LINKSFOUNDATION.COM

FONDAZIONE links
PASSION FOR INNOVATION

Use of authenticated Galileo signals for the synchronization of telecom networks

The H2020 ROOT project

MARCO PINI | HEAD OF SPACE AND NAVIGATION TECHNOLOGIES AREA

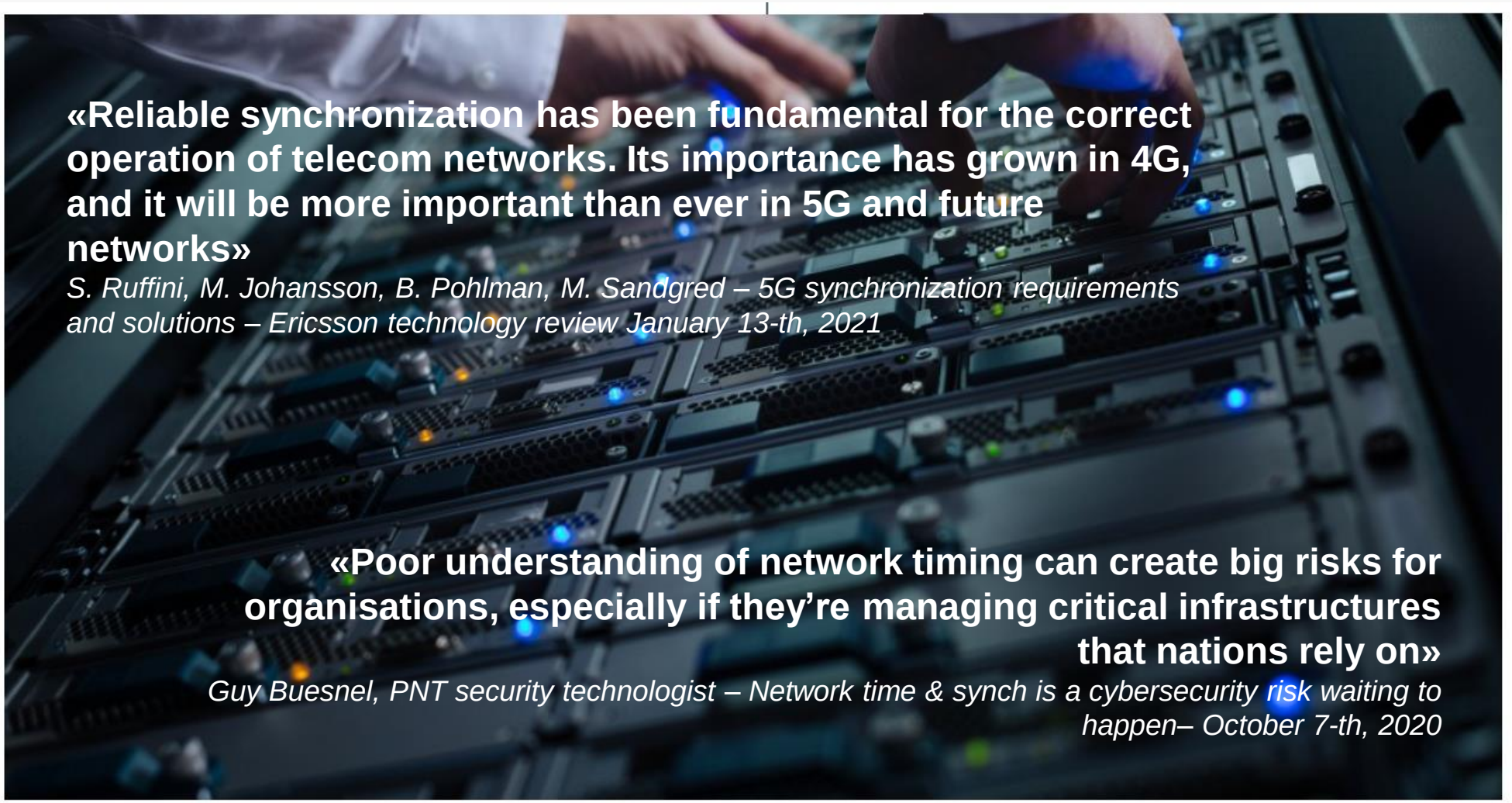
RNN WEBINAR, 11/05/2021

Outline

- **Background** — Technological trends and new GNSS signals
- **ROOT** — Motivation, Consortium, objectives and results of first 2 quarters
- **Perspectives** — Planned work and milestones

Background

Synchronization in telecom networks



«Reliable synchronization has been fundamental for the correct operation of telecom networks. Its importance has grown in 4G, and it will be more important than ever in 5G and future networks»

S. Ruffini, M. Johansson, B. Pohlman, M. Sandgred – 5G synchronization requirements and solutions – Ericsson technology review January 13-th, 2021

«Poor understanding of network timing can create big risks for organisations, especially if they're managing critical infrastructures that nations rely on»

Guy Buesnel, PNT security technologist – Network time & synch is a cybersecurity risk waiting to happen– October 7-th, 2020

Background

Technological trends

Satellites dependency

Telecommunications is a sector where GNSS plays a key role. GNSS is a timing source, defined as «*backbone of the connected world*» and also the «*invisible utility*»

5G

5G networks pose new challenges to the **management of multiple timing sources across the network**. To realize the benefits of 5G, highly accurate time synchronization is needed almost everywhere in the network. There is also a need for increasing reliability in the timing source

Intentional attacks

The risk associated to the unavailability of GNSS also includes the **growing cyber threats** (no longer a research curiosity) and the potential domino effects, even if users continue to consider GNSS a pure, non-critical, commodity

New countermeasures

New receiver-based countermeasures and best practices for increasing operations resilience. Authenticated civilian GNSS signals: Open Service Navigation Message Authentication (OSNMA)

Background

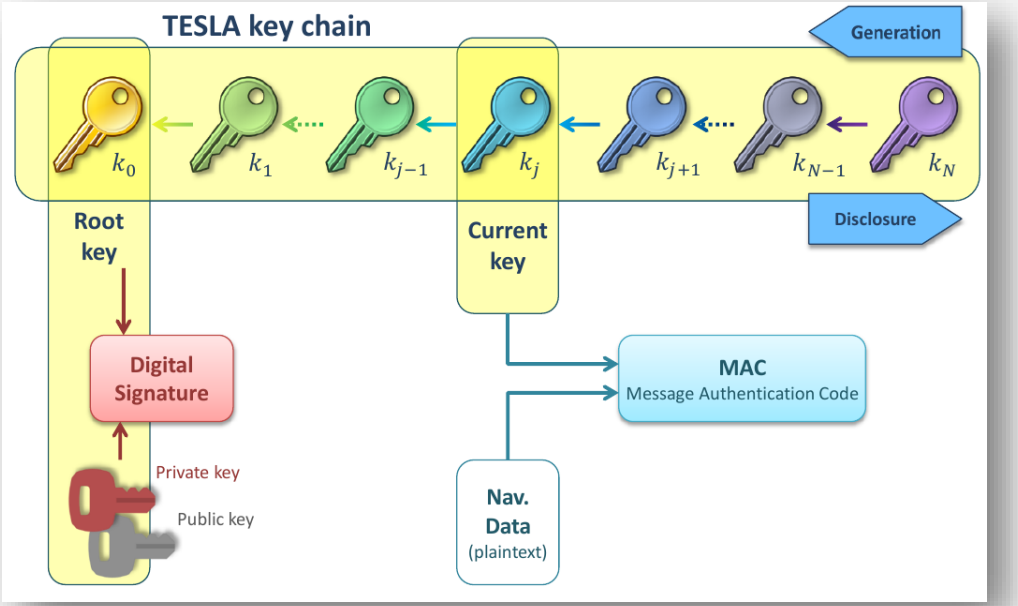
The OSNMA signal

> *Galileo has started testing Open Service Navigation Message Authentication (OSNMA) in the signal-in-space, allowing the first-ever OSNMA-protected position fix to be successfully computed. This is the first-ever transmission of authentication features in open GNSS signals of a global navigation system"*
>
> 11th of February 2021 - https://www.gsa.europa.eu/newsroom/news/tests-galileo-osnma-underway

Based on the **Timed Efficient Stream Loss-tolerant Authentication (TESLA)** protocol, including the transmission of:

1. a **Message Authentication Code (MAC)**, to authenticate the navigation message

2. the delayed **key** to compute the MAC:
   a) the key belongs to a **chain of keys**
   b) the chain starts with a random secret key k_N, and ends with a **public root key** k_0, certified as authentic, before starting the authentication verification.



Why this project ?

Main motivation behind our proposal

1. Is OSNMA enhancing the protection of GNSS receivers used as timing source in telecom networks (and in general in all networks timing dependent upon GNSS) ?

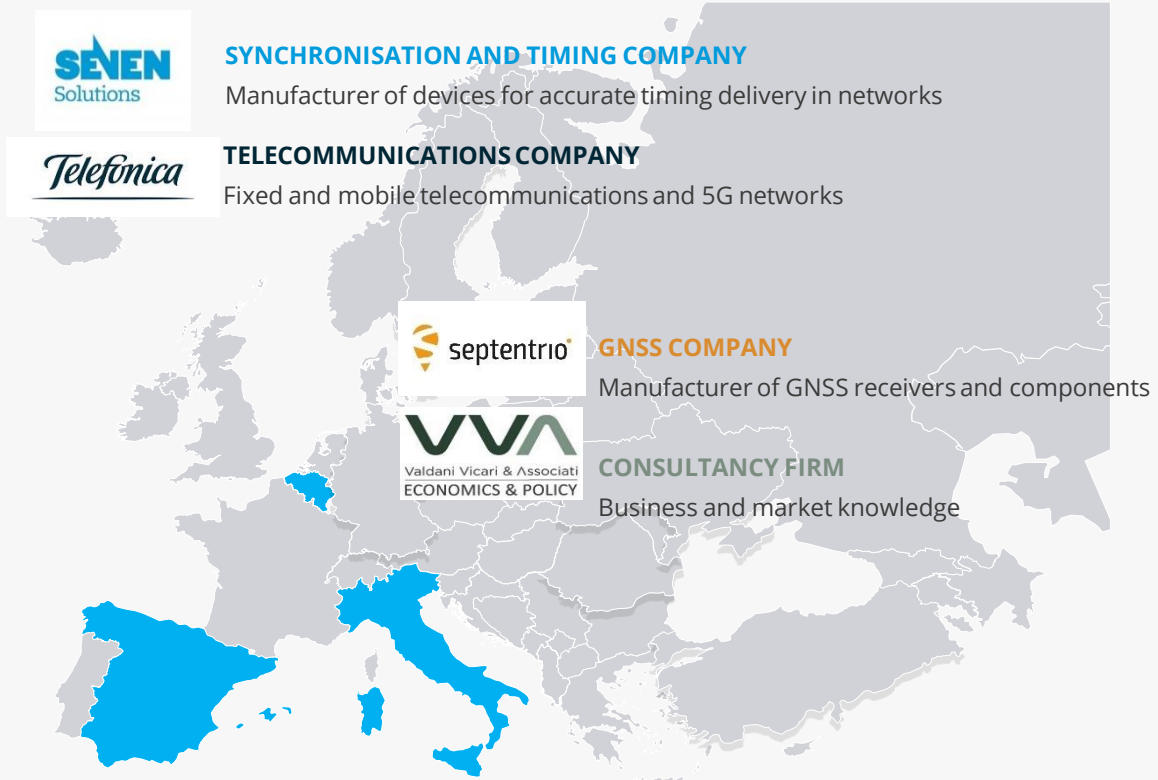
ROOT: Rolling Out OSNMA for the secure synchronization of Telecom networks

2. Can we assess the benefits (limits) of the OSNMA for networks synchronization in a real operational context ?

= *no further desk analysis, but experimental assessments….*

ROOT in a nutshell

A team of experts covering the whole value chain



SYNCHRONISATION AND TIMING COMPANY
Manufacturer of devices for accurate timing delivery in networks

TELECOMMUNICATIONS COMPANY
Fixed and mobile telecommunications and 5G networks

GNSS COMPANY
Manufacturer of GNSS receivers and components

CONSULTANCY FIRM
Business and market knowledge

RESEARCH CENTRE
Applied research in GNSS, cyber security and networking
Coordinator

ENGINEERING UNIVERSITY
Research in GNSS, telecommunications and cyber security

18 months
KO: November 2020 | End: April 2022

1.3 MEuro total budget
EU funds equal to 1.06 MEuro

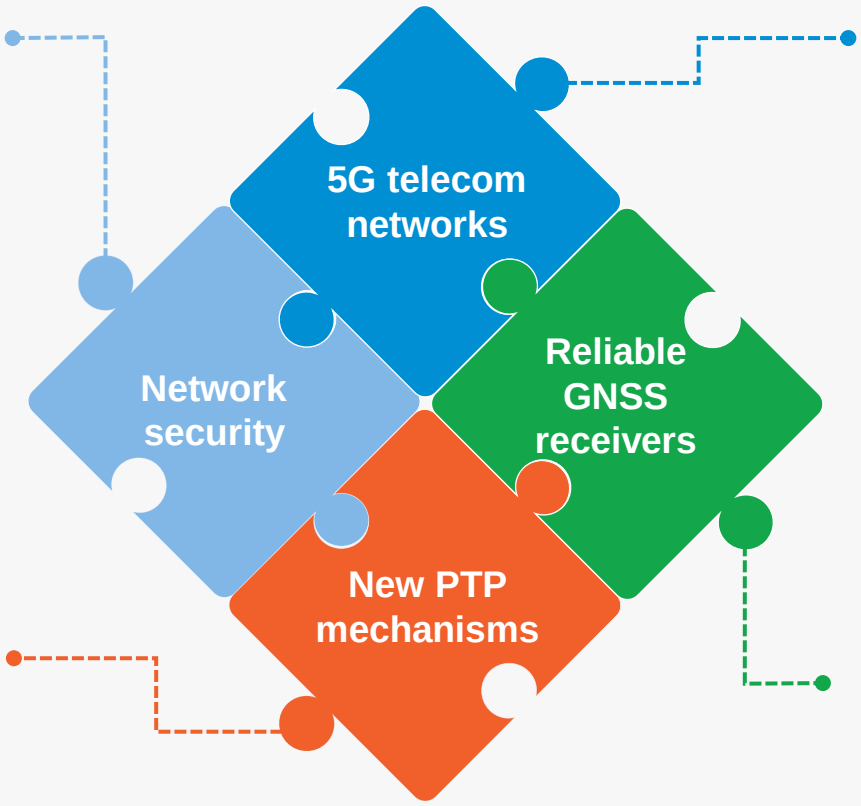
24% on experimental tests
An entire WP dedicated to experimental tests, using live signals. WP overlaps with Public Test Phase

3 members of Advisory Board
1. Joint Research Centre of the EC
2. European Union Agency for Cybersecurity (ENISA)
3. Italy's national metrology institute

A mix of emerging technologies

Progress beyond the state state of the art

- **Integrity check and remote attestation** of the software running on network devices
- Secure network communication



- LTE-A, LTE-TDD and 5G introduce new stringent requirements and phase synch (e.g.: 65 to 260 ns)
- Evolution to phase-synch is done via **Distributed Grandmaster Clocks** (D-GMC)

- Resilient architectures for long-distance accurate time distribution (e.g.: WR-PTP)
- **Autonomous switch** between different GNSS time source

- From GPS-only, single-frequency receivers to high-end GNSS, multi-constellation, multi-frequency receivers
- Featuring **anti-jam and anti-spoofing mechanisms**

ROOT objectives

01

Reference 5G architecture

Increase the resilience of telecom networks, proposing enhanced synchronization architectures for 5G networks

02

RF interference countermeasures

Assess performance of new multi-frequency Galileo receivers, OSNMA enabled, to monitor intentional interference

03

Prevent network cyberattacks

Experimentally assess secure solutions able to mitigate specific cyberattacks to the distribution of time synch over the network

04

Experimental test campaign

Quantify improvements introduced by reliable synch mechanisms built upon the combination of OSNMA and secure network synch distribution

05

Business perspectives

Launch a successful market entry of the ROOT solution

06

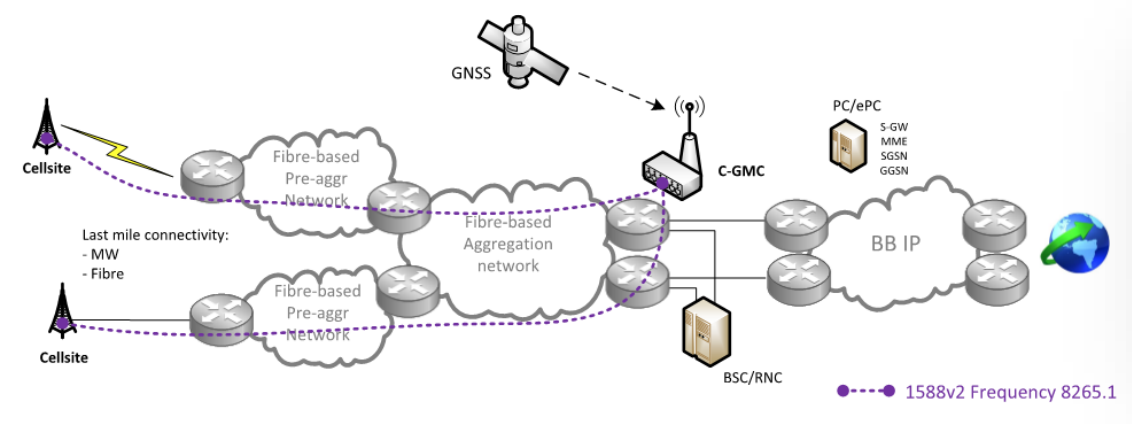
Increase awareness

Foster the introduction of Galileo OSNMA for the synchronization of the next generation of telecommunication networks

Synch implementation

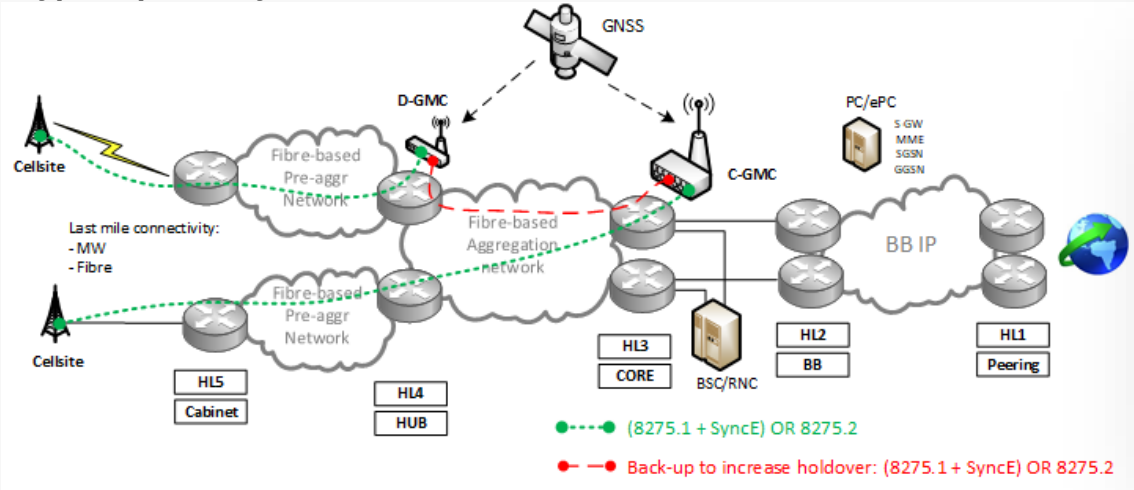
Objective 01

Typical frequency synchronization distribution in 2G/3G networks



- Frequency synchronization provided by the Centralized Grandmaster clock
- C-GMC combined with GNSS becomes a Primary Time Reference Clock (PTCM)

Typical phase synchronization distribution with enhanced holdover

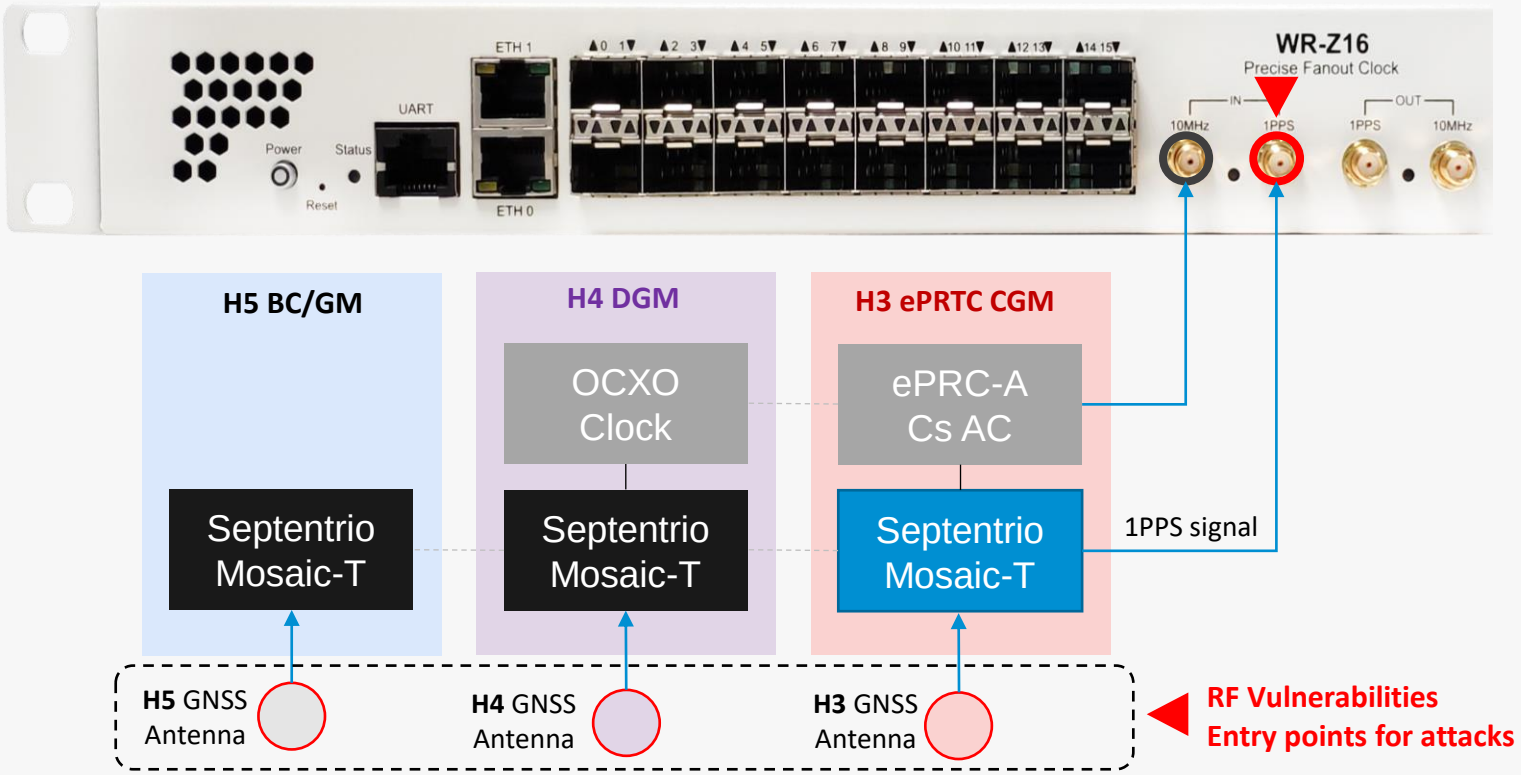


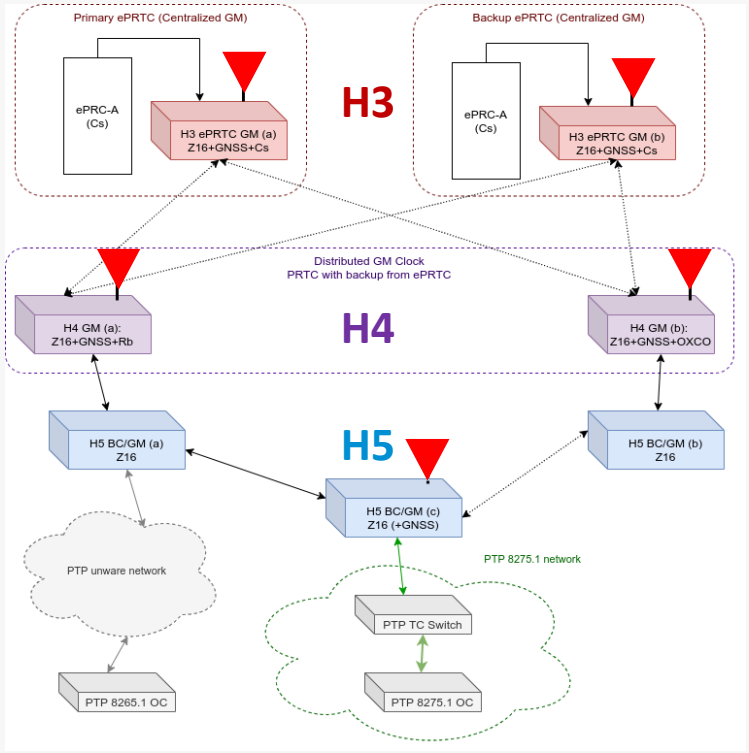
- LTE-A, LTE-TDD and 5G requires phase synch
- Evolution to phase synch support is done via **Distributed GMC (D-GMC)** → clock densification
- Points of vulnerabilities to jam and spoofing

I. De Francesca (Telefonica) @ ESA NAVISP thematic open calls «PNT in 5G», 21/10/2020

ROOT Reference Architecture

Objective 01





The team identified a “reference” architecture, representative of **3 hierarchical levels** of operational networks

It will be the basis for the system set up during the experimental campaign. It will be installed at Telefonica labs (Madrid)

Conclusions

Next steps toward the experimental phase

- Reliable synchronization of networks is more and more important, considering the evolutions requiring multiple clocks
- ROOT is an initiatives that wants to use/assess live authenticated GNSS signals in an operational context
- ROOT already identified a reference architecture that:
  - Is used to define the test plan, considering the RF/cyber interfering attacks selected
  - Will be set up at Telefonica premises and used for the experimental analysis
- In parallel ROOT:
  - Performs business/market analysis for introducing the ROOT solution in the market
  - Works on dissemination activities, trying to engage relevant stakeholders and increase the level of awarness on networks (critical infrastructure) vulnerabilities and protections provided by new SIS and technologies

https://www.gnss-root.eu/

FONDAZIONE links

PASSION FOR INNOVATION

Thank you for your attention.

Questions?

FONDAZIONE links

PASSION FOR INNOVATION

CONTACTS

Marco Pini

Head of Space and Navigation Technologies Research Area

p. +39 011 2276 436

e. marco.pini@linksfoundation.com

FONDAZIONE LINKS

Via Pier Carlo Boggio 61 | 10138 Torino

P. +39 011 22 76 150

LINKSFOUNDATION.COM