended to infiltrate control systems and give hackers the power to take out part of the grid** (2017)

Hackers gained access to a telecom network used by transmission operator in the UK and **installed a virtual wire tap to monitor all unencrypted traffic passing through the routers in Northern Ireland and Wales** (2017)

Attackers targeted industrial control systems at three Ukrainian energy companies which **left 225,000 citizens in the dark** (2015)

A second attack on the Ukrainian grid caused another blackout. The attack appears to be a trial run for a much larger attack. The Crash Override malware communicated directly with ICS to turn power off **and shows the attackers ability to automate such attacks in the future.** (2016)

Using locations in Asia, Night Dragon hacked into the applications of oil, gas and petrochemical companies in Kazakhstan, Taiwan, Greece and the United States, thus **acquiring proprietary and confidential business and personnel information** (2011)

Unknown adversaries unleashed coordinated attack on northern California-causing more than **$15M in damages after severing 6 underground lines and firing at substation transformers** (2013)

Dragonfly/Energetic Bear targeted grid operators and electricity-generation firms in several countries, including the Middle East, injecting **malware and Trojan viruses into several industrial control systems** during a cyber espionage campaign (2014)

US utility's **control system network was comprised in an advanced cyber attack via its internet portal**, after hackers brute-forced their way through its simple password mechanism (2014)

US Power Company **Fined $2.7 Million Over Security Flaws** Impacting 'Critical Assets' (2018)

Famous hacker team "Redhack" hacked into power admin system and canceling **~$650K of electricity bills** to be paid to an electricity production company (2014)

State sponsored hackers **infiltrated the critical safety systems** for industrial control units used in nuclear, oil and gas plants, halting operations at least one facility. (2017)

Since 2012, hackers under the name of "Operation Cleaver" have been building their skills to evade detection by security technologies with ease. To date, they have successfully **penetrated and stolen data from 50+ companies** worldwide (2014)

Shamoon virus targeted major energy companies operating in the Middle East, **shutting down 30,000 computers and destroying hard drives and data** at a state-owned energy company (2012). It came back again in a more destructive variant in November 2016 and January 2017.

Programmable logic controllers were targeted by the Stuxnet computer virus, causing 20% of Iran's uranium enrichment **centrifuges to spin out of control** (2010)

Source World Economic Forum, 2019

ENGINEERING

Antonello Corsi

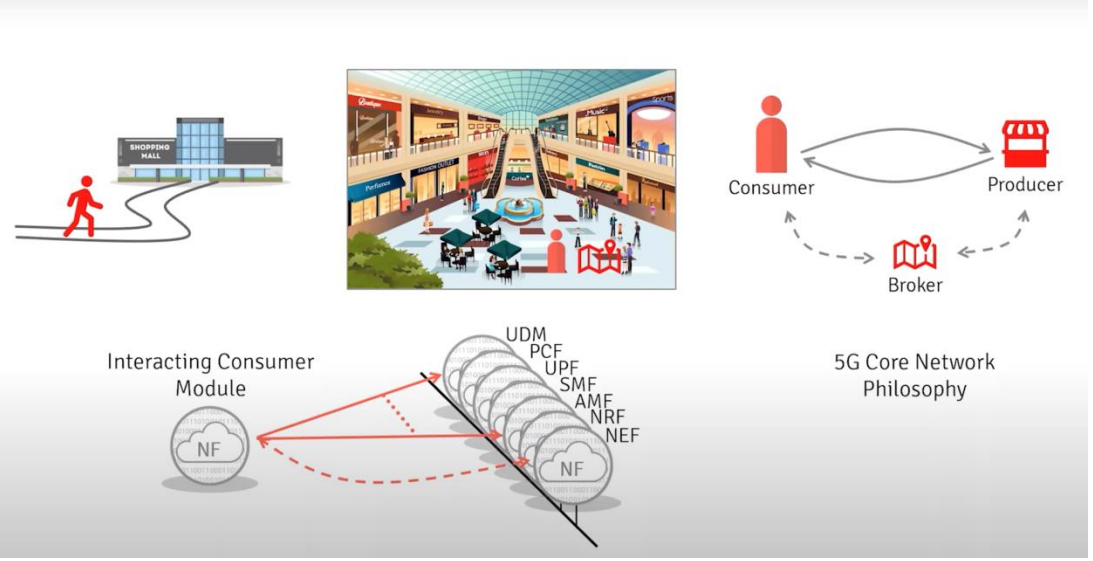
Technical Leader

antonello.corsi@eng.it

NetApp concept for verticals

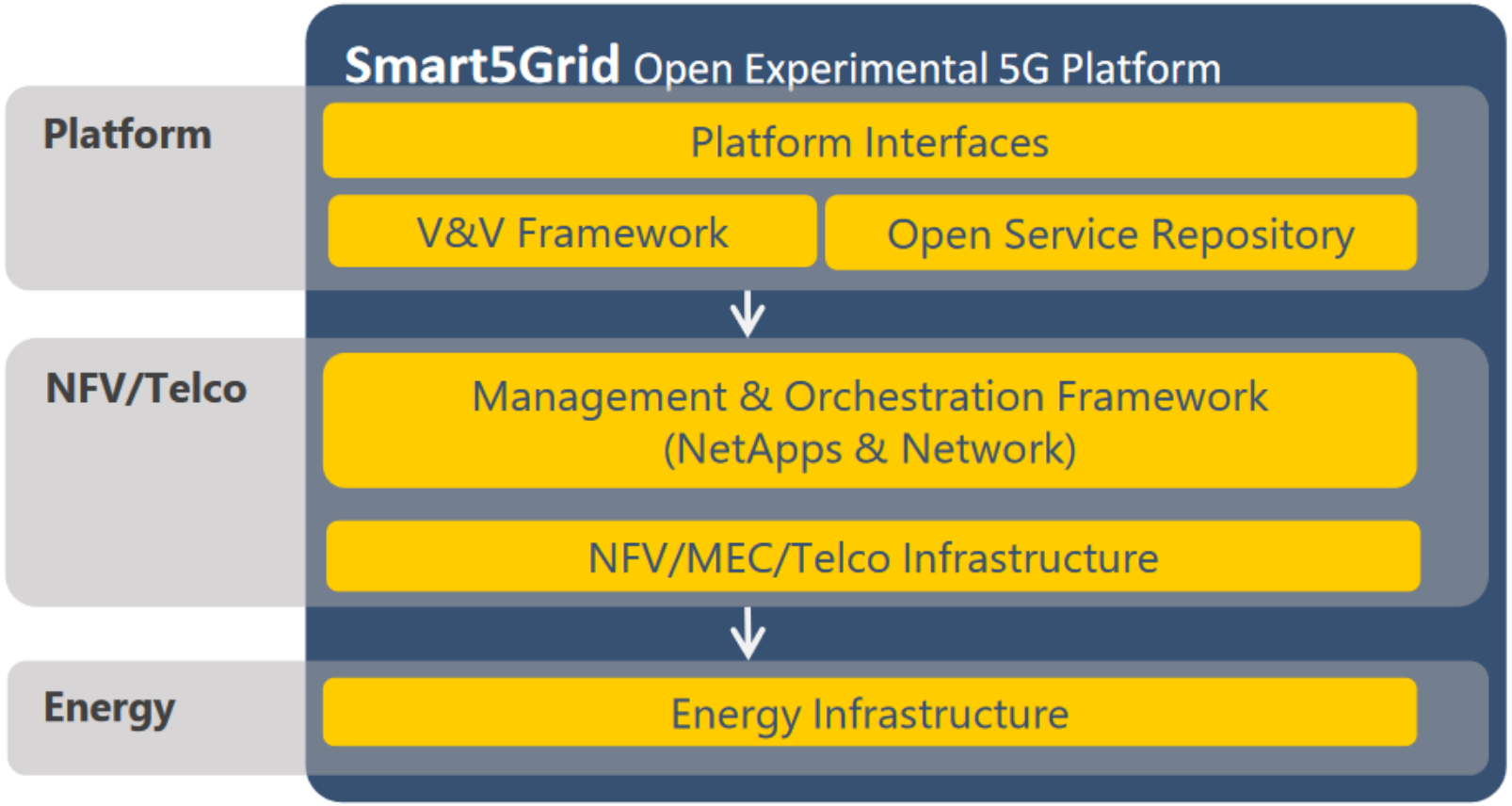
- What is a NetApp ?
  - Specific Challenge: Software networks provide high flexibility through implementation of virtual network functions (VNFs).
  - Chaining of all these functions can create a Network Applications (NetApps) tailored to the requirements of specific tenants, as demonstrated under previous 5G PPP phases.
  - This requires open platforms that provide access to networks resources which can then be used to develop NetApps supporting requirements and developments from specific vertical sectors.

Service Based Architecture



- Extract revenue from network information
- Every Function can be producer or consumer of every function
- NetApp built on top of it exploits this characteristic providing a useful abstraction
- This calls for a transformation of the 5G Core VNFs into a microservices-based model or, more precisely, deconstructing those VNFs into microservices that
  - i) will be deployed on a shared cloud infrastructure
  - ii)will accommodate microservices orchestration tooling
- Such an envisioned service-based core architecture will re-quire several techniques being applied in unison, i.e., Network Functions Virtualization (NFV), Software-Defined Networking (SDN) and service-based interactions facilitated among control-plane functions

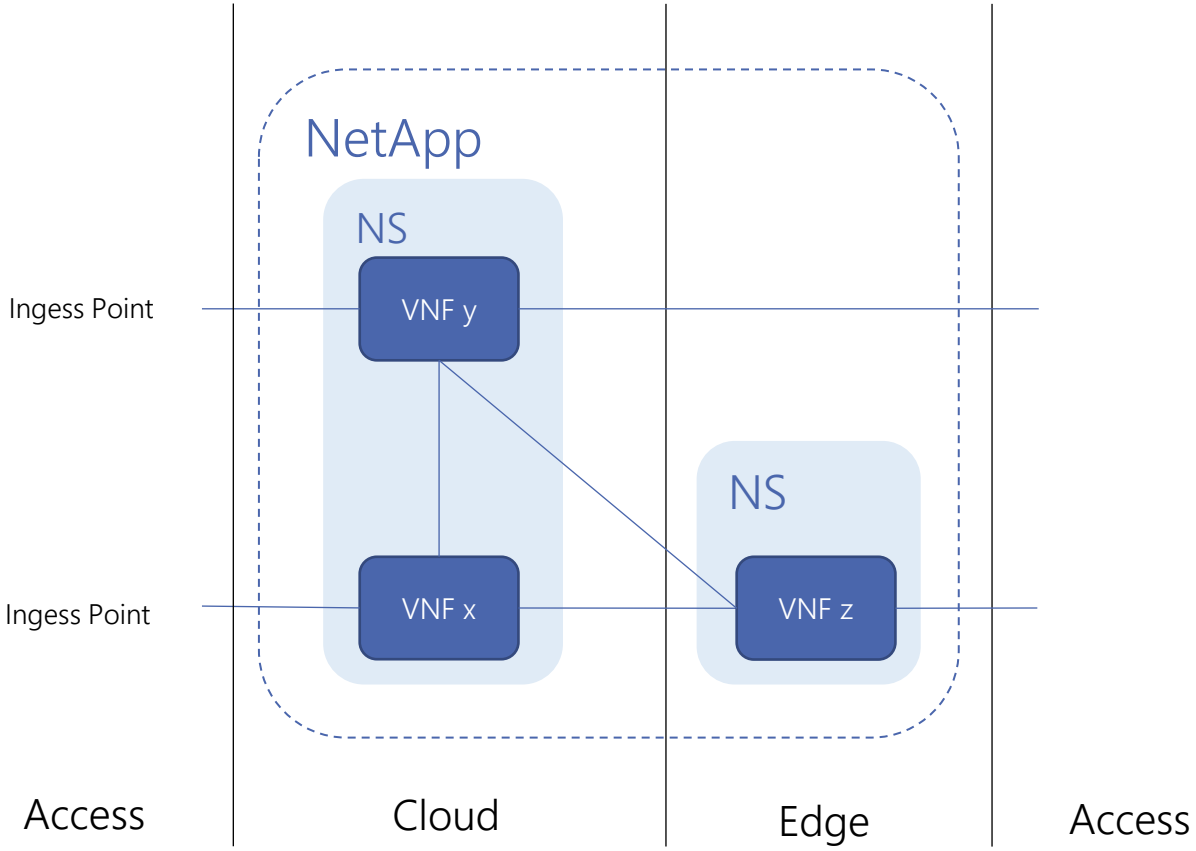
Smart5Grid NetApps



Smart Grid Transition

The **Smart5Grid platform** will embrace DevOps practices and leverage the latest NFV, MEC and Slicing technologies to allow developers to validate 5G enabled **NetApps** specifically designed for energy focused scenarios. The validated NetApps will then be made available on **an Open Service Repository** for discovery, inspection and consumption by 3rd parties.

Smart5Grid NetApps



The Smart5Grid NetApp concept intends to:

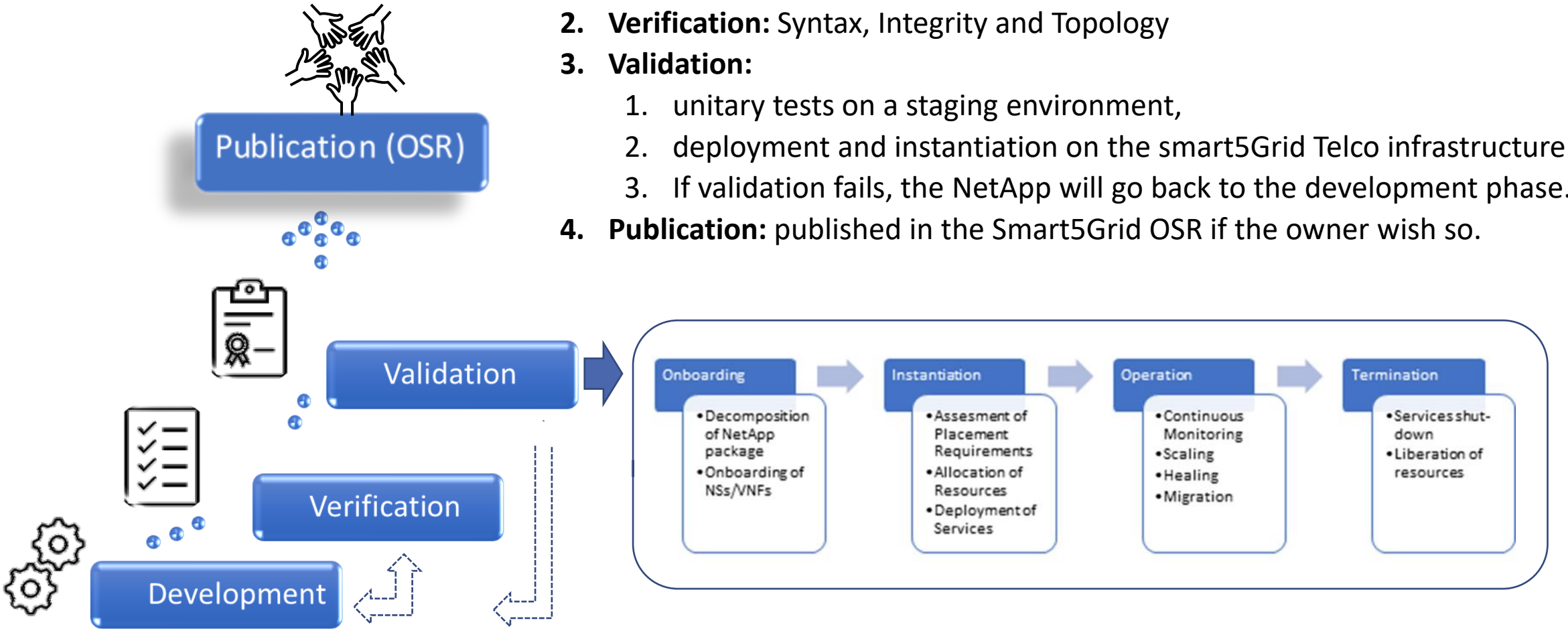
- provide a solution for developers to define vertical applications
- While abstracting the complexities of the network.
- Reducing the level of networking expertise required

cloud-native application made up of VNFs based on containers technology.

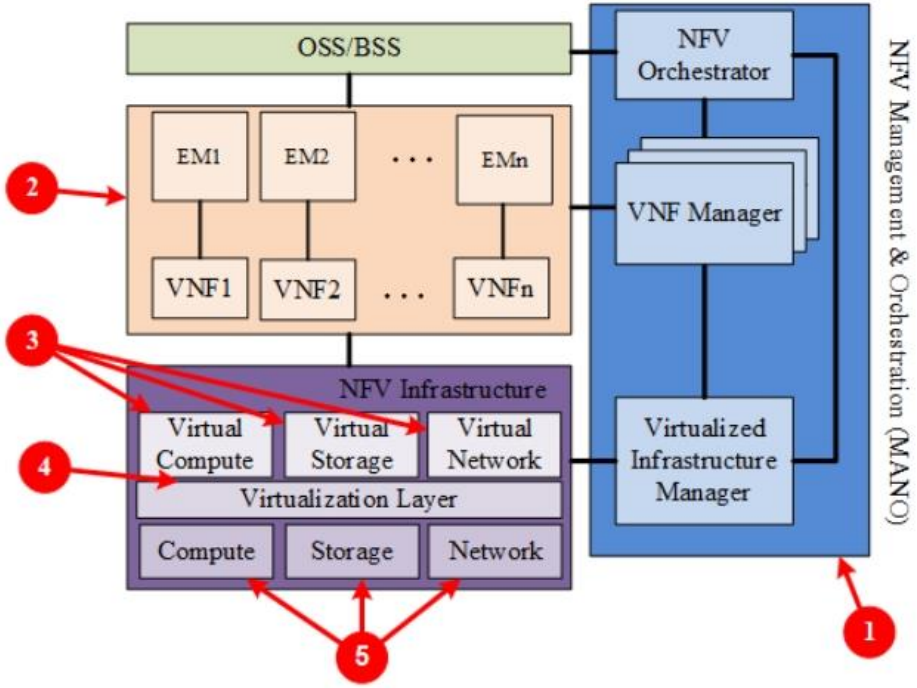
By splitting the functionality of the NetApp into decoupled VNFs, the reutilization of software functions is encouraged, but also, whenever possible from an implementation point of view, the opportunity to take advantage of the cloud/edge infrastructure depending on the application needs.

Smart5Grid NetApps

1. **Development:** according to Smart5Grid NetApp convention
2. **Verification:** Syntax, Integrity and Topology
3. **Validation:**
    1. unitary tests on a staging environment,
    2. deployment and instantiation on the smart5Grid Telco infrastructure.
    3. If validation fails, the NetApp will go back to the development phase.
4. **Publication:** published in the Smart5Grid OSR if the owner wish so.



Attack / weakness to virtualized infrastructure



The figure shows our NFV architecture consisting of four main parts:

i) Cloud networks, each of which is managed by a Virtual Infrastructure Manager (VIM; e.g., OpenStack),

ii) VNF Managers (VNFMs) that are responsible for managing and monitoring a set of VNFs in the same slice during the ir runtime,

iii) a NFV Orchestrator (NFVO) that is responsible for creating, managing and orchestrating all VNF instances indifferent cloud networks and

Cyber attacks to a virtualized infrastructure

- Attacks against VNFs and Network Services in Containers
  - T1.1 Exploit software vulnerabilities and misconfiguration
  - T1.2 Compromise auxiliary network services
  - T1.3 Perform denial-of-services
- Attacks against Container Management
  - T2.1 Compromise credentials
  - T2.2 Bypass authentication and authorization
  - T2.3 Denial-of-service against container management
- Exploiting Access to the Container Management
  - T3.1 Ex-filtrate and manipulate data and sensitive information
  - T3.2 Manipulate configurations
  - T3.3 Abuse of tenant resources
  - T3.4 Inject malicious container images
- Exploiting Access to Containers
  - T4.1 Ex-filtrate sensitive information through side-channel attacks
  - T4.2 Escape container confinement
  - T4.3 Spoofing and eavesdropping on network trafficT4.4Attack internal network services

Smart5Grid

JOIN OUR COMMUNITY

Visit our website:
www.smart5grid.eu

- Webinars, Trainings, Workshops
- Participation and use of the NetApp Experimentation Facility

Smart5Grid

Demonstration of **5G** solutions for **SMART** energy **GRID**s of the future

GENERAL INFORMATION

THE CONSORTIUM

24 EUROPEAN PARTNERS COVERING 7 EU STATES

DURATION

3 YEARS

TOTAL BUDGET

8M€

Consortium Composition

24 partners, 4 Linked Third-parties, 13 SMEs

Smart5Grid

Coordinator

enel

TELCOs

WINDTRE

OTE GROUP OF COMPANIES

VIVACOM

Tech Companies

ENGINEERING

Atos

gridspertise
accelerating your electric future

Universities/Research institutions

i2cat

HELLENIC REPUBLIC
National and Kapodistrian University of Athens
EST. 1837

University of Cyprus
ΚΟΙΟΣ

DSOs

e-distribuzione
e-distribución

TSOs

ECO ЕАД

ադμηε

SMEs

EIGHTBELLS
Independent Research & Consultancy

INFOLYSIS

SC

NEARBY COMPUTING

axon logic

ubiwhere
SUITING THE FUTURE

athonet

SETECHCO

SIDROCO

ENTRA ENERGY

UBITECH
digitizing energy

nosia
- SEÑALIZACIÓN INDUSTRIAL
- EQUIPAMIENTO PARA LA INDUSTRIA

STAM
MASTERING EXCELLENCE

(Linked third-parties of Enel Grids)

Follow us!

Check out our channels

Smart5Grid

smart5grid.eu

Thank you!

Daniele Porcu
Project Coordinator
daniele.porcu@enel.com

Antonello Corsi
Technical Leader
antonello.corsi@eng.it