Need for AI/ML based Timing solutions for Cloud based Telco RAN deployements

WSTS 2023, March 13th – 16th, Vancouver, Canada.

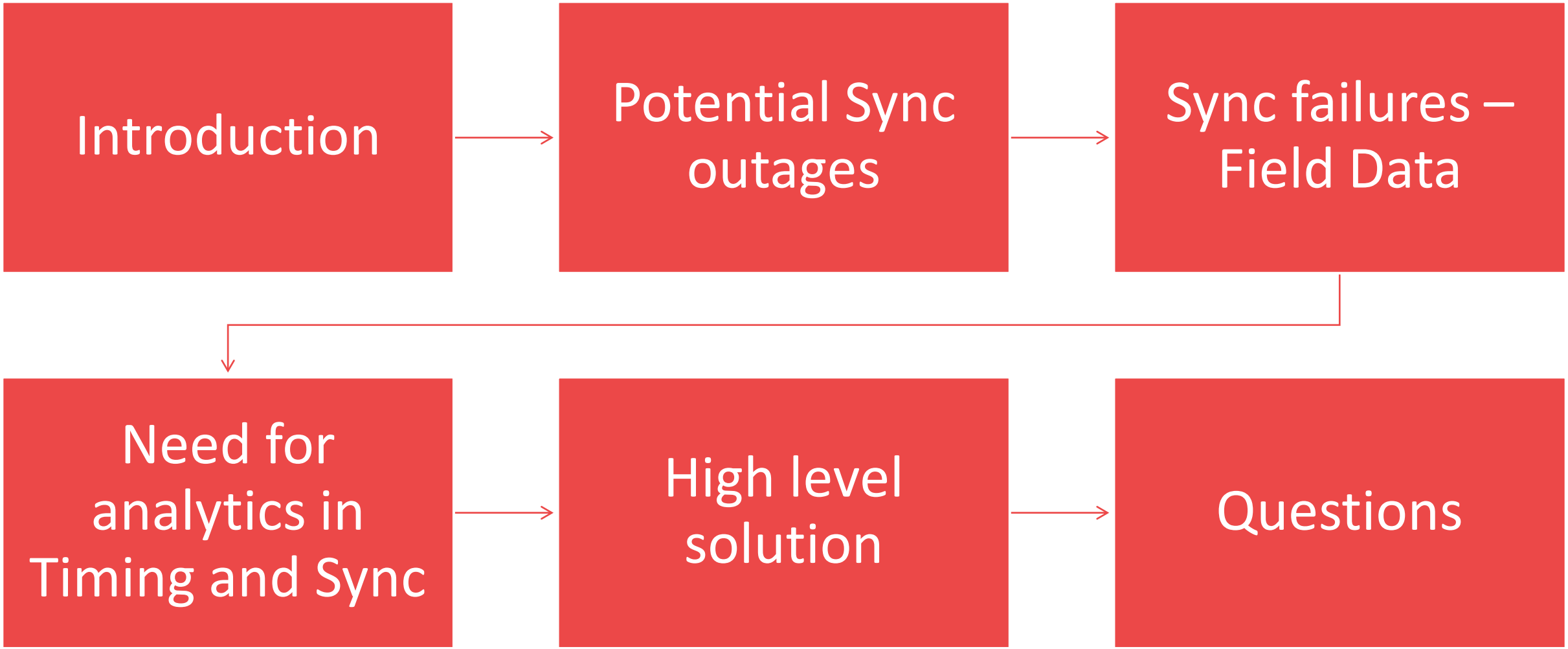
M. Ramana Reddy,

Director – Timing & Sync Platform

Rakuten Symphony, Rakuten Group Inc.

Rakuten Symphony

Agenda


Introduction
Potential Sync outages
Sync failures – Field Data
Need for analytics in Timing and Sync
High level solution
Questions

Introduction

PRTC sync source(w/ GNSS) is considered as primary sync source in most of the FH and MH networks of O-RAN/C-RAN.

GNSS Security threats and/or outages.

Impacts of GNSS failures on the cell/sector KPIs varies based on the deployment type.

Cloud based deployements needs accurate monitoring(reactions and corrections).

Need for central, intelligent and real-time monitoring to improve timing KPIs/cell availability using AI/ML.

Potential Sync outages

GNSS outages/failures.

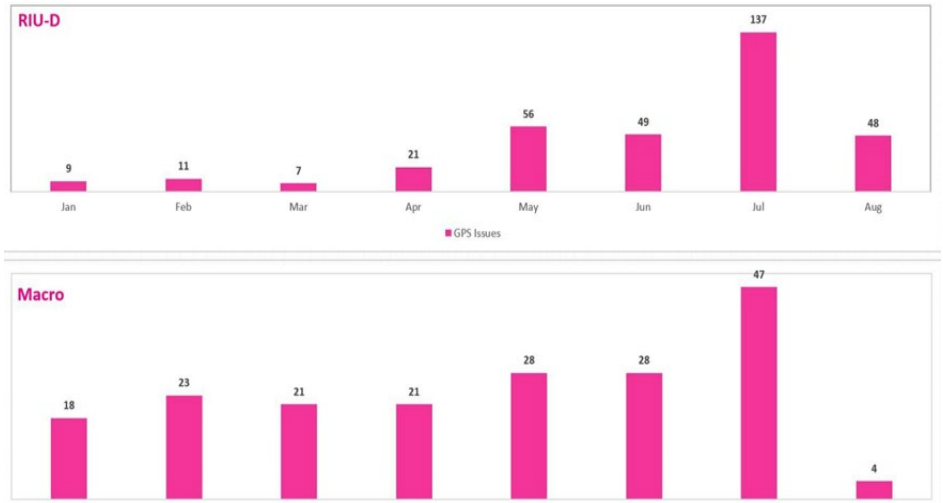
GNSS Signal jamming/interference
GNSS Signal Spoofing:
Signal blockages, multipath errors.
Ionospheric effects/geographical issues.
HW/Cable faults
Bad weather conditions.

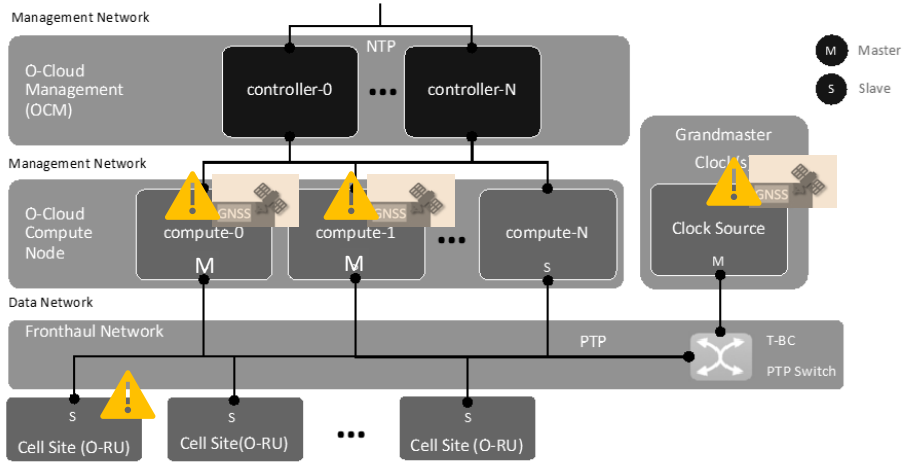
Leap Second warnings.

PTP and/or SyncE packet drops, Clock class/quality degradations etc..

Sync Failure(s):Field Data

- **July 2022 – Sep. 2022**: More than **1K GNSS holdovers** happened in the RMI network, more than **100 GPS failures** was reported.
- **Failure reason include:** GNSS receiver HW failure, cable, jamming, interference, signal blockage, weather condition, PTP packet drops etc.
- Maintaining clock stability during GPS failure completely reply on auto holdover technologies - OCXO or PTP/SyncE backup. **Network operation** and **KPI** may be **seriously impacted** before holdover mode switching is triggered.
- RMI has only **8 hours overnight** to respond and fix the GPS issue before the holdover period expires which is **very risky**.
- Trouble shooting GPS failure issues remotely or in the field consumes a lot of **engineering time/resource** and becomes more concerned as the RMI network scales further up.



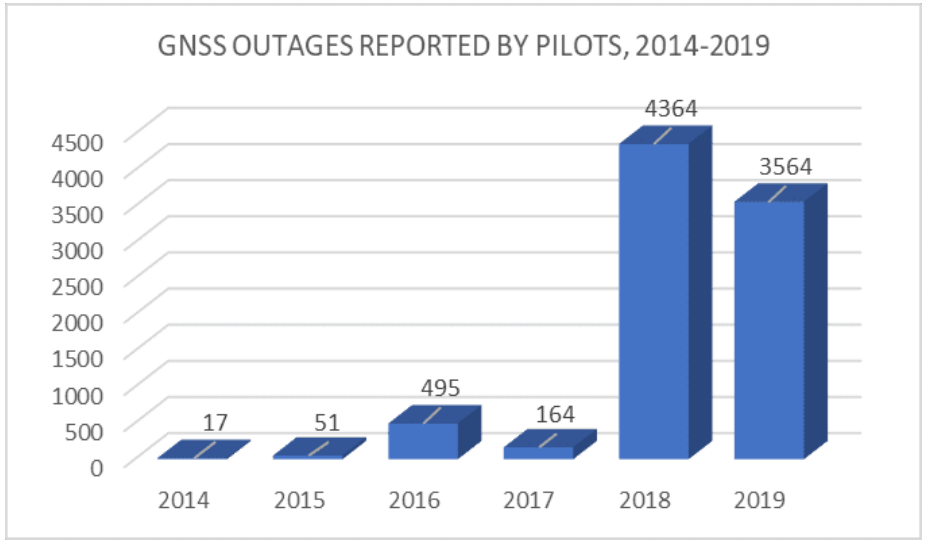


GNSS Security Threat Concerns

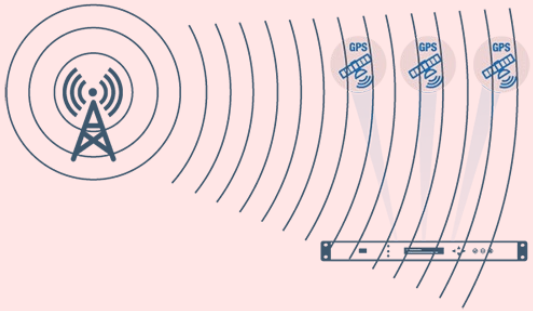
Cellular (4G/5G/6G) networks provide vital infrastructure for business, mission and society-critical applications -> national security concern

- July 2020 - June 2021, the telecom industry was the most targeted (40% attacks VS 10% for the next-highest industry vertical)

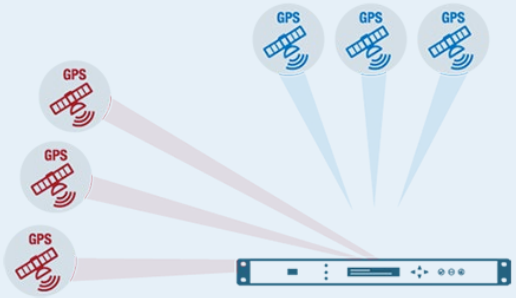
- GPS security threat is rising fast
  - solar activity,
  - man-made interference (jamming)
  - malicious faking of GPS signals (spoofing)
  - manipulation of position and timing information



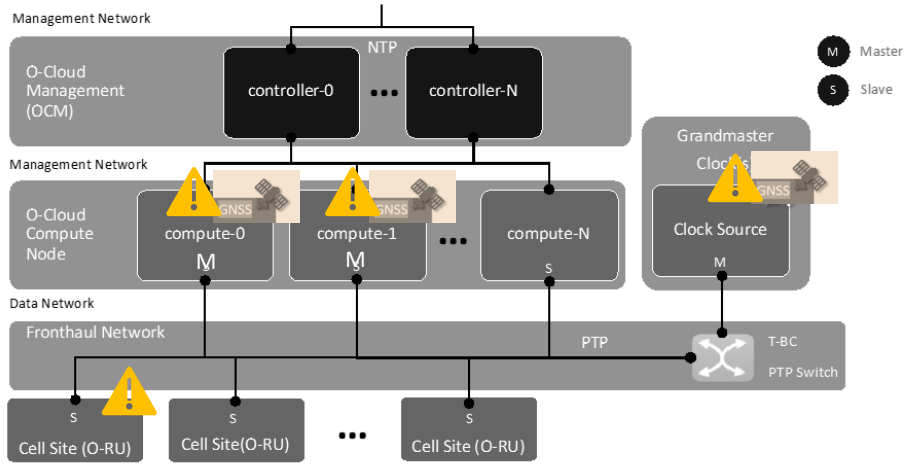
Source: EUROCONTROL EVAIR



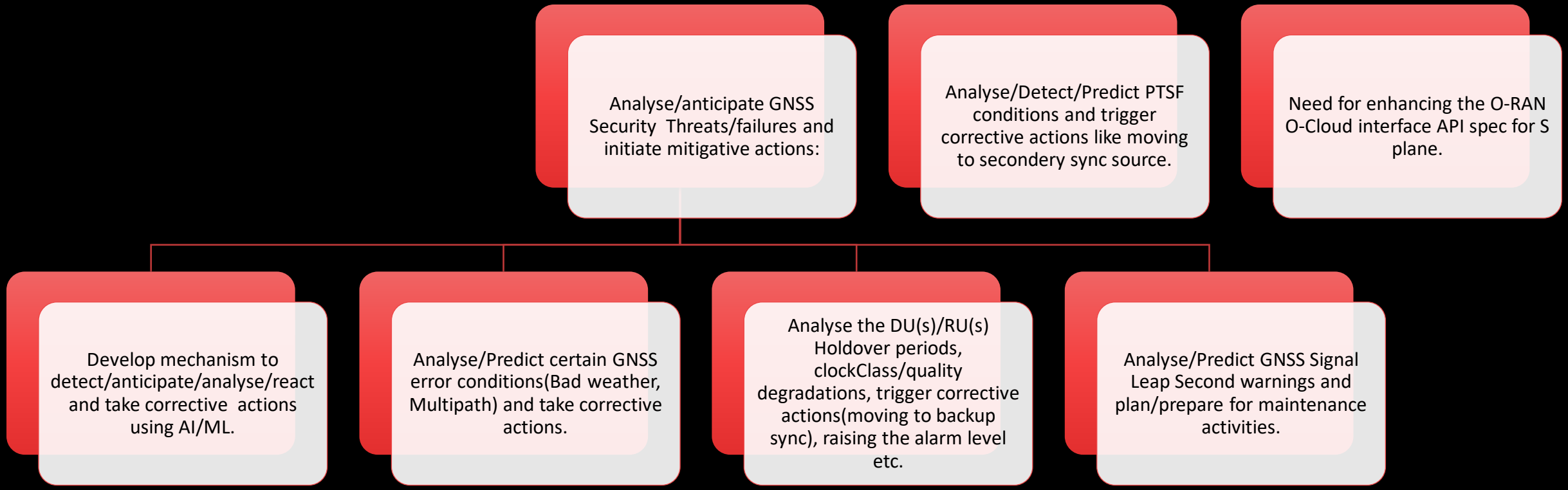
GNSS Jamming: Jamming creates noise which prevents GNSS receivers from locking on to authentic GNSS satellites.



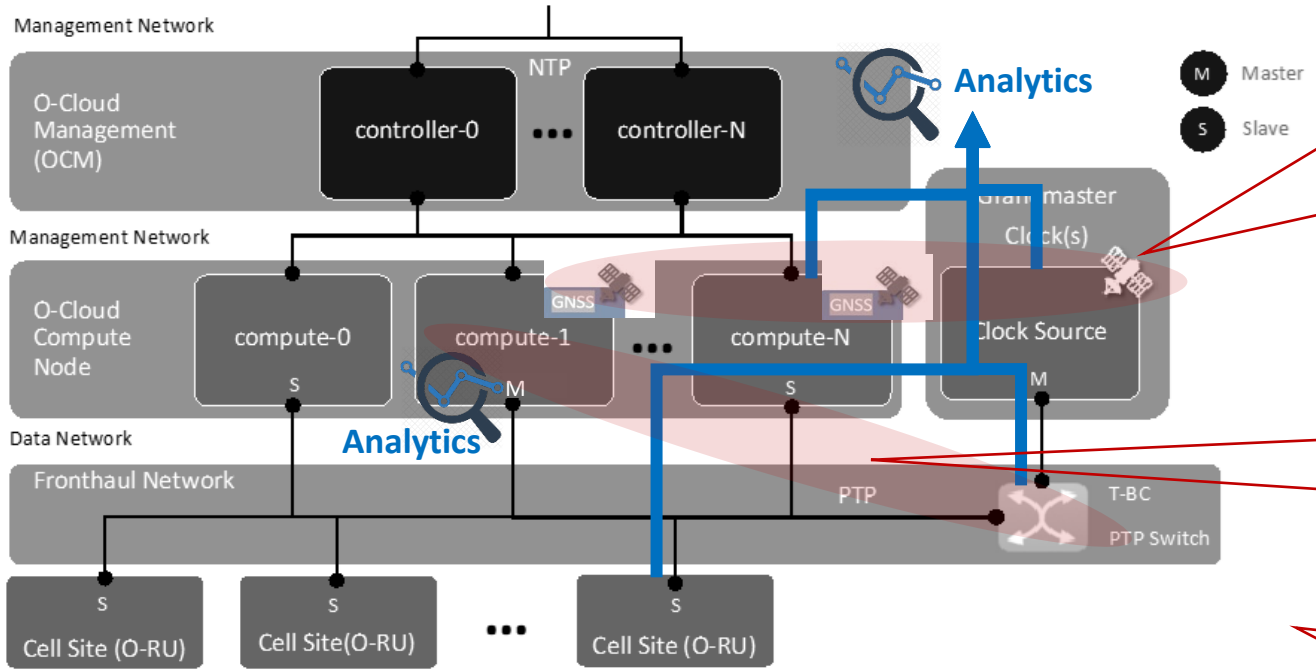
GNSS Spoofing Spoofing mimics authentic GNSS satellites to hijack GNSS receiver tracking loops



Need for analytics in Timing



High-Level Solution



Analyze and predict **GNSS failures** and initiate **mitigative actions**

- GNSS Signal jamming, spoofing, interference, security threat (1st priority)
- Signal blockages/multipath errors (due to tree canopies in rural areas/urban large glass structures)
- Ionospheric effects/geographical issues
- HW faults connecting GNSS receivers
- Bad weather conditions

Deployment: **Local DU algorithm**(1st priority) or **cloud-based analytic services**

Analyze and detect **PTP pkt drops** or **PTP clock quality** degradations and trigger switchover to secondary sync source.

- PTP packet drops/PTP clock quality degradations/PTP clock advertisements
- SyncE clock quality degradations

All of these mechanisms need KPIs to be reported over **O-Cloud Interface (O2)** and bring in necessary contributions to **WG6 O-Cloud API spec** for S plane.

Rakuten Symphony

Questions?

Ramana Reddy
ramana.machireddy@rakuten.com


Rakuten