A Multi-Level Approach for Integrating GNSS Integrity into Critical Timing Applications

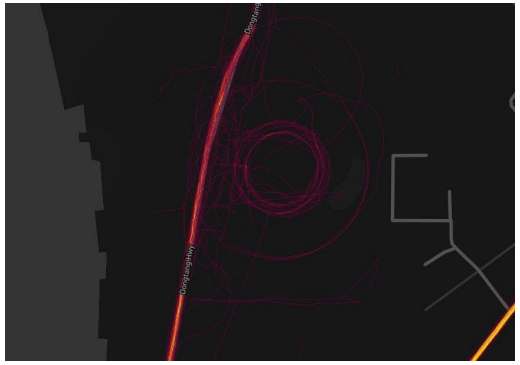
WSTS 2020 – Virtual Webinar Series
Session 3: Timing Security, Resilience and GNSS Issues

Josh Clanton & David Hodo
Integrated Solutions for Systems, Inc (IS4S)

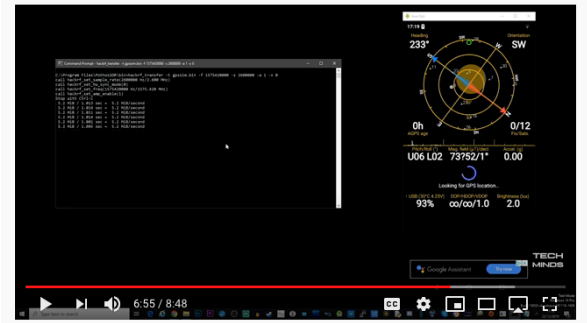
This work is funded by the Department of Homeland Security, Science and Technology Directorate, contract # 70RSAT18CB0000020.

Motivation

- Critical infrastructure is heavily reliant on precision timing from GPS
- GPS spoofing is no longer just a lab experiment
  - Many incidents documented in open literature
  - Step by step guides freely available online

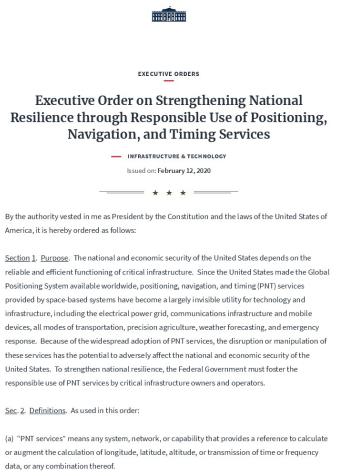


GPS “Crop Circles” near Port of Shanghai from Strava



Online Spoofing Tutorials Using Inexpensive Hardware

- Timing systems in critical infrastructure must be resilient to these threats
- IS4S and Auburn University funded by DHS S&T to develop a non-proprietary GPS Anti-Spoofing Toolkit for use by industry in developing resilient timing systems



EXECUTIVE ORDERS

Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services

INFRASTRUCTURE & TECHNOLOGY

Issued on: February 12, 2020

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. The national and economic security of the United States depends on the reliable and efficient functioning of critical infrastructure. Since the United States made the Global Positioning System available worldwide, positioning, navigation, and timing (PNT) services provided by space-based systems have become a largely invisible utility for technology and infrastructure, including the electrical power grid, communications infrastructure and mobile devices, all modes of transportation, precision agriculture, weather forecasting, and emergency response. Because of the widespread adoption of PNT services, the disruption or manipulation of these services has the potential to adversely affect the national and economic security of the United States. To strengthen national resilience, the Federal Government must foster the responsible use of PNT services by critical infrastructure owners and operators.

Sec. 2. Definitions. As used in this order:

(a) "PNT services" means any system, network, or capability that provides a reference to calculate or augment the calculation of longitude, latitude, altitude, or transmission of time or frequency data, or any combination thereof.

February 2020 Executive Order Requiring Resilient PNT in CI

Alignment with DHS Resilient PNT Conformance Framework

IS4S Integrated Solutions for Systems

- Anti-Spoofing Toolkit is part of a larger effort by DHS S&T to develop a framework for resilient PNT (Positioning, Navigation, and Timing)

- Provides guidelines for creating and evaluating resilient timing sources with emphasis on:
  - Critical infrastructure applications
  - Timing sources that are tied to GPS and other satellite or terrestrial navigation systems

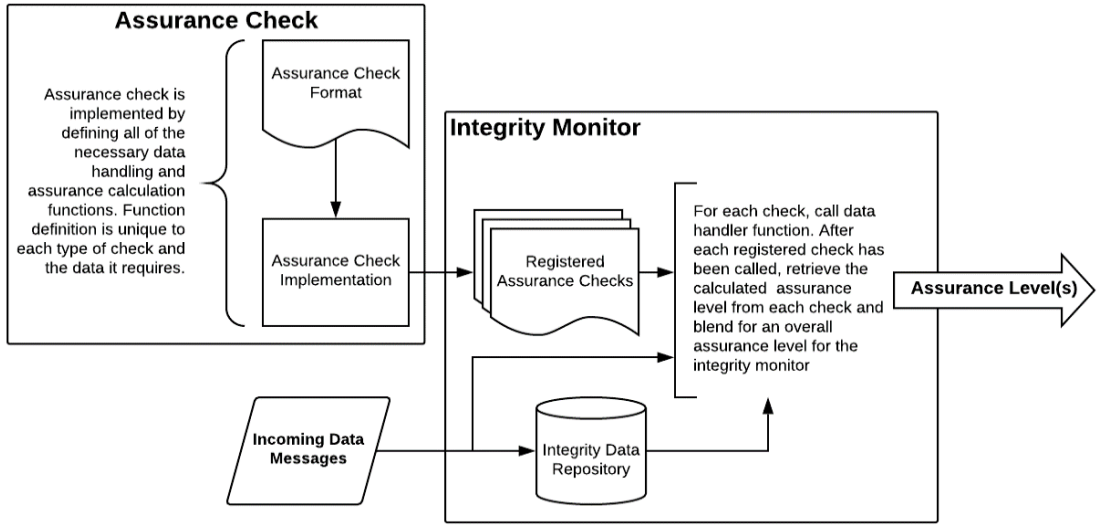
- Key Concepts
  - Provides guiding principles for system design that comprehensive, simple, consistent, and non-prescriptive
  - Defines resilience levels for quantifying performance of resilient PNT systems
  - Calls for a Defense-in-Depth with 3 core functions

- Detection is needed across the core functions
  - Detecting anomalies in GPS measurements is challenging
  - Must be able to expand as threats and detection techniques evolve

Project Goals

- Project goal is to develop a set of GPS spoofing detection methods, software, and tools for use in critical timing applications
  - –Reduce development time required to develop resilient timing systems
  - –Lower burden on manufacturers / end users for deploying resilient timing systems
  - –Educate community
  - –***NOT*** *to provide a turn-key solution/product that competes with existing industry offerings*

- Resources provided
  - –Architecture and software implementation
    - Data model definitions for receiver observables
    - Initial set of configurable integrity checks
    - Extensible framework for adding additional checks
    - Cross-platform C++ implementation
  - –Demonstration Kit
    - Hardware design
    - User interface

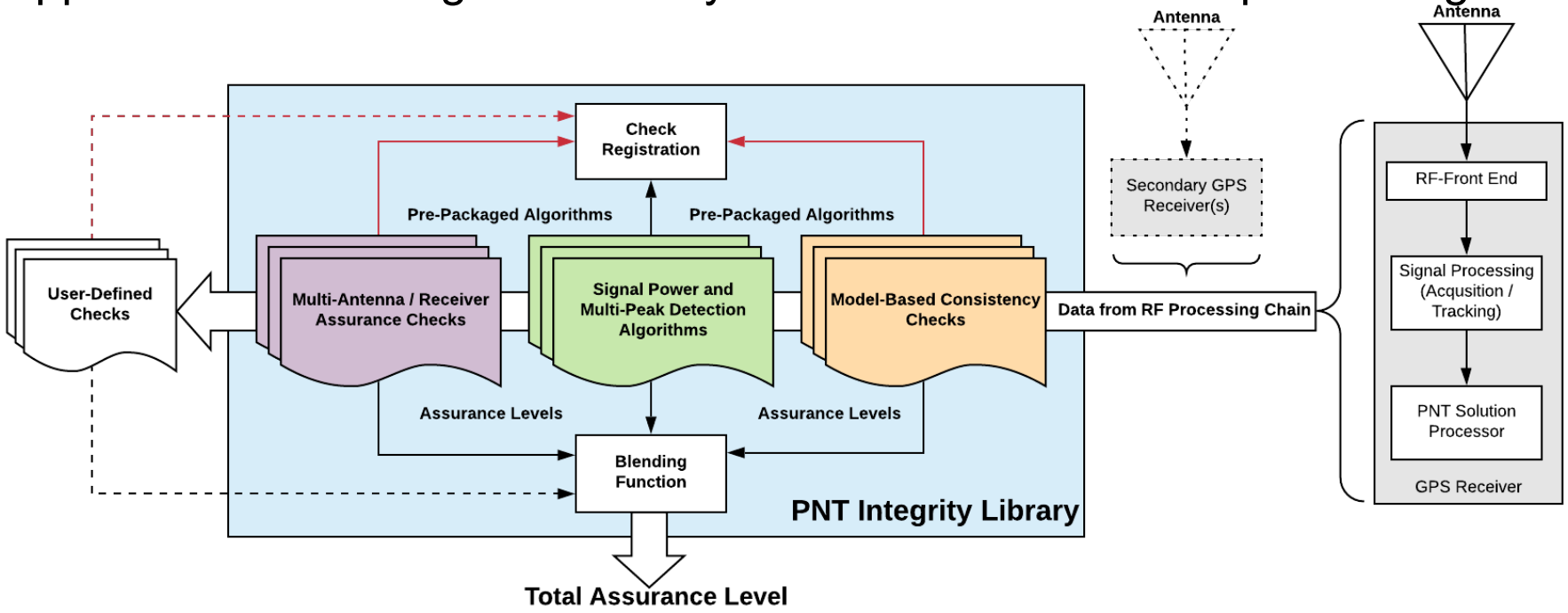


PNT Integrity Library Overview

- Open architecture approach to GPS spoofing detection

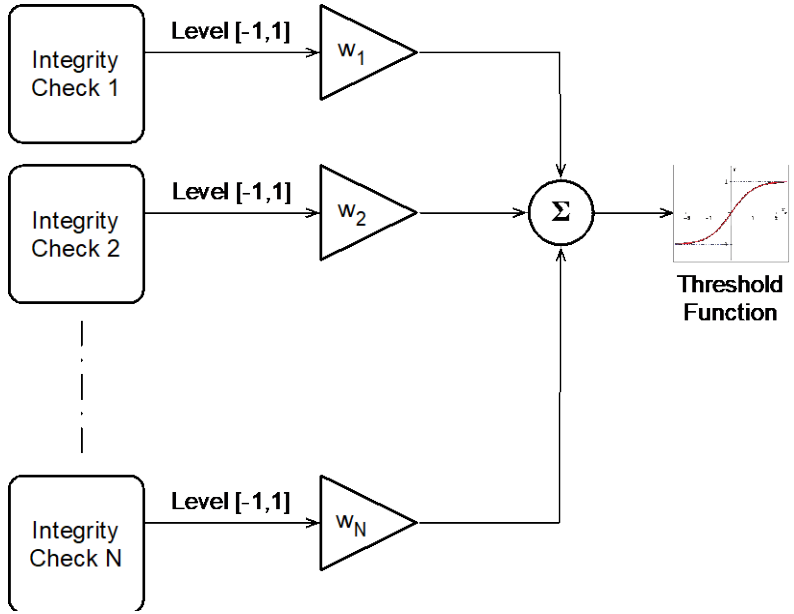
- Defines data models and API (application programming interface) for
  - Receiver observables (inputs)
  - Assurance check definitions (processing)
  - Assurance levels (output)

- Multi-layered approach allows integration at any level in the receiver RF-processing chain



Combining Assurance Checks

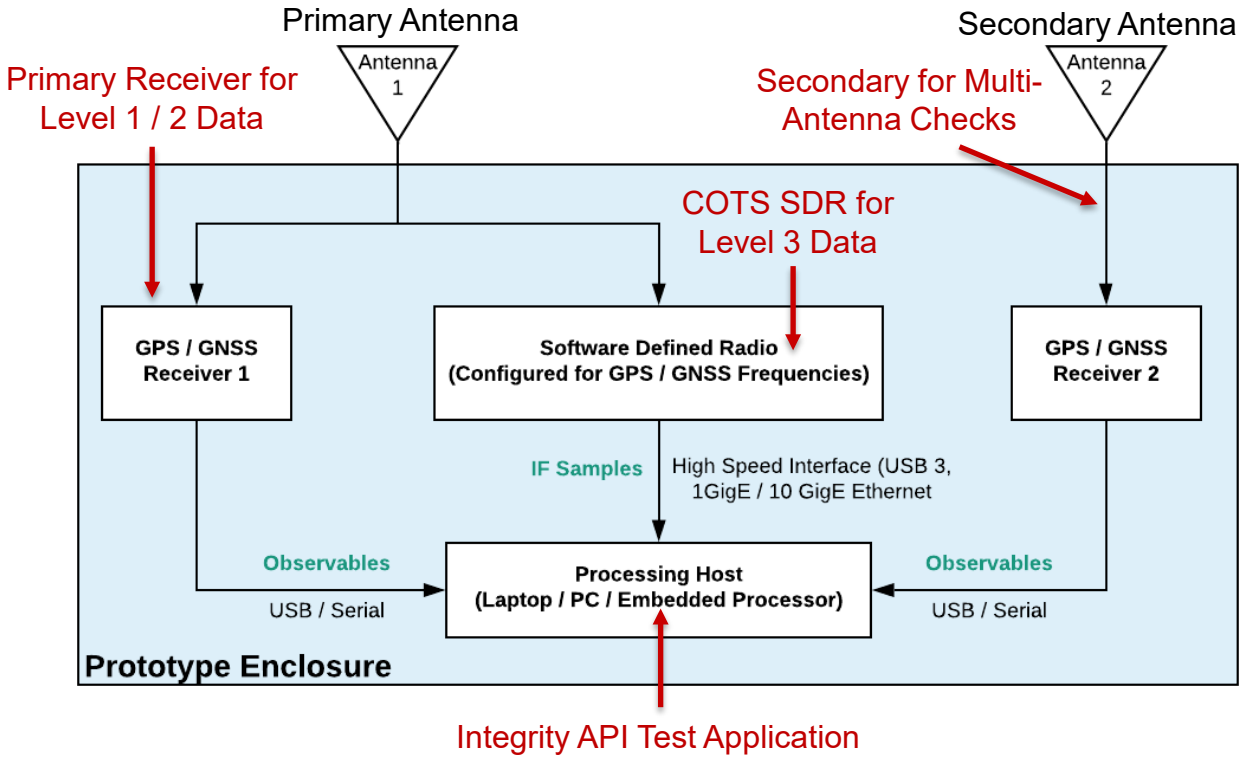
- Each registered check takes in receiver observables and outputs an assurance level
- A weight is assigned to each check
  - –Assigned by integrator
  - –User / platform specific
  - –Ideally based on P_D / P_{FA}
- Weighted values are summed and thresholded to produce one of four assurance levels

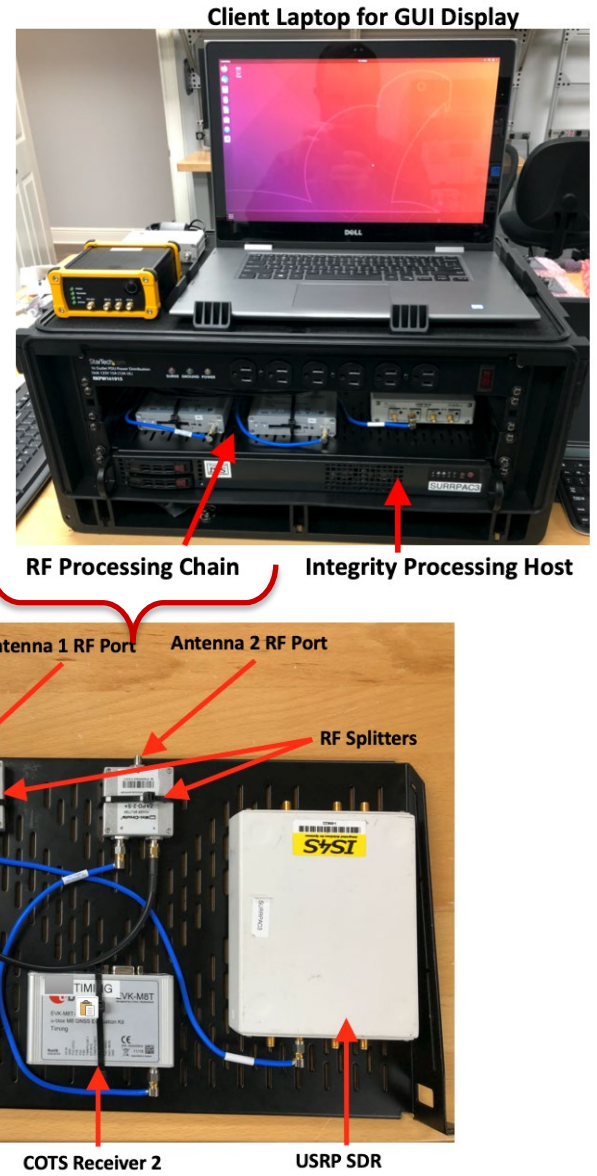


Level Name	Value	Description
Unavailable	0	Level is unavailable (insufficient data or has not yet been processed)
Unassured	1	Indicates a high likelihood that the measurement / source CANNOT be trusted
Inconsistent	2	Cannot reliably determine the validity of the measurement / source
Assured	3	Indicates a high-likelihood that measurement / source CAN be trusted

Demonstration Kit

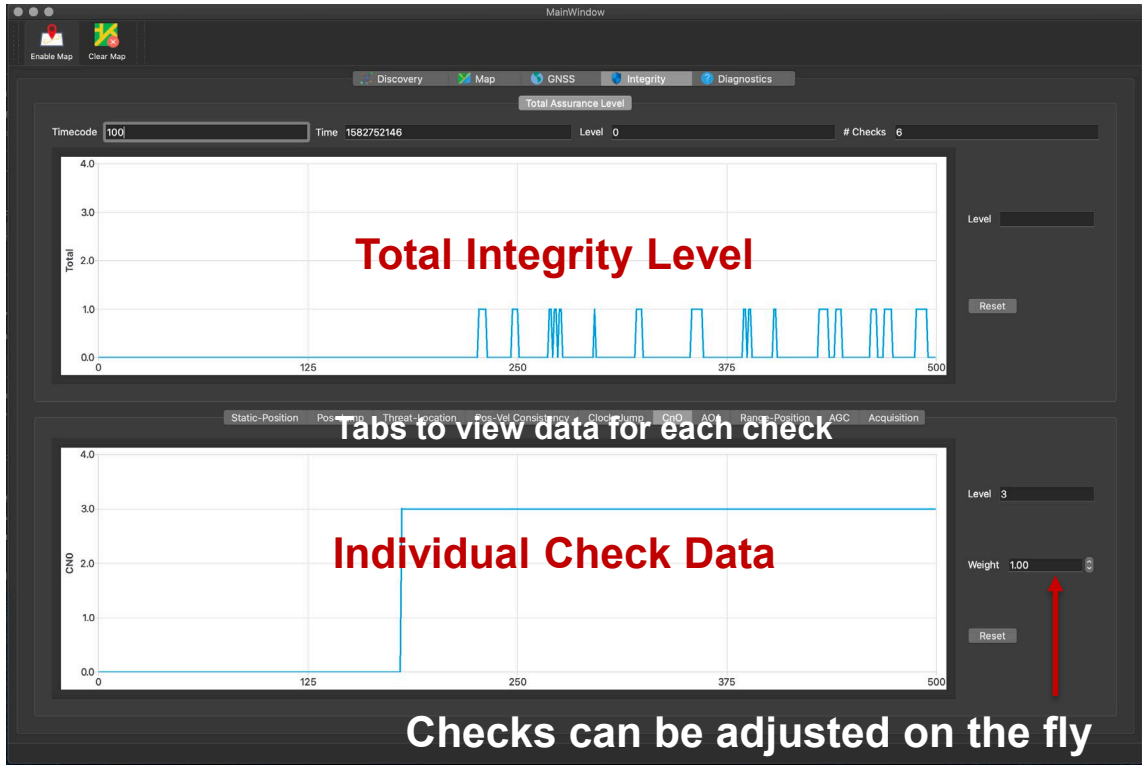
- Assembling a portable platform to demonstrate integrity library and integration with RF processing chain
- Integrity library integrated with receiver drivers and COTS hardware





Demonstration Application and User Interface

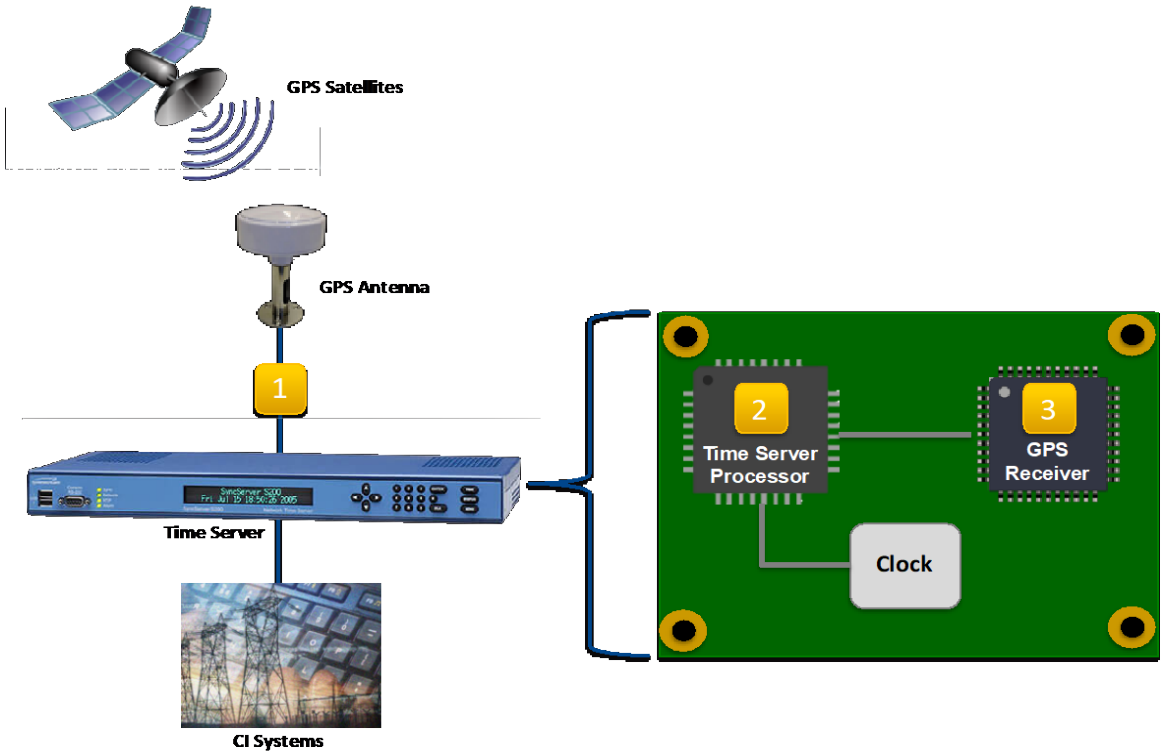
- Receiver interfaces and GUI to demonstrate integrity library and processing chain integration
- Checks can be added or removed to demonstrate effectiveness at different integration levels
- Displays receiver observables as well as integrity library data



Integration Options

- Toolkit components can be integrated at multiple levels by:
  1. End Users
  2. System Integrators
  3. Manufacturers

- Integrity library can be embedded in receiver or timing devices
  - –Integrator responsible for reading GPS observables and converting to standardized data model
  - –Library provides assurance level to allow operating through the event or alerting a user



- End-User Development Kit can be used standalone to provide alerts to users or feed other legacy timing devices

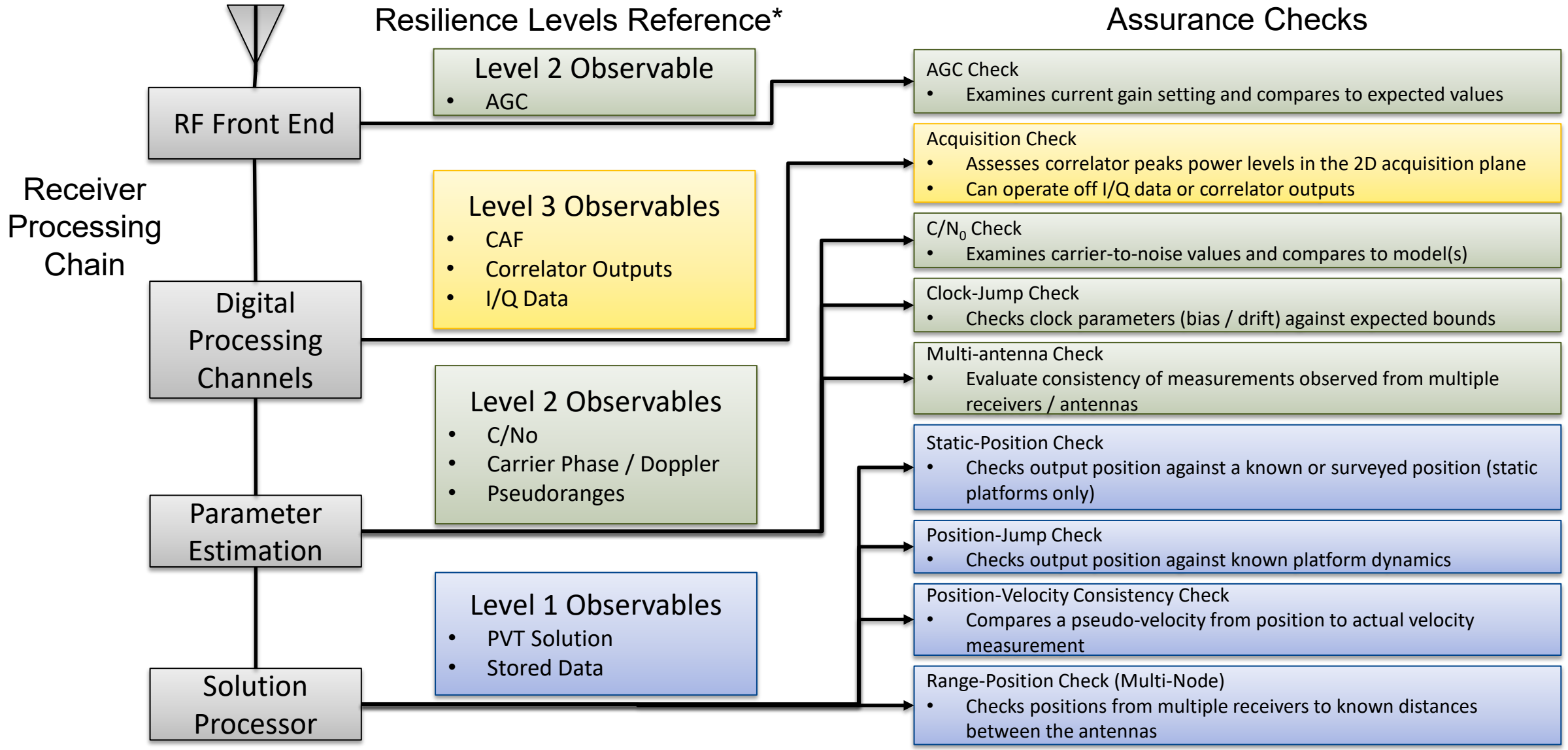
Wrap-Up

- Questions / Discussion

- Points of Contact
  - Josh Clanton, IS4S Technical Lead
    - josh.clanton@is4s.com
  - David Hodo, IS4S Program Manager
    - david.hodo@is4s.com

- IS4S would like to thank DHS S&T for their sponsorship of this effort

Alignment with PNT Conformance Framework

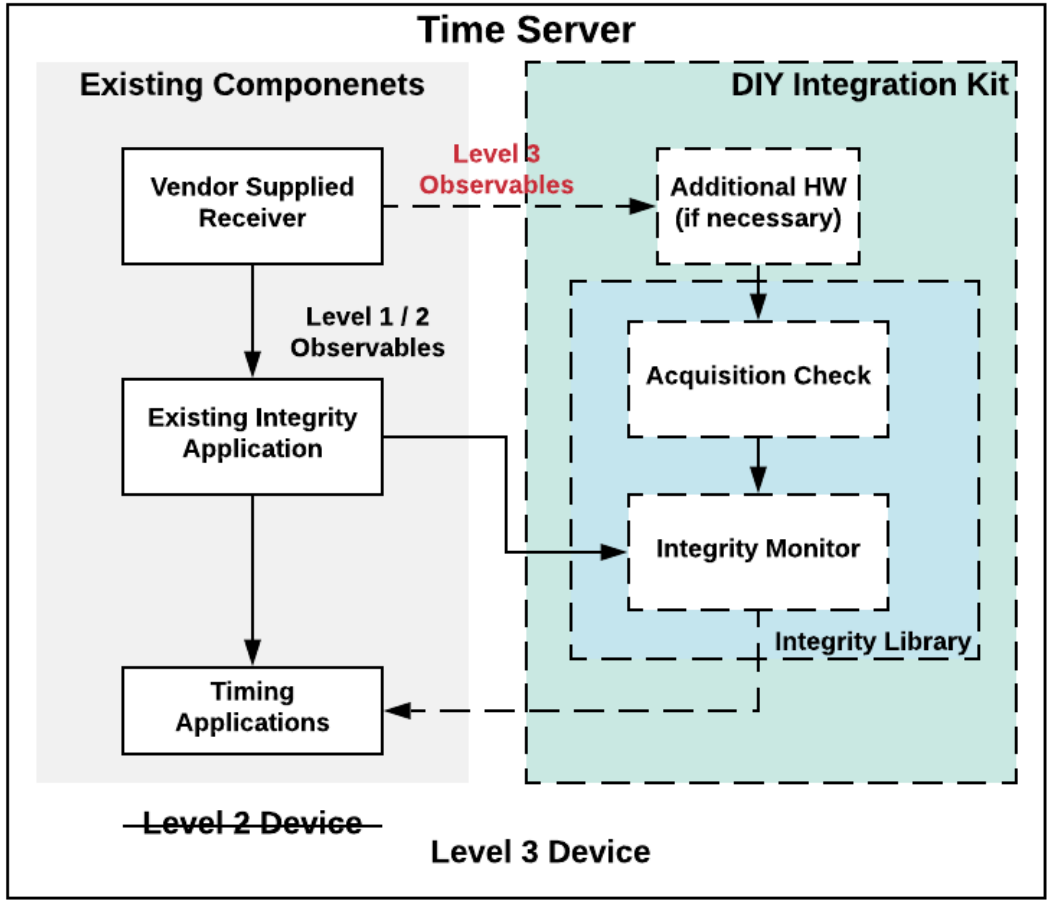


*As currently defined by DHS S&T / HSSEDI Resilient PNT Conformance Framework working group

Available Resources Forthcoming to the Community

IS4S
Integrated Solutions for Systems

- Integrity open-architecture reference implementation to be available as a software library from DHS S&T
  - Reference system for system integrators
  - Fill gaps in current offerings (i.e. adding software capability to go from a Level 1 to 2, for example)
  - Modular framework allows SI's to add their own flavor to spoofing mitigation
- Adaptation of the demonstration platform into a DIY kit available to the community
  - Not intended to be a competing product with current industry offerings
  - Best solutions will come from system integrator products
  - Targeted to end-users who need something quickly with no current market offerings meeting requirements
  - Could also be assembled as a reference system for Resilient PNT Conformance guidelines from DHS / HSSEDI



Homeland Security
Science and Technology

HSSEDI
Homeland Security Systems Engineering & Development Institute™