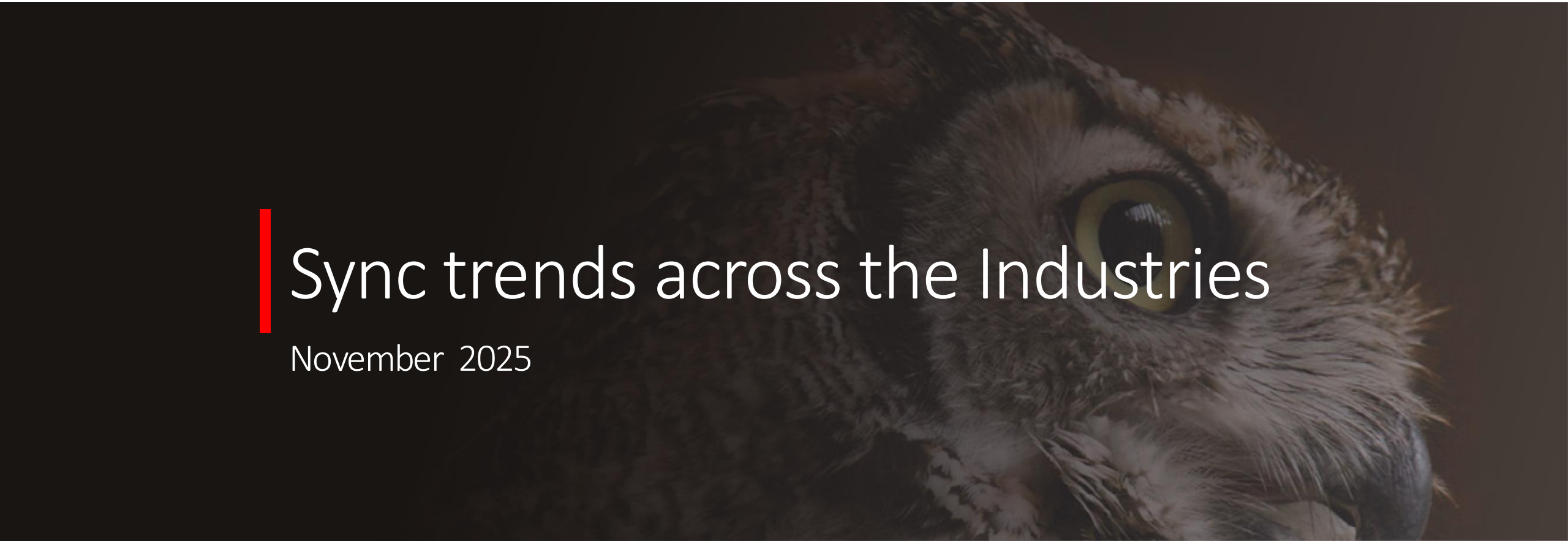


Sync trends across the Industries

November 2025

calnexsol.com

Stefano Ruffini

Strategic Technology Manager, Calnex

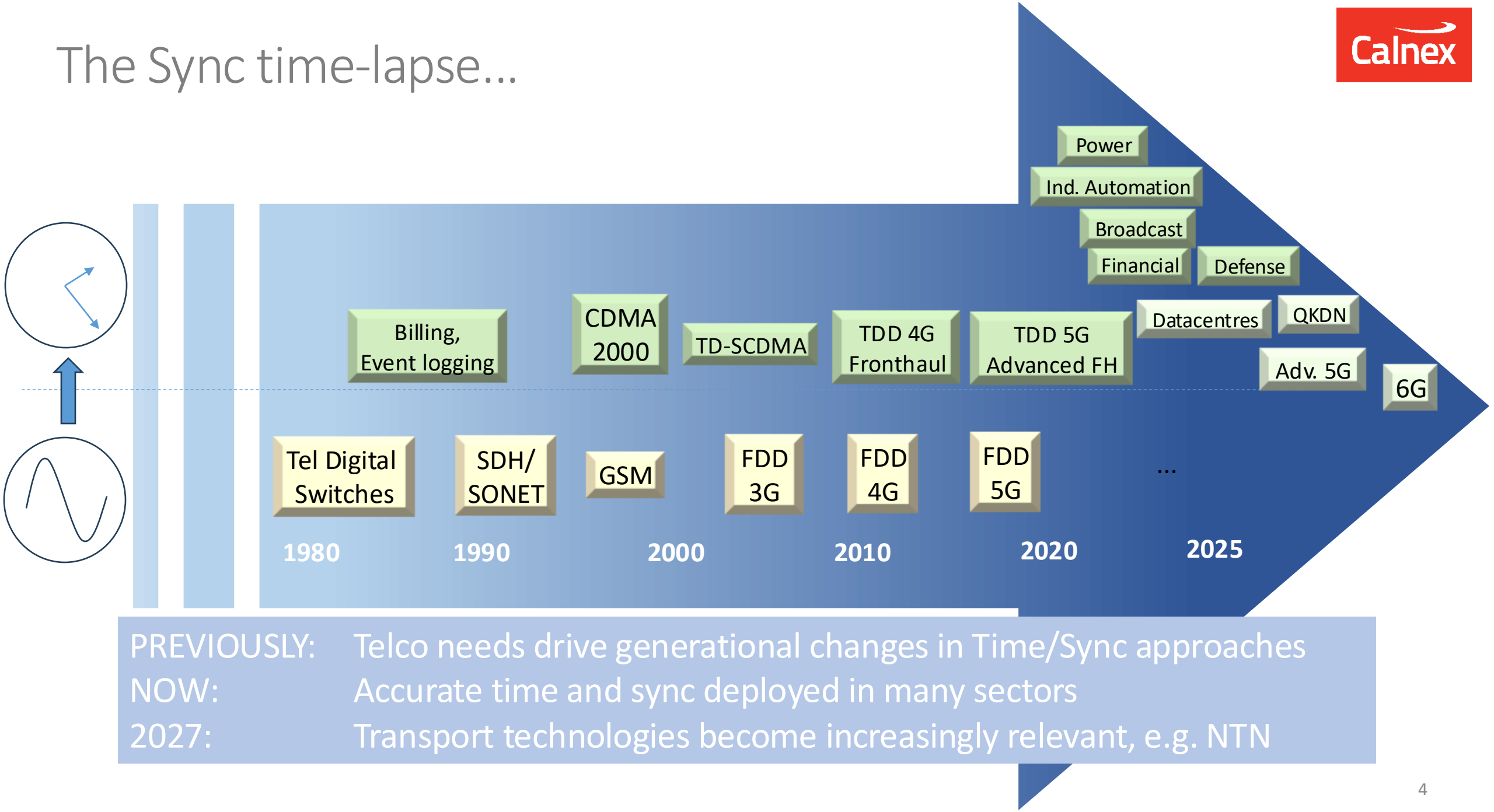
Summary

- Increasing Time/Sync Deployments
- Focus on subsystems
- Resilience is non-negotiable
- Towards 6G

- *Conclusions*

Time and Sync are deployed deeper and wider

The Sync time-lapse…

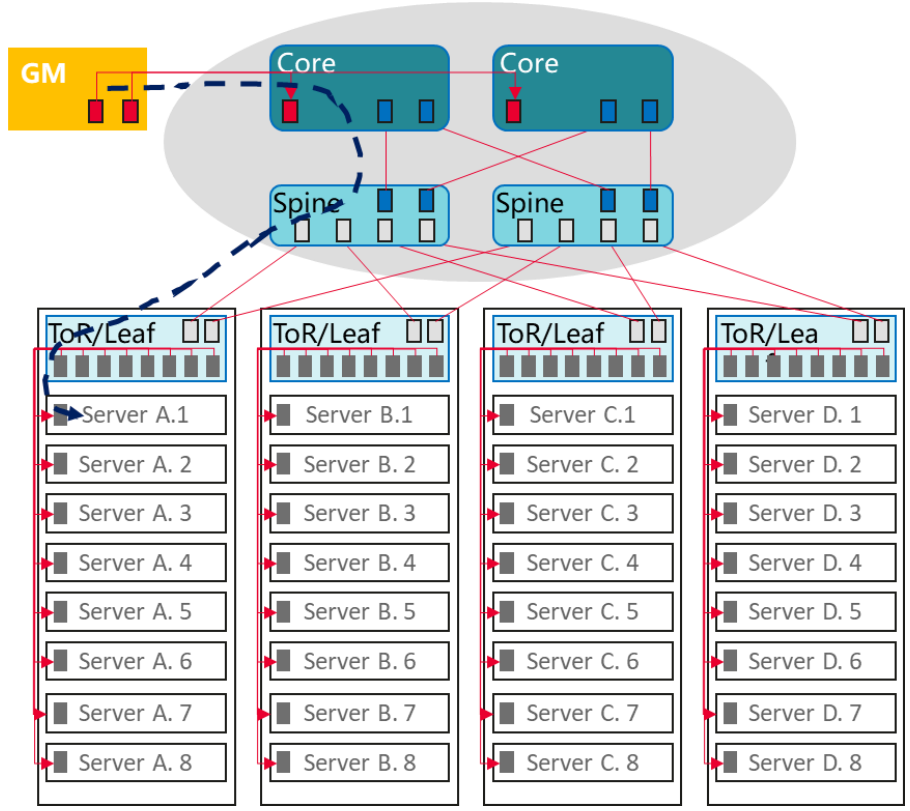


PREVIOUSLY: Telco needs drive generational changes in Time/Sync approaches
NOW: Accurate time and sync deployed in many sectors
2027: Transport technologies become increasingly relevant, e.g. NTN

Synchronization in data centres

Enhanced Sync enables:

- Consistent operation between distributed data centres, minimizing latency.
- Event logging; Diagnosis and analysis of problems
- Power consumption reduction
- Improvements of the overall performance of Artificial Intelligence and Machine Learning (AI/ML).
- Also, supports regulatory requirements (financial)



From ITU-T G Suppl.92

Sync solutions have been implemented by major data centre operators
Ongoing efforts to provide standardized solutions

ITU-T Supplement on synchronization in Datacentres

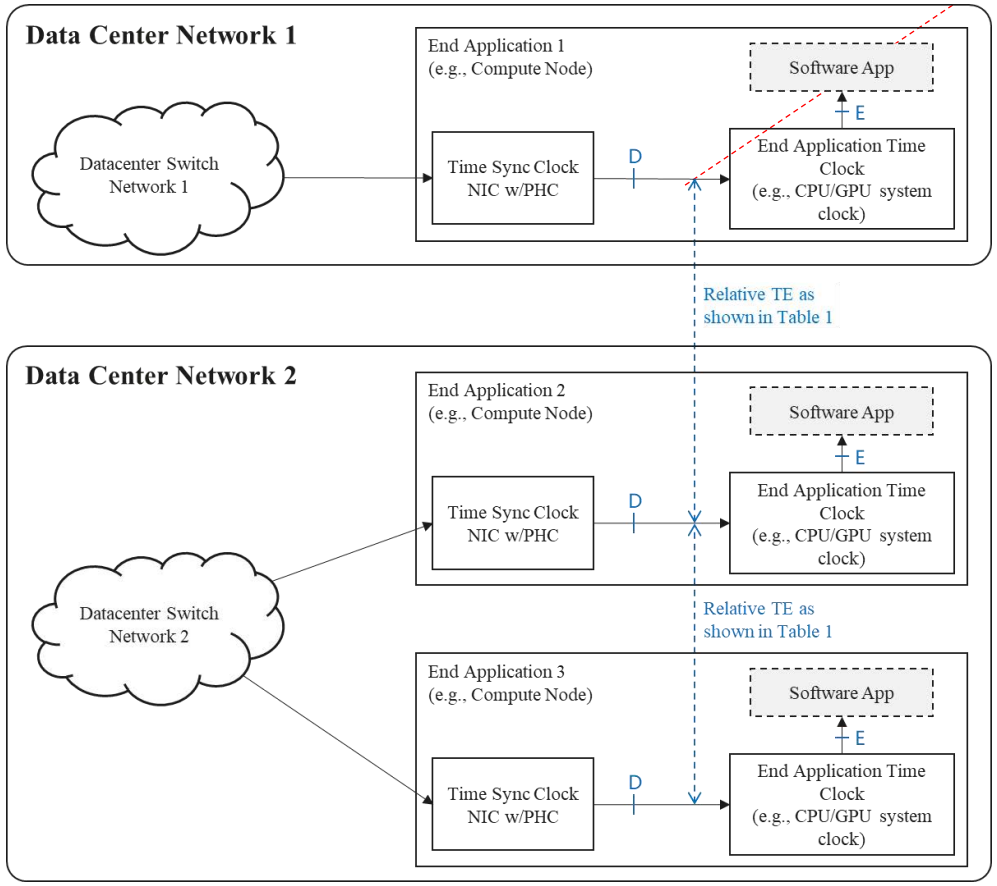
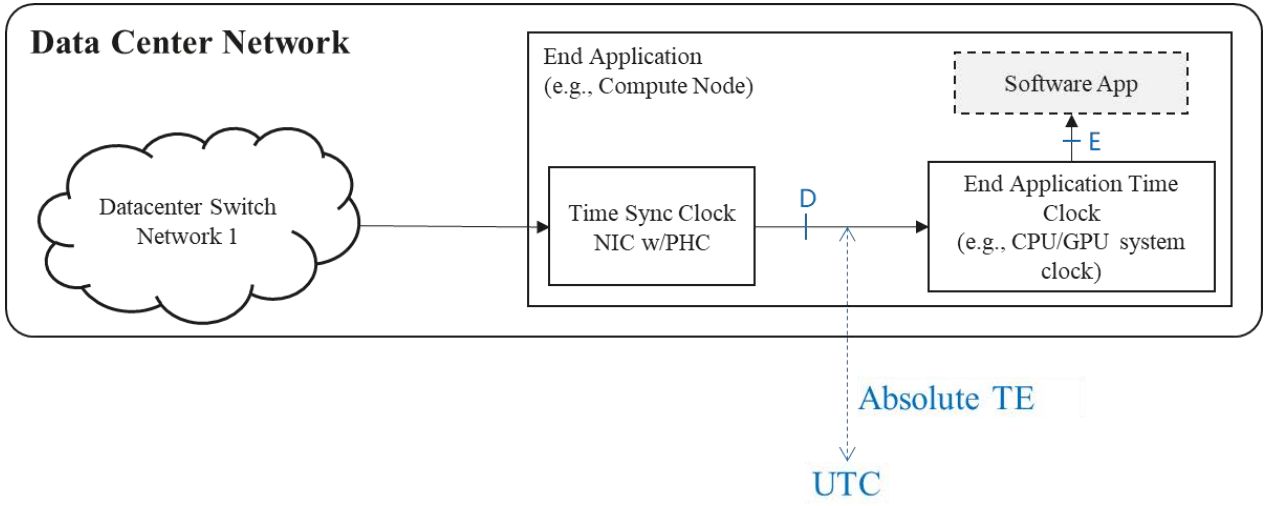


Table 1 - From draft ITU-T G Suppl.DCSync (June 2025)

Accuracy Class at Time Sync Clock	rTE between Time Sync Clocks	Typical applications
1	5µsec	Distributed databases, applications profiling
2	1µsec	High-Frequency Telemetry, Multi-node performance analysis tools
3	200nsec	Congestion control based on one way delay Time synchronized collective communication

The Absolute TE req't at Time Sync Clock output is half the rTE req't shown in Table 1

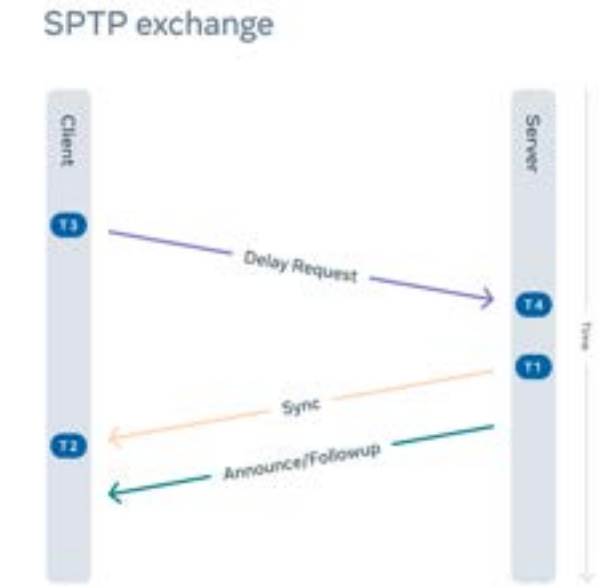
ITU-T Supplement on synchronization in Datacentres

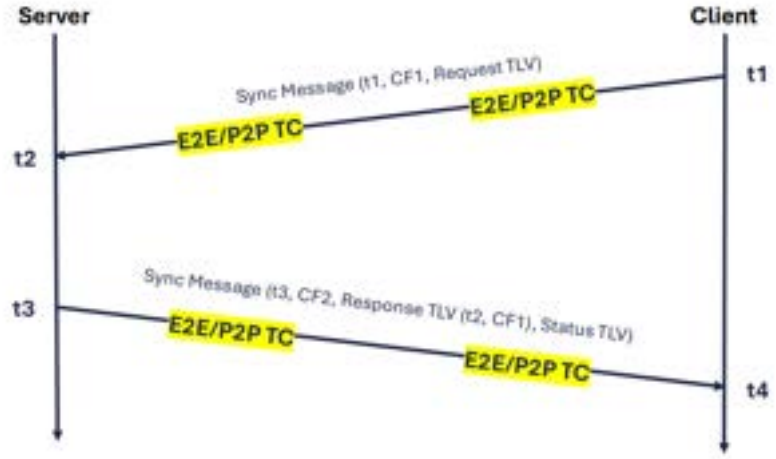


Accuracy Class: End Application Time Clock vs. Time Sync Clock	TE req's: End Application Time Clock vs. Time Sync Clock (from ref. point D to E)	Implementation Notes
A	2µsec	Typically, without PTM
B	200nsec	Typically, with PTM
C	50ns	Typically, physical clock signal (e.g. PPS OUT of Time Sync Clock, IN to End Application Time Clocks)

PTP-based Solutions for datacentres

- Data centres may need to use different PTP profiles to address different use cases and network topologies.
  - PTP based on Ethernet local link multicast communication
    - ITU-T G.8275.1 profile can be used as a baseline.
  - PTP based on IP unicast communication
    - IEEE IM/ST/PNCS Working Group currently developing IEEE P1588.1, a client-server PTP (CSPTP) based on IP unicast communication.
    - Simple PTP as an alternative until P1588.1 is released
- To ensure the highest accuracy of time delivery, the PTP profile for data centres should support full PTP timing support from the network.
  - In case of unicast, full timing support with transparent clocks may still generate some error (but limited by the longest distance, e.g., could be controlled within 10 us)





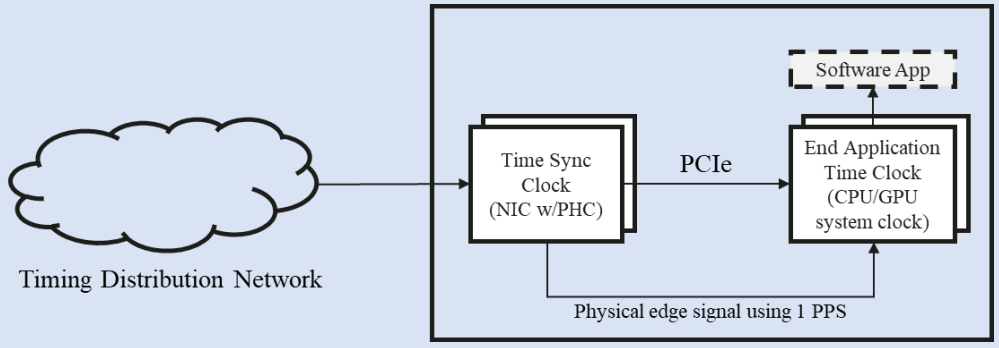
Subsystem Timing becomes a significant factor

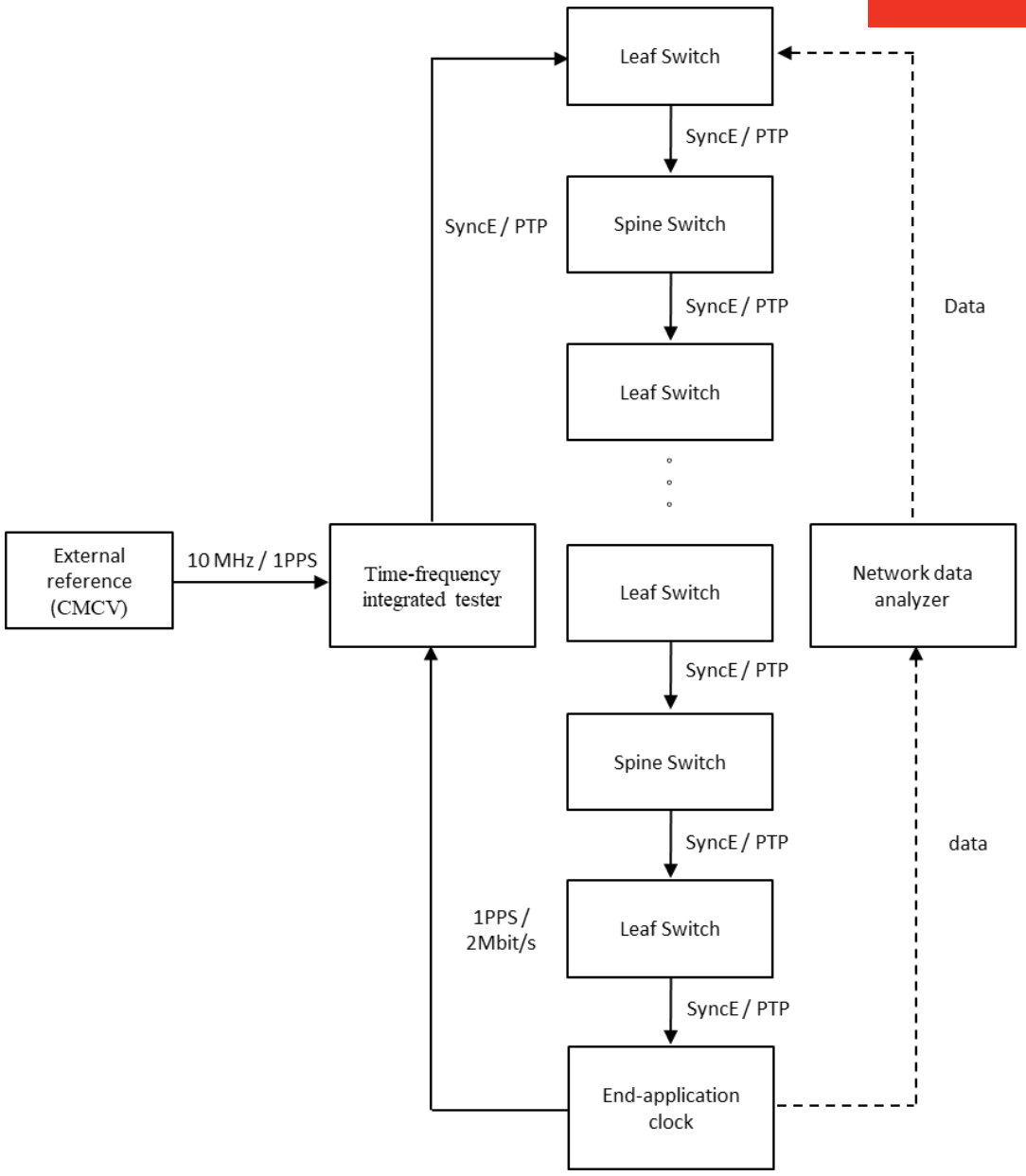
Sync Verification points for Data centres

Both network testing and lab testing required

New concepts for testing the CPU/GPU system clock performance

- PTM (Precision Time Measurement)
- TGPIO* (Time-Aware GPIO)





*Pin clocked by timekeeping hardware

From WD13-72 (Q13/15 Paris , June 2025)

PTM (Precision Time Measurement)

PREVIOUSLY:

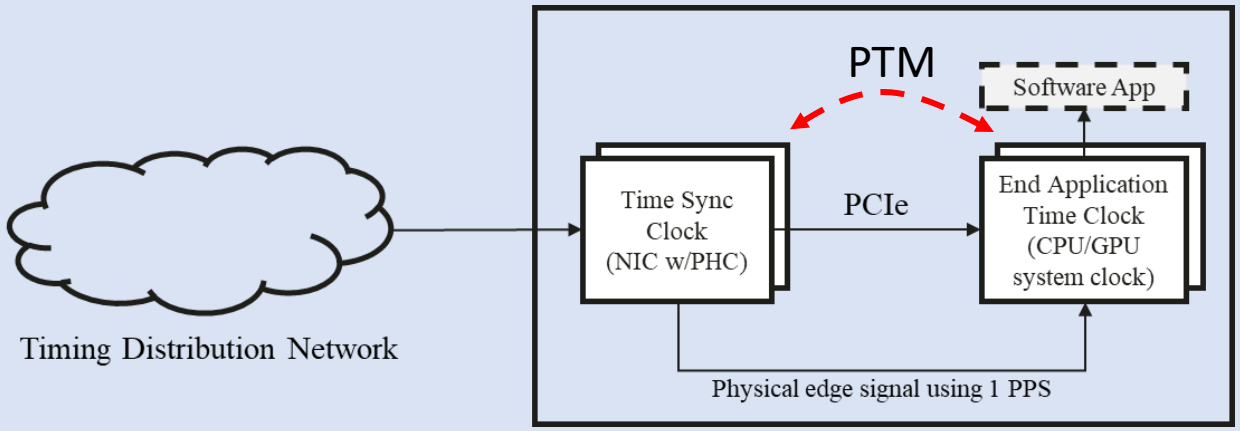
Hardware protocol used to sync HW elements using Transaction Layer Protocol (TLP) messages over PCIe bus

NOW:

Test and verification of PTM performance will allow the next level of deployment accuracy

2027:

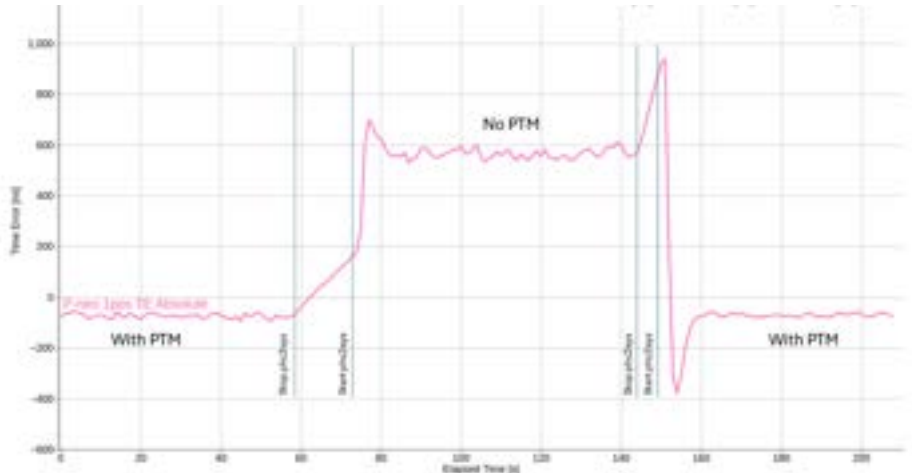
SW applications run under the same strict timing boundaries currently limited to the network layer.



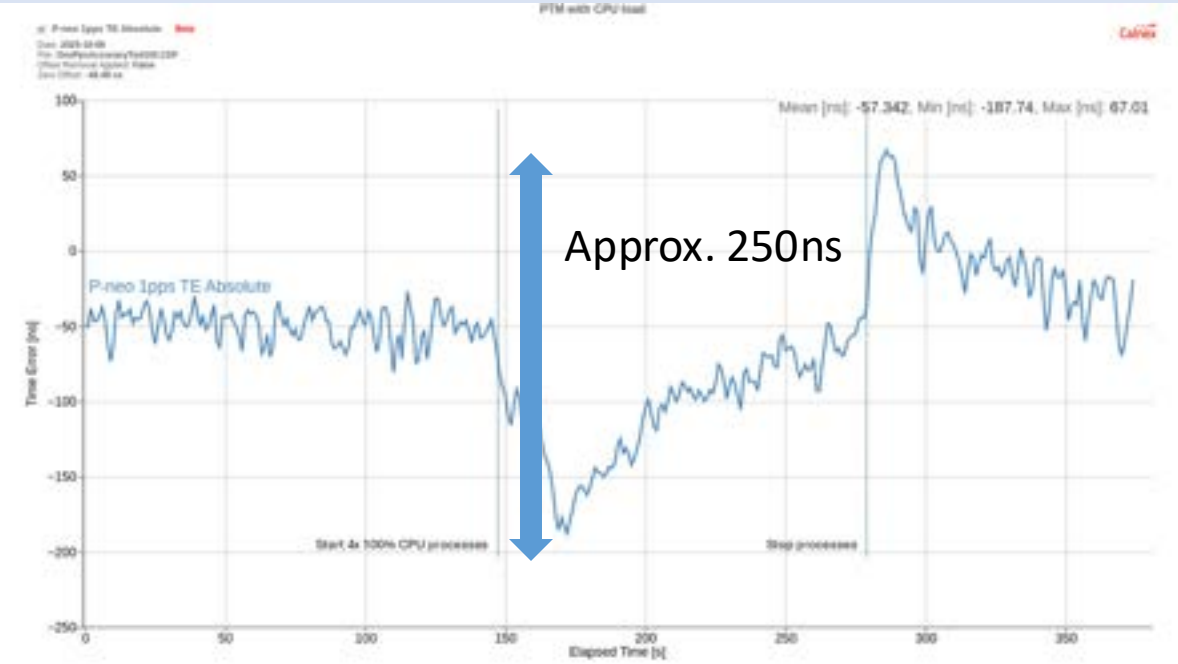
Example data:

Time Error on the NIC PPS output, using the timecard as a clock/PPS reference

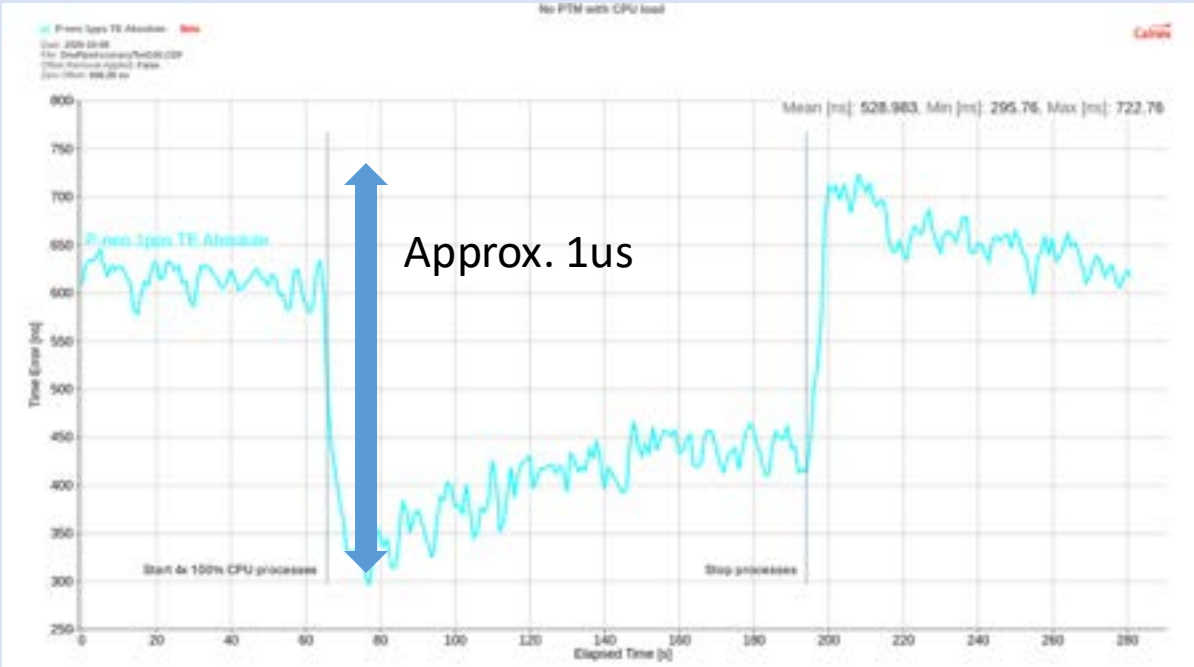
PTM to enhance accuracy



Impact of Load: with and without PTM



With PTM:
phc2sys *is* impacted by changes of CPU load but manages to go back around its baseline when the CPU load is constant.



Without PTM:
Impact on time error is higher.
Even with constant CPU load, unable to recover to base line.

High Speed Optical Interfaces

PREVIOUSLY*:

With the increase of data rates, new optical interfaces increasingly used, e.g.,

- Coherent optics
- PAM4

NOW*:

Work ongoing to minimize the impact on performance:

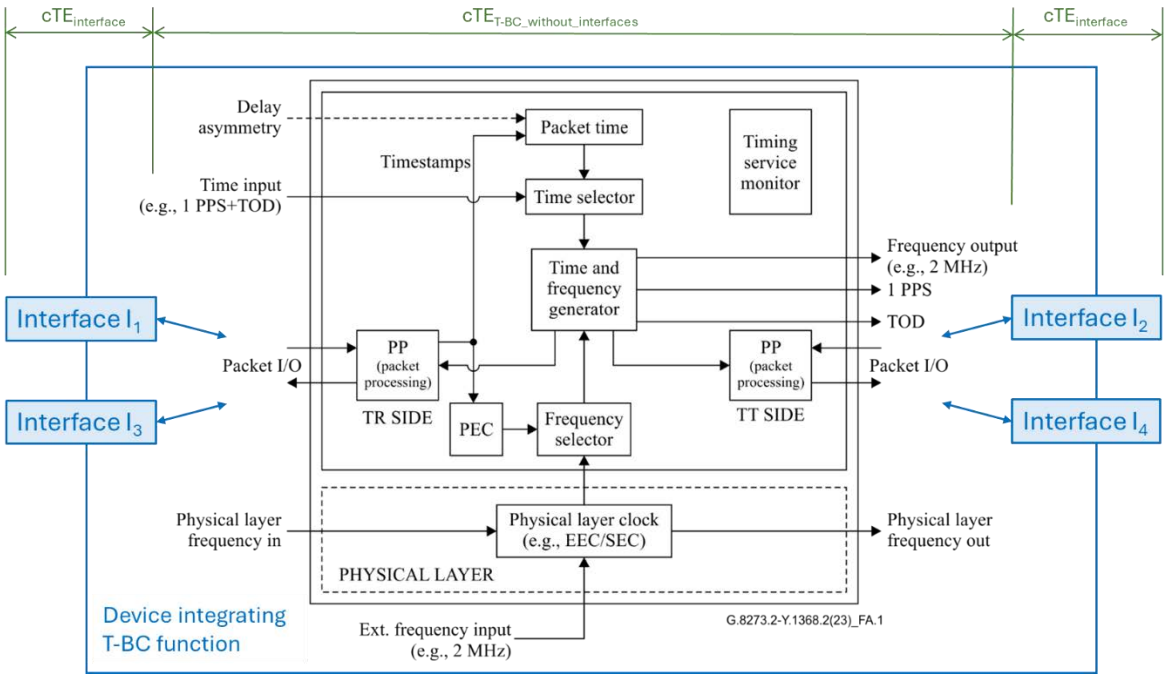
- classify optical pluggables as a % of T-BC cTE
  - e.g., **class C.10** = **10%** of the cTE for a **class C** clock
- Asymmetry compensation: store known Tx and Rx delay data in the optical pluggables

2027:

Widespread **and standard** use of the above techniques

New interfaces to increase performance:

- LPO (Linear Pluggable Optic)..?



***More detailed explanations are available via online resources, inc. previous ITSF papers**

Timing performance with LPO (studies ongoing)

Key points:

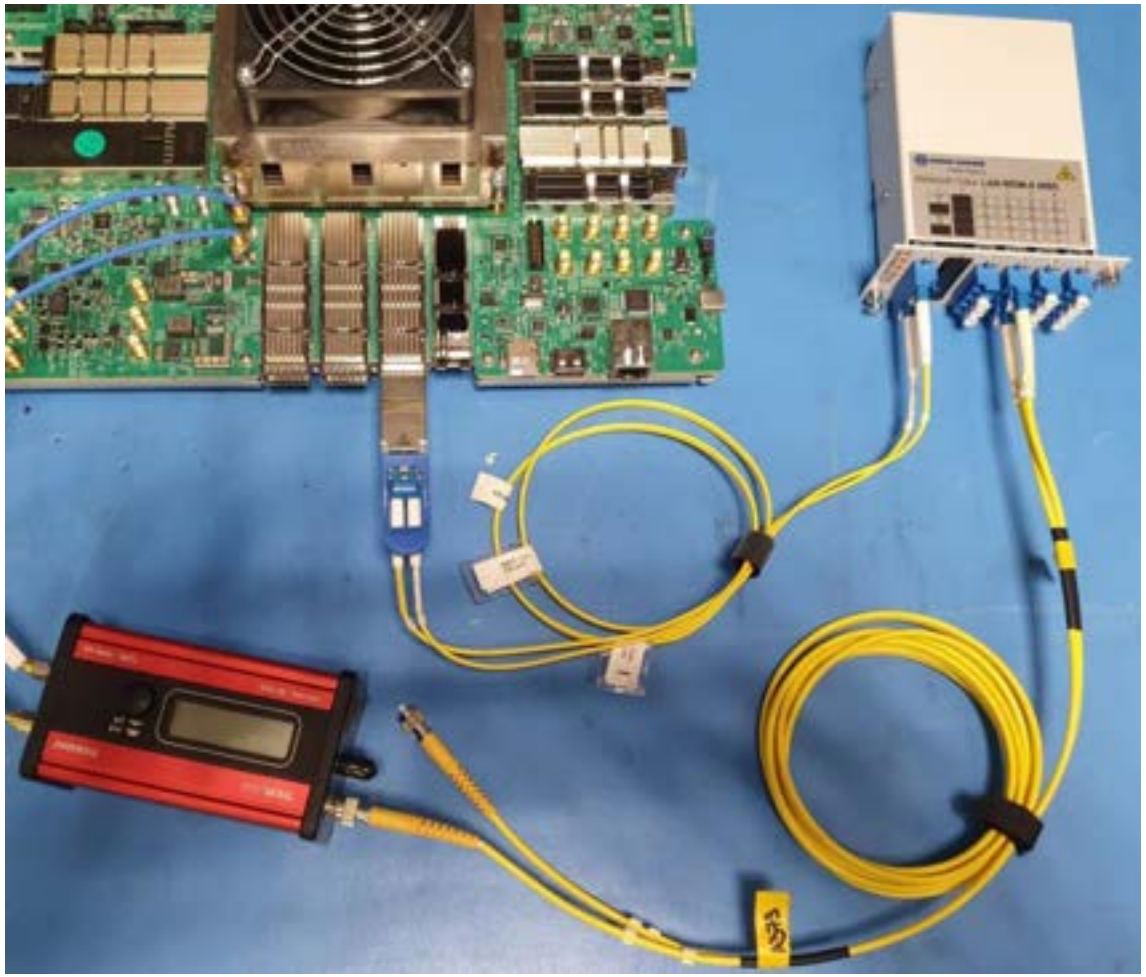
Pros:

- Tx Latency = Rx Latency = 0.5ns
- Minimal latency variation

Cons:

Very High Bit Error rates (more than can be corrected by FEC) unless Host device contains DSP

Example testbed topology:



The need for resiliency continues to increase

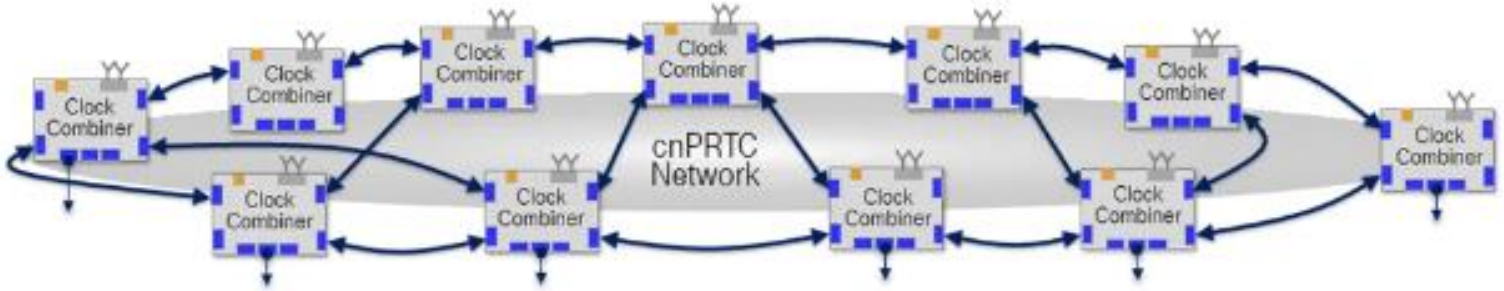
The need to increase resiliency

- Synchronization is essential for key infrastructures like telecom, power, transport, and finance, with serious risks if disrupted.
- GNSS is a primary timing source but is vulnerable to errors, interference, spoofing, and jamming.
- Other timing threats exist, such as at the packet layer.
- These issues have been discussed extensively, leading to efforts like **IEEE P1952** to improve timing resilience.

The need for redundancy and robustness in sync in telecom has always been a major requirement. Now even more so, and across multiple applications

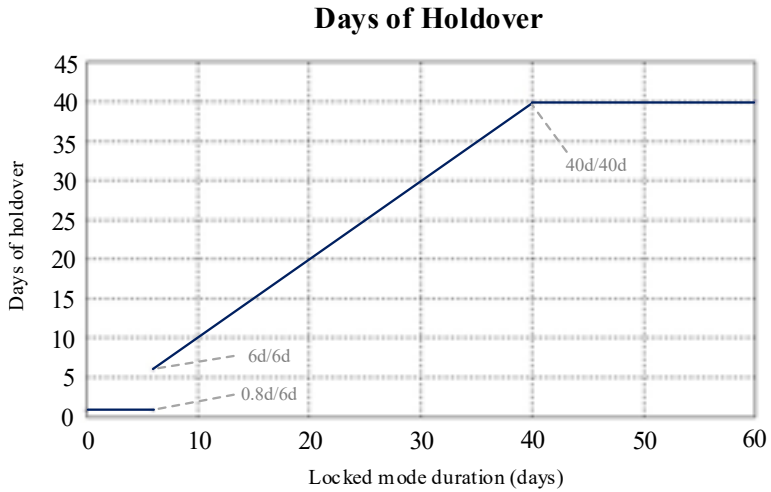
How to increase resilience in Sync?

- **Architecture**: Redundant PRTC / Grandmaster and Redundant paths
- **Geographical distribution** of GNSS Receivers; use of multiple constellations (GPS, Galileo, etc.)
- Increased **Holdover**: via physical layer support (SyncE), or enhanced PRTCs (ePRTC, cnPRTC)
- Increased **monitoring** solutions (E.g., G.8275 Annex F)
- **Protection** at timing protocol (incl. PTP over MACSec)



cnPRTC (Coherent PRTC):

PRTCs network at the highest core or regional network level to maintain network-wide ePRTC time accuracy, even during periods of GNSS loss

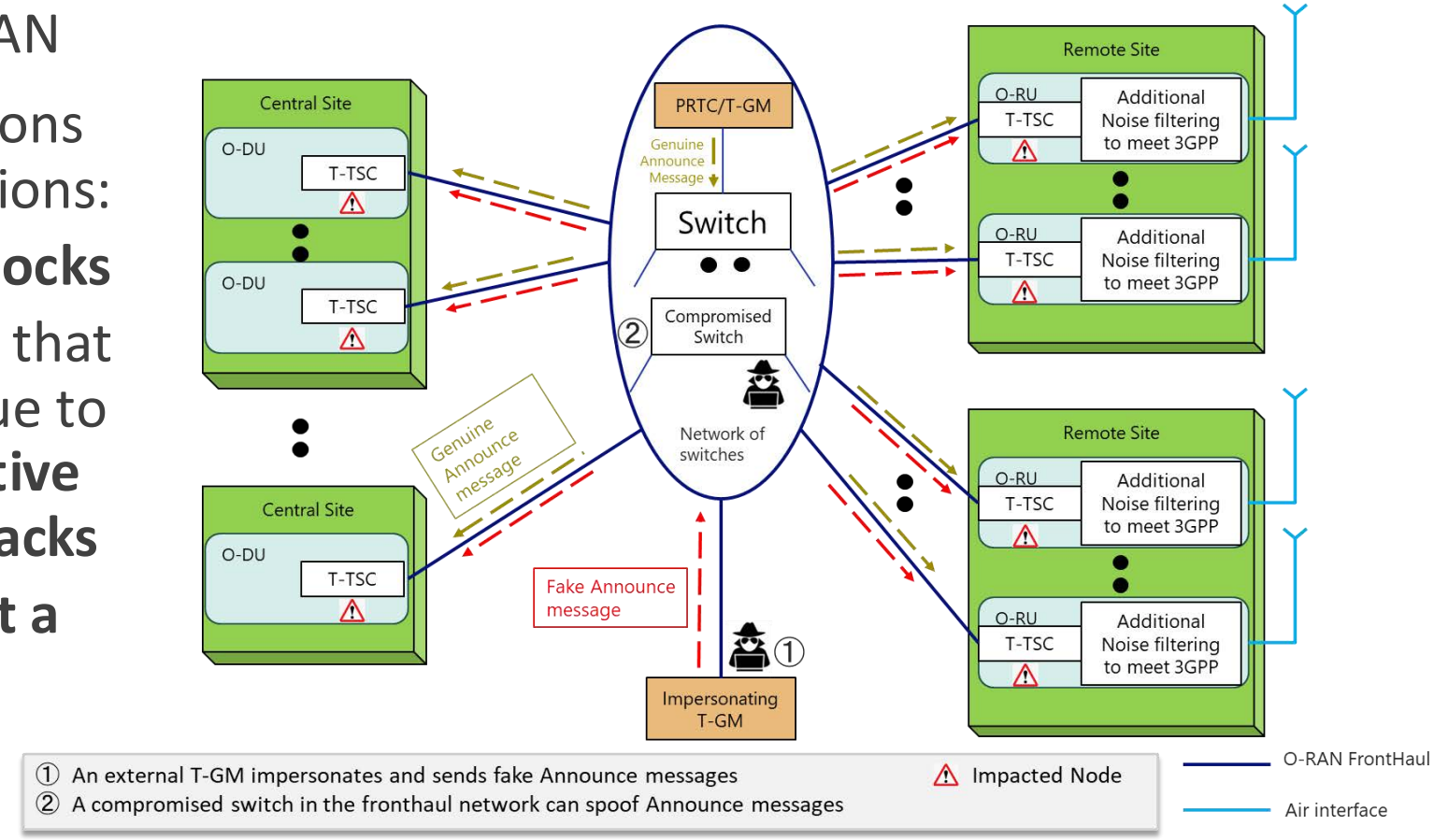


Enhanced PRTC specified in G.8272.1

[ITU News: New ITU clock concept for more resilient synchronization networks - ITU]

Security scenarios for PTP

- Addressed in both ITU-T and O-RAN
- Requirements and test specifications in O-RAN, with reference to solutions:
  - prevent **spoofing of master clocks**
  - protect against **MITM attacks** that degrade the clock accuracy due to **packet delay attacks** or **selective interception and removal attacks**
  - protect for **DoS Attack against a timeTransmitter**



MACSec vs. 1588 TLV: O-RAN with normative requirements

- O-RAN.WG11.TS.SRCS.0-R004-v13.00, Security Requirements and Controls Specifications:
  - **SEC-CTL-OFSP-4**: The Open Fronthaul Synchronization architecture **may** support **MACsec** for securing PTP messages. (…*MACsec as a mechanism to provide source authentication, message integrity, and replay attack protection for S-plane*.)
  - **SEC-CTL-OFSP-3:** The Open Fronthaul Synchronization architecture **may** support IEEE 1588-2019 [27] Authentication TLV for securing PTP ANNOUNCE messages. (…*IEEE 1588-2019 AUTHENTICATION TLV (clause 16.14) to provide source authentication, message integrity, and replay attack protection for PTP ANNOUNCE messages within a PTP domain*.)

For event messages, care must be taken to make sure that time stamping accuracy is not decreased when updating the **AUTHENTICATION TLV. This can be especially demanding for 1-step clocks.** Another aspect to consider is that **PTP messages are sent in clear text making them at risk of man-in-the-middle attacks delaying PTP event messages in a manner that impacts the timing accuracy**. It should also be noted that the **PTP integrated security mechanism only addresses PTP security, not any other L2 protocol**. This will impact the security posture if the goal is to be consistent with a zero trust architecture (ZTA).

MACsec provides security using end-to-end and hop-by-hop modes on Ethernet links. …However, PTP over MACsec implementation has its challenge related to timestamping of PTP event messages. …. This can be more demanding for 1-step clocks than 2-step clocks. … **A benefit of using MACsec is that all ethernet frames can be encrypted to provide confidentiality and integrity protection, decreasing risk of MitM attacks**.

MACsec is being considered to provide confidentiality and integrity protection on the Open Fronthaul S-Plane. Hop-by-hop **MACsec has additional benefits** protecting all traffic on the LAN segment, not only S-Plane.

Towards 6G and beyond

Non-Terrestrial Networks (NTN)

PREVIOUSLY:

- Non-Terrestrial Networks are part of 3GPP specifications for 5G and will be part of 6G.
- Initial work done in Transparent mode, NTN Network will be used to bounce the signal.

NOW:

- (Rel19 - 20) will include NTN with a regenerative - or packet-processing - payload, in which a **complete gNB is placed on the satellite**
- LEO satellites are used for 5G. Current releases focus on FDD with loose time sync requirements
- The latency is too large for timing signals to be sent, unless they are using Transparent mode.

2027:

- Solution: GNSS on the cell phone . The satellites will also have GNSS capability, hence impacts from latency can be controlled.

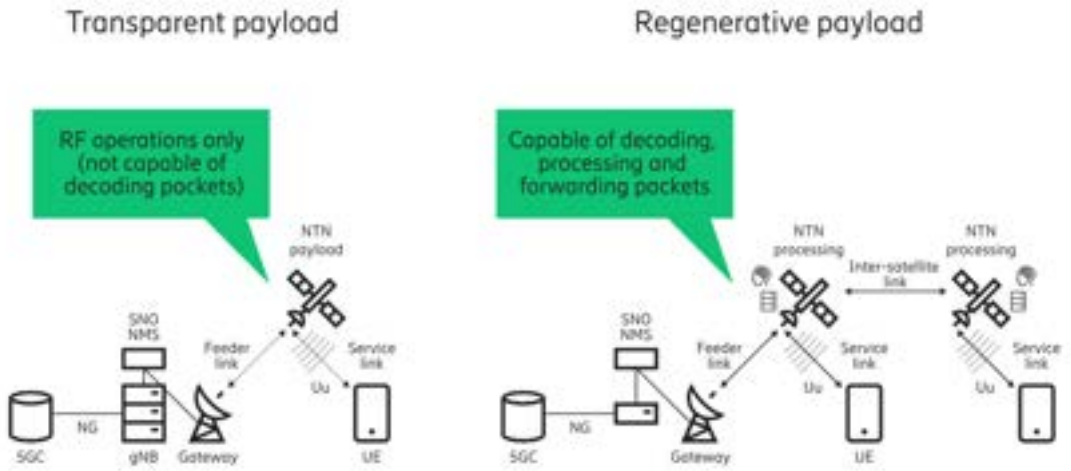
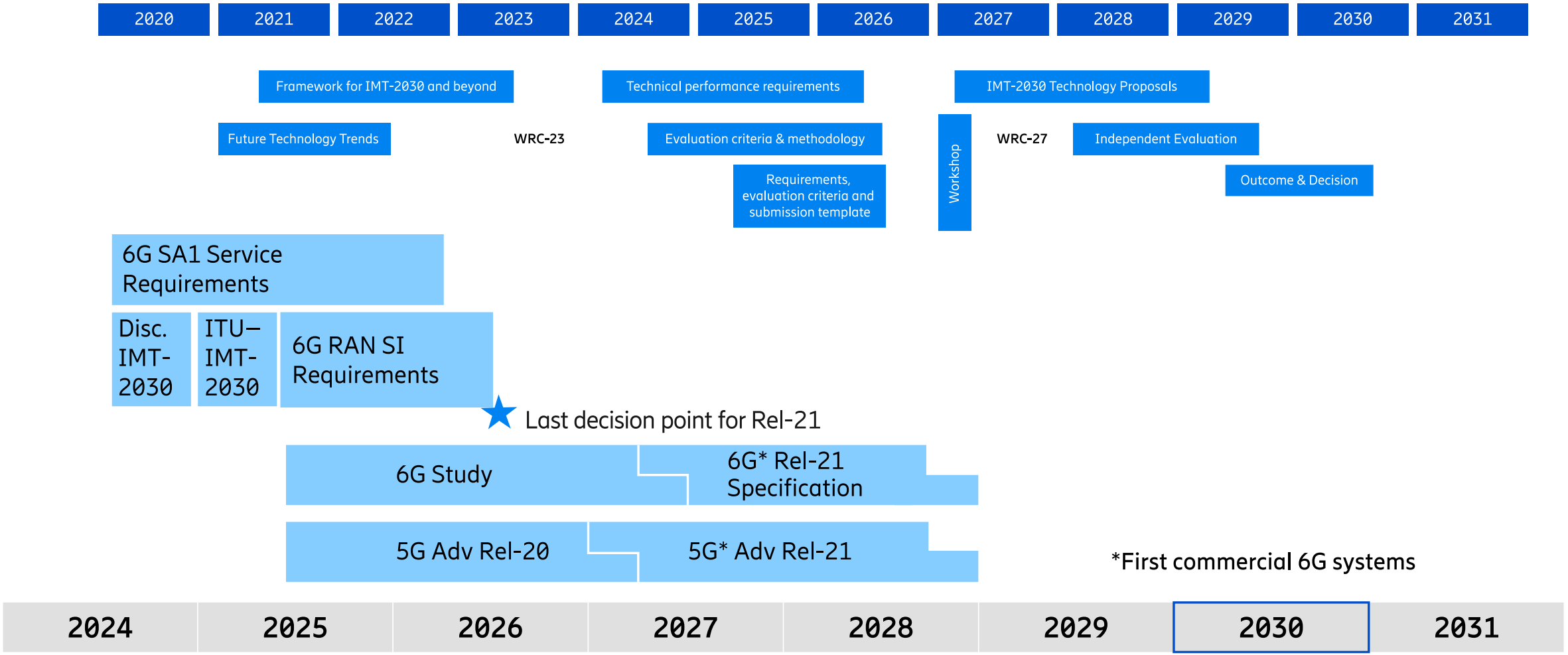


Figure from Ericsson blog:
[5G Non-Terrestrial Networks in 3GPP Rel-19 - Ericsson]

Future: Mobile towards 6G

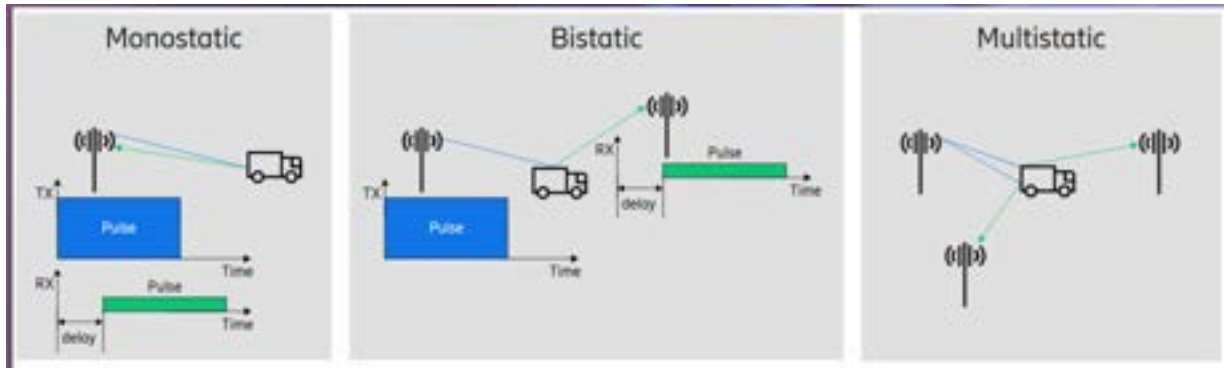


* Indicative timeline Ericsson view

ITU designates 6G as IMT-2030, with 5G referred to as IMT-2020, 3G as IMT-2000, and 4G as IMT Advanced.
[6G standardization timeline and principles - Ericsson]

Future: Expectations for sync in 6G

- Higher focus on coordination between base stations:
  - Coherent Joint transmission (C-JT)
  - Integrated sensing and Communication (ISAC)
  - Positioning (sub-meter)
- Use of Higher order modulation, leading to need for higher stability
- Key requirements: relative time and frequency stability
- Increased importance of timing delivery over the radio



ISAC scenarios

From Synchronization in 2030 perspective
(ITU Workshop on “Future Optical Networks for IMT2030, AI, broadband and more")

Forward looking:
Sync in Quantum Key Distribution Network (QKDN)

Calnex

- ITU-T SG13 is now releasing Recommendations and Supplements on Quantum Key Distribution including sync implications
  - e.g. Y.Sup89 “Analysis of time synchronization in Quantum Key Distribution Networks”.
- ITU-T JCA-QKDN (Join Coordination Activity) coordinates standardization work on quantum key distribution networks (QKDNs). Related work:

Y.Sup80	**Use cases of quantum Key Distribution Networks**
ITU-T Y.3825	**Integration of quantum key distribution network and time-sensitive network - framework**
ITU-T Y.Sup69	**Analysis of Synchronization in Quantum Key Distribution Networks**

- Use cases for **Quantum time synchronization:**
  - Quantum time sync in telecoms
  - Secure quantum clock synchronization
  - A quantum network of entangled clocks
- Time sync needs and solutions to support QKDN:
  - e.g. absolute time distribution in ms, **point-to-point rTE sub-ns**

Summary

- Synchronization continues to be a fundamental function as networks and applications evolve
- We expect increasing focus in the next 2 years on:
  - Telecom supporting connected applications: Industrial Automation, Data centres, etc.
  - New interfaces carrying timing
  - Increased resiliency (GNSS protection, PTP security, sync monitoring, holdover, HA links from Metrology labs, etc.)
  - Emerging needs in mobile networks: e.g. 5G Advanced, NTN integration
- We won't stop there!:
  - 6G (local timing / higher stability); Sync over radio
  - New applications with particularly stringent timing requirements, e.g. quantum key distribution (QKD)

Deployments are becoming increasingly varied. The impact of bad sync can increasingly result in disruptions in critical infrastructure:

Verification of the various technologies and scenarios remains key to prevent issues

Calnex Solutions

Insight and Innovation

calnexsol.com

Stefano Ruffini Strategic Technology Manager