# Time Sync Integrity

## *Aerospace and Safety Application*

Abdul Jabbar
GE Research

# Objective

- **Review integrity requirements for aerospace**
- **Discuss 802.1AS methods to support integrity**

# Time Synchronization Integrity

## Integrity Definition

“Integrity is the measure of the trust that can be placed in the correctness of the information supplied by a navigation system. Integrity includes the ability of the system to provide timely warnings to users when the system should not be used for navigation”

**https://gssc.esa.int/navipedia/index.php/Integrity**

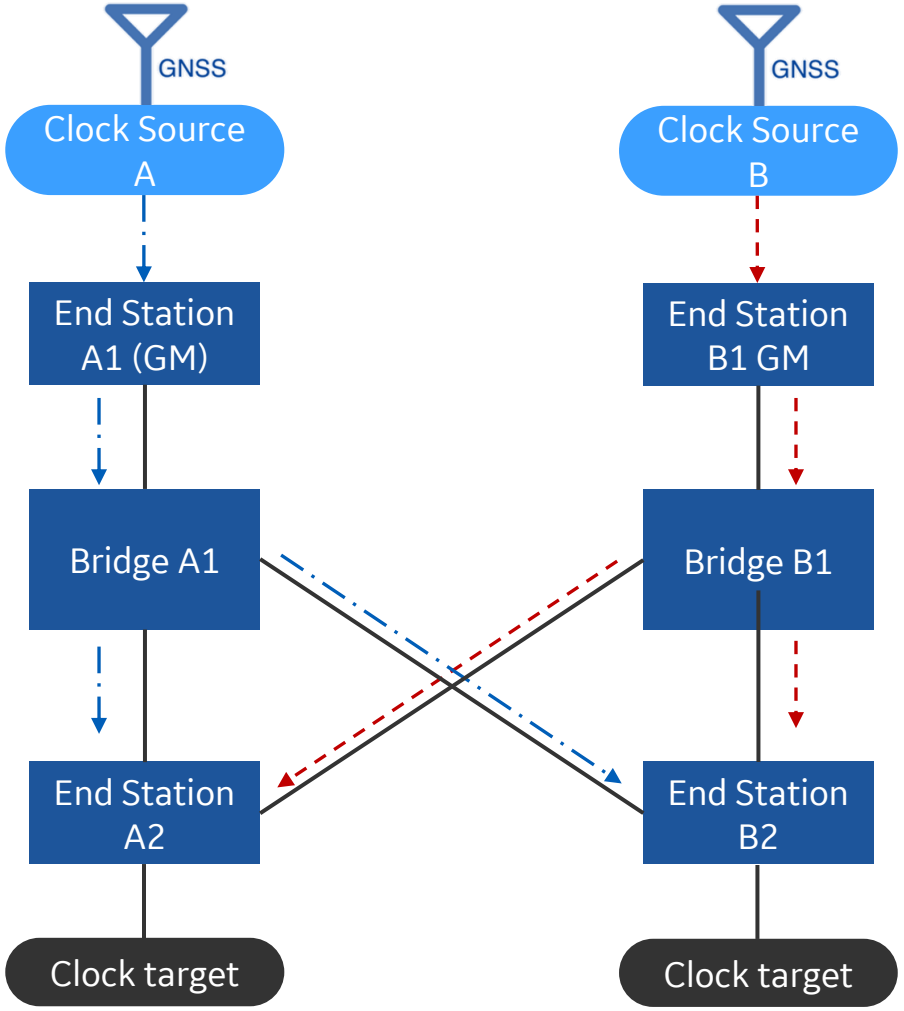
## Time Sync Integrity Definition in the context of TSN and 802.1AS

Integrity is the measure of the trust that can be placed in the correctness of the time supplied by a PTP system. Integrity includes the ability of the system to provide timely warnings to users when the PTP system should not be used for safety functions

# Time Synchronization Integrity for Aerospace

- High time integrity in the presence of link, bridge, end station, and GM faults and failures
  - Requirement to tolerate multiple (typically 2) simultaneous arbitrary faults
- Since PTP requires computations along the network path, end-to-end (higher-level) integrity mechanisms do not work. PTP must natively address integrity.
- System design is responsible for achieving the desired integrity level utilizing mostly/exclusively PTP features
- Under faulty conditions, a correctly operating end station shall be able to maintain the target max time error relative the correctly operating GM. If unable to maintain the max time error, the correctly operating end station shall detect an erroneous time sync state.
  - Assumes that system design provides for a non-faulty time distribution tree between the clock source and clock target

# Time Sync Integrity Example

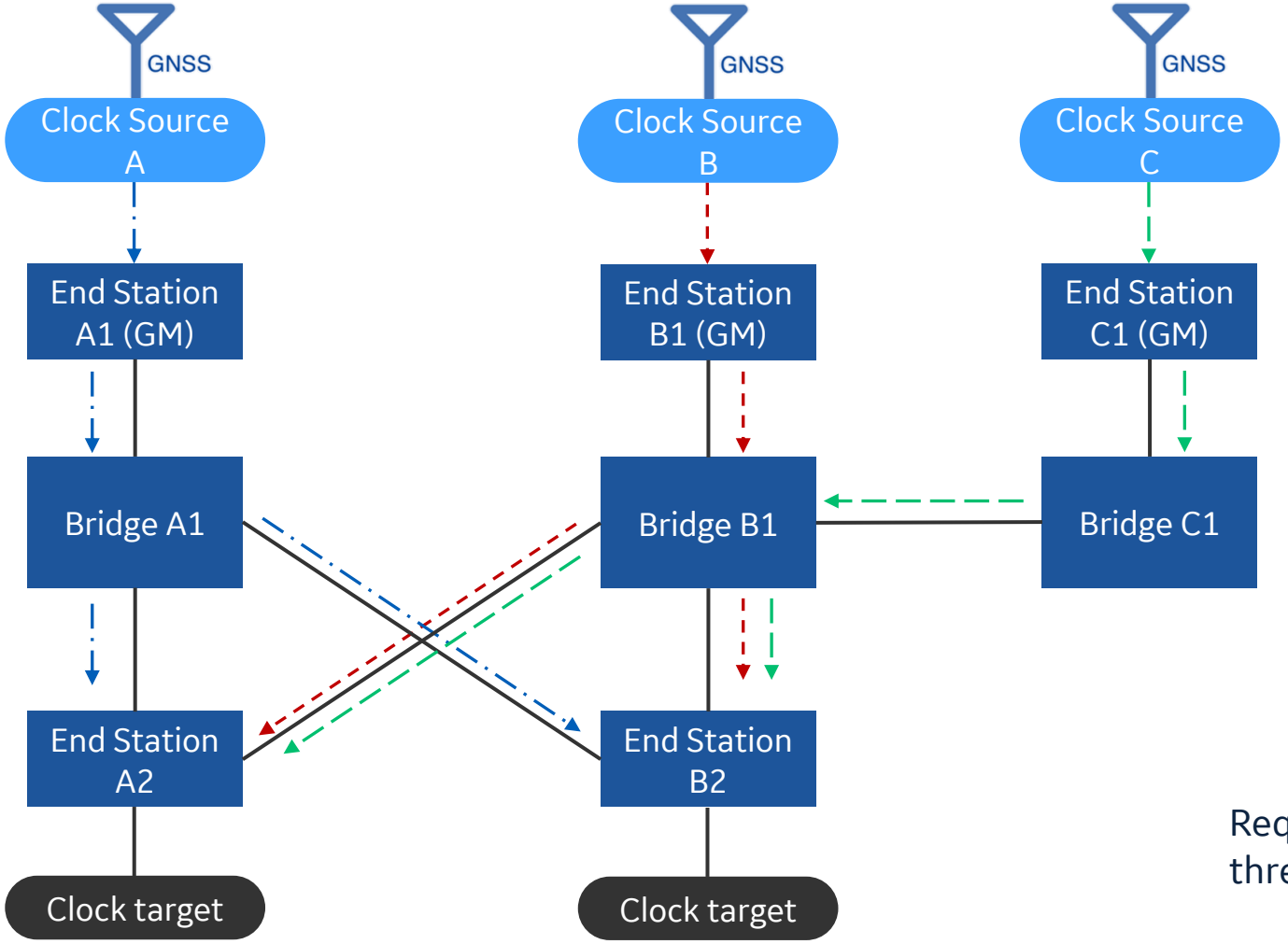



Domain 1 Sync Tree

Domain 2 Sync Tree

Requirement: Compare time value received over the two domains to detect integrity issues

# Time Sync Integrity Example



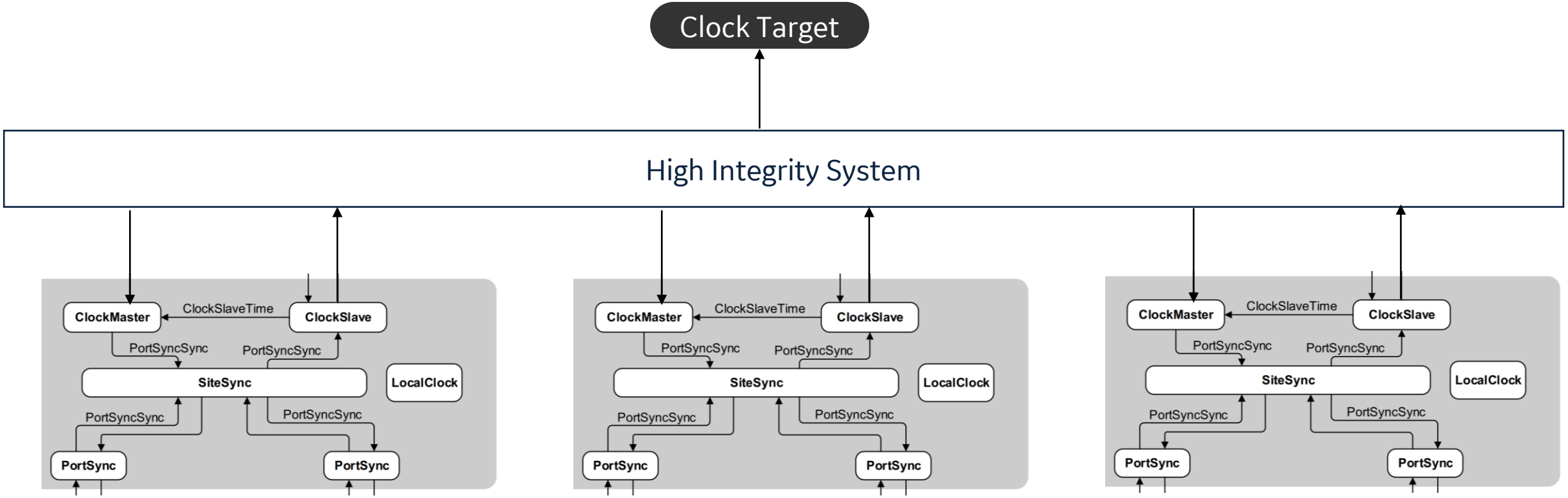

Domain 1 Sync Tree

Domain 2 Sync Tree

Domain 3 Sync Tree

Requirement: Compare time value received over the three domains to detect and correct integrity issues

# Potential Solutions?

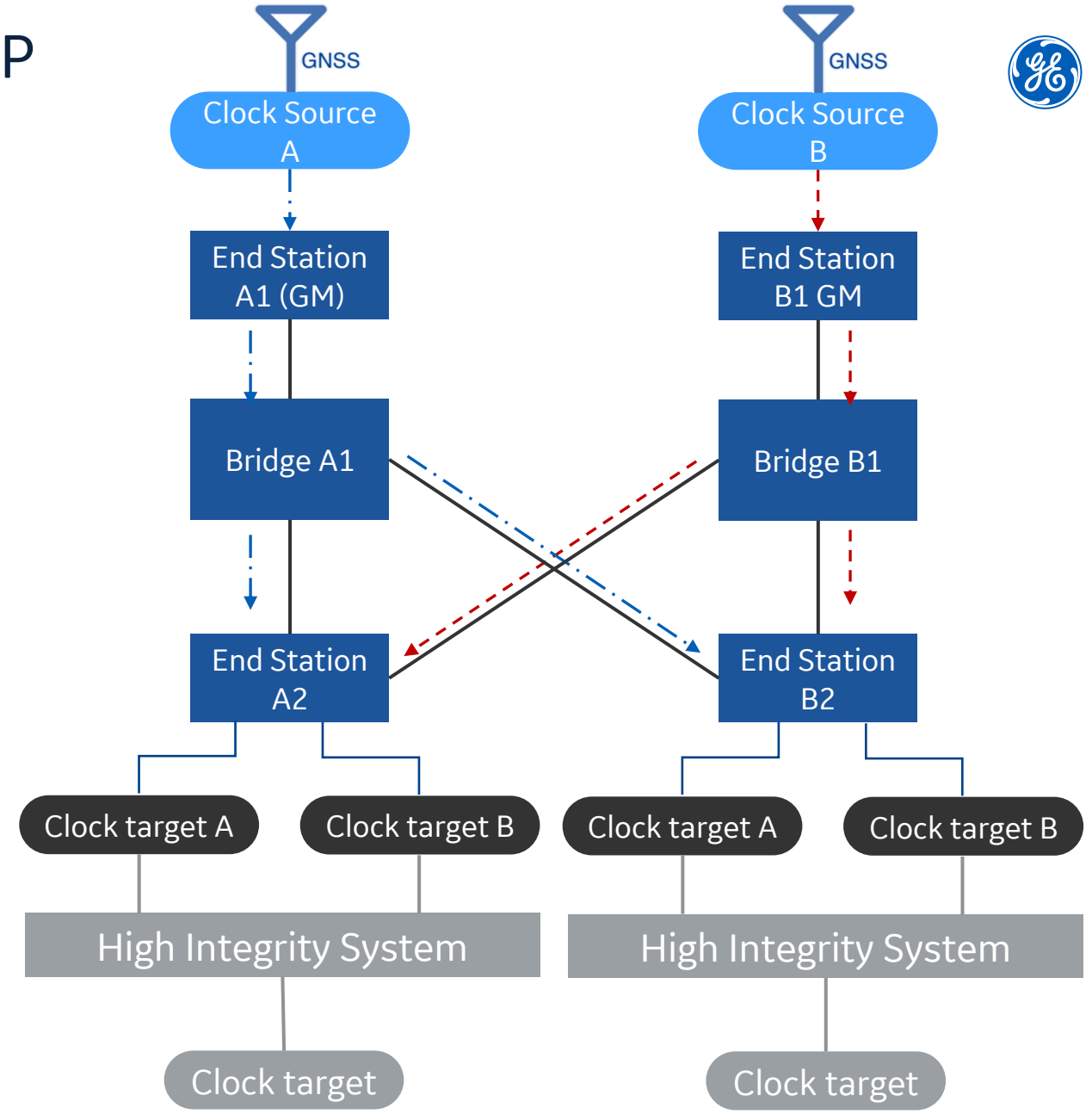


# Time Sync Integrity – Outside of PTP

Domain 1 Sync Tree

Domain 2 Sync Tree

Requirement: Compare time value received over the two domains to detect integrity issues



# Discussion

1. Practical uses will include both high availability (like hot standby) and high integrity.  It might be not possible to keep these isolated
2. Other integrity-like issues may apply to single time distribution trees as well. For example, profile defined method (state machine) for isSynced that overwrites clause 17.5.3.3 in ASdm
3. Many of the current profiles – industrial automation, automotive, and aerospace – require time sync to have integrity or integrity-like functions
4. How should we proceed?
    1. DP recommends a design pattern with application-level integrity check. Lat
    2. New project on AS for integrity and other features for safety applications – David McCall presentation
    3. Some other approach?

# Path Forward

1. 802.1 AS stays as is or takes normal development path; DP does all the heavy lifting by restricting and limiting options to the extent that is possible. Need to give profiles large leeway.
2. 802.1AS is modified (with purpose) to a accommodate the safety application use cases
   Proposal: Overhaul 802.1AS in a project to isolate core parts and make that mandatory and make everything else optional
3. Safety applications to use a completely different profile of 1588 or a different time sync protocol. Can DP still be a TSN profile, if it does not use 802.1AS
4. Aerospace and other applications cannot have a TSN profile, and the industry devolves to mutually incompatible fractured per-project solution