The Flip:
More Robust Timing Applications using GPS

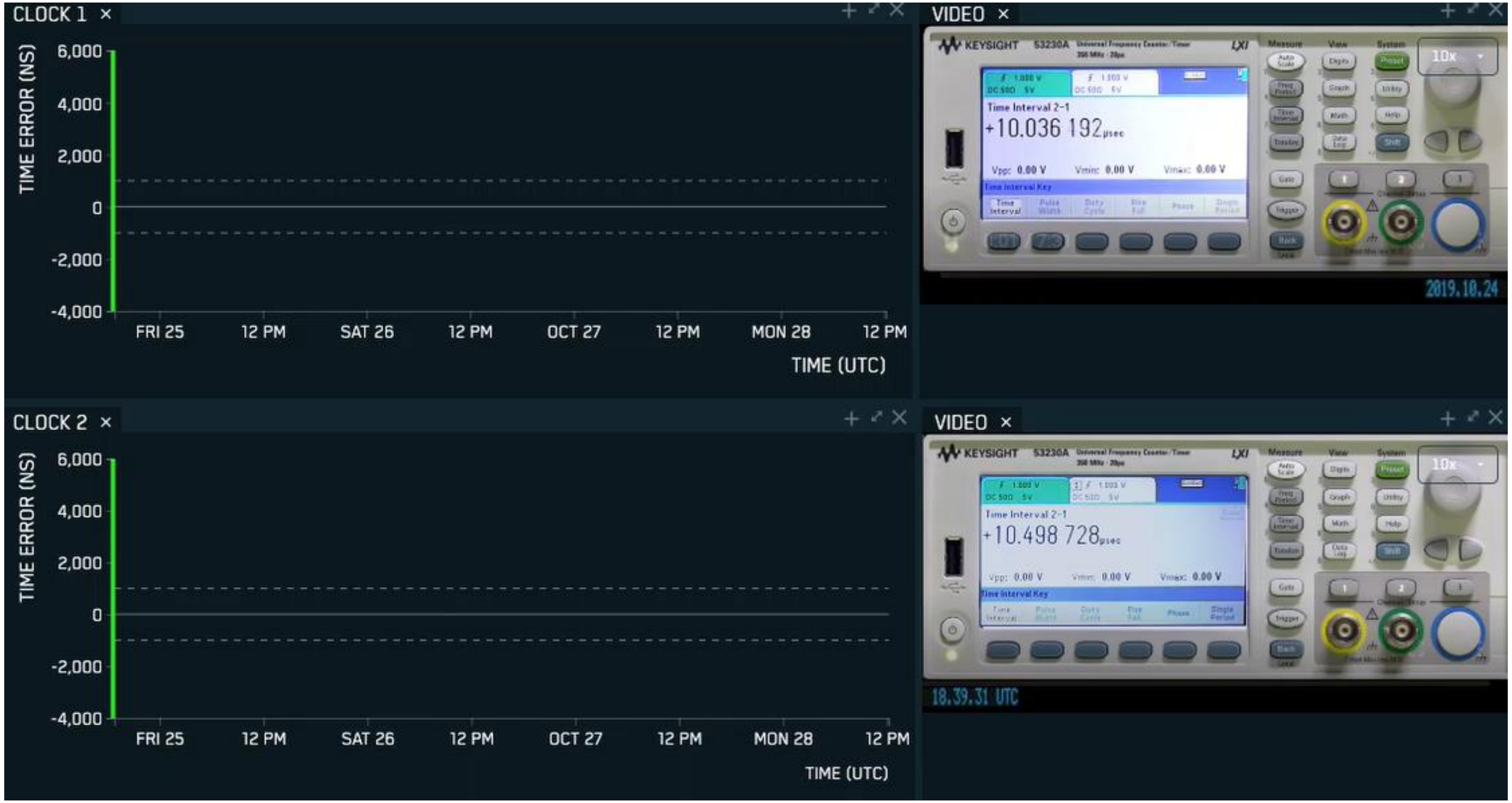
The research in this presentation was conducted under contract with the U.S Department of Homeland Security (DHS) Science and Technology Directorate (S&T), under task order 70RSAT19FR0000040. The opinions contained herein are those of the contractors and do not necessarily reflect those of DHS S&T.

HSSEDI POC: Dr. Arthur K. Scholz
ascholz@mitre.org

HSSEDI is a trademark of the U.S. Department of Homeland Security (DHS).
The HSSEDI FFRDC is managed and operated by The MITRE Corporation for DHS.

Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

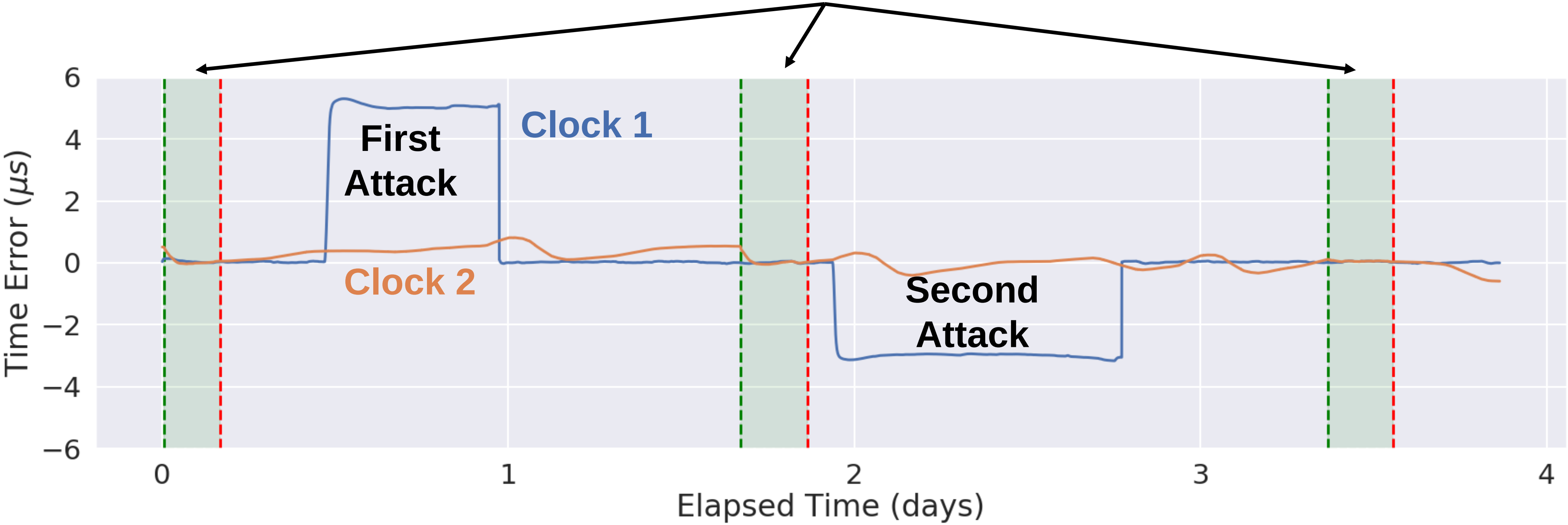
A tale of two clocks…



Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

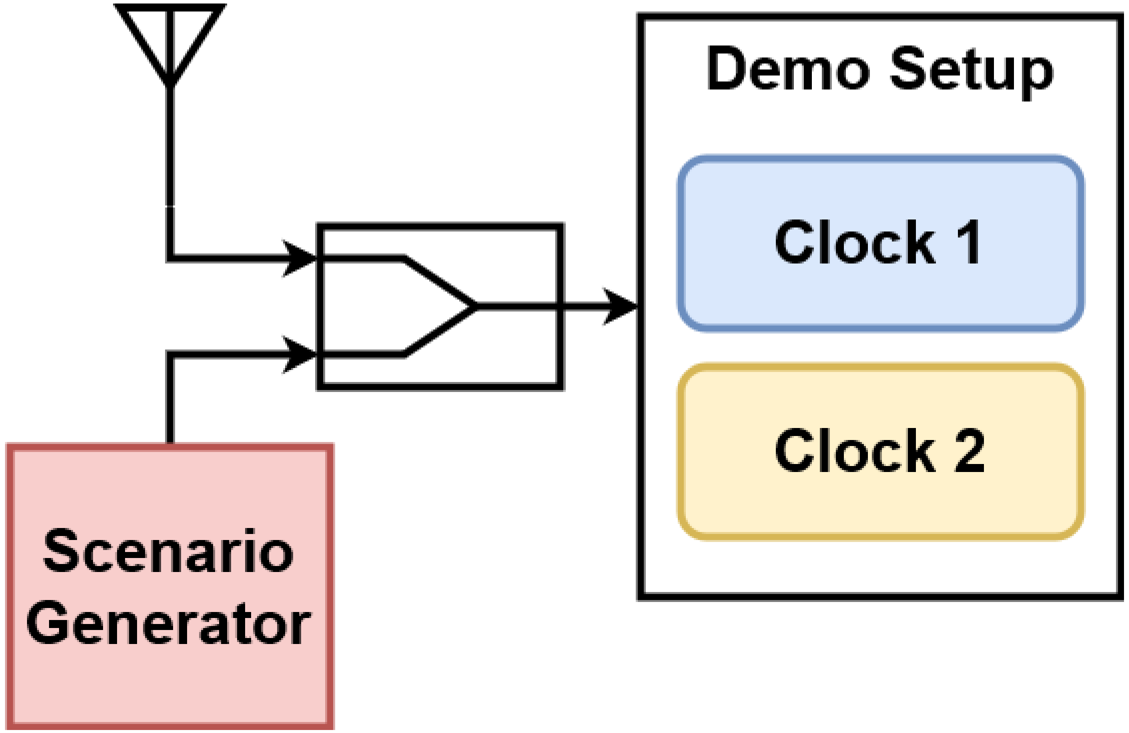
Scenario Review

Intermittent Disciplining of Clock 2



Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

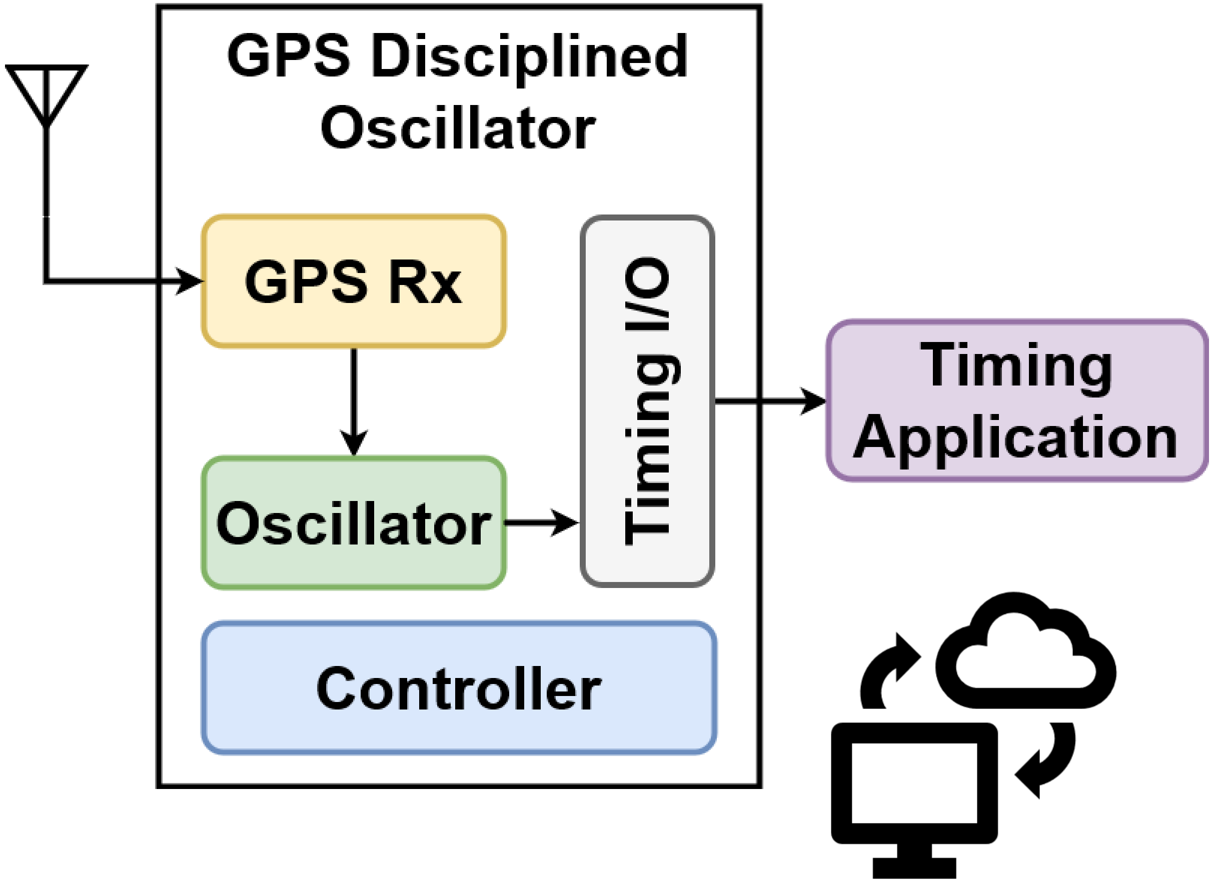
Attack Review



- **GPS Simulator transmitting spoofing signals for visible satellites**
- **Scenario:**
  - Spoofing signal powers 6 dB higher than live-sky
  - Initially aligned in time and position
  - Measurement spoofing: 10 ns/s walk-off rate to fixed offset

GPS Disciplined Oscillator

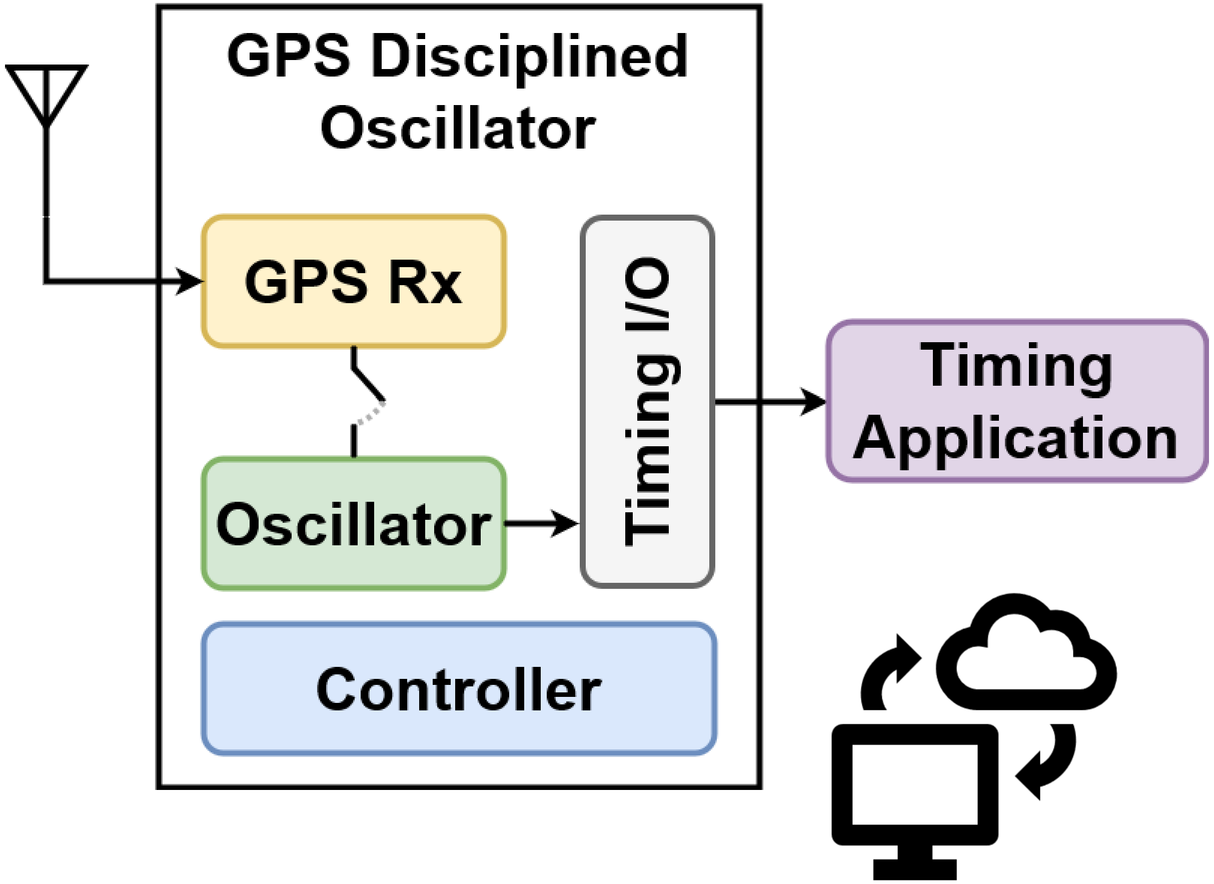
- **Notional GPS Disciplined Oscillator:**
  - High quality oscillator stable over hours; drifts over days
  - GPS receiver time accurate on average, but fluctuates over short time scales
  - Disciplining leverages the short-term stability of the local oscillator with the high average accuracy of GPS time transfer
  - When GPS receiver is vulnerable to spoofing, continuous disciplining makes the oscillator vulnerable also



Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

Flip Concept

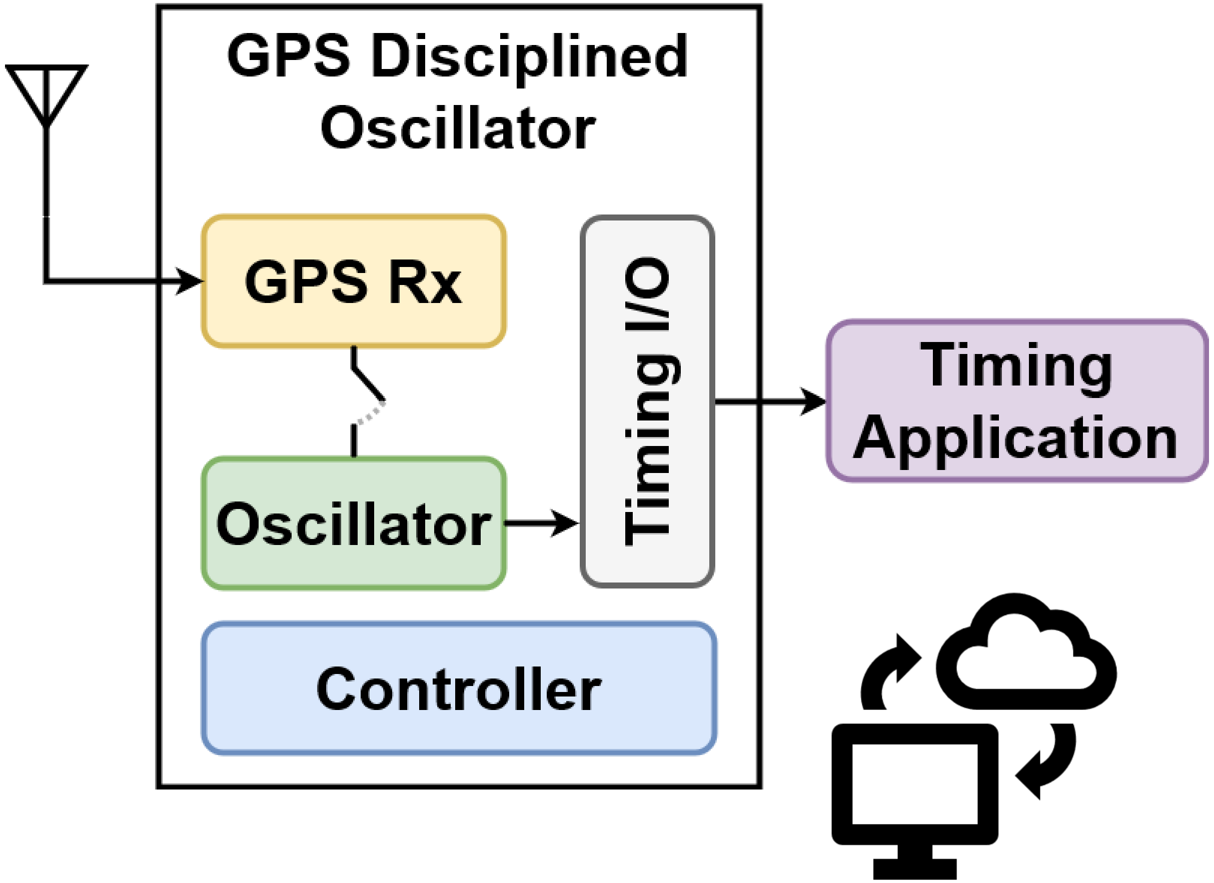
- **Trust the oscillator**
  - Oscillator can free run for a long (hours to days) time while meeting needs of many applications
  - During free run, the GPS receiver can be powered down and thus is not vulnerable to attacks
- **Discipline intermittently**
  - The oscillator will wander while free running
  - Intermittent GPS disciplining prevents time error from exceeding the tolerance of the application



Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

Flip Concept

- **Trust the oscillator**
  - Oscillator can free run for a long (hours to days) time while meeting needs of many applications
  - During free run, the GPS receiver can be powered down and thus is not vulnerable to attacks
- **Discipline intermittently**
  - The oscillator will wander while free running
  - Intermittent GPS disciplining prevents time error from exceeding the tolerance of the application



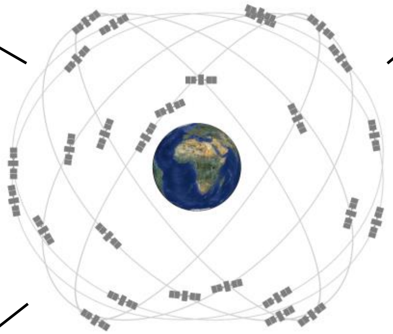
Remote attackers can’t spoof or jam a free running oscillator

Today, GPS Is the World’s Clock

- **GPS is an inexpensive and accurate source of time**
- **Many fielded GPS receivers are vulnerable**
- **Need greater robustness and resilience**

> ***“… ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on system resources …”***

NIST SP 800-160



Threat Classes

- **Interference or jamming**
  - RF waveforms obscure signals; deny or degrade receiver's processing of signals
- **Measurement spoofing**
  - False signals mimic true signals, introducing incorrect measurements of delay, carrier frequency, carrier phase; deny, degrade, deceive position/velocity/time (PVT) solution
- **Data spoofing**
  - False signals mimic true signals, introducing incorrect data message bits; deny, degrade, deceive receiver operation and PVT solution
- **Attacks on timing equipment and through network**
  - Analogous to attacks on other computers and networks: supply chain, insider, malware, …; deny, degrade, deceive receiver operation
- **Attacks on system infrastructure**
  - Kinetic or nonkinetic attacks on infrastructure providing information to receiver; deny, degrade, deceive receiver operation

Any technology potentially vulnerable; multiple access points; combinations possible

Threat Classes

The Flip lowers the probability of successful spoofing

- **Interference or jamming**
  - RF waveforms obscure signals, deny or degrade receiver’s processing of signals
- **Measurement spoofing**
  - False signals mimic true signals, introducing incorrect measurements of delay, carrier frequency, carrier phase; deny, degrade, deceive position/velocity/time (PVT) solution
- **Data spoofing**
  - False signals mimic true signals, introducing incorrect data message bits; deny, degrade, deceive receiver operation and PVT solution
- **Attacks on timing equipment and through network**
  - Analogous to attacks on other computers and networks: supply chain, insider, malware, …; deny, degrade, deceive receiver operation
- **Attacks on system infrastructure**
  - Kinetic or nonkinetic attacks on infrastructure providing information to receiver; deny, degrade, deceive receiver operation

Defenses need to be cost-effective, reducing vulnerability consistent with application

Limitations of Current Implementation

- **Receivers being used are highly susceptible to spoofing**
  - Promiscuous—appear to acquire first and strongest signals
  - Initial time uncertainty during (re)acquisition not constrained by external oscillator
  - Accept time jumps of multiple microseconds
- **Disciplining times not randomized**
  - Prevent attackers from knowing when to strike
- **No situational awareness**
  - E.g., detect multiple received signals with same pseudo-random noise (PRN) sequence
  - Situational awareness reduces susceptibility during acquisition
- **No spoofing resistance during disciplining**
  - Use oscillator models to detect and mitigate

Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

The Flip Concept

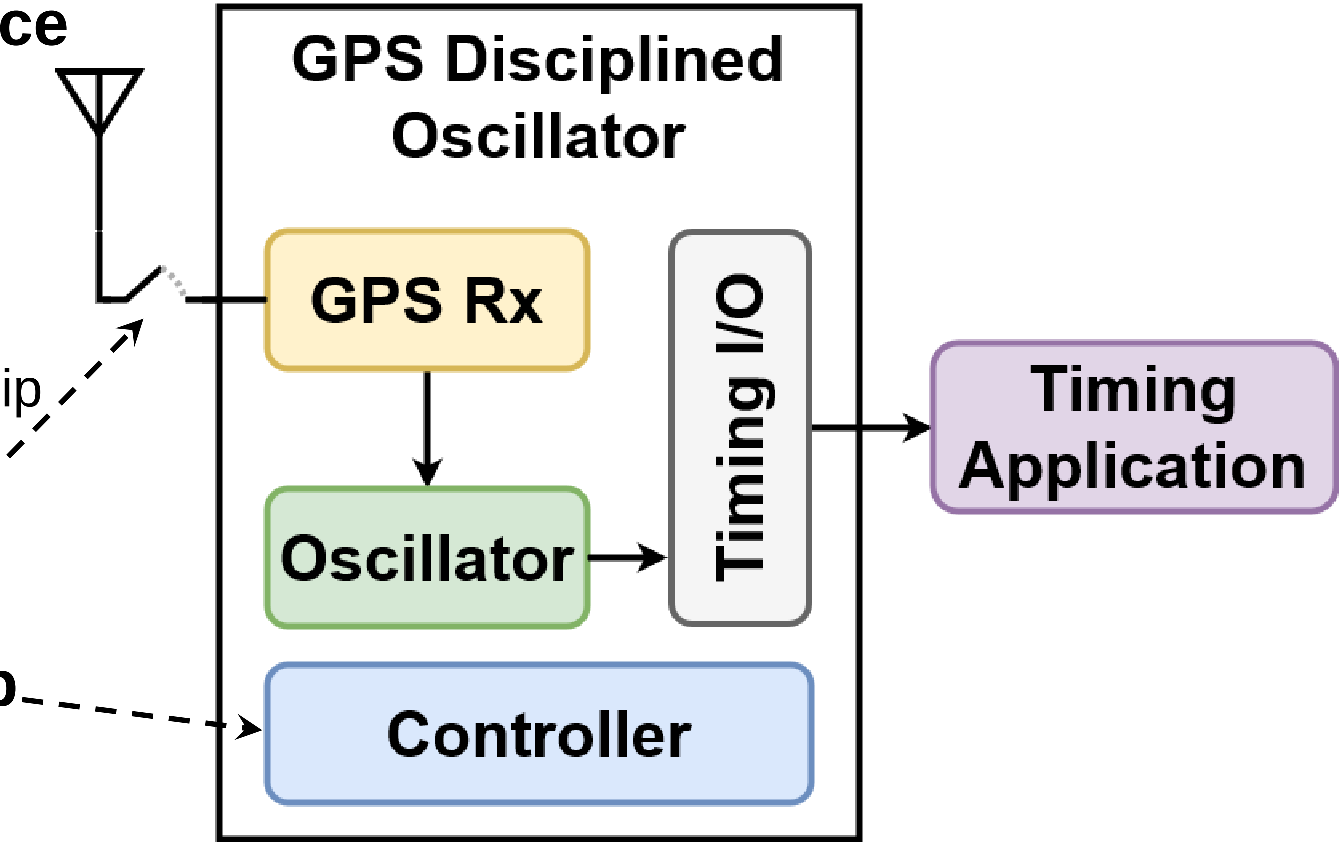
- **Basic Flip**
  - Modify a standard timing system to randomly discipline the oscillator at a low duty cycle
  - Reduces the probably of being spoofed to the duty cycle
  - No changes to the GPS receiver
  - Reduces the asymmetry of attacks against unprotected GPS receivers

- **Enhanced Flip**
  - **Reduced duty cycle:** oscillator modeling, dual-frequency receivers
  - **Situational awareness:** Know when to discipline and when not to
  - **Spoofing resistance:** Reduce vulnerability during disciplining
  - **Resilience:** Recover gracefully from any compromise

Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

Engineering the Flip

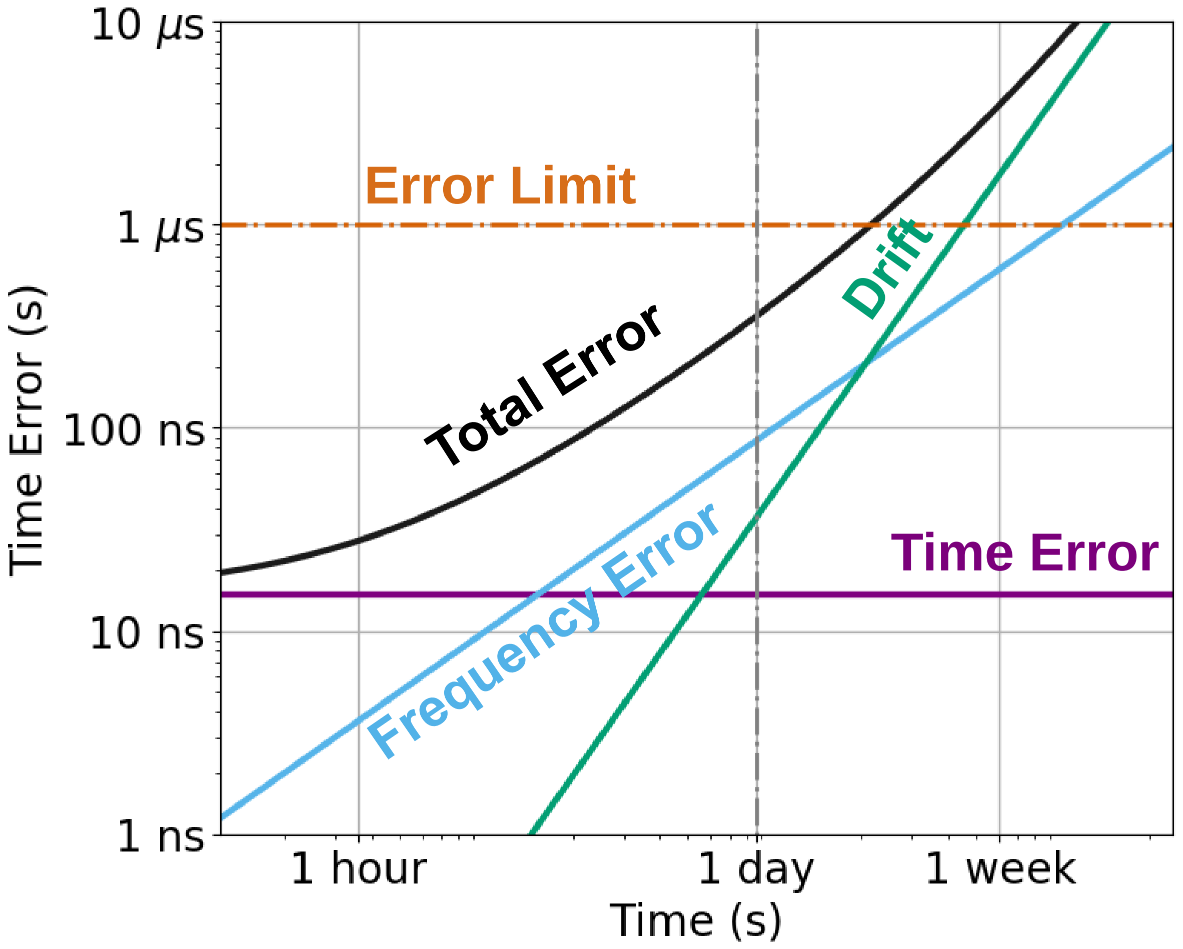
- **Key step: select duty cycle to balance timing requirements and oscillator quality**
  - Establish time needed to discipline
  - Randomize disciplining times
  - Add selected enhancements to the Basic Flip
- **Hardware implementation**
  - In-line device randomly interrupts RF to receiver, causing fallback to oscillator
- **Software implementation of The Flip**
  - Network
  - Serial port



How Long to Free Run – Time Error Over Time

- Time Error components: initial Time Error, initial Frequency Error, Drift, Temperature Effects
- Disciplining reduces initial Frequency Error and initial Time Error
- Drift dominates for a long free run

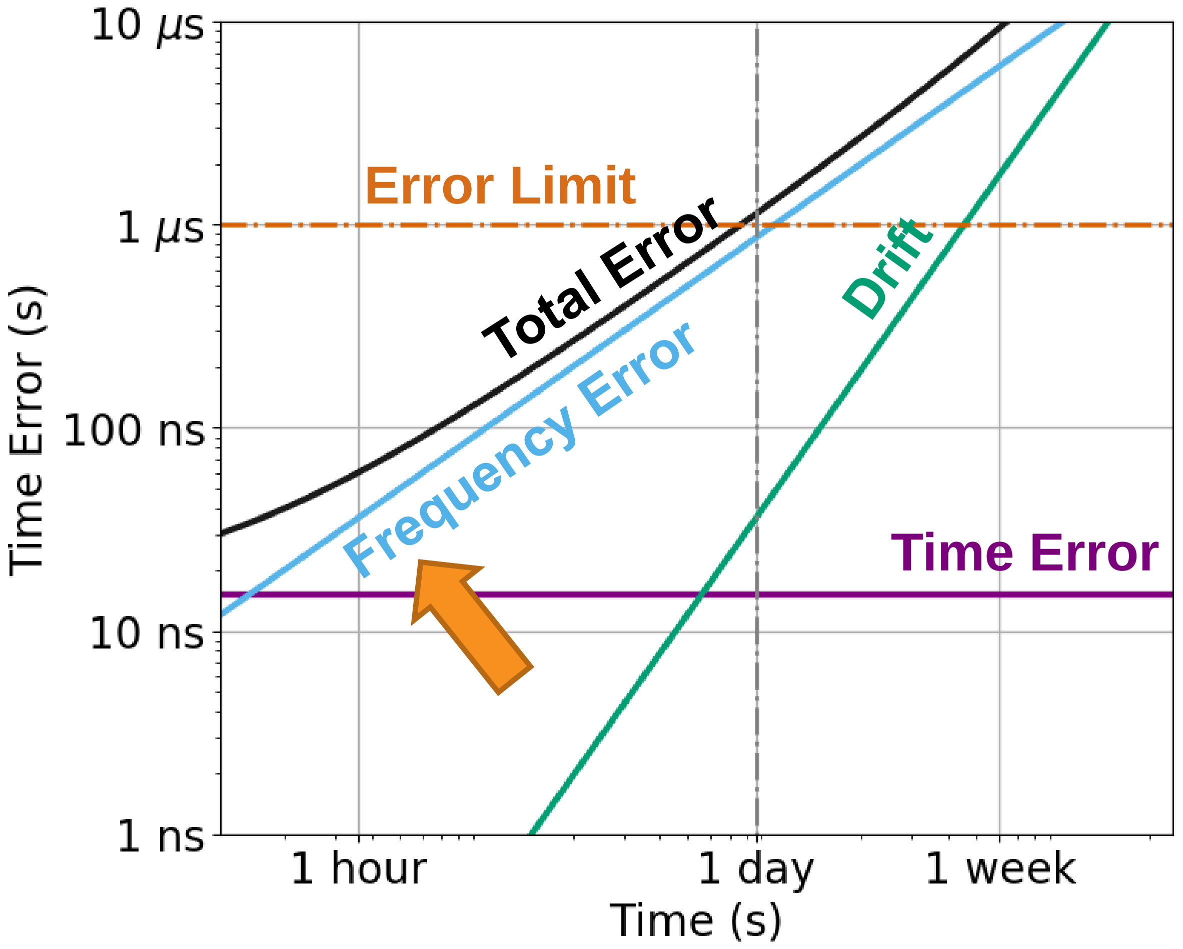
Disciplining Time chosen to reduce Frequency Error; Drift is then the limitation on holdover duration



How Long to Free Run – Time Error Over Time

- Time Error components: initial Time Error, initial Frequency Error, Drift, Temperature Effects
- Disciplining reduces initial Frequency Error and initial Time Error
- Drift dominates for a long free run

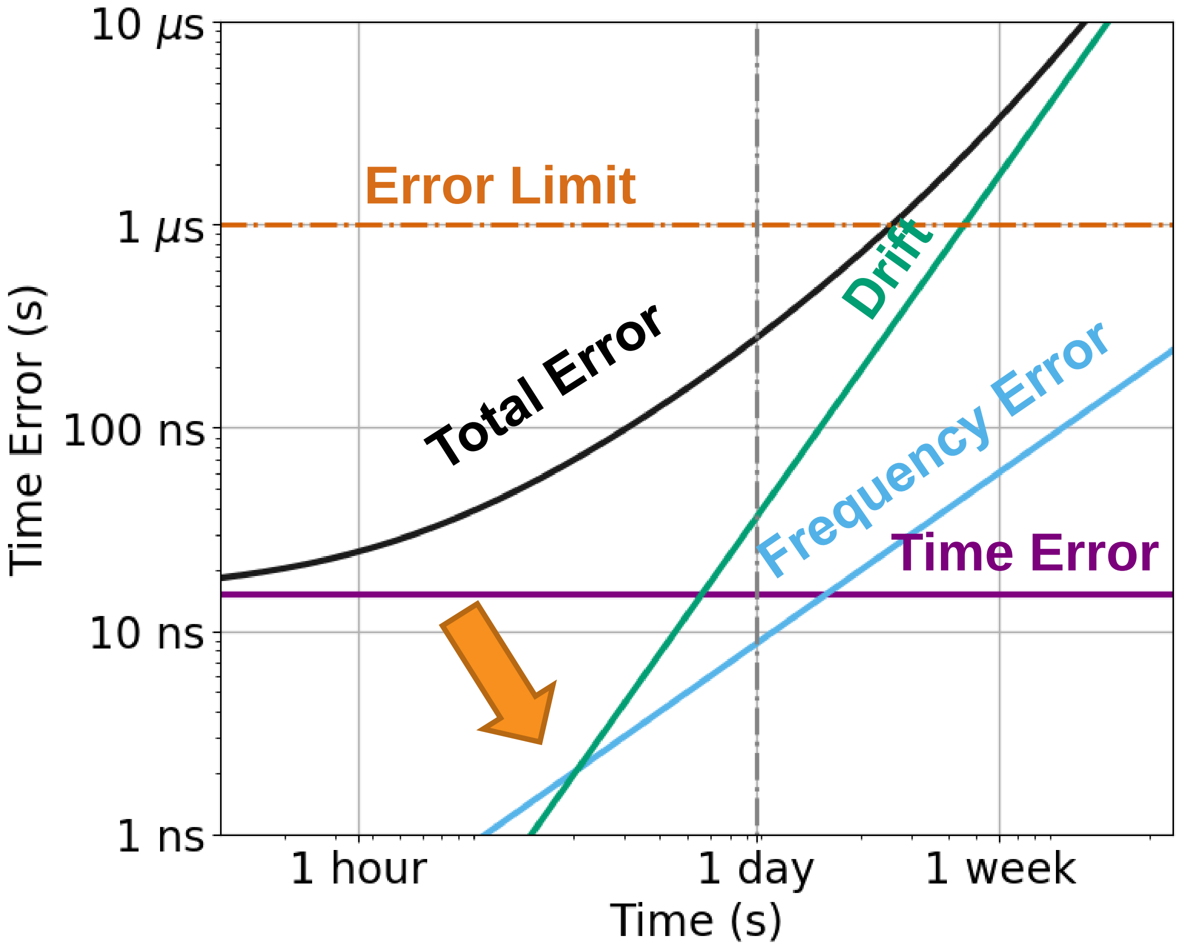
Shorter Disciplining Time results in a higher initial Frequency Error



How Long to Free Run – Time Error Over Time

- Time Error components: initial Time Error, initial Frequency Error, Drift, Temperature Effects
- Disciplining reduces initial Frequency Error and initial Time Error
- Drift dominates for a long free run

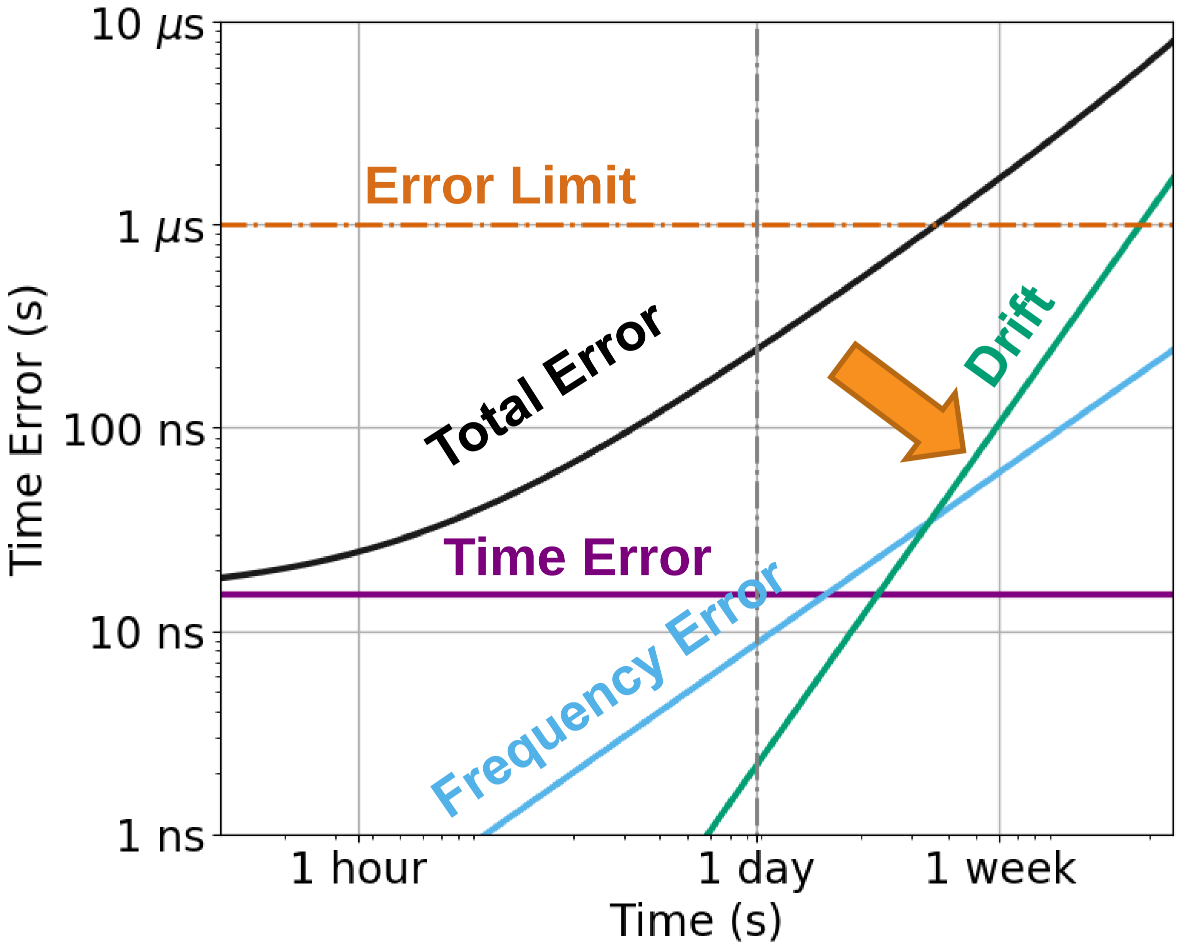
Improvements from longer Disciplining Time are limited by Drift



How Long to Free Run – Time Error Over Time

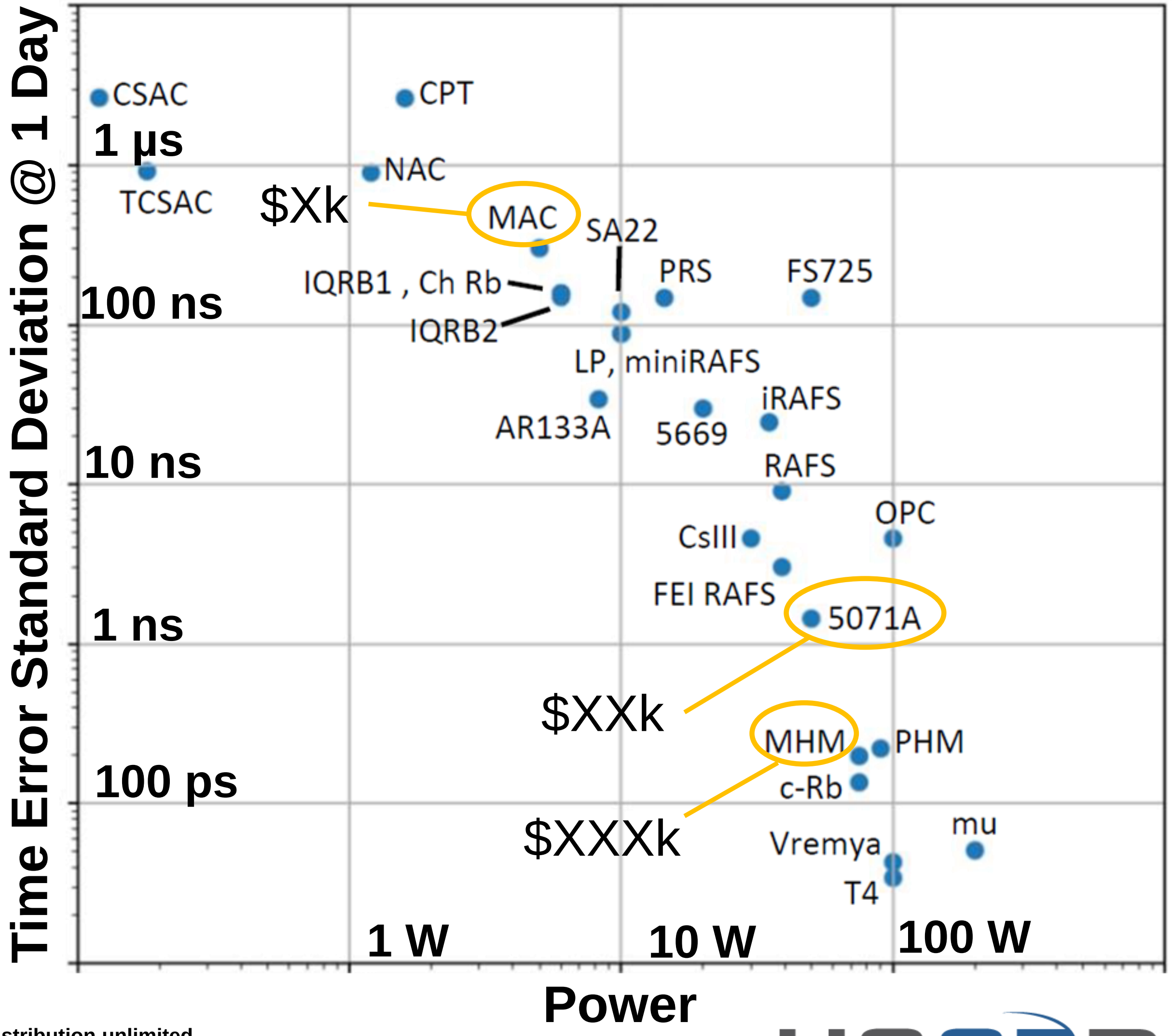
- **Time Error components: initial Time Error, initial Frequency Error, Drift, Temperature Effects**
- **Disciplining reduces initial Frequency Error and initial Time Error**
- **Drift dominates for a long free run**

High quality oscillators allow longer free run periods and reduced duty cycle



Oscillator Quality Dictates Performance of The Flip

- **Better oscillators allow longer free run, reducing vulnerability**
  - Trade against cost and power
- **End users should understand their timing needs**
  - Impact of time error
  - Impact of compromised time



D. Scherer et al., "Current and Future Atomic Clocks – Roadmap and Applications", CGSIC Meeting (2019)

Ongoing and Future Work on The Flip

Things in the plan

- **Reduced Duty Cycle**
  - Oscillator models
  - Control algorithms
- **Situational awareness**
- **Spoofing resistance**
  - Anti-Spoof algorithms
  - Incorporation of multiple sources
- **Resilience**
  - Timing architectures

Things not in the plan

- **Development of new oscillator technology**
- **Advanced receiver architectures, e.g. vector delay lock loops**
- **Development of alternate sources**

Analysis tools and algorithms will be published through DHS S&T

Summary

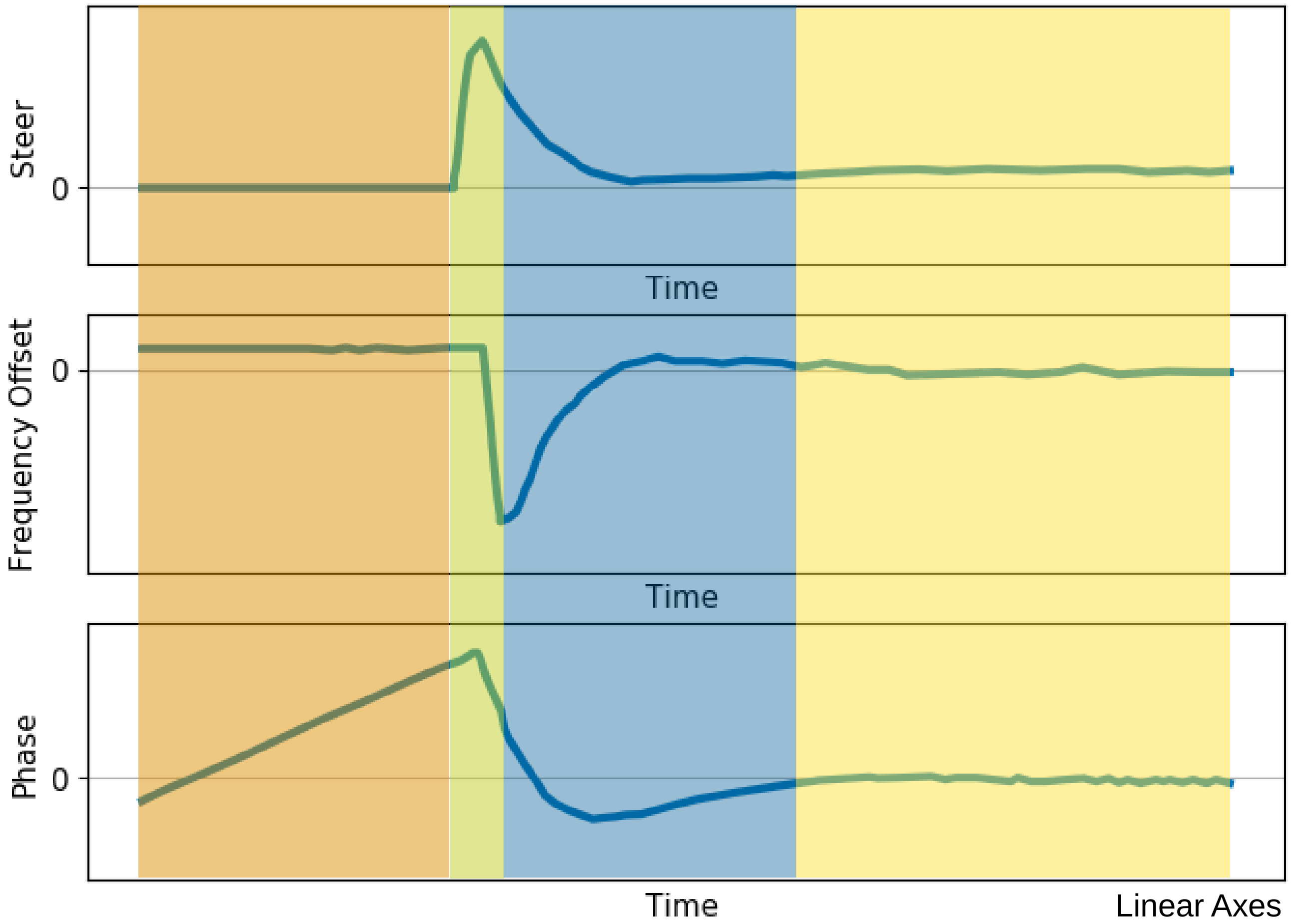
- **GPS-based timing remains important for critical infrastructure**
  - Short term: protect existing receivers
  - Long term: improve receiver robustness and resilience; alternative sources of time
- **Evaluate alternative sources of time**
  - More isn’t always better—account for vulnerabilities, cost-effectiveness
- **The Flip provides a low-cost and rapid way to improve robustness of existing timing receivers**
- **Enhanced Flip protects further against many attacks**

Backup Slides

Disciplining Variations

- **There are many different disciplining algorithms with varying complexity.**
  - Some include Artificial Intelligence (AI) and other tools to apply efficient and effective disciplining.
- **Precise predictions are only possible with knowledge of the details of the disciplining algorithm used, which are often proprietary.**
- **For example, the Fractional Frequency Error can be intentionally offset to counteract the effects of Drift and Temperature changes.**
  - Disciplining algorithms that implement this intentional offset may be used to increase free-running times.
- **General assumptions were used to make the estimates presented here.**
- **Future work will focus on researching and demonstrating specific disciplining algorithms that are well-suited for use in a FLIP system.**

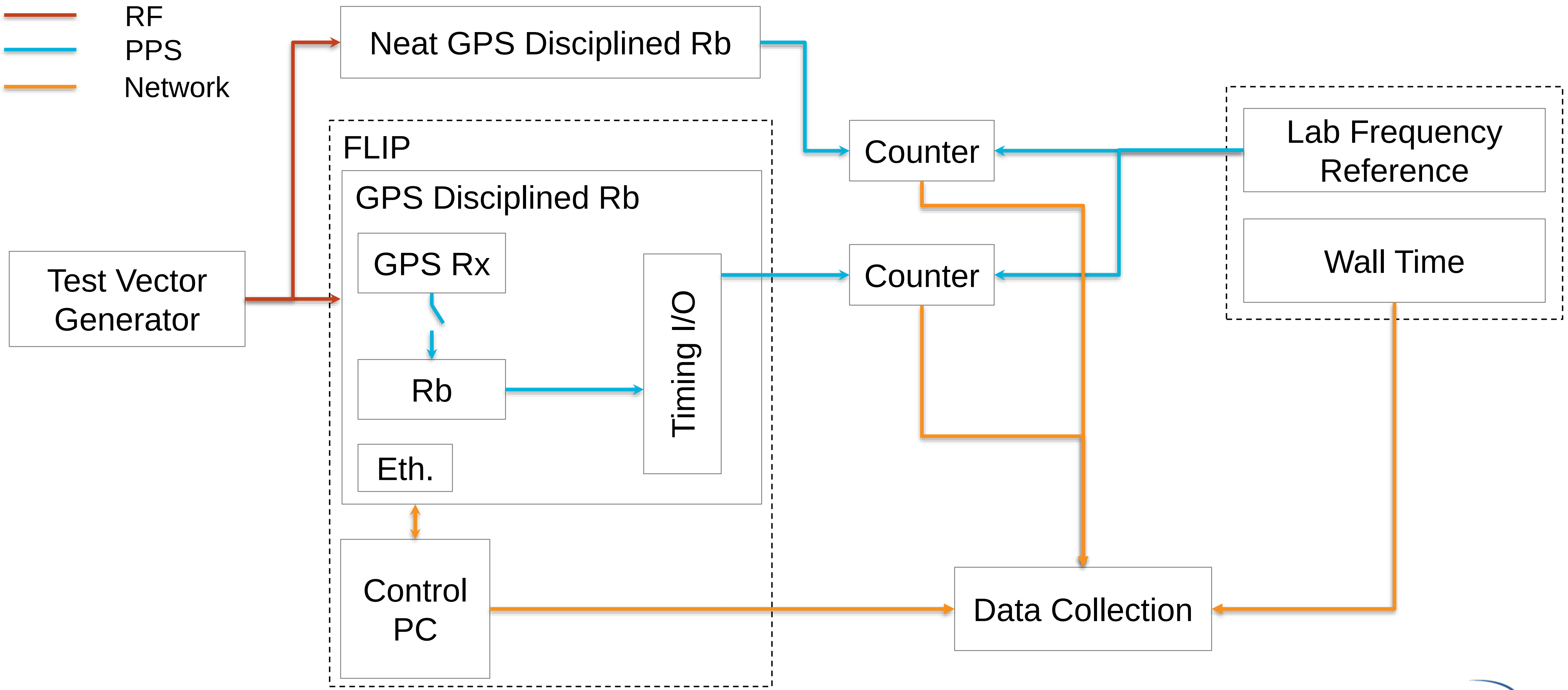
Notional Disciplining Process



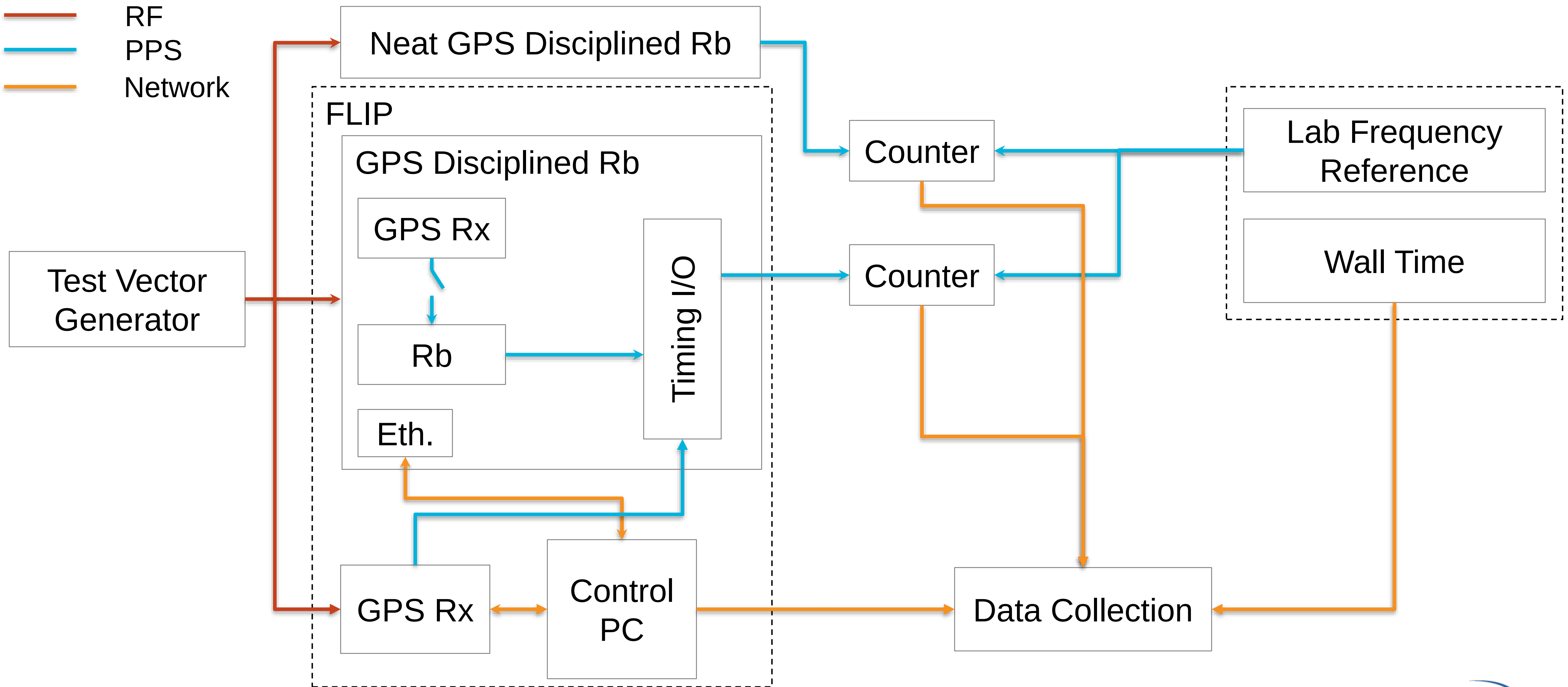
- Error accumulates
- Frequency is deliberately steered to adjust time error
- Steering is gradually reduced as frequency and time error decreases
- Small frequency changes for final correction of time error and frequency
- Disciplining must allow time for both time error and frequency correction
- Error at the end of disciplining period affects how long the clock can free run
- Reference:
  SA.45S CSAC User Guide Revision D

Disciplining needs time to correct both frequency and phase.

Level 0 Demo – Intermittent GPS, No Checks



Level 1 Demo – Intermittent GPS, Monitoring Receiver



Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19

Acknowledgement for DHS Sponsored Tasks (last slide)

The Homeland Security Act of 2002 (Section 305 of PL 107-296, as codified in 6 U.S.C. 185), herein referred to as the "Act," authorizes the Secretary of the Department of Homeland Security (DHS), acting through the Under Secretary for Science and Technology, to establish one or more federally funded research and development centers (FFRDCs) to provide independent analysis of homeland security issues. MITRE Corp. operates the Homeland Security Systems Engineering and Development Institute (HSSEDI) as an FFRDC for DHS under contract HSHQDC-14-D-00006.

The HSSEDI FFRDC provides the government with the necessary systems engineering and development expertise to conduct complex acquisition planning and development; concept exploration, experimentation and evaluation; information technology, communications and cyber security processes, standards, methodologies and protocols; systems architecture and integration; quality and performance review, best practices and performance measures and metrics; and, independent test and evaluation activities. The HSSEDI FFRDC also works with and supports other federal, state, local, tribal, public and private sector organizations that make up the homeland security enterprise. The HSSEDI FFRDC's research is undertaken by mutual consent with DHS and is organized as a set of discrete tasks. This report presents the results of research and analysis conducted under:

70RSAT19FR0000040
Resilient Position, Navigation, and Timing
The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Resilient Position, Navigation, and Timing (PNT) Program mission is to reduce vulnerabilities to and increase the resilience of critical infrastructure during PNT disruptions. Understanding the vulnerabilities is important, as is conducting outreach to relevant stakeholders. This program will develop and evaluate mitigation technologies, best practices, alternative PNT technologies, voluntary standards, and other resilient PNT activities.

The results presented in this report do not necessarily reflect official DHS opinion or policy.

Approved for public release. Distribution unlimited.
Case Number 19-3554 / DHS Reference Number 70RSAT19FR0000040-01 11/08/19