Resilient, High Accuracy Time Synchronization for Financial Industry Data Centers

WSTS 2021

Steve Guendert, Ph.D.
IBM Z Engineering/Development
Steve.Guendert@ibm.com

Abstract-Session Description

- Resiliency, security and highly accurate time synchronization are absolutely critical to banks and the world's financial system. This session will discuss (summarize) a "system of systems" technology approach that these banks use to meet their demanding requirements. This discussion will include a discussion of server time protocol (STP), processor and oscillator redundancy, monitoring, authentication, geographically dispersed data centers, and best practices for time synchronization network architectures in a data center.
- The speaker is IBM Z's Timing Team Lead/Architect and represents IBM in multiple time synch focused working groups and standards development orgs.

Agenda

- Intro: 3 Definitions
- Accuracy
- Resiliency/Security
- Recommendations

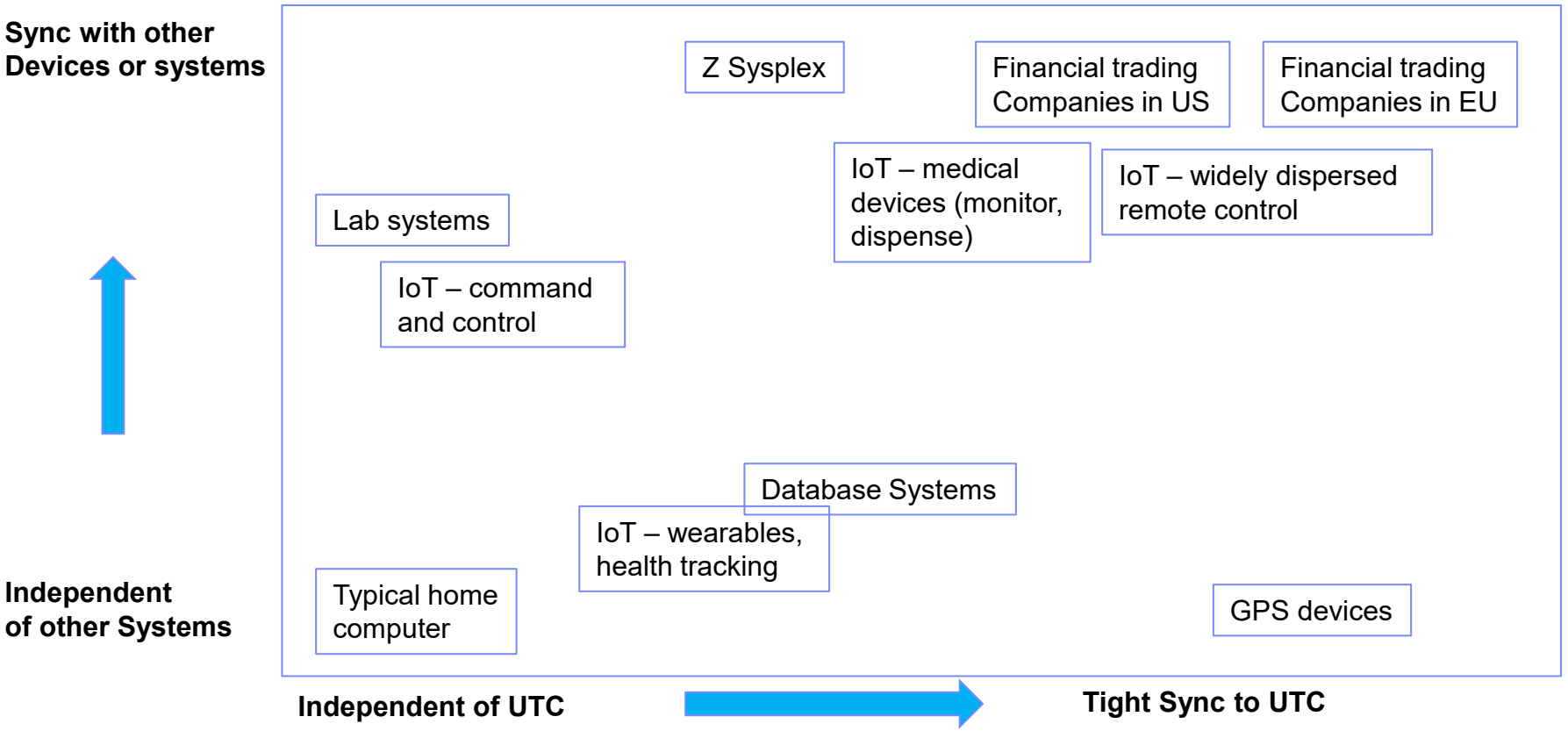
Definitions

- **Accuracy**
  - Measure of how closely a system can be synchronized to a known, standard reference (typically UTC).
  - How closely can devices within a data center be synched to each other?
  - Goes hand in hand with stability.
- **Resiliency**
  - the ability to "provide and maintain an acceptable level of service in the face of faults and challenges to normal operation."
  - Threats and challenges for services can range from simple misconfiguration over large scale natural disasters to targeted attacks.
- **Cybersecurity**
  - the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Accuracy

2 aspects of accuracy in the data center

Examples of the differences



Accuracy

- Compliance with financial industry regulations
  - FINRA/CAT, MIFID II, PCI, etc.
  - Typically require within “x” of UTC, and level of granularity
- Data integrity
  - Parallel processing sysplex (cluster) OLTP environments
    - Stratum 1 server connected to PTP/NTP external time reference
    - Uses Server Time Protocol (STP) to keep up to 32 coupled servers with multiple LPARs within 10 µsec of each other
- Oscillator technology used in the server
  - Oven Controlled Crystal Oscillators (OCXO)
  - Emerging atomic clock on a chip technologies
- Hardware vs software/OS timestamping
  - PTP
  - Network card technology

Threats and Risks to Accuracy

Inaccurate time on systems can lead to a variety of issues for the enterprise

- Failure to satisfy regulations and/or SLAs
- Disruption of applications and services (especially crypto)
- Loss of data (data integrity)
- Impact on effective troubleshooting and forensic efforts

Resiliency and Security

Go hand in hand with each other

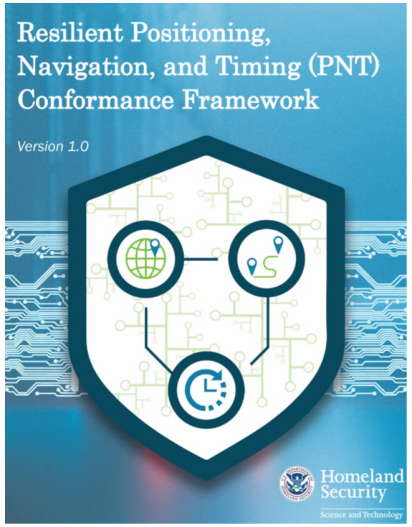
Resiliency

- Finance/banking industries are intimately familiar with resiliency best practices
  - Multiple decades of business continuity planning
- **High availability (HA)**
- Resiliency of time synch networks has become increasingly important
  - US Federal Govt. “attention”
- GPS was never intended to be the nation’s time standard. However……
  - Low barrier to entry, precision, and wide availability have made GPS the de- facto national reference.
  - At the same time, such wide adoption means its vulnerabilities pose a near-existential threat.
- Resilience arises not just from individual component capabilities (such as holdover devices or new external time reference sources), but also how they are architected

High Availability and time synch

- Directly related to resiliency
- Dedicated network for time synch?
- “Five 9s” or better network for time synch?
  - Switch characteristics, network design, multiple adapters on servers
- Use GPS/GNSS? Backup/alternate?
- Do multiple sites need to be synchronized? Over what distance?
  - Geographically Dispersed Parallel Sysplex (GDPS)
- Power/cooling?
- Redundant external reference sources?

DHS Resilient PNT Conformance Framework

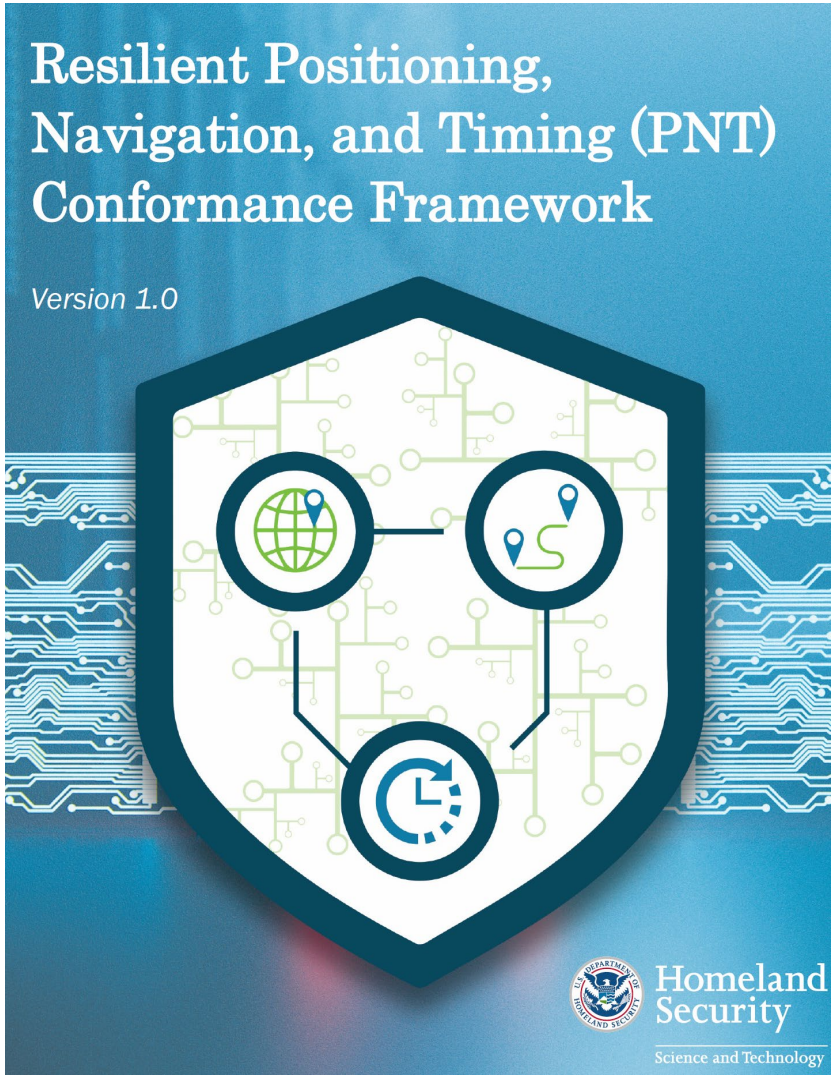


- Sponsored by U.S. Department of Homeland Security Science and Technology Directorate.
  - Developed in coordination with industry and federal agency experts.
- Core functions: Prevent, Respond, Recover
- Contains four levels of resilience so that end-users can select a level that is appropriate based on their risk tolerance, budget, and application criticality.
- Resilience arises not just from individual component capabilities, but also how they are architected within PNT systems.
- Defense in depth
  - Resilience should be designed and incorporated throughout the entire processing chain and system (via the core functions).
  - Diversity of both PNT sources and resilience mechanisms will increase the robustness of the implementation

4 Resilience Levels

- **Level 1: Able to recover from what happened**
- **Level 2: Able to continue, but in a degraded state**
- **Level 3: Able to continue, “bounded” degradation**
- **Level 4: Able to continue with no degradation**

Levels are cumulative, with requirements in each level carrying over into the next. This results in higher levels corresponding with greater resilience.



Threats to the protocols (network and time)

- **Network protocols themselves**
  - Consider having a dedicated internal time synch network to mitigate
- **Time protocols (NTP and PTP)**
  - Originally, not much of a concern about security of time
  - NTP: Publicized vulnerabilities in 2010s, (Autokey vulnerability)
    - Led to development of NTPv5 and to NTS RFC development work in the IETF
  - PTP
    - Originally treated as optional starting with 1588-2008 (optional annex)
    - As adopted increased and expanded into new industries (Finance), by 2019 it was a more integral part of the new IEEE-2019 standard.

Time protocols and security

- **RFC 7384:** Security Requirements of Time Protocols in Packet Switched Networks **(2014)**
  - Threat modeling
  - Pointed out the issues/vulnerabilities/threats with recommended remedies
- **Authentication mechanisms**
  - Verification that you are receiving time from a trusted source (who you think it is)
- **Encryption Mechanisms**
  - Does time info/data truly need to be encrypted?
  - Impact on performance/accuracy?
  - Internal requirements for network security
- **Quantum safe??**

PTP Specifics Annex P: 4 Prong Approach to Security

- **PTP Integrated Security Mechanisms (Prong A)**
  - Section 16.14 Authentication TLV
    - Immediate security processing: the Group Domain Of Interpretation (GDOI) method defined in IETF RFC 6407
    - Delayed security processing: the TESLA method defined in IETF RFC 4082
- **External Transport Security Mechanisms (Prong B)**
  - MACsec
  - IPsec
- **Architecture Guidance (Prong C)**
  - Planned redundancy
- **Monitoring and Management Guidance (Prong D)**

Thoughts on Improving Time Synchronization Network Resiliency

- Discussions on resiliency are about the triad of high availability, redundancy, and security
- The Global Positioning System is not about position, its about time
  - Need to have a backup plan
  - What are you going to do?
- Network security vulnerabilities due to network design, poor habits, or protocol vulnerabilities
- Dedicated network for time synchronization?

Thoughts on Improving Time Synchronization Network Resiliency

- Time synchronization information is not a secret-it does not need to be encrypted
  - However, some end users require all networks to be encrypted
- Robust authentication must be used
- PTP standard's security annex should not be considered "optional"
- Accuracy is important, but not the be all end all
- Standards need to incorporate resiliency (security). The argument that its incorporation hurts performance may be valid, but not valid enough to exclude

If you don't have enough resiliency, and something bad happens, is anyone going to care about what kind of performance you had

Recommendations-call to action

- **If you use GPS to provide your time, do you have a plan for a backup? If not, get one.**
- **Read the DHS Working Group Document**
  - How can you implement its ideas?
- **Familiarize yourself with the latest security aspects of your time protocol and implement them**
  - Security is not “optional”