

Protecting Time Sync Integrity in Industrial Systems: Detecting PTP Manipulation

Jack Visoky, Kevin Riederer, Todd Wiese
Rockwell Automation

October 21, 2026

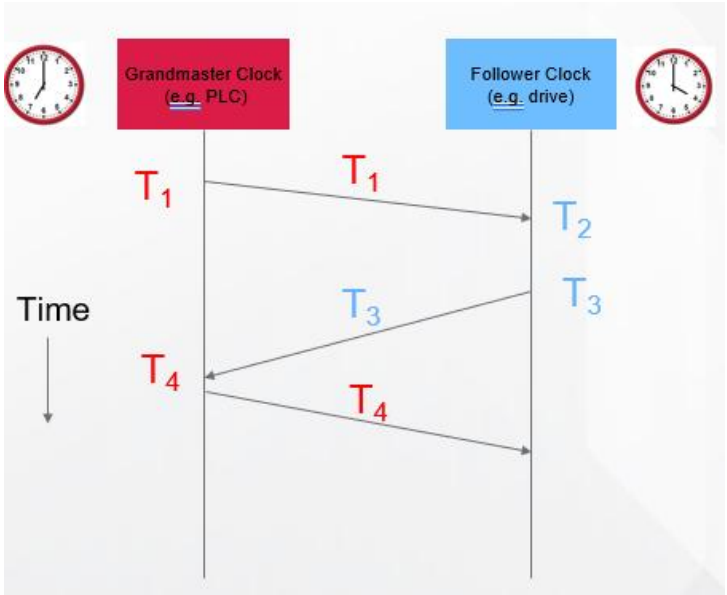
Introduction

- PTP is a time synchronization protocol used in some industrial automation products, especially motion products
- The CRA requirement for secure in transit are mostly met by CIP Security, but PTP is not a CIP protocol
- There is no clear alternative path to securing the protocol, creating a CRA gap

© 2026 ODVA, Inc.
All rights reserved.

What is PTP?

- PTP Precision Time Protocol (Also referred to as IEEE 1588) is UDP protocol that provides a mechanism to synchronize time between network nodes. Note that this is different from NTP, which is commonly used to synchronize time on IT networks
- A PTP system consists of a time server (grandmaster) as well as time clients which synchronize their clocks to the grandmaster clock.
- PTP devices periodically exchange messages that allow the following:
  - Detection of GM clock in system. If multiple clocks could serve as GM an algorithm decides which clock is best. If GM goes offline another clock can be dynamically promoted to GM.
  - Clients synchronizing time with controller. Every device has an independent clock that ticks continuously when device is powered up. The device's PTP subsystem calculates offset that translates client time to GM time (system time).



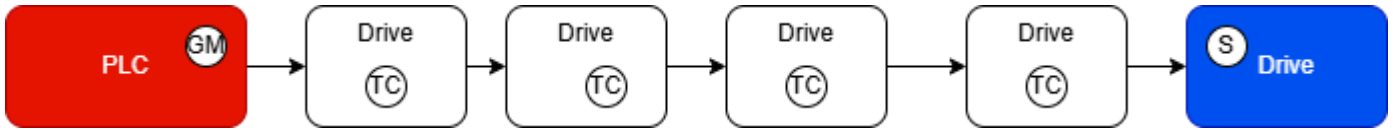
$$\text{Offset} = (T_1 - T_2 + T_4 - T_3) / 2$$

© 2026 ODVA, Inc.

All rights reserved.

PTP Hardware - Device use HW to increase accuracy

- **Hardware timestamping** decreases firmware jitter
- **Hardware tunable clock** further improves accuracy, by adjusting frequency
- **Transparent Clocks** are switches that updates PTP time fields as sync packets flow through, allowing for better accuracy, especially as number of switch hops increase



- Devices typically employ all 3 hardware mechanisms
- PTP devices can synchronize within < 100 ns accuracy (Motion applications recommend < 10 us)

© 2026 ODVA, Inc.
All rights reserved.

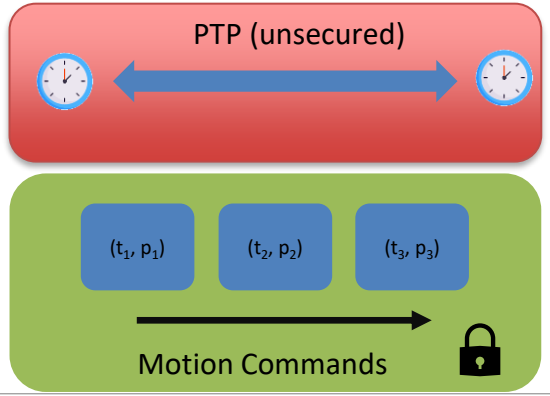
How is PTP Used in CIP Devices

CIP Motion – Used to establish a shared time base between the controller and drive. Needed to allow for synchronized motion between axes

Axis Produce/Consume – Controller feature allowing synchronization of axes between PLCs

Sequence of Event (SOE) I/O Blocks – I/O blocks that provide high-precision timestamping of digital inputs or scheduling of digital outputs using PTP time. This eliminates the polling delays typically encountered during reading I/O.







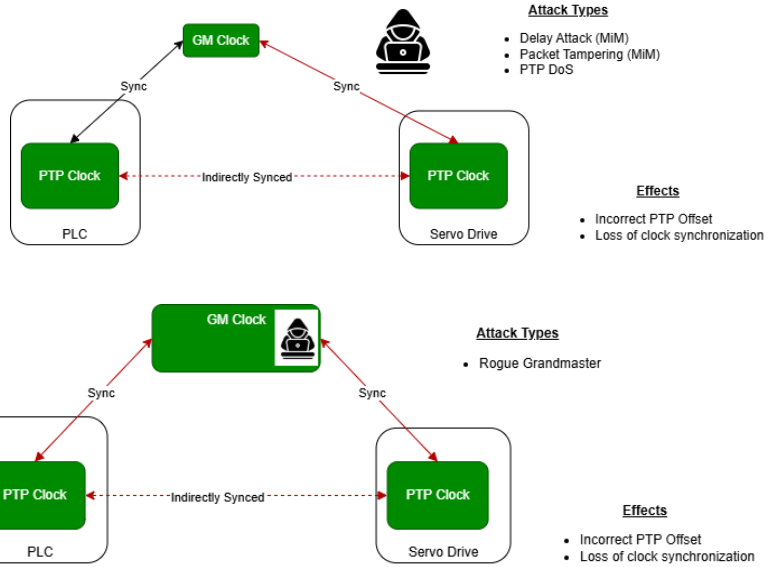
CIP Motion Drive

© 2026 ODVA, Inc.

All rights reserved.

Potential PTP Attacks

- **Packet Tampering/Spoofing (MiM)** – An attacker can intercept and modify PTP packets in route between master clock and end nodes. By manipulating timestamps in these PTP packets, the synchronization of the clock being attacked and the rest of the system can be compromised
- **Delay Attack** – Because PTP depends on a symmetric delay between sender and receiver, a man-in-the-middle attacker can intercept and delay packets going in one direction, thereby affecting the ability of the PTP client to accurately synchronize to the master clock
- **Denial of Service** – This category of attack prevents PTP packets from being transferred between master and client, thereby causing client clocks from drifting away from the master
- **Rogue Grandmaster –** An attacker can pose as a high-quality clock and take over GM role, then manipulate time



Time manipulation can manifest itself in uncontrolled motion

© 2026 ODVA, Inc.
All rights reserved.

Challenges to Securing PTP

The PTP Protocol has several characteristics that make it difficult to secure

- **Transparent Clock Functionality –** Tight accuracy depends on specialized switch hardware that modifies PTP packets as they pass through
- **Protocol is Hierarchical** – Clocks can sync to other clocks in large PTP networks.
- **Grandmaster Election** - PTP dynamically switches to best clock available (self reported)
- **Timing Attacks** – Attacker can selectively delay sync packets to affect performance, even without modifying packets
- **Legacy Device Concerns –** Any new solution would need to be rolled out across all devices in PTP domain; Potentially non-RA devices

© 2026 ODVA, Inc.
All rights reserved.

Potential Solutions

- While no complete, robust solution has been identified, there are strategies to significantly improve PTP security that can be employed
- The IEEE 1588 spec suggests (non-normative) several categories of solutions that can work:
  - **Integrated Security Mechanism -** The protocol has an optional authentication protocol that protects the integrity of the PTP packets; doesn't work for transparent clock adjustments
  - **External Transport Security** – Rely on existing transport level security protocols such as MACsec or IPsec; this requires special infrastructure and complicated configuration
  - **Architecture Mechanisms (Redundancy) –** Can implement a redundant clock or network to augment PTP
  - **Monitoring and Management Mechanisms –** Various parameters within the PTP subsystem can be monitored. When values go outside of baseline, device can fault/alarm indicating a time attack may be underway

© 2026 ODVA, Inc.
All rights reserved.

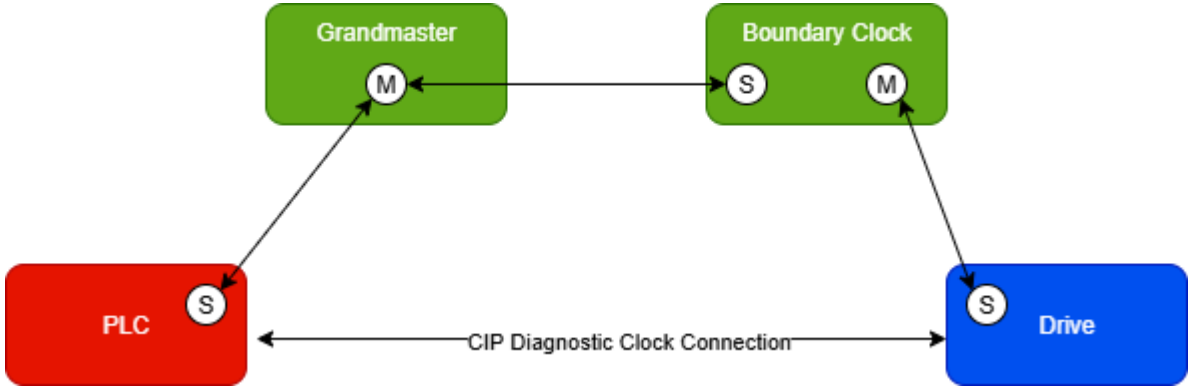
Evaluation

Selection Criteria	Weighting	Authentication TLV	MACsec	IPSec	Proposed Solution
Impact on Existing Brownfield Systems / Backward Compatibility	High	Bad	Bad	Bad	Good
Ability to Detect Time Integrity Manipulation	High	Good	Good	Good	Medium
Leverage Existing CIP Security Mechanisms	High	Bad	Bad	Bad	Good
Compatibility with Existing CIP Sync / EtherNet/IP Architectures	Medium	Good	Bad	Bad	Good
Deployment and Operational Complexity	Medium	Bad	Bad	Medium	Good
Infrastructure Independence	Medium	Bad	Bad	Medum	Good
Architectural Scalability and Future Alignment	Low	Good	Good	Good	Good

© 2026 ODVA, Inc.
All rights reserved.

CIP Diagnostic Clock

- A simplified, point-to-point version of PTP is implemented on top of the CIP protocol
- This allows us to leverage existing CIP Security infrastructure to secure protocol
- CIP Diagnostic clock would run between application endpoints in a PTP network (e.g. controller and drive)
- Diagnostic clock would be compared against PTP clock. Clock deviations would be treated as faults/alarms



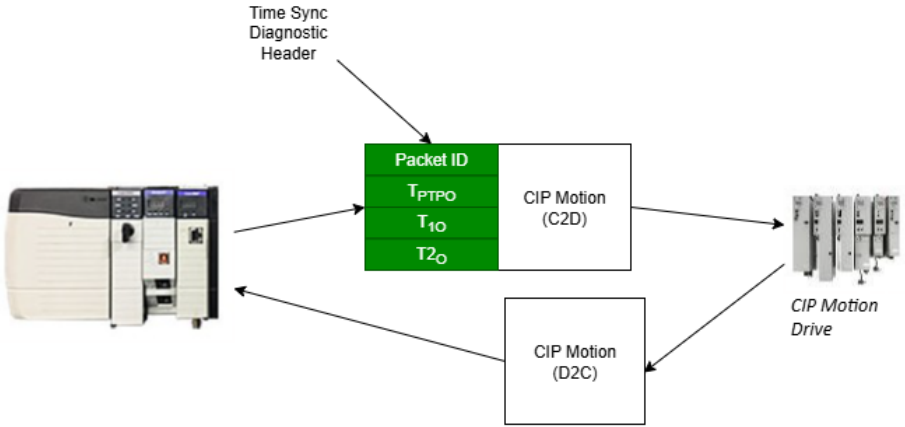
© 2026 ODVA, Inc.

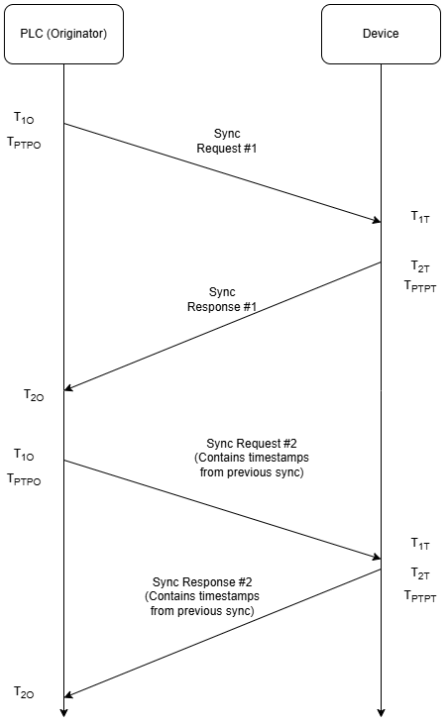
All rights reserved.

CIP Diagnostic Clock - Continued

The concept to secure PTP follows a redundant clock solution

- Timestamps needed for Diagnostic Clock added as header to O->T packets
- These timestamps allow the Target to calculate diagnostic clock offset from Originator



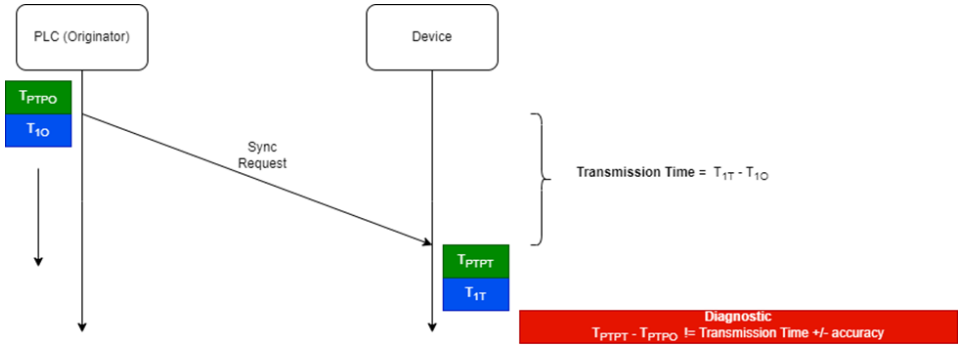


© 2026 ODVA, Inc.

All rights reserved.

Clock Diagnostic Algorithm

- I/O packets are timestamped with PTP and CIP Diagnostic Clock timestamps
- When packet is received by device, transmission time as calculated by CDC can be compared to that calculated by PTP timestamps
- If these values deviate by a big enough threshold, an alarm/fault will occur
- Threshold can be dynamically determined by how tightly the clocks are synchronized



© 2026 ODVA, Inc.

All rights reserved.

Conclusion

- Industrial automation increasingly depends on precise, synchronized time for motion control, distributed I/O, and other precision applications.
- IEEE 1588 PTP delivers required accuracy but has limited built-in security, creating potential attack vectors.
- The proposed diagnostic clock solution:
  - Provides a redundant, continuously monitored reference to detect potential PTP attacks.
  - Leverages existing CIP communications and CIP Security, enabling incremental deployment without replacing PTP infrastructure
  - Offers a practical path to stronger time synchronization security for current and future automation systems.



© 2026 ODVA, Inc.
All rights reserved.


2026
ODVA
Industry Conference and Annual Meeting