PTP Authentication for Secure LAN and WAN Time Synchronization in the Power Grid

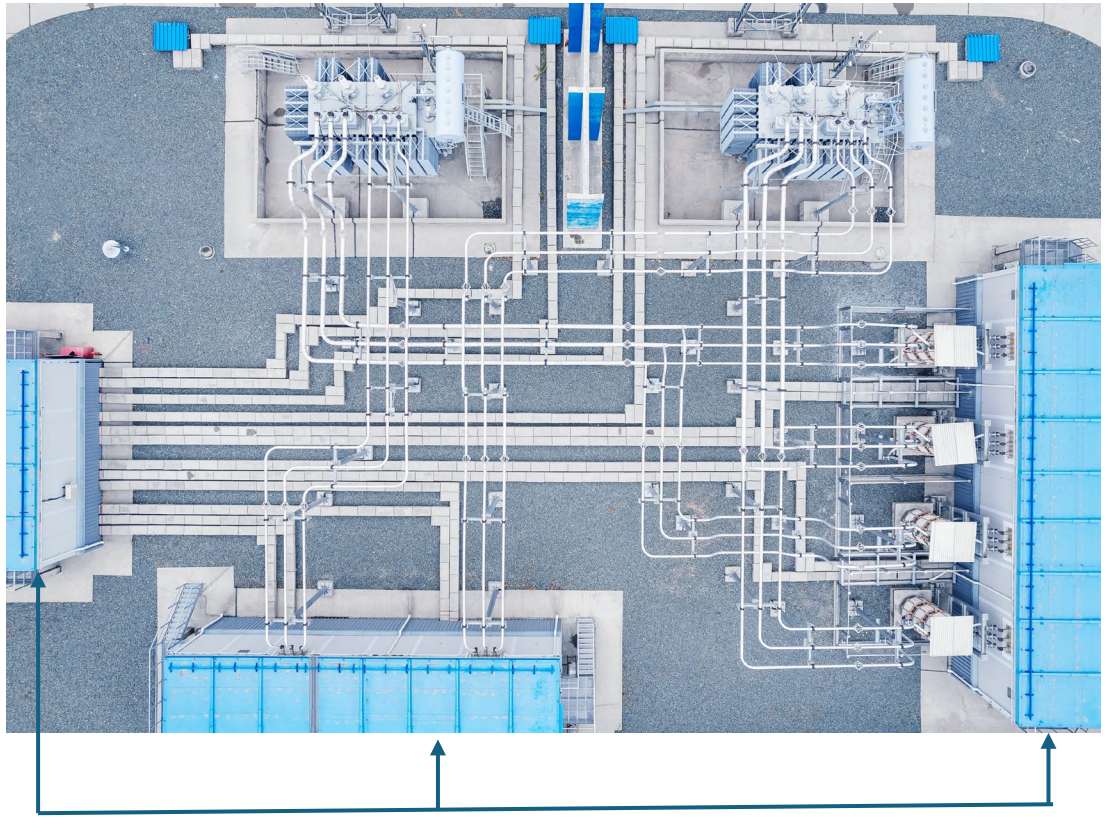
The ATIS Workshop on Synchronization and Timing Systems

May 4-7, 2026 | Bellevue, WA

To be Covered

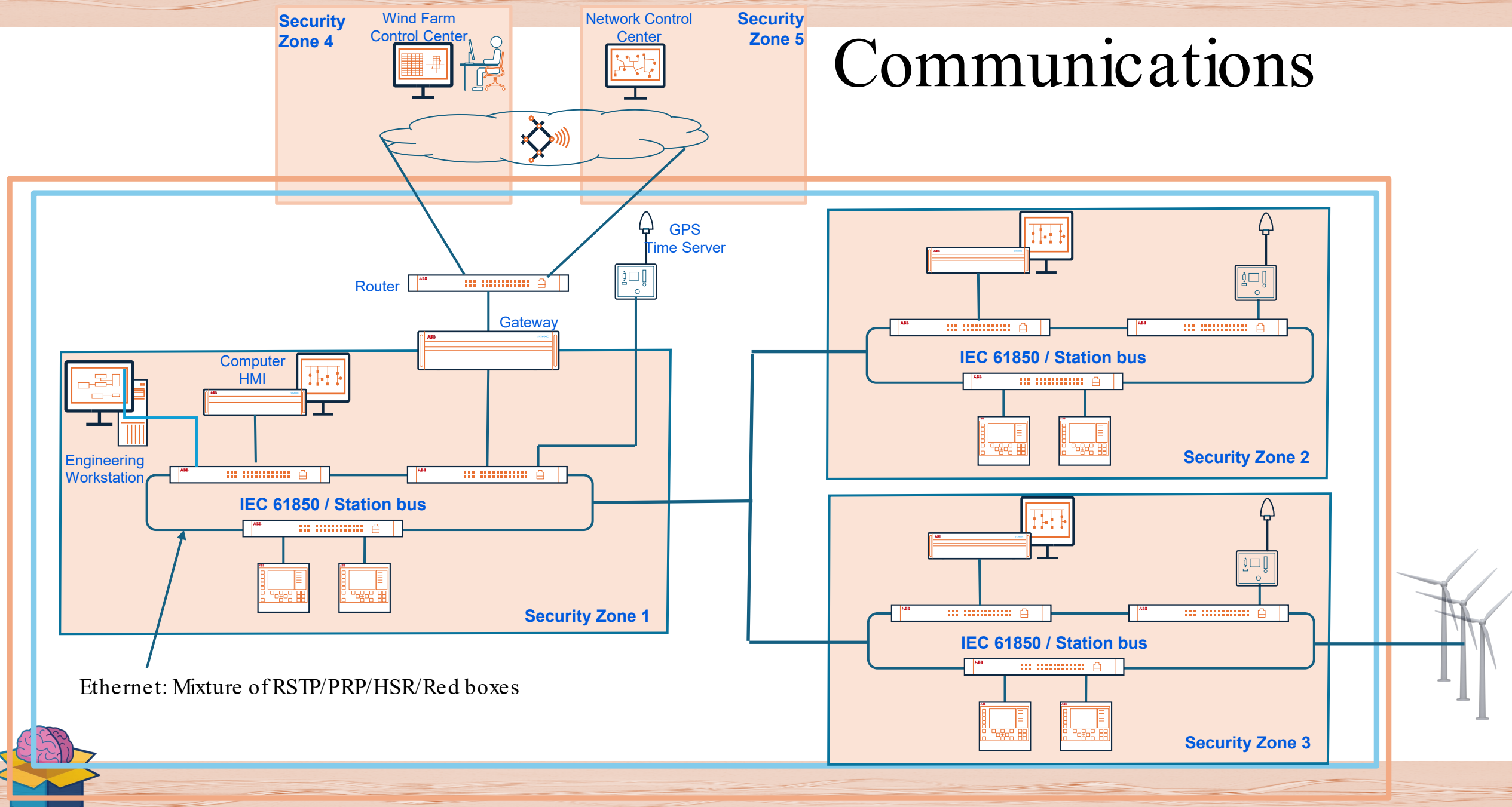
- Introduction to Substation PTP use
- PTP threat vectors and counters
  - GNSS Spoofing
  - Unauthorized Clocks
- The 1588 Authentication TLV
  - Centralized Management
  - Use in testing
- IEC 62351-9/61850- Group Domain of Interest Solution

A Typical Substation



Control House
(potentially IEC/ISA62443
Security Zone)

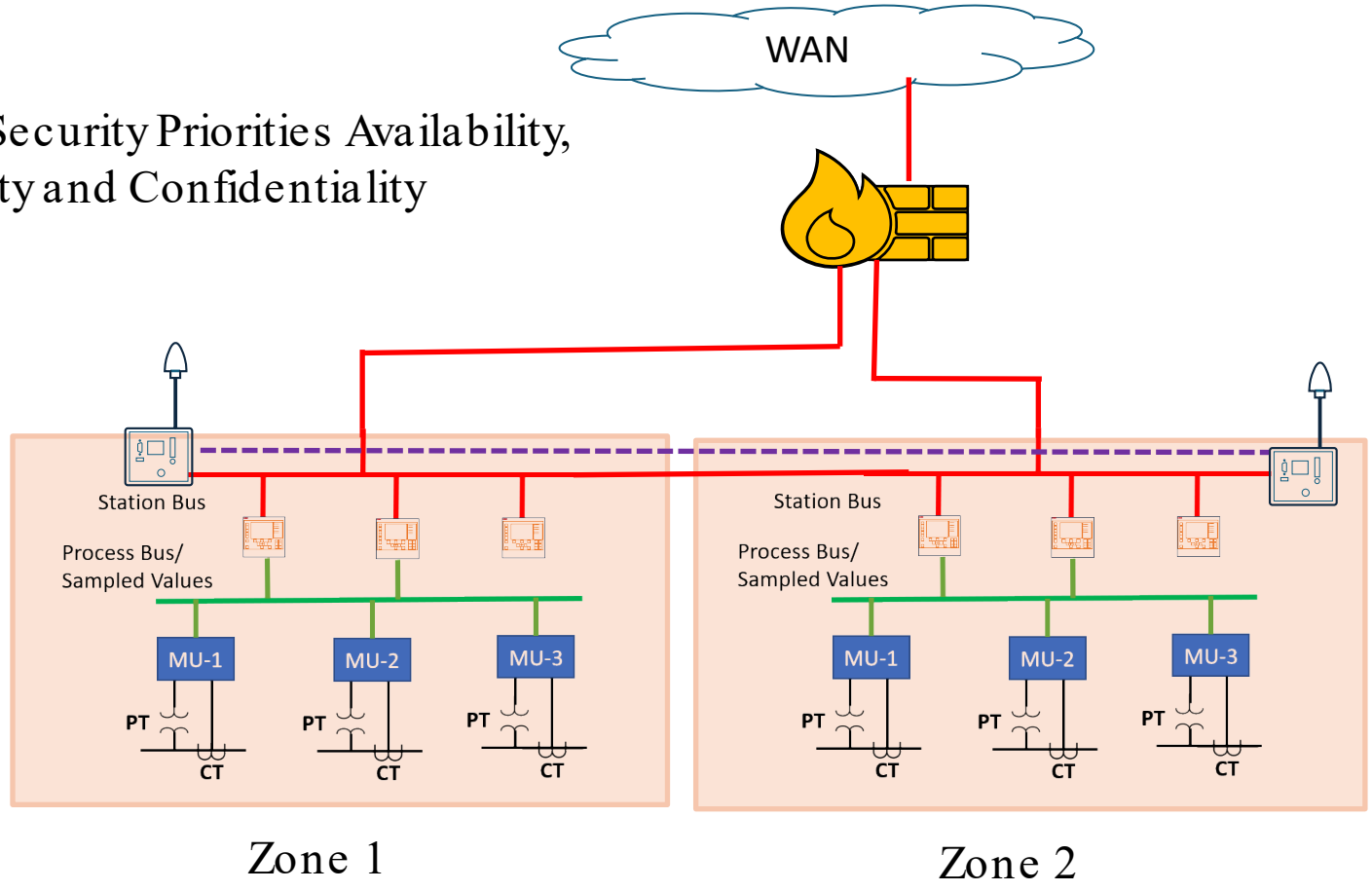
Communications



Ethernet: Mixture of RSTP/PRP/HSR/Red boxes

AIC Drives some changes – PTP Resiliency

AIC – Security Priorities Availability, Integrity and Confidentiality



Have multiple grand masters in multiple zones

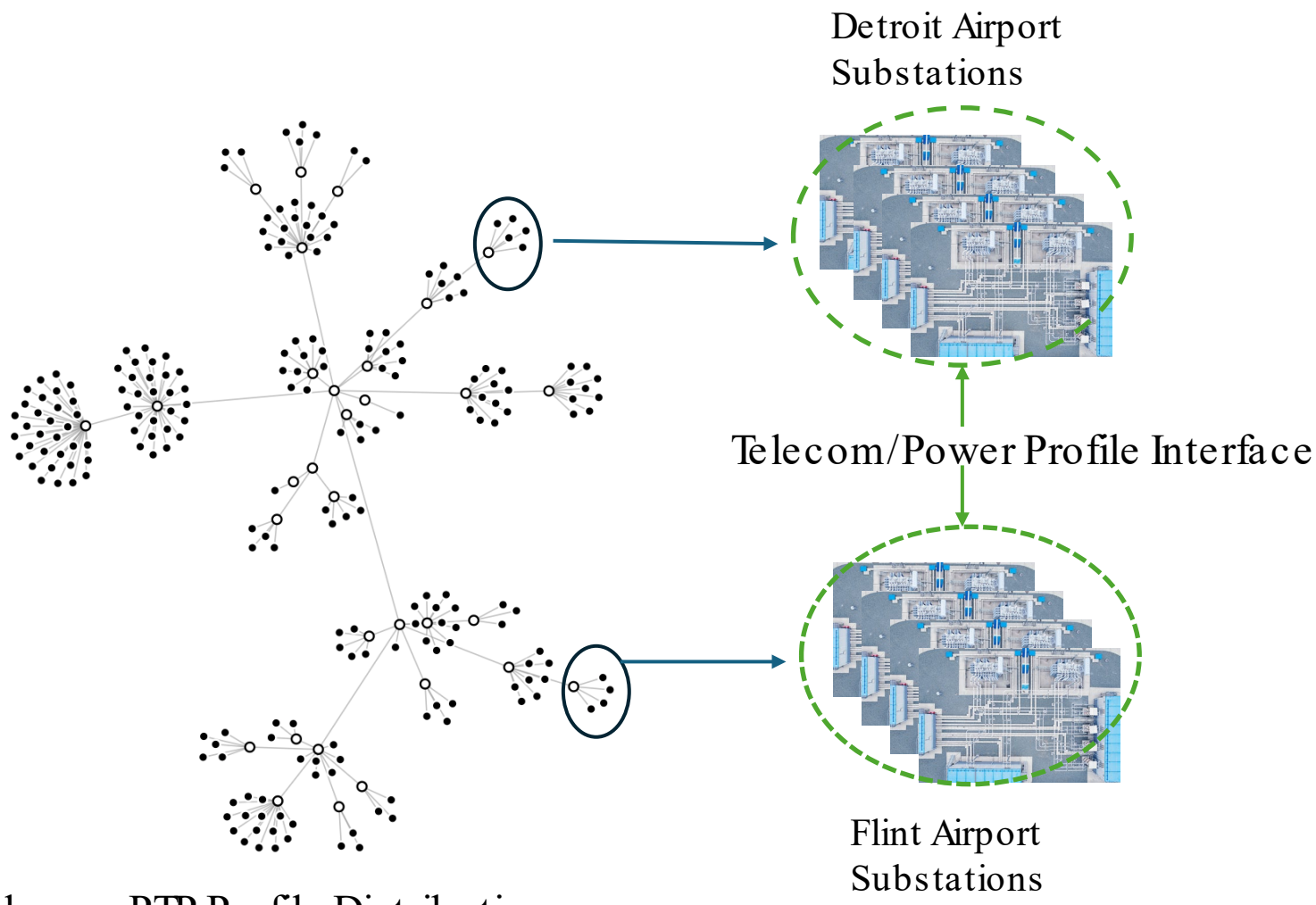
Possible Solutions:

- Deploy multiple GMs in each zone
- Deploy an adequate Boundary Clock in each zone

- Zone to Zone Security
  - Deploy point-to-point MACSec
  - Deploy PTP Security to provide Authentication (Authentication TLV).

GNSS Spoofing and Jamming

- Substations are “small” geographical areas
- Are susceptible to GNSS spoofing and jamming.
- Protection applications that coordinate between substations need to stay synchronized.
- Solution: Use terrestrial distribution of PTP (Telecom profile).



Some Observations:

- Typical large substations are 100-200 devices.
- Data Center Substations are approaching 2000-15000 devices not including Ethernet Switches
- Managing Shared MACSec keys Inhibits topology changes (Telecom and Power Profiles)
  - Difficult to Revoke a node (unauthorized or compromised)

Conclusion: Need Centralized Management

PTP Authentication TLV

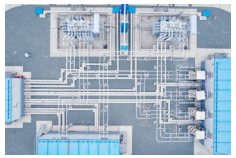
Needed Characteristics

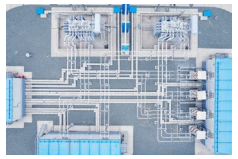
- Ability to rotate keys and policies
- Ability to remove node from

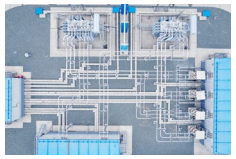
Power Profile

- Standardized as part of IEC 62351-9
- Integrates into Public Key Infrastructure. Uses X.509 Certificates
- Use of Certificates allows detection of unauthorized or revoked nodes
- Allows test equipment/Intrusion Detection Systems (IDSs) to participate in one or more PTP security domains

IEC 62351-9 (Group Domain of Interpretation)



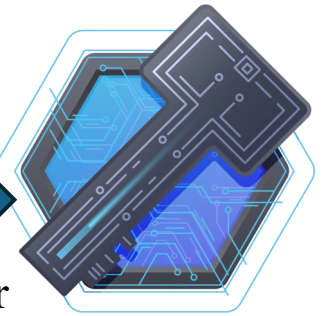




IEC 62351-9 PTP Group Definition

ptpDomain (per IEEE 1588)
ptpSubDomain (Optional per IEEE 1588)
keyMngtDomain (User assigned String)

IEC 62351-9
Key Distribution Center (KDC)



Request for domain

Each group is single use (has its own keys and policies)

Utilities tend to templatize deployments of substations:

Means: Same PTP DomainID is typically used.

Solved by 62351-9 group definition

What is delivered?

- 2 Keys used for Authentication TLV
  - Current Key with remaining lifetime (ID for key also)
  - Next Key (ID for key also)
  - Activation delay (allows either the current key or next key to be used during this period)

- Policies for each key
  - Key type
  - Authentication algorithm to use
  - Key rotation interval
  - More…

Example:

If key rotation time is 24 hours, delivery provides 48 hours of protection.

IEC 61850 IOP 2026

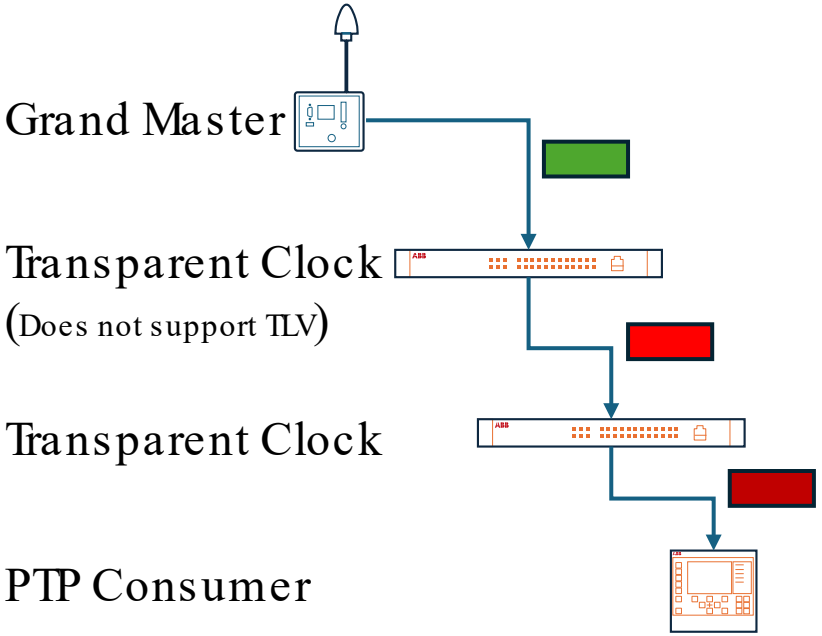
- Trying to determine the impact of an infrastructure where transparent clocks don't support the Authentication TLV.
  - Will devices lose synchronization?
  - Will power grid protection be lost?
  - Will devices crash?
  - What is the best option for the TLV's use?
    - Should it include or exclude the correction factor?
  - Impact on corrections?

Why are we discussing this…

- During finalization of IEEE/IEC 61850-9-3, found some issues some of which are in scope for 62351-9, others not.

- Just some perceptions:
  - Auth TLV is the only mechanism that provides system end-to-end integrity of PTP packets. This brings an issue that 62351-9 can address.
  - Systemic analysis (preparation for the 61850 IOP) is bringing more.
  - 62351-9 is based on the premise of single use keys (e.g., one for PTP group). What is this impact on transparent clocks?

APTP System (impact on Brownfield System?)



Why?

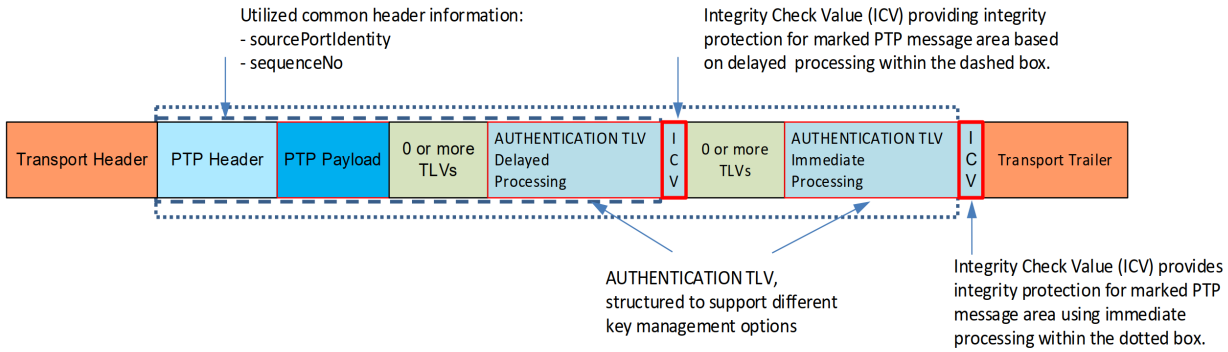
Each transparent Clock adjusts the correction factor causing the Auth TLV to be incorrect.

— Valid Auth TLV

— Invalid Auth TLV

— ? Reconstructed Auth TLV

What IEEE 1588 has to say:



The ICV calculation shall not include the ICV of the AUTHENTICATION TLV itself, However, it shall include the correctionField if required by the security policy. If the security policy does not require the inclusion of the correctionField, the ICV calculation shall use the value 0 (zero) instead of the value of correctionField when computing the ICV.

62351-9 missed this policy setting, could add it by adding an additional SA-TEK payload (rfc 8052):

Attribute	Value	Type
Reserved	0	
SA_ATD	1	V
SA_KDA	2	B
Unassigned	3-28671	
Reserved for Private Use	28672-32767	

What appears to be missing in 1588/62351-9:

- IEEE 1588: Is a reconstructed Auth TLV valid, what are the rules. May need a 62351-9 policy.

- Logging of incorrect and reconstructed or bad Auth TLVs.
  - 62351-9 could add this, but we would need to be careful. Probably don't want log every minute.

- What to do if the Auth TLV is causing systemic issues (focus on priorities of Availability, Integrity, and Confidentiality - AIC):
  - 62351-9 has no way to disable/indicate to ignore the TLV. Prefer ignore.

More information:

- IEEE 1588 clause P is being changed:
  - Management of inclusion of the correction field for the Authentication TLV
  - GDOI will be able to set the initial sequence number and window (protects from spoof and replay attacks).

    Specifics in 62351-9 are being worked on.
- UCA IOP will be testing:
  - GDOI for Auth TLV
  - Telecom-to-Power Profile conversion

Thank You

Contact Information:

Herbert Falk
Outside the Box Consulting Services, LLC
email: herb.falk@otb-consultingservices.com