Time Sync for Aerospace

Continued...

Abdul Jabbar
GE Research

Objective

- **Review DP approach to Time Synchronization**
- **Seek input from group**

Time Synchronization Requirements for Aerospace

Lots of discussion on the use of Time Sync for aerospace – particularly around availability and integrity.

See contributions on DP home page.

Objectives for this presentation:

1. Summarize the proposed approach by the group
2. Discuss dependent vs. independent domains
3. Example design patterns being considered

Time Synchronization Requirements for Aerospace

Fault Tolerance

Tolerate multiple (typically 2) simultaneous arbitrary faults in end stations, bridges, links, GMs

Under faulty conditions, a correctly operating end station shall maintain the target max time error relative to the correctly operating GM. If unable to maintain the max time error, the correctly operating end station shall detect an erroneous time sync state.

Availability:

- Reception of a time value at a given PTP receiver (instance)
- Deals with loss of SYNC/FOLLOW_UP message due to link, bridge, end station, and GM faults/failures

Integrity:

- Correctness of a time value received at a given PTP receiver (instance)
- Deals with error in the SYNC/FOLLOW_UP message due to arbitrary faults in the link, bridge, end station, and GM

Proposed Solution Elements

From a profile/standards perspective

1. Multiple domains and therefore multiple PTP instances
2. Multiple Grand Masters
3. Fault Tolerant Module at each time-aware bridge and end station

Assumptions: Static network, static configuration, no BMCA, static port states, no administrative reconfiguration during run-time

Proposed Solution Elements

Multiple PTP domains

- More than one domain is required for fault tolerance in aerospace networks
- Considering domains for redundant paths, redundant GMs, redundant clock sources, a lot more domains might be needed. For example, two GMs distributing time over two redundant trees requires 4 domains and therefore 4 PTP instances at each bridge and end station.
- DP needs to specify a minimum number of domains for interoperability (Shall, should, may)
- PTP domains can be independent or dependent

Proposed Solution Elements

Dependent PTP Domains

PTP Domains that have some common time source components:

- Share a GM (e.g. redundant sync trees)
- GMs are synchronized to one another (e.g. Hot Standby GMs)
- ? GMs connected to same (direct) clock source

Note: Does not include considerations related to shared links and nodes (a.k.a path commonalities)

Use in Aerospace

- Improve the availability of a single time source
- Cannot be used for integrity checks

Discussion

May need a better term than "dependent"

Proposed Solution Elements

Independent PTP Domains

PTP Domains that do **not** have any common time source components like:

- Share a GM (e.g. redundant sync trees from a GM)
- GMs are synchronized to one another (e.g. Hot Standby GMs)
- GMs share a common (direct) clock source

Note: Does not include considerations related to shared links and nodes (a.k.a path commonalities)

Use in Aerospace

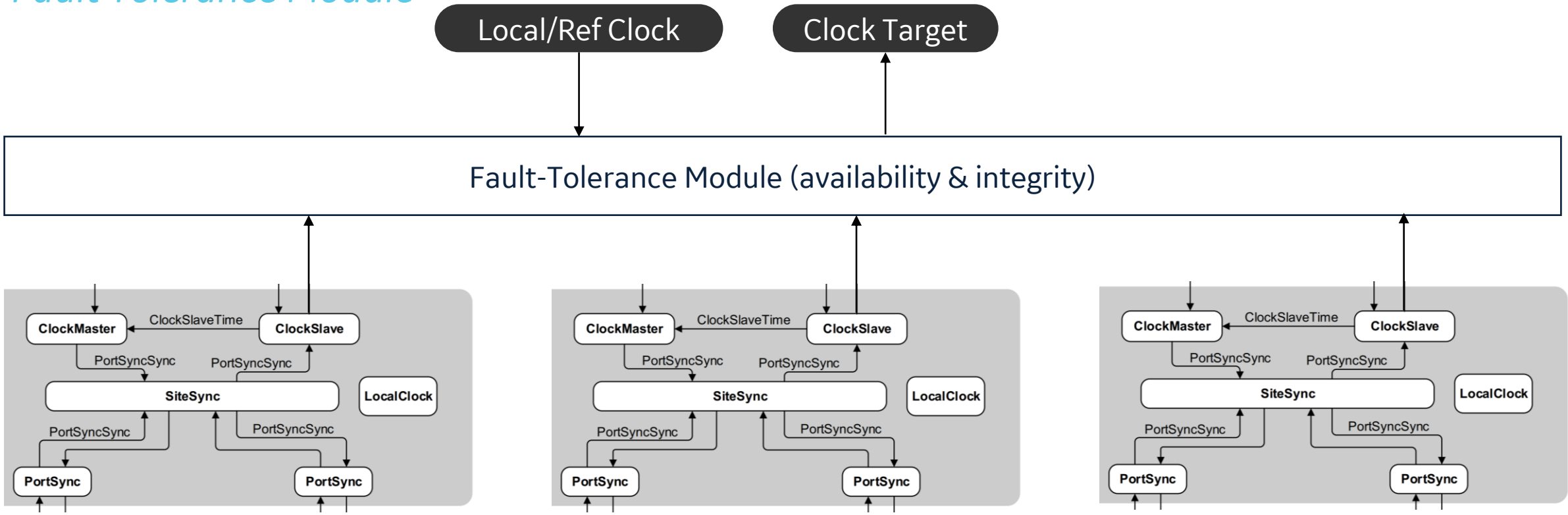
- Typically used for correctness checks (integrity)
- Could also be used to improve availability

Discussion:

- How to identify independent vs dependent domains: GM/ClockIndentity, Domain ID coding, timeBaseIndicator coding?
- May need a better term than “independent”

Proposed Solution Elements

Fault Tolerance Module



1. Fault-tolerance module as an application function. Defines structure, interfaces, and a default selection algorithm(s). Applies to both end stations and bridges.
2. Default selection algorithms based on dependent and independent PTP domains
3. A quality local clock may serve as an additional time reference for integrity calculations

Proposed Solution Elements

Recap

DP standard requires support of

1. Multiple PTP domains (and PTP instances) at each time-aware bridge and end station
2. Fault Tolerance Module (as an application function) at each time-aware bridge and end station

Implementer Considerations (Annex?)

- Appropriate use of dependent and independent domains to meet both availability and integrity aspects of fault tolerance.
- Attention to common-mode failures across domains due to Sync Tree Paths

Next Steps

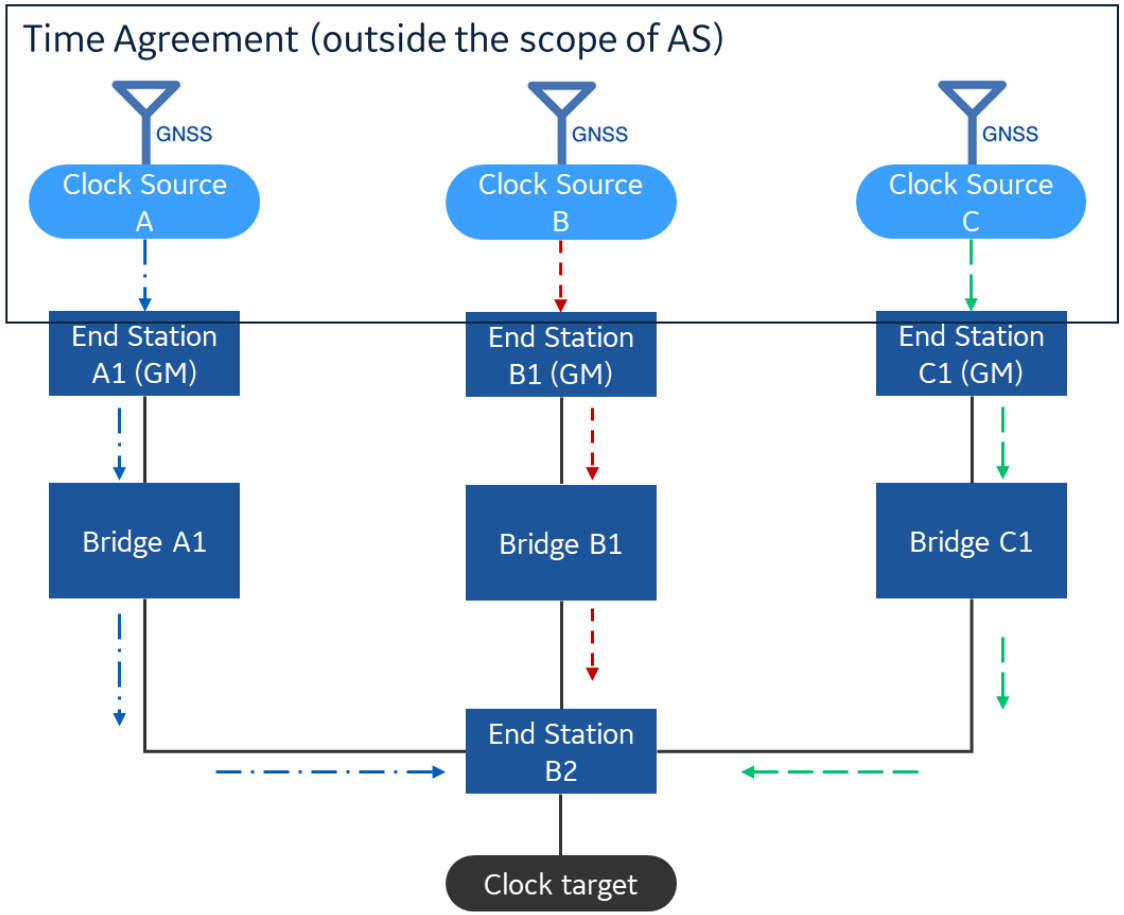
- Develop and review potential design patterns based on this core proposal
- Contributions expected from aerospace industry participants

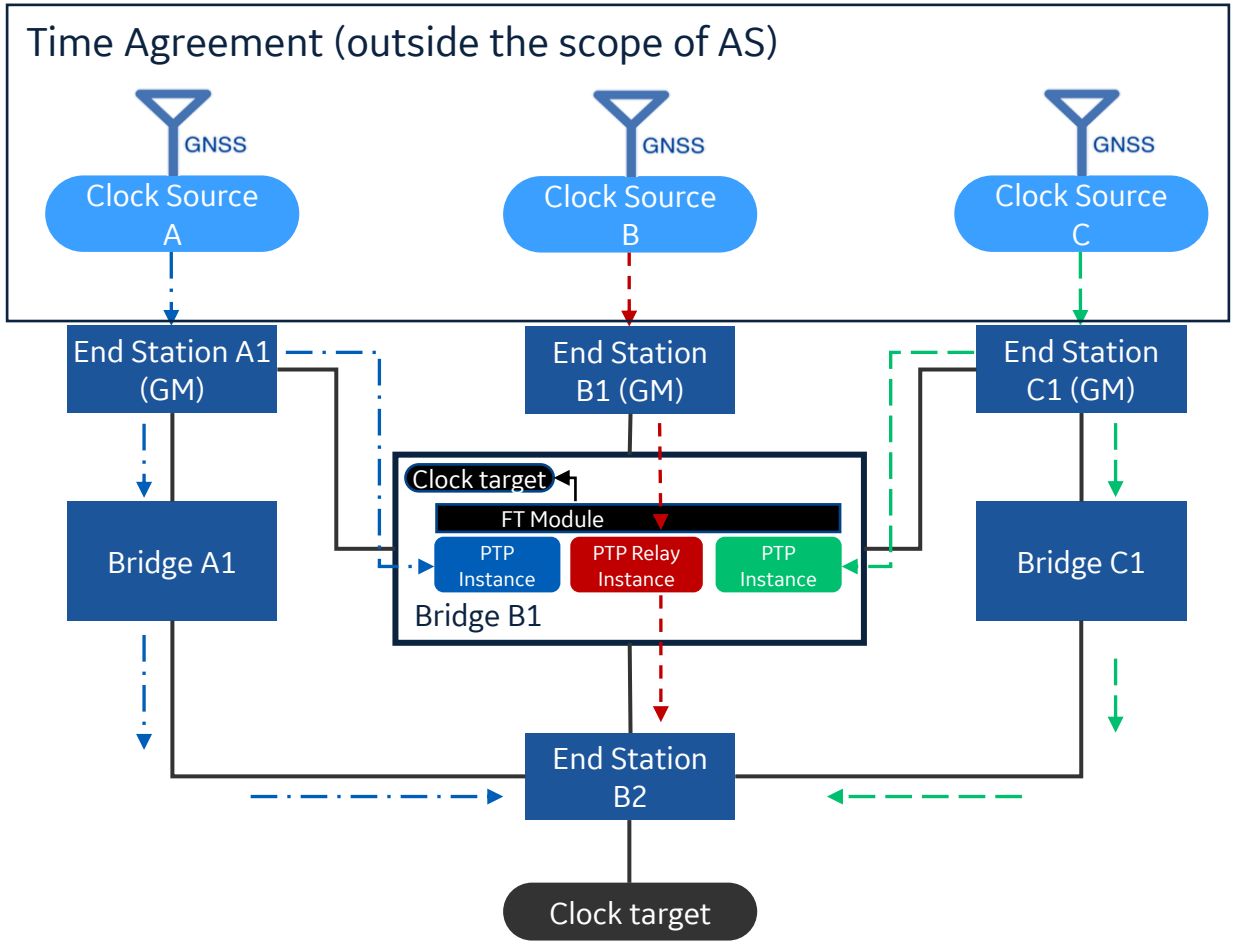
Basic Example

Domain 1 Sync Tree

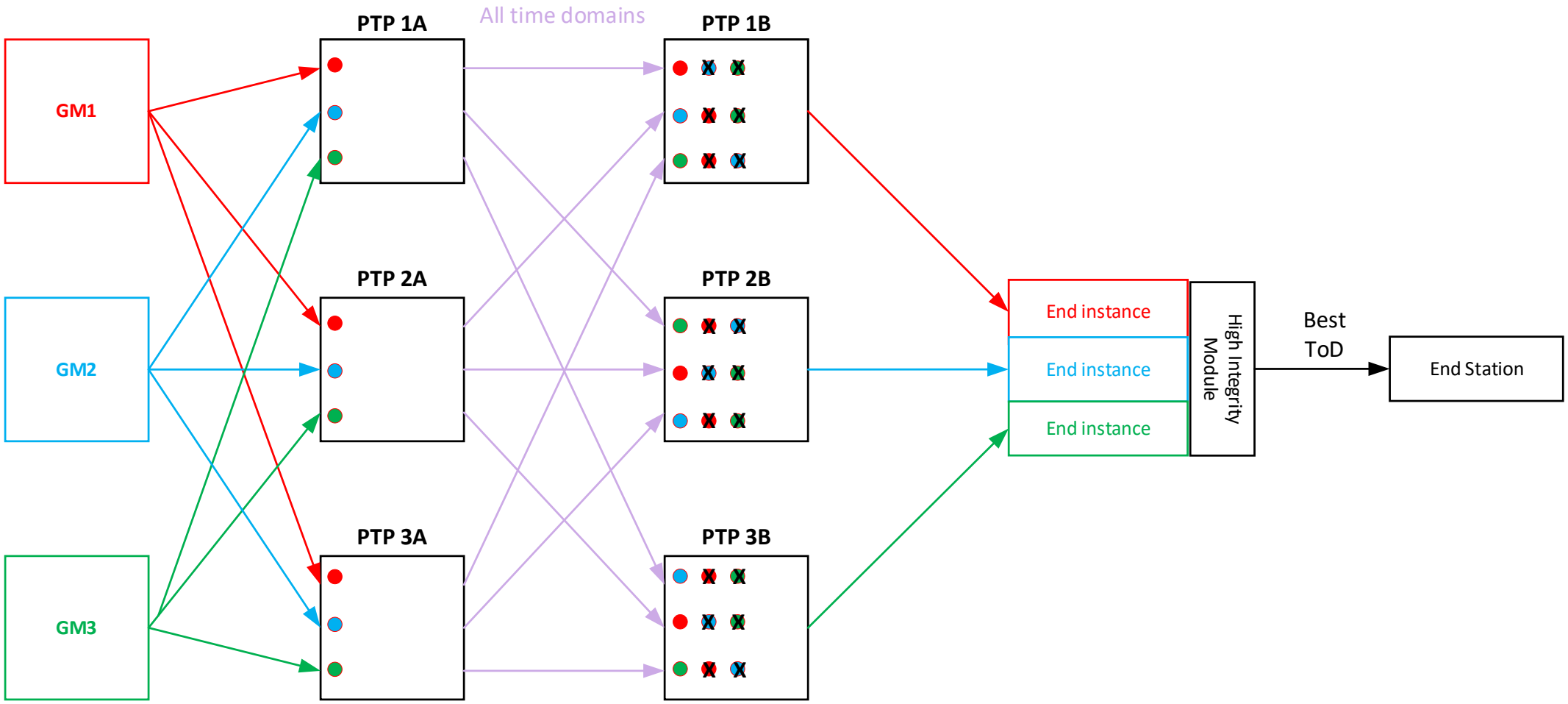
Domain 2 Sync Tree

Domain 3 Sync Tree





Example Design Pattern



Credit: Example produced by Richard Tse