Control Algorithms for Resilient Timing

Dr. Ilya Udovydchenkov, Lead Electrical Engineer

Dr. Patricia Larkoski, Senior Electrical Engineer

FFRDC POWERED BY S&T™

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.

MITRE Corporation

21 September 2020

HSSEDI POC:
Dr. Arthur Scholz, Principal Engineer
ascholz@mitre.org

Approved for public release. Distribution unlimited.
Case Number 19-03383-02 / DHS Reference Number 17-J-00100-05

HSSEDI
Homeland Security Systems Engineering & Development Institute™

Resilient Timing

- **Withstand the threat by preventing or responding to corrupted input from external sources**
- **Implement recovery when measures to withstand the threat are not sufficient**
- **Manufacturers and system integrators are building systems with some resilient timing features, but there need to be technical ways to communicate resilience with users**
- **Users should be aware of resilient features in timing equipment that benefits their application**

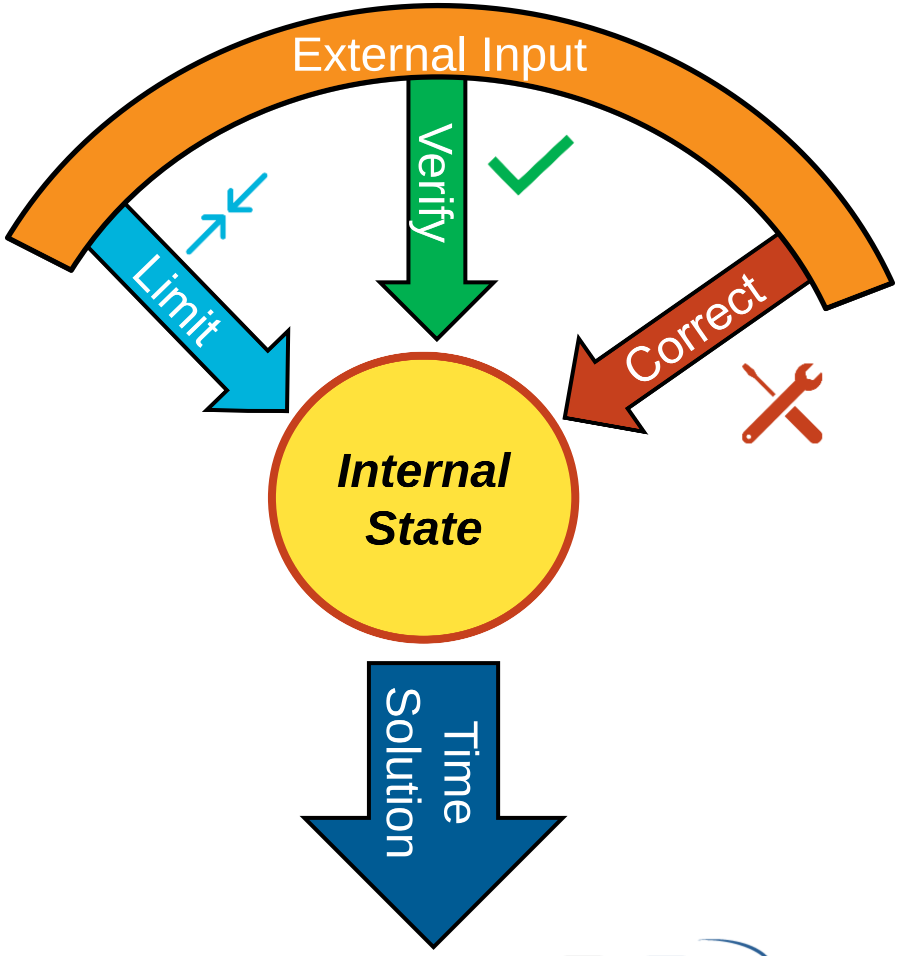
Resilient Techniques	Examples
Verify quality and accuracy of PNT solutions and other observables	Anti-spoof and anti-jam techniques; whitelist checks against standards
Limit the influence of external input	Only discipline an internal clock when needed
Correct PNT solutions	Apply corrections using a synthesizer
Predict future solutions	Use Kalman filter for verification and corrections
Recover system and/or component performance	Manual reset capability, rollback to a good state

Resilient PNT

- **Threats: malicious degradation or manipulation and/or naturally occurring corruption or degradation of external inputs to the timing control system**
  – Ex: GPS service is degraded when satellites are not visible and in the presence of malicious jamming, and/or spoofing
- **Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience***
  – *“The term "resilience" means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.”*
- **Executive Order 13905 of Feb 12, 2020, *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services***
  – *“ ‘Responsible use of PNT services’ means the deliberate, risk-informed use of PNT services, including their acquisition, integration, and deployment, such that disruption or manipulation of PNT services minimally affects national security, the economy, public health, and the critical functions of the Federal Government.”*

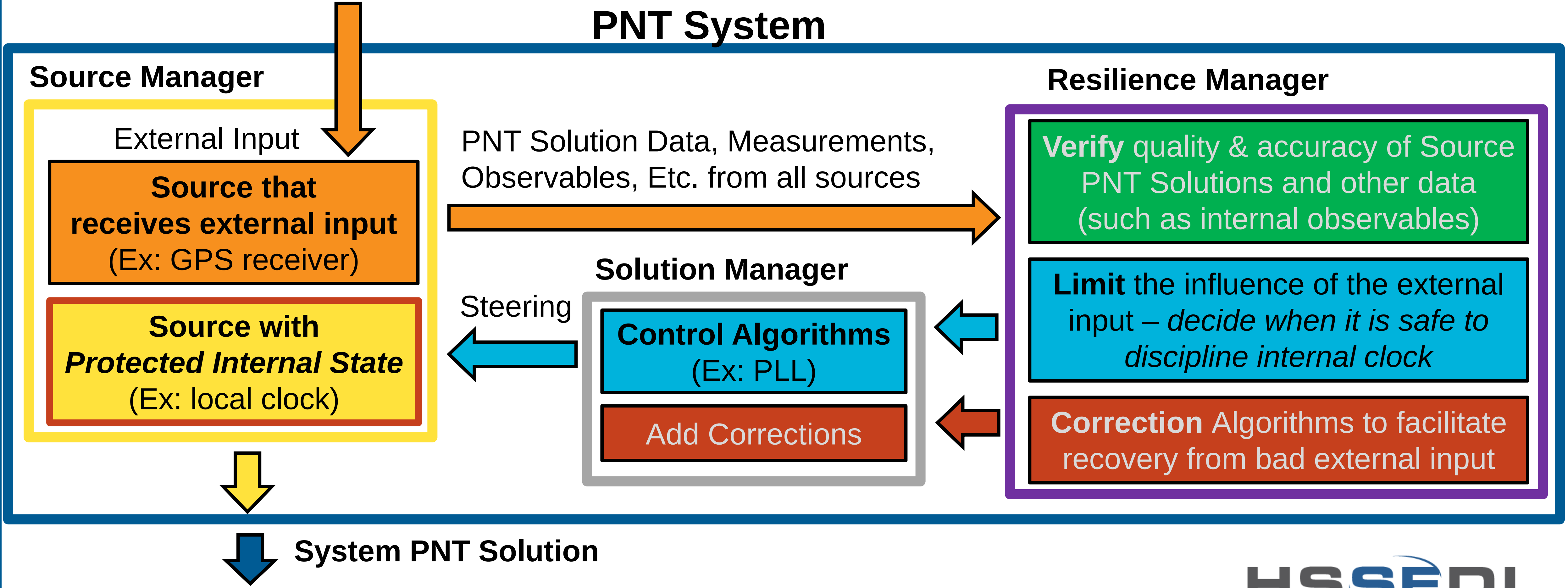
Protect an Internal State

- **Use known Resilient PNT techniques to withstand threats by *maintaining a protected internal state***
  - Ex: a local clock/oscillator
- **The more isolated the internal state is from the rest of the system, the more protected it is from corrupted external input**
  - If external input can influence the internal state, protection may include:
    - **Limit external input** when possible (isolate the internal state as much as possible)
    - **Verify external input** before it influences the internal state
    - Implement algorithms to **apply corrections** if corrupted external input infiltrates (recovery)



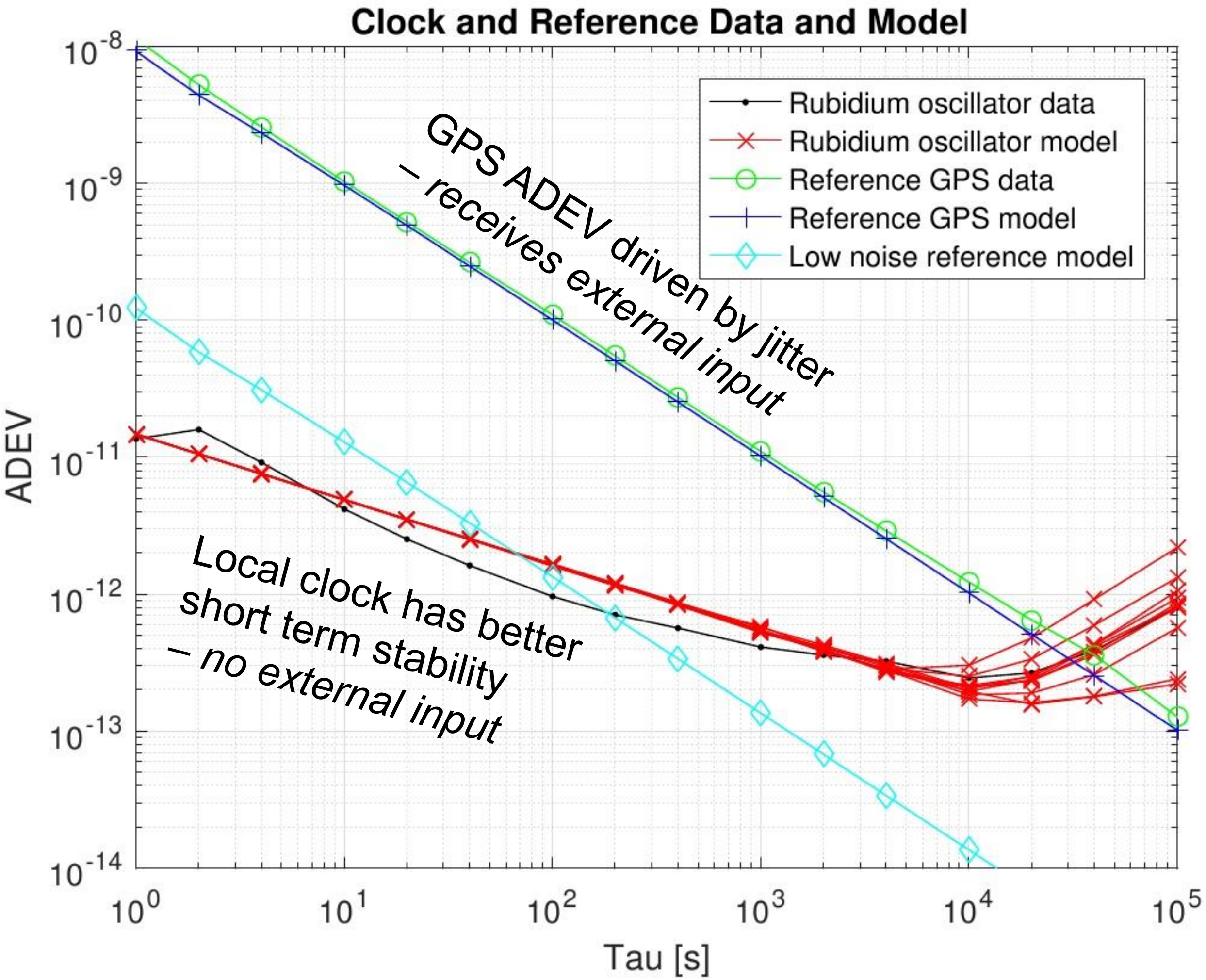
Applying Resilience to Timing Control

- **A typical control algorithm uses external input to discipline/steer the internal state**



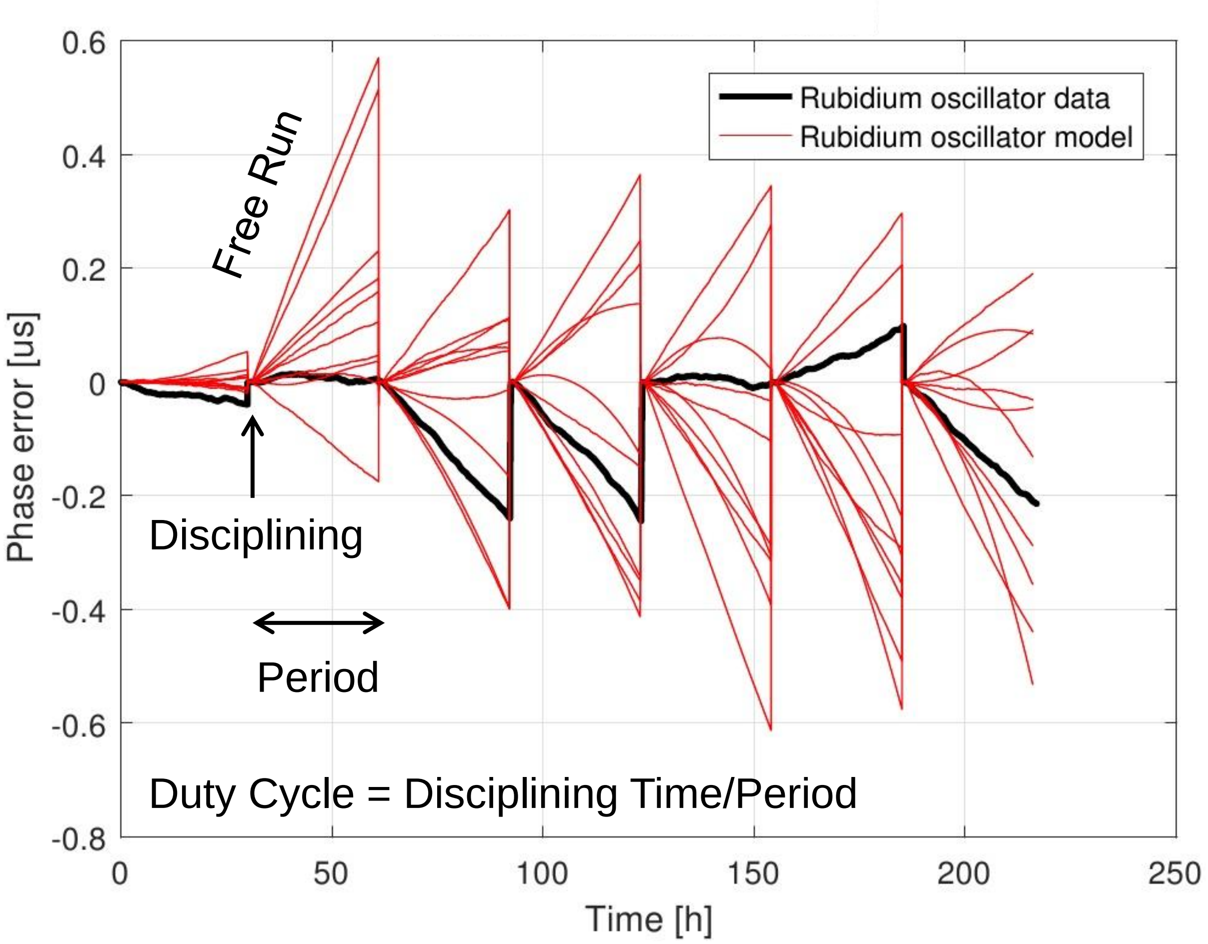
Choice of PNT Sources

- **PNT Sources with *no external input***
  - Not vulnerable to external threats *if the internal state is protected*
  - Example: local clock, good for short-term stability
- **PNT Sources with *external input***
  - Are vulnerable to external threats
  - Example: GPS receiver, good for long-term stability
- **Resilient Control: Combine sources to get stability and *maintain a protected internal state***



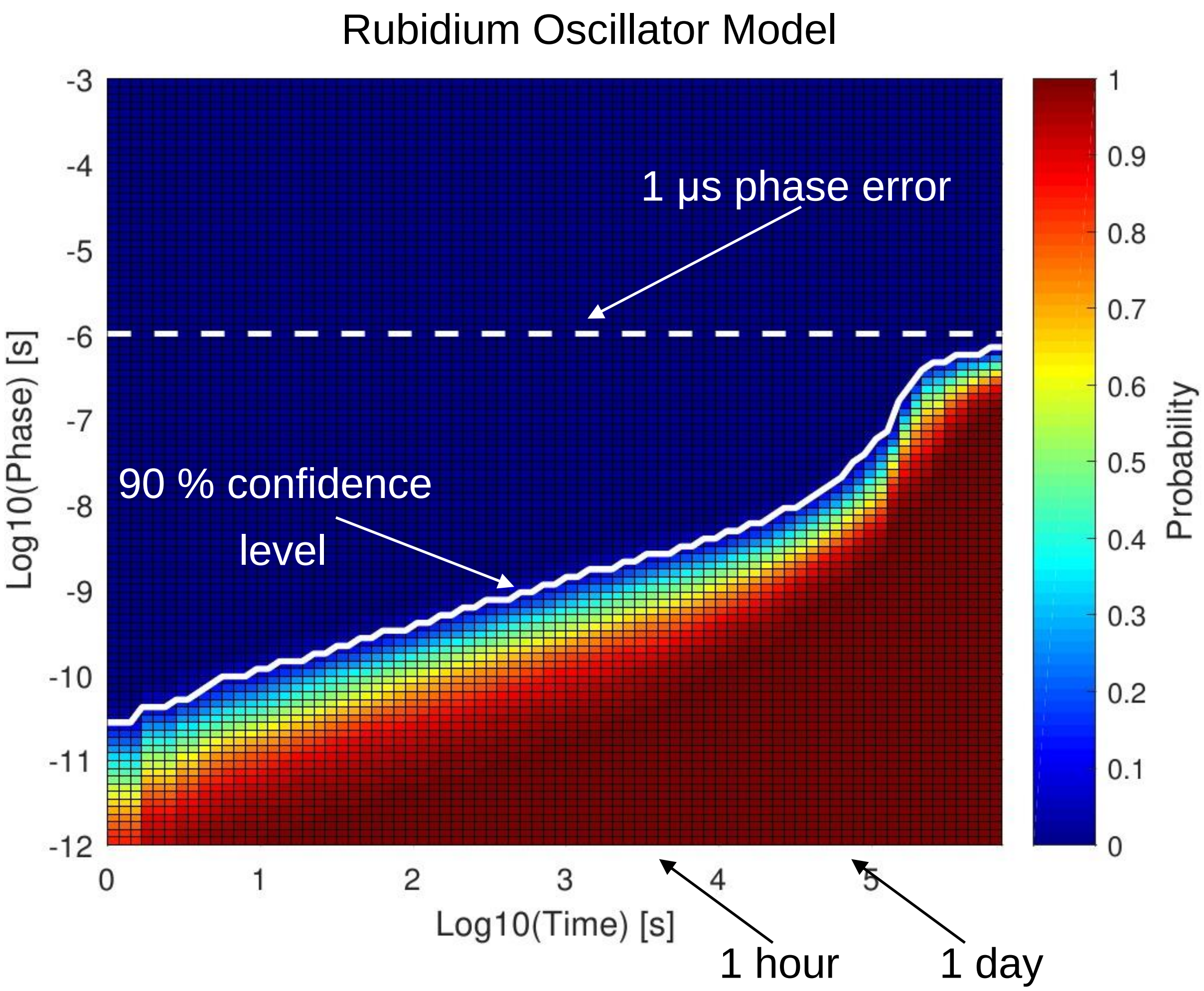
Data Example of Resilient Disciplining Control

Time Series Comparison of Data and Model



- **Disciplining: Phase Lock Loop (PLL) with low noise reference for 1 hour on, 30 hours off (free run)**
- **Occasional disciplining result:**
  - Duty Cycle = 1/31 = 3.2%
  - Accuracy = ±250 ns
- **With constant disciplining**
  - Duty Cycle = 100%
  - Accuracy = ±10 ns
- **Low noise references are not available for most applications**
- **GPS is widely available and affordable**
- **Good data/model agreement**

Clock Accuracy Metric



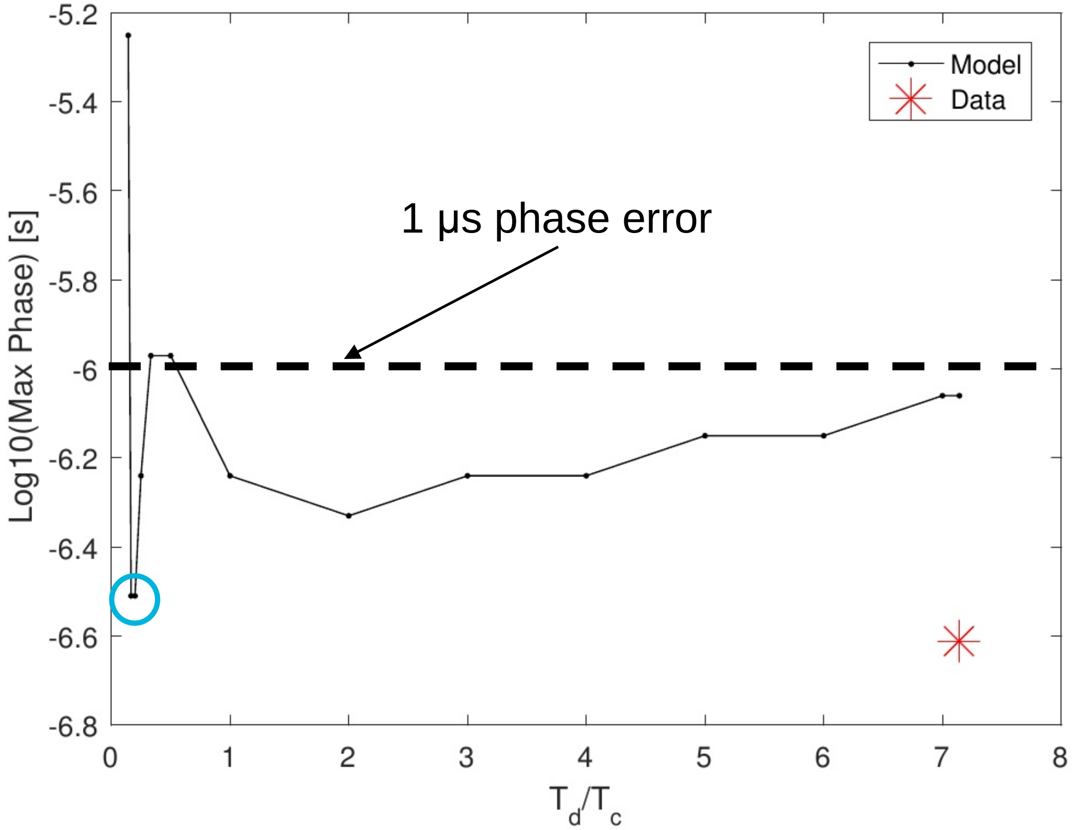
- **Need a metric to quantify trade-off between accuracy and resilience over time**
- **Define the probability of a clock to exceed a given phase error over given run time (colorbar)**
- **Estimate 90% confidence interval**
- **Example:**
  - 0.1 ns reference noise
  - Period = 31 hours
  - Disciplining time = 1 hour
  - Time constant = 504 sec

Approved for public release. Distribution unlimited.
Case Number 19-03383-02 / DHS Reference Number 17-J-00100-05

Natural Loop Time Constant Choices with a Low Noise Reference

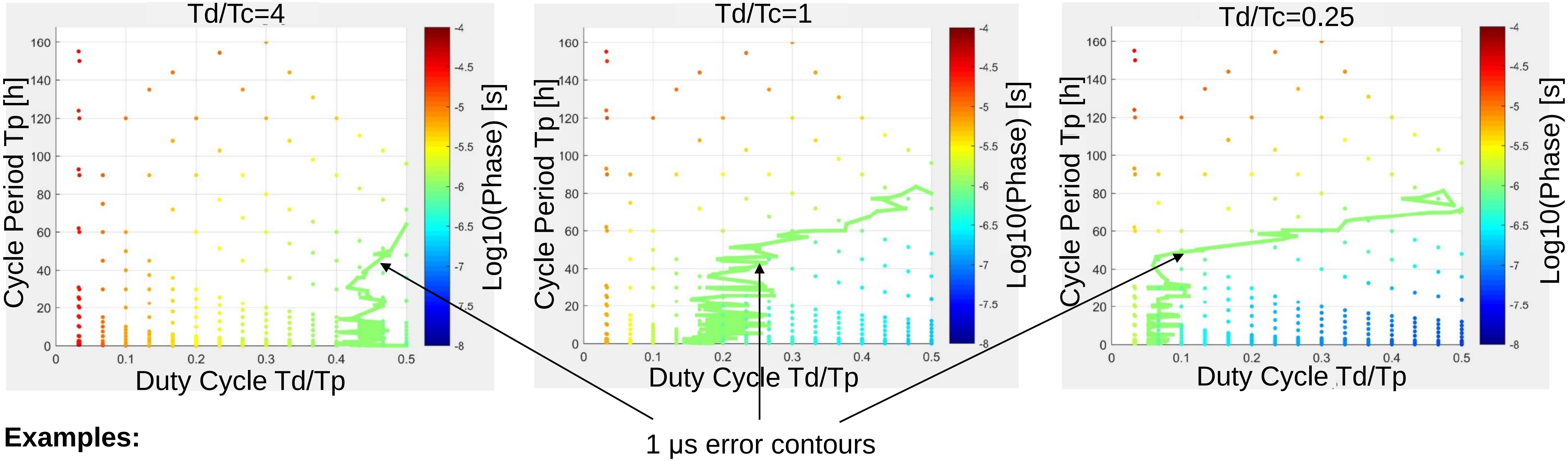
- **With a low noise reference, given a set duty cycle (period and disciplining time), there is freedom to choose the best time constant for accuracy**
  - 0.1 ns reference noise in the model
  - Period = 31 hours
  - Disciplining Time = 1 hour
  - Time Constant varied to get different (Disciplining Time)/(Time Constant) ratios

Vary the Time Constant with a Low Noise Reference



Natural Loop Time Constant Choice with 7.5 ns GPS Noise

Worst case: Best case:



Examples:

- Time Constant = 1 h
- Disciplining Time = 4 h
- Free-Run Time = 6 h
- Cycle Period = 10 h

- Time Constant = 4 h
- Disciplining Time = 4 h
- Free-Run Time = 16 h
- Cycle Period = 20 h

- Time Constant = 4 h
- Disciplining Time = 1 h
- Free-Run Time = 19 h
- Cycle Period = 20 h

Considerations for a Resiliency & Accuracy Figure of Merit

- **Accuracy, Stability, and Resilience are connected**
  - The noise of the sources effects the implementation of resilience techniques
- **Goal: define quantitative metrics that combine resilience and accuracy**
- **Resilience Metric examples: see table**
- **Accuracy Metric examples:**
  - Maximum time error
  - Mean and standard deviation of time error distribution
- **Resilience information included with accuracy information will help with consumer decisions**

Resilient Techniques	Example Metric
Verify quality and accuracy	The fraction of the threats detected in a standardized list. May be weighted by threat importance or difficulty.
Limit the influence of external input	The fraction of time the internal state (clock) is protected from external information (GPS)
Correct PNT Solutions	The fraction of the threats corrected in a standardized list. May be weighted by threat importance or difficulty.
Predict future solutions	Covariance matrix
Recover performance	Mean time to recover

Approved for public release. Distribution unlimited.
Case Number 19-03383-02 / DHS Reference Number 17-J-00100-05

Conclusions

- **Resilience is an important consideration in a PNT system design**
- **Protect the internal state to achieve resilience**
  - Limit the time when external input (GPS) can influence a protected internal state (local clock)
- **There are trade-offs in the design parameters of a resilient PNT system**
  - Balance between the convergence rate of a steering algorithm and the amount of system and external reference noise should be considered
- **Further development of resilient control algorithms is needed**
  - **Example:** randomize duty cycle to prevent threats from predicting vulnerability
  - **Example:** combine resilience techniques: verify external input and only discipline the protected internal state when it is safe to do so

Approved for public release. Distribution unlimited.
Case Number 19-03383-02 / DHS Reference Number 17-J-00100-05