How Aerospace and Defense can benefit from Telecom

WSTS 2026

Adam Paterson
Head of Product Management
Stefano Ruffini
Strategic Technology Manager

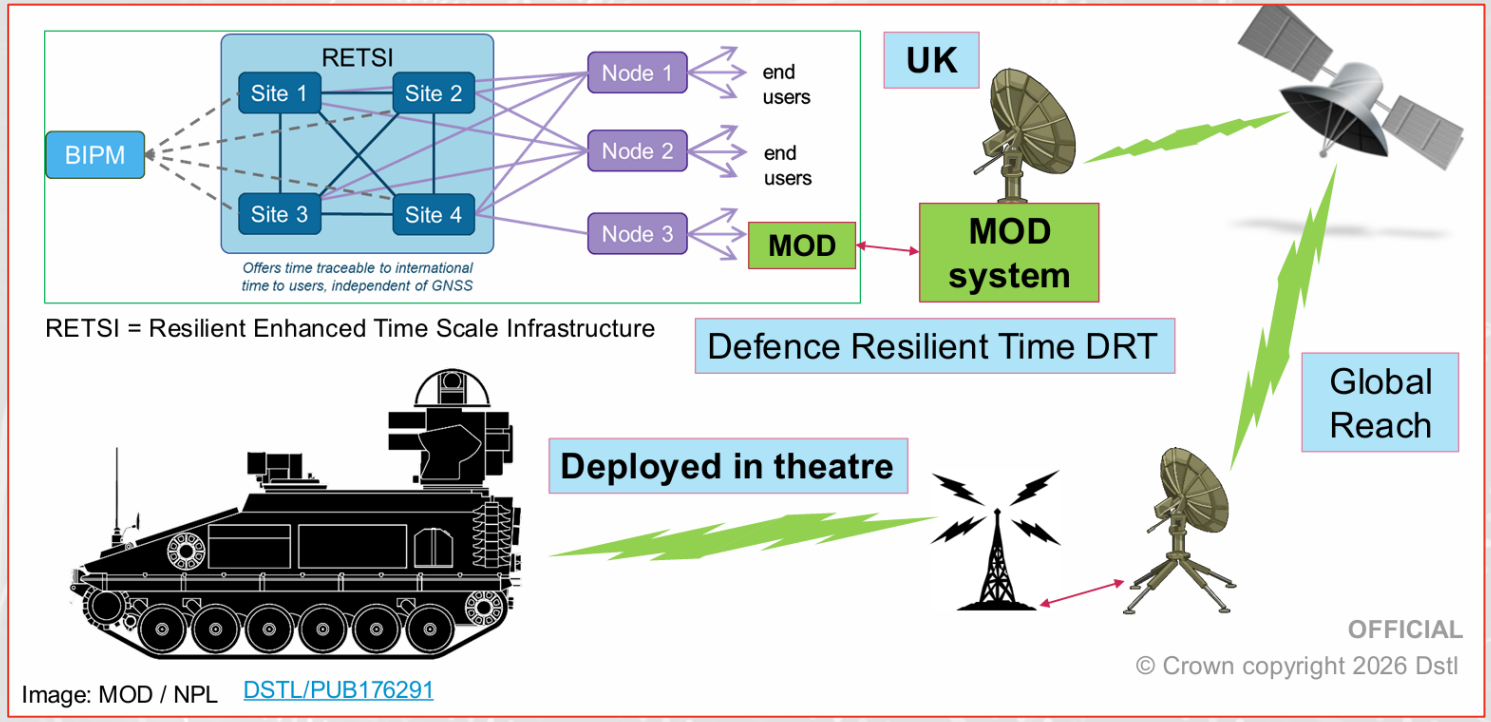
Contents

- Introduction
- Requirements – some examples
- Additional considerations based on applications
- Potential leverage from Telecom solutions to Defense/Aerospace
- Conclusions

Introduction – Timing in Military Platforms

Summary/Examples below of systems with a range of timing and synchronization requirements

- Ranging and optical system characterisation
- Surveillance and detection
- Identification Friend or Foe
- Electronic Intelligence, Signals Intelligence
- Guidance systems
- Synthetic Aperture Systems
- Electronic Countermeasures
- Navigation



[Courtesy of "MOD and the National Timing Community, March 2026", Bryn James, (NPL 2nd National Timing Community Engagement Forum)]

Consider also: Aerospace Related Requirements

P802.1DP/D3.0/SAE AS6675-2025 describes Time-Sensitive Networking for Aerospace Onboard Ethernet Communications:

…deterministic IEEE 802.3 Ethernet networks that support aerospace onboard applications […] requiring:

- Security
- High availability and reliability
- Maintainability
- Bounded latency

Time sync: IEEE Std 802.1AS-2020 (amended by IEEE Std 802.1ASdm-2024)
Fault-tolerance mechanisms: IEEE P802.1ASed

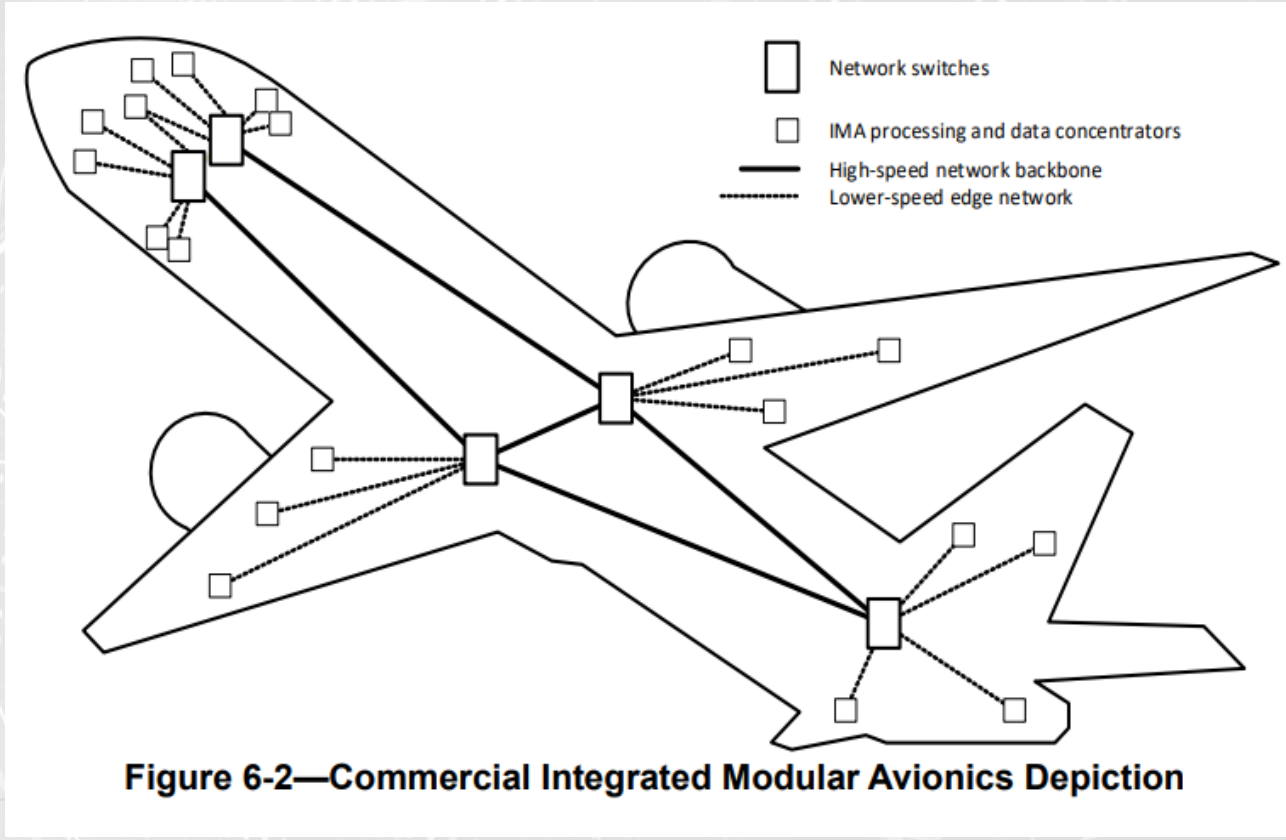


Figure 6-2—Commercial Integrated Modular Avionics Depiction

Requirements

"Table Stakes"?

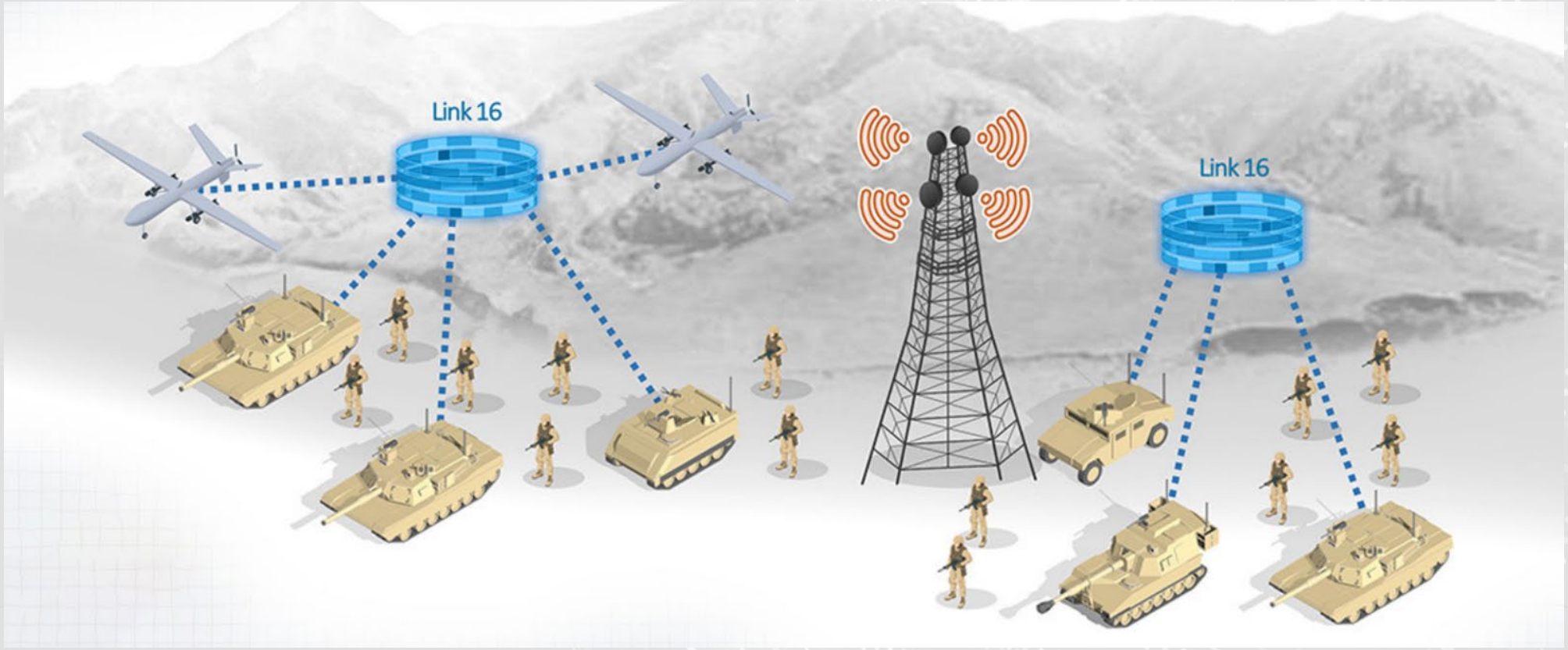
- Precision
- Reliability
- Interoperability

Requirements for deployment:

- Robust
- Resilient
- Covert

Resilience, Secrecy (cont'd)

- Loss/corruption of comms is a major threat vector
- Reliance on fixed points of signal both provides a point of attack and reveals platform locations



Defense needs continued: Timing as security

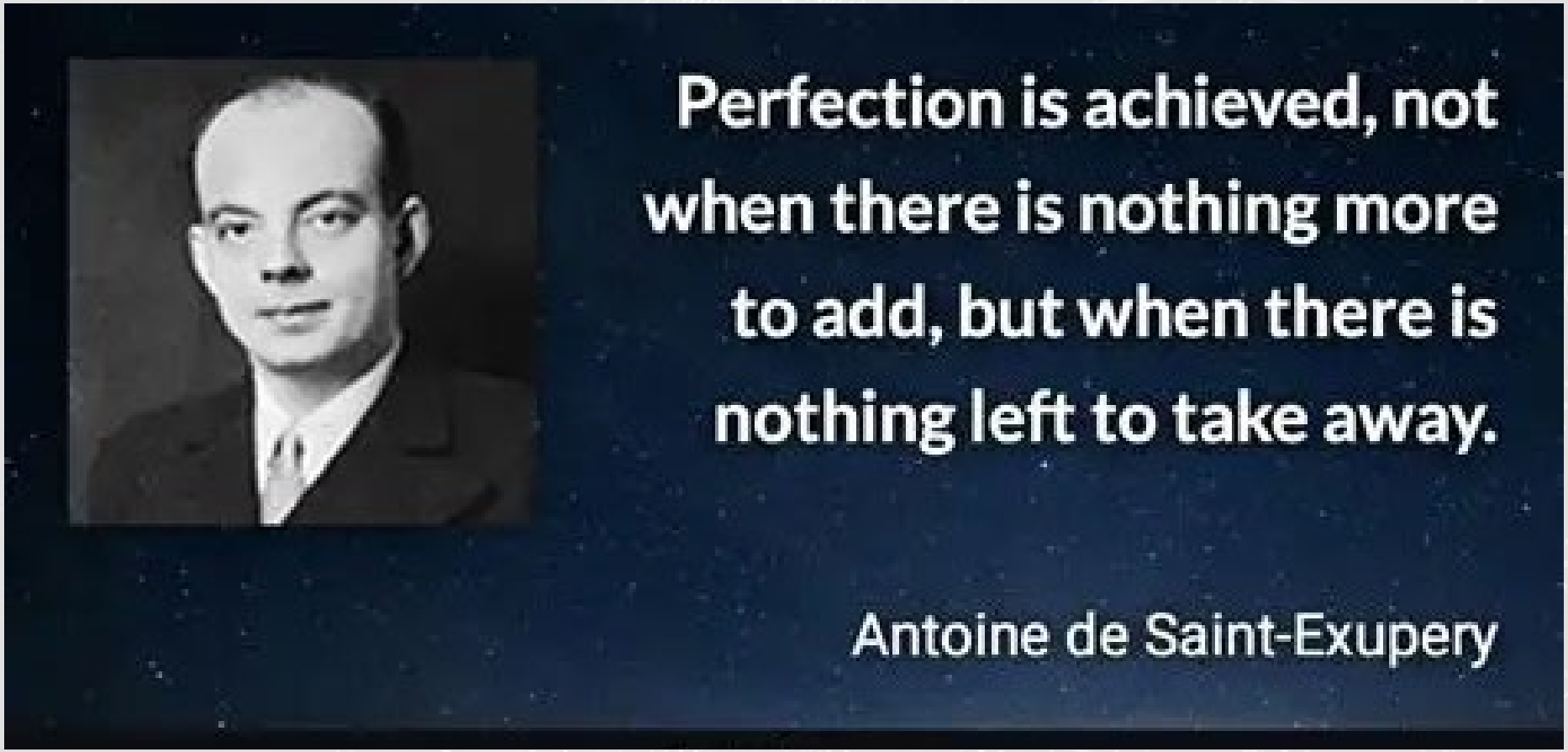
- Time drifts within systems present opportunities for malicious actors to gain access.
- After which they can wait to create further system exploits
- Robust time awareness in the system closes this loophole

> "Synchronization is not just about getting things right; it is also an important security function.
>
> Malicious individuals can take advantage of synchronization errors to insert false information, delay emergency signals, interfere with industrial controllers, or carry out denial-of-service attacks"
>
> (Narula & Humphreys, 2017; Yiğitler, Badihi, & Jäntti, 2020).

Requirements, continued: Defense demands efficiency

Commonly, equipment should be as simple as possible to:

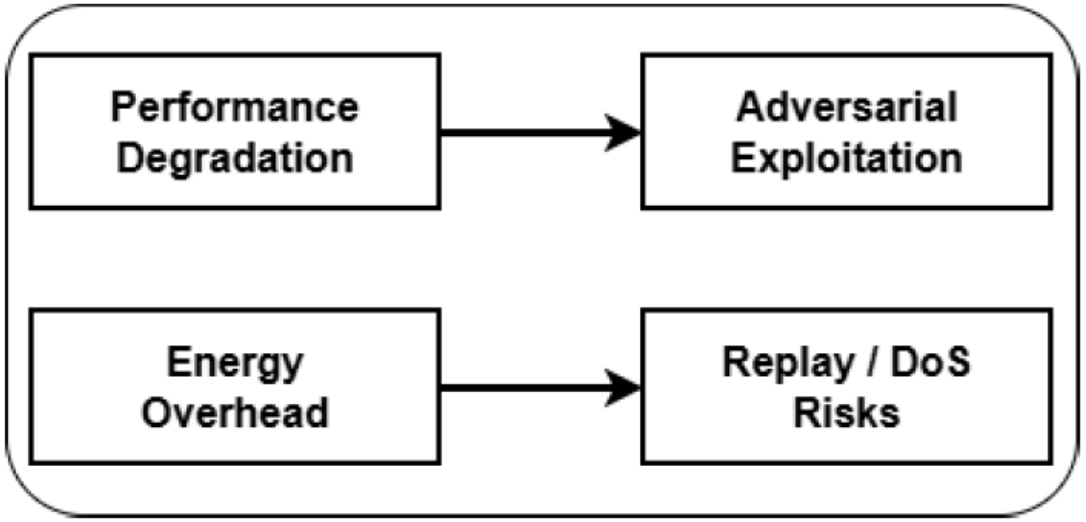
- Procure
- Install
- Maintain
- Operate
- Dispose of
- Update



Trade-offs between technical and security factors

Making the best choice is deployment dependent. Example factors are as below.

Synchronization Method	Efficiency	Security Resilience
Closed-loop	Low drift, energy intensive	Vulnerable to jamming
One-bit feedback	Efficient, scalable	Susceptible to feedback manipulation
Two-way sync	Robust timing	Resilient but replay-prone without authentication



Solutions: why «dual use»?

- Telecom, Aerospace and Defense share many common requirements
- This already leverages use of standardized solutions (e.g., PTP)
- New architectures further allow for dual use of infrastructure: 5G slicing allows support for specific network requirements
- Existing large scale development and deployment of technologies in the Telecoms space can provide options for faster development and deployment for e.g. defense requirments, with a benefit of economies of scale

Application of Telecom Solutions to Defense/Aerospace

Telecom can be considered as critical infrastructure, and disruption of timing can have serious consequences (think of e.g. 911 disruption)

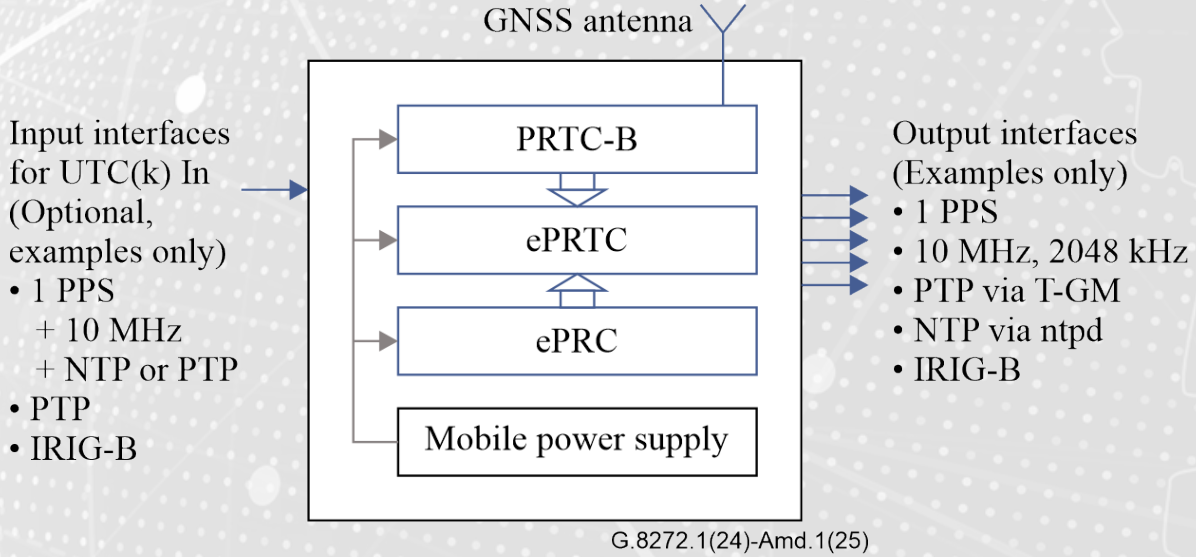
Several Solutions with enhanced robustness have been defined over the years:

- 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)
- Travelling Clock
- Increased monitoring solutions
- Protection at timing protocol (e.g., PTP MACSec)

The drive to support wider commercial applications also leads telecoms technology to continue to innovate and update

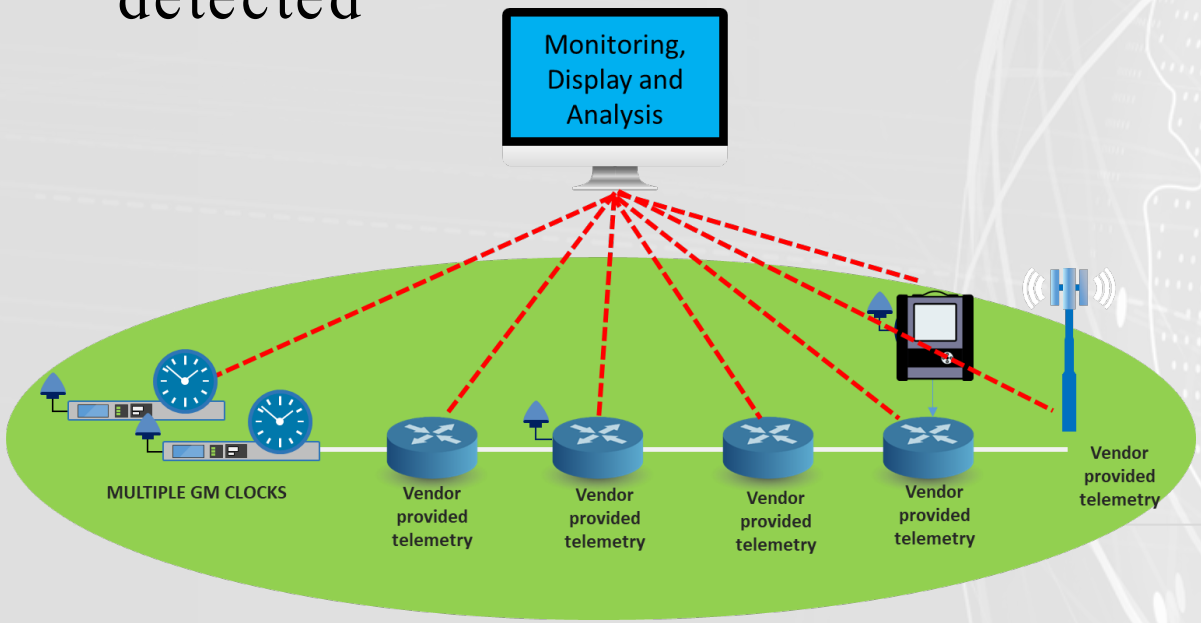
Moving objects, secrecy: Travelling Clock? (G.8272.1)

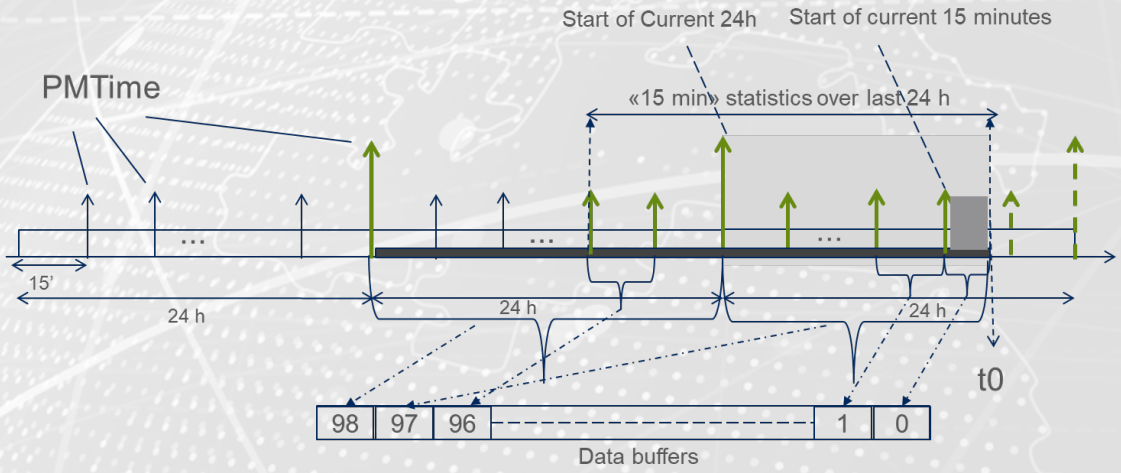
- ePRTC system in holdover mode (GNSS or UTC locked before) along with an active ePRC, could be utilized as a powered-up mobile travelling reference clock system
- Purposes:
  - measurement reference usage
  - delay compensation
  - disaster recovery at locations where GNSS cannot be consistently used



Threat detection: Sync Network advanced monitoring?

- ITU-TG.8275 specifies a set of statistics to monitor performance of PTP.
- Data is collected periodically from all Network elements and can include configuration information etc.
- Misconfigurations, Network failures, rearrangements, security attacks, can be detected





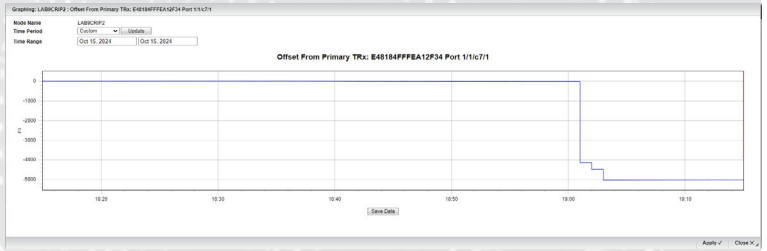
PMTime: start of the 15minutes / 24h periods

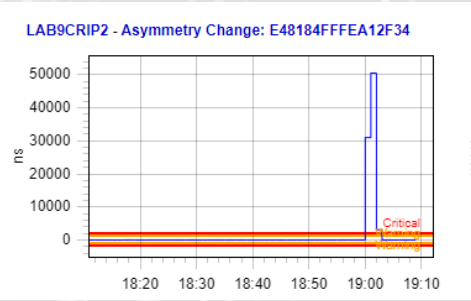
Data used for the statistics stored in the buffer

Data used for the current 24h value

Data used for the current 15 minutes value

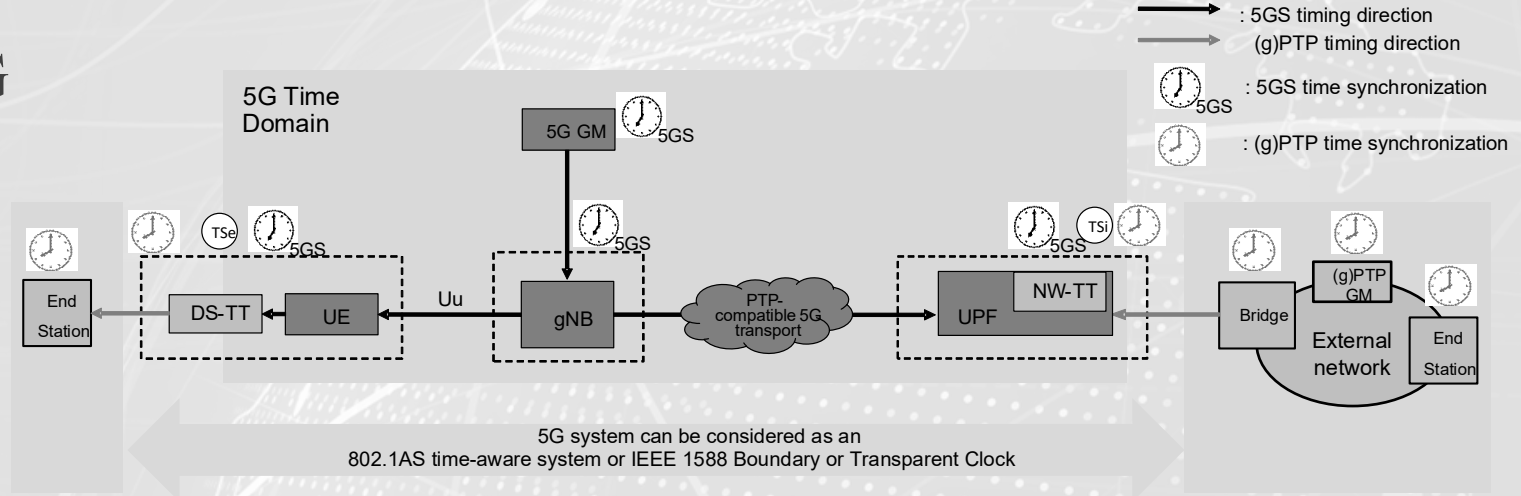
t0 Indication of current time when accessing the PM data





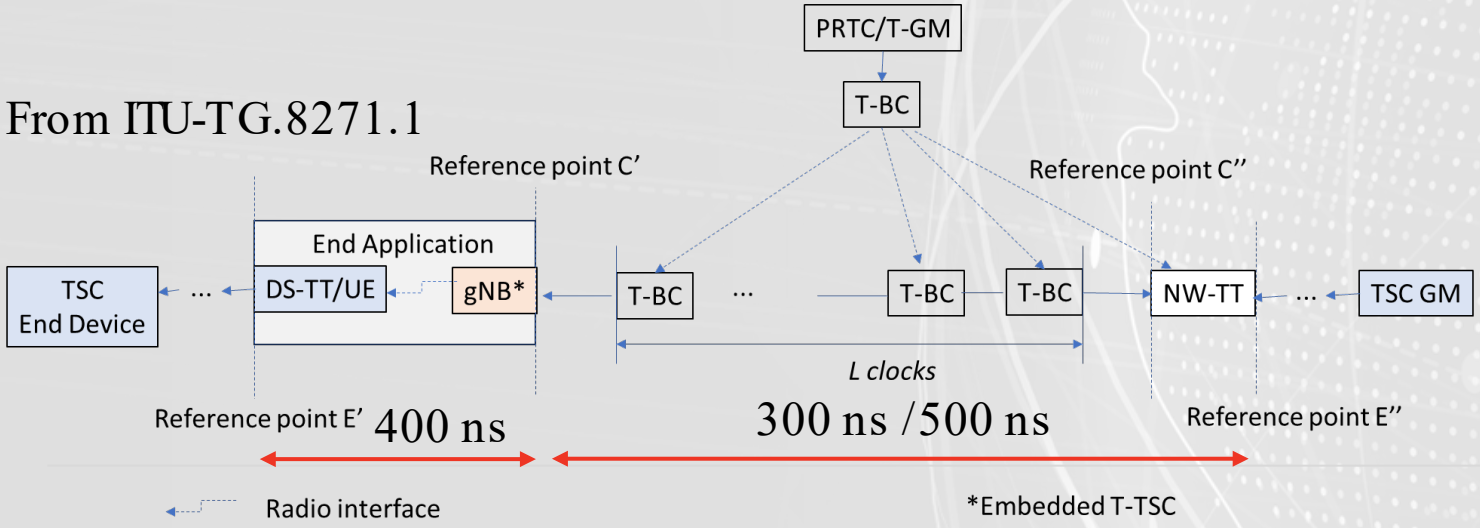
Platform to Platform: Timing delivery over 5GS?

- Solution to deliver a UTC traceable timing source over 5G radio.
- Related to 3GPP studies on integration of 5GS (5G System) with Industrial Automation application ("TSN")



From 3GPP TS 23.501

From ITU-TG.8271.1



Target requirements for the 5G segment: 700 ns or 900 ns:

✓ Would also be suitable for e.g. Ship-to-ship comms requirements

How Timing over 5GS could support Defense needs

Initial discussions have highlighted potential crossover with Private 5G implementations to accelerate deliverables for next gen ship-to-ship comms

"some" reuse from industry is acceptable, but disaggregated solutions preferred to allow 'in-house' ownership of security-critical components

Summary

- Many current and future technical developments in aerospace, defense, telecoms and other areas can provide mutual benefit
- Reliability and accuracy remain key requirements for Defense and Aerospace
- The challenges of moving objects and potential need for covert capabilities create additional challenges
- Dual use may be suitable in some cases, providing potential performance benefits and economies of scale
- In validating devices and systems for use, care must be given to the priority needs of the applications: resilience and security may take precedence over pure performance

Thank You

Adam Paterson
Head of Product Management

Stefano Ruffini
Strategic Technology Manager