Time Synchronization using PTP – Application in Power Systems & Security Options

Andrej Görbing, Steffen Fries, Siemens AG

SIEMENS

Agenda

1. Precision Time Protocol (IEEE 1588) Introduction
2. Time Synchronization in Power Systems using PTP
3. PTP Security Options
4. Outlook

SIEMENS

Time Synchronization using the Precision Time Protocol (IEEE 1588)

- Precision Time Protocol (PTP) is standardized in IEEE, latest version IEEE 1588:2019
- Enables time synchronization via packet based networks → Eliminates the need for a separate synchronization network
- Provides higher precision compared to other time synchronization mechanisms like NTP, GPS, etc. → Microsecond to sub-microsecond accuracy and precision
- As authenticity and integrity of time synchronization is crucial, IEEE 1588:2019 offers an integrated security option as well as further security recommendations
- Application area examples
  - Power system automation, e.g., protection, synchrophasor communication, fault localization
  - Industrial automation, e.g., for motion control, event stamping and correlation
  - Telecommunications, e.g., to ensure service quality (mobile networks)
  - Financial Industry, e.g., synchronize transactions

SIEMENS

PTP Time Synchronization in Power Systems: Inside Substations

- Grandmaster clocks (GMC)

  IEEE 1588 time synchronization to station bus and process bus networks

- Ethernet switches and redundancy boxes

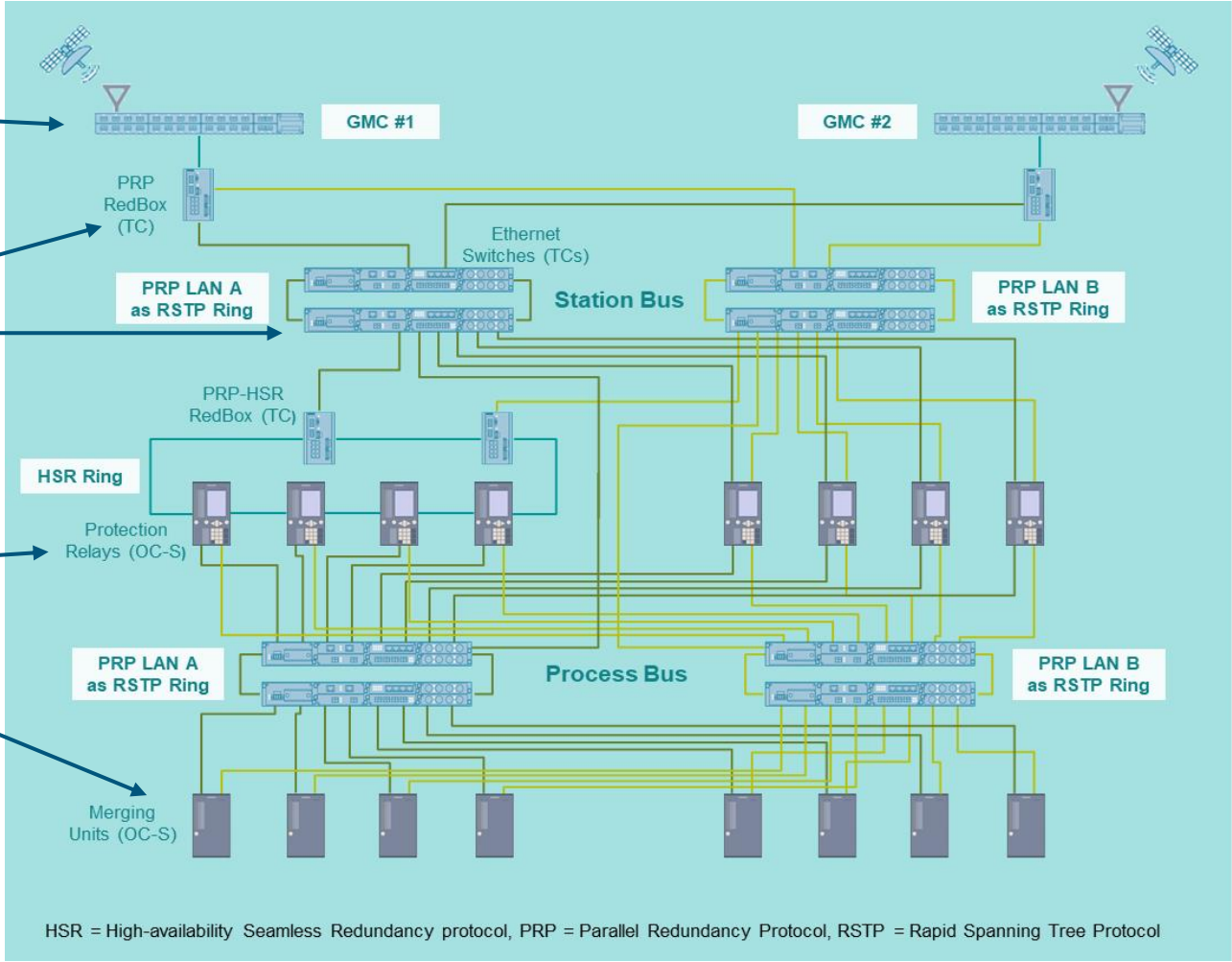
  Transparent clock (TC) or boundary clock (BC) function

- Protection relays, merging units and other intelligent electronic devices (IEDs)

  Ordinary slave clock (OC-S) function

- Seamless redundancy

  IEC 62439-3 HSR and PRP, the latter in combination with IEEE 802.1Q RSTP



SIEMENS

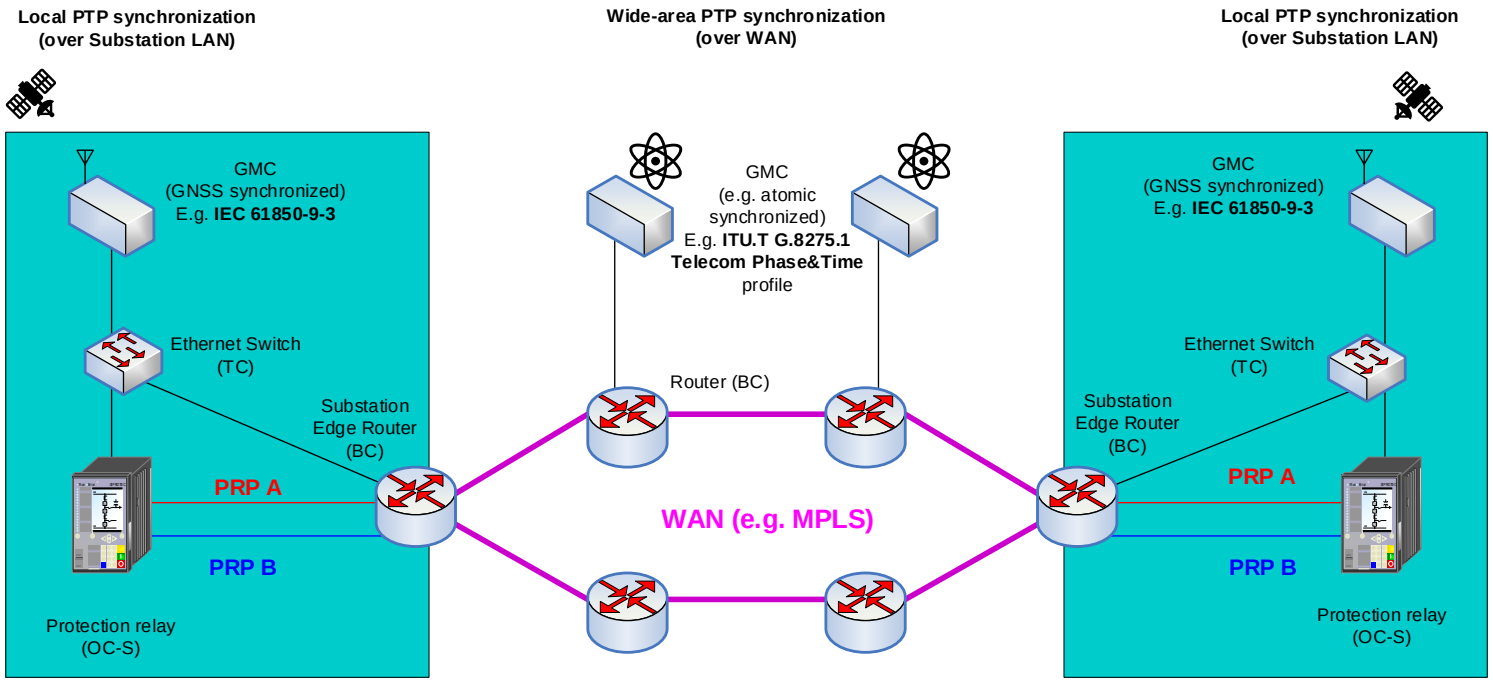
Time Synchronization in Power Systems: Two PTP profiles

- IEC/IEEE 61850-9-3:2016 Power Utility Profile
  - Based on IEEE 1588:2008 Annex F (PTP transport over IEEE802.3/Ethernet) and Annex J.4 (Peer-to-Peer Default PTP profile)
  - Requires network time inaccuracy better than ± 1 µs after crossing approx. 15 TCs or 3 BCs
  - Requires time inaccuracy of GMC < 250 ns, BC < 200 ns, TC < 50 ns, holdover time at least 5 s
  - PTP synchronization over HSR and PRP networks (optional, defined in IEC 62439-3)
- IEEE C37.238:2017 Power Profile
  - Extension of IEC/IEEE 61850-9-3:2016, especially:
  - Profile-specific IEEE_C37_238 TLV with optional 16 bit GrandmasterID and totalTimeInaccuracy
  - Optional ALTERNATE_TIME_OFFSET_INDICATOR (ATOI) TLV, according to IEEE1588:2008

- Revision of IEC/IEEE 61850-9-3:2016 is currently ongoing in the joint IEC/IEEE PSCC P20 working group

PTP Time Synchronization in Power Systems: Inter Substation

- Power substations and control centers are usually interconnected via the utility enterprise WAN (e.g. MPLS based)
- PTP synchronization from e.g. atomic clocks over WAN can be needed since utilities may not accept GNSS-driven substation PTP synchronization or require redundant synchronization for reliability reasons



- Since usually different PTP profiles are deployed in WANs (e.g. ITU-T G.8275.1) and in substations (e.g. IEEE/IEC 61850-9-3), a profile conversion / profile interworking function is needed
- This function can be realized by substation edge routers (in boundary clock role)

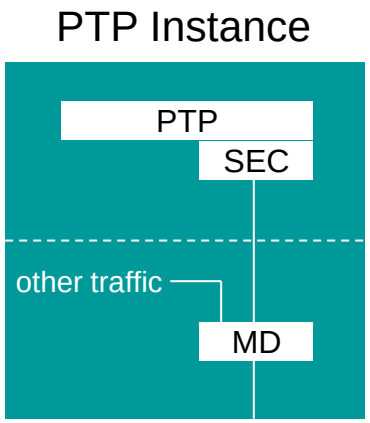
SIEMENS

PTP Security Motivation and Approach

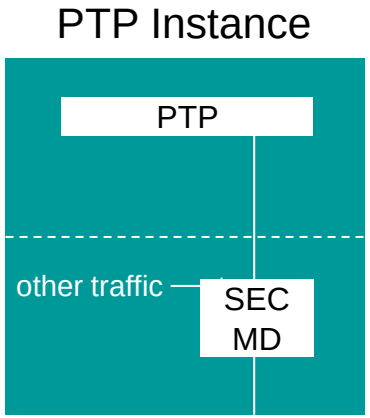
- Main thread: Unauthorized manipulation of synchronization messages to influence time based execution and audit
- Requirements
  - Source authentication → identify and authenticate PTP Instances
  - Integrity → detect unauthorized changes of PTP messages during transit
- Boundary conditions
  - Support of unicast (Provider Backbones) und multicast (Automation Environments) messages
  - Transparent clocks → intermediate components (switches) change PTP message (correction value)
- Domain specific profiles, e.g., in IEC 61850-9-3 / IEEE C37.238 for power system domain, will adopt security measures as needed

Security approaches

- PTP Instances using PTP integrated security option:
  - Prong A: AUTHENTICATION TLV



- PTP Instances using PTP external transport specific security means:
  - Prong B: MACsec or IPSec

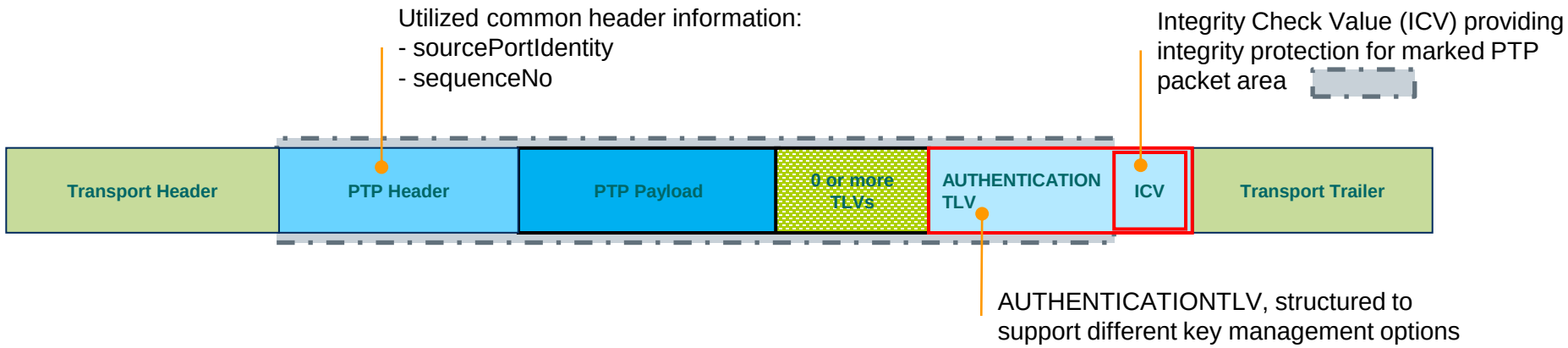


- Further Guidance
  - Prong C: Architecture means
  - Prong D: System monitoring

SIEMENS

PTP Integrated Security – AuthenticationTLV

- Approach: Enhancement of PTP packets with AuthenticationTLV to provide source authentication and message integrity

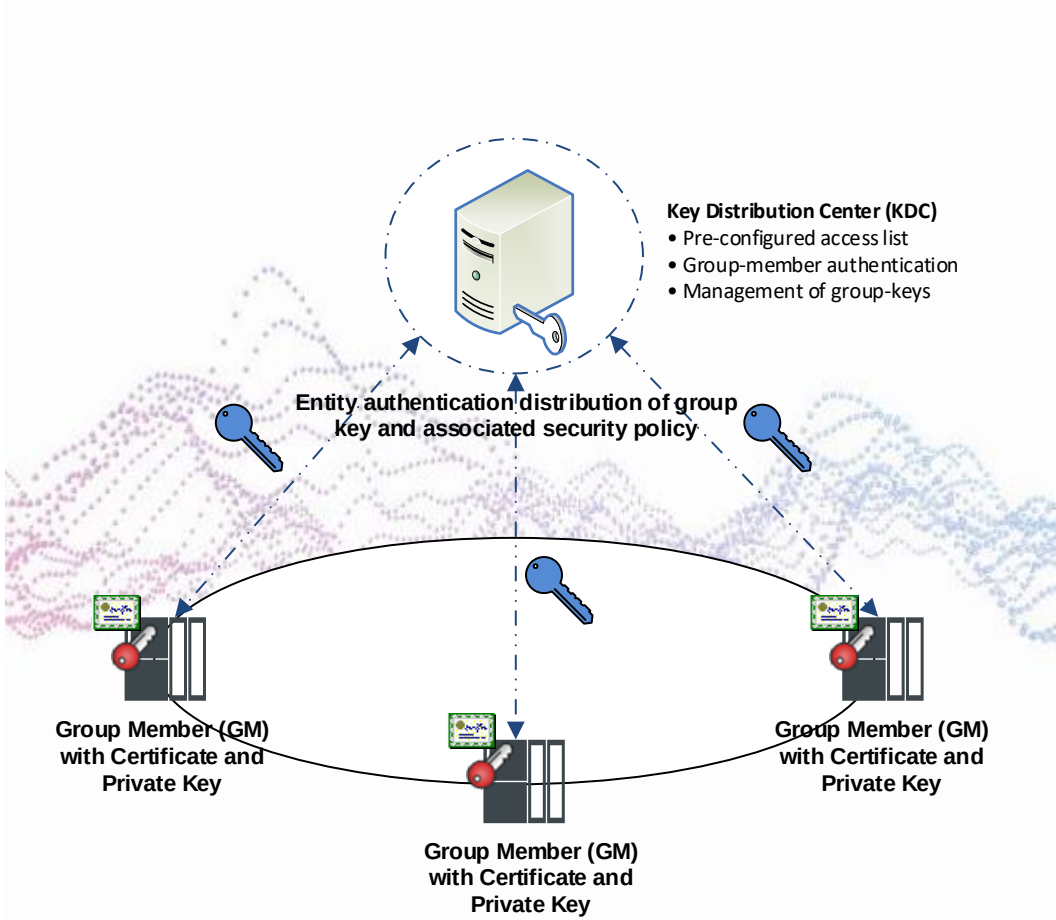


- Necessary prerequisite to enable the integrated security option is a key management to allow for automated distribution of cryptographic and security (note that manual management is also possible, but cumbersome).
- IEEE 1588:2019 refers to example key management schemes, which also support group-based communication to tackle both, unicast and multicast PTP
  - Group Domain of Interpretation (GDOI, IETF RFC 6407)
  - Timed Efficient Stream Loss Tolerant Authentication (TESLA, IETF RFC 4082)
- Further work started to enhance Network Time Security (NTS, IETF RFC 8915) to provide PTP security parameter

SIEMENS

PTP Security in Power System Automation

- Revision of IEC/IEEE 61850-9-3 for profiling of PTP for the power system domain started
- If PTP integrated option is applied, preference to utilize GDOI, as it is already used in Power Systems to distribute cryptographic key information for other power system specific communication protocols like GOOSE and Sampled Values.
  - PTP Instances authenticate towards Key Distribution Center (KDC) using PTP instance specific X.509 certificates and corresponding private keys
  - KDC distributes group key and group policy (applicable for IEEE 1588:2019)
  - Group key utilized for PTP message integrity in the context of the AuthenticationTLV
- Power system specific enhancements to GDOI can be directly applied.
- Preparation to enable using GDOI for PTP currently done in the revision of IEC 62351-9, defining key management in power system applications.



SIEMENS

Outlook

- Revised IEC/IEEE 61850-9-3 is going to specify security and security key management as optional features,
  with reference to the below standards.
- IEEE 1588 Amendment **(P1588d),** currently in ballot phase, enhances the information on using GDOI to ease the integration into domain specific PTP profiles.
- IEC 62351-9 currently in revision will specify the provisioning of parameters for PTP integrated security option using GDOI.

SIEMENS

Contact

Andrej Görbing
System Architect
Communication

Wernerwerkdamm 5
13629 Berlin, Germany
Mobile: +49 (30) 5859-23053
E-mail: andrej.goerbing@siemens.com

Steffen Fries
Principal Key Expert

Otto-Hahn-Ring 6
81739 Muenchen, Germany
Mobile: +49 (89) 7805-22928
E-mail: steffen.fries@siemens.com

SIEMENS

Contact

Published by Siemens 2021
Smart Infrastructure / Digital Grid
Humboldtstr. 59
90459 Nuremberg
Germany

For the U.S. published by
Siemens Industry Inc.
100 Technology Drive
Alpharetta, GA 30005
United States

Siemens Infrastructure – Grid Security

Siemens – Cyber Security

SIEMENS