GPS Receiver Allow List Development Guide

July 12, 2021

Homeland Security

Science and Technology

Abstract

This publication presents a software assurance approach as a means of addressing potential vulnerabilities and increasing reliability of Global Positioning System (GPS) receivers. The approach utilizes input data validation based on allow list constraints to minimize the processing of malformed navigation messages entering a GPS receiver. An example allow list was implemented for the navigation data fields documented in the interface specification for a GPS signal; some benefits, limitations, and caveats of the approach are discussed here. Example allow lists are presented to illustrate the concept. Guidance is also provided for navigation device developers seeking to create, implement, and verify GPS allow lists customized to their particular systems.

Key Words

1. Allow list
2. GPS
3. LNAV
4. Software Assurance
5. Input Validation

Table of Contents

List of Tables

1 Introduction

Historically, Global Positioning System (GPS) receivers have been considered single-purpose appliances similar to radios. Radios required very focused, application-specific hardware but placed less emphasis on software. In contrast, today's receivers are implemented and integrated as embedded software applications distributed over general purpose processors with special GPS hardware accelerators. Depending on the application, receivers can be stand-alone embedded processing systems (e.g., u-blox NEO-M8N) or part of more complex systems (e.g., Qualcomm Snapdragon 410 systems-on-chip). In either case, receiver applications should be included within the security scope of a larger software system and protected by the same software assurance techniques used to reduce vulnerabilities and improve reliability of platform software. Good software assurance adds steps throughout the software development lifecycle to ensure reliability and minimize vulnerabilities within a final product,[1] and encompasses a large number of techniques, e.g., code analysis (static and dynamic), code structure, and error handling.

This document focuses on the software assurance technique of input data validation using allow list constraints as a means of minimizing the effects of malformed navigation (NAV) data entering a GPS receiver, either through the broadcast signal-in-space or possibly the control interface. It is assumed the reader has a detailed understanding of GPS system operations and GPS receiver design practices pertaining to navigation data. Data validation in this context provides confirmation that data entering a receiver are as correct as possible, given the information available. The validation constraints are codified in a series of rules (a "allow list") defining the values and behaviors (in time and/or state) of acceptable input data. Despite an allow list's limited ability to confirm the "correctness" of inputs in an absolute sense when inputs fall within expected bounds or behave in an expected manner, the application of allow list constraints helps prevent failures during software execution resulting from improper inputs, and does so without having to explicitly know the mode of failure.[2] Because allow list constraints do not identify failure modes, they do not require frequent updates as new failure modes are revealed; revisions are only necessary when the set of rules change or when new parameters are added.

Applying the concept of data validation using allow lists to GPS satellite downlink data is a simple, broad method to improve the reliability of GPS receivers. Moreover, it complements existing performance-improving techniques used in the navigation community. While Receiver Autonomous Integrity Monitoring (RAIM; it cross-checks navigation solutions to detect erroneous measurements) and augmentation systems (e.g., Wide-Area Augmentation System [WAAS]; used to correct errors in measurements) handle errors in intermediate processing products, allow list enforcement catches errors in the inputs to the receiver before navigation processing takes place. A drawback to data validation of GPS downlink data using an allow list is that GPS data messages are periodically modified in small ways, which can necessitate allow list updates. Also, implementing data validation requires additional Source Lines of Code (SLOC) to be developed and maintained for the receiver.

[1] The exact definition of software assurance varies, depending on organization. For example, the National Aeronautics and Space Administration (NASA) includes the development process as part of the assurance system. Safecode extends their definition further to include the interaction between software, hardware, and the surrounding services

[2] Allow lists thus differ from "blocklists," which identify specific "known-bad" cases.

To illustrate the application of the data validation technique to GPS signals for the purposes of software assurance in receivers, we present in this document an allow list for NAV data received via GPS satellite signals. The allow list is designed to ensure that a GPS receiver's input conforms to the United States (U.S.) Government's documented GPS signals and, as a result, a receiver's software executes as intended. We also present guidelines for development, implementation, and verification of application-customized allow lists.

2 Example GPS Allow List

2.1 Description

An exemplar allow list has been developed for the GPS legacy navigation (LNAV) message data structure specified in Appendix II of GPS Space Segment/Navigation User Segment Interface Specification IS-GPS-200L [1]. This "LNAV allow list" uses information from the Appendix II of IS-GPS-200L, the GPS Standard Positioning Service Performance Standard (SPS) [2], and simple physics of satellite orbits to identify constraints and behaviors of various fields of the LNAV message, from which a series of "checks" or "rules" for LNAV message data have been derived. These checks not only confirm that the NAV message demodulated by a GPS receiver is consistent with the signal-in-space specification but serve to identify errant signals as well.

To confirm agreement with the operational system, the rules included in the example allow list have been tested against several months of messages received in 2018 from the then current on-orbit GPS constellation. The tests demonstrated that its interpretation of the IS-GPS-200L descriptions are correct and permitted pruning of rules which caused false identifications under off-nominal conditions (e.g., signal blockages, satellite rising/setting, etc.) and rules which were susceptible to changes in constellation operation.

The example allow list for GPS LNAV message data is provided in Table 1. The table is organized by data field and has eight columns. The first three columns provide the data field name, description/purpose, and a text description of each allow list rule for that data field. The remaining columns provide reference information for traceability and ease of use. References to the specific paragraph(s) in IS-GPS-200L describing the field and its behavior are provided in the fourth column. Columns 5-8 detail the exact location of the bits in the LNAV message corresponding to the data field in question by subframe (SF), page, word, and bit number, and unambiguously indicate where each allow list rule should be applied. To simplify the table appearance, two short hand notations are used in Columns 5-8: (1) the "ALL" indicator in page and SF columns (Columns 5 and 6) specifies that the data field is contained in every SF or page; and (2) the "ALM" indicator is used in the page column (Column 6) to specify any/all pages containing almanac data, which are detailed in Table 20-V of IS-GPS-200L.

Table 1. Exemplar Allow list

Field Name	Field Description	Necessary Condition/Rule	IS GPS 200L References	SF	Page	Word	Bits
Data ID (SF 4)	Identifies the format of the navigation data modulated onto the signal	Must always be "01" for LNAV	20.1, 20.3.3.5.1.1	4	All	3	1-2
Data ID (SF 5)	Identifies the format of the navigation data modulated onto the signal	Must always be "01" for LNAV	20.1, 20.3.3.5.1.1	5	All	3	1-2
Preamble	Allows user equipment (UE) to achieve subframe sync	Must always be one value known *a priori*: 0x8B	20.3.3.1	All	All	1	1-8
Time of Week (TOW)	Time of transmission (within the GPS week) of the next subframe to arrive. Within a given GPS week, represents the master counter. Uniquely labels subframe.	(a) Must monotonically increase by 1 (corresponding to 6 seconds) over time relative to a known good time of week (modulo weekly rollovers) (b) Must be no more than 100,799 (c) Must be consistent with the true transmit TOW, if such an estimate is available from an independent source	20.3.3.2	All	All	2	1-17
Week Number (WN)	Master counter of GPS week number. Subject to rollover.	(a) Must always increase by 1 over time (modulo 1024-week rollovers) relative to a known good week number (b) Must only increment at midnight between Saturday and Sunday of GPS time (c) Must match the true GPS Week Number (modulo 1024) (d) Increases must align with the Time of Week rollovers	20.3.3.3.1.1	1	All	3	1-10
Codes on L2	Flag that indicates what spreading code is being transmitted on the L2 carrier	Must be one of 01 = P, 10 = C/A, or 00 = reserved	20.3.3.3.1.2	1	All	3	11-12

Field Name	Field Description	Necessary Condition/Rule	IS GPS 200L References	SF	Page	Word	Bits
Ephemeris SV health	Indicates potential issues with portions of signals or entire signals, such as the NAV data or the power of the carrier	Must only take on values that make sense given the configuration code of the satellite vehicle (SV).	20.3.3.3.1.4	1	All	3	17-22
Reference Time: Clock (t_{oc})	Reference time used in the SV clock offset computation	(a) Maximum value is 604,784. (b) Must follow fixed relationships between fit interval/transmission interval and offset to t_{oc} captured in Table 20-XIII	20.3.3.3.3.1	1	All	8	9-24
Square root of the semi-major axis (ephemeris)	Square root of the orbital semi-major axis	Must be greater than the Earth's radius for all SVs, but can be on the order of the distance of Earth's surface from the Earth's center for a generic transmitter. Tighter bounds can be set for SVs by limiting to low earth orbit (LEO) - high earth orbit (HEO) orbit heights.	20.3.3.4.3	2	All	8,9	17-24, 1-24
Reference Time: Ephemeris (t_{oe})	Reference time of week used throughout the satellite position computation algorithm. ln some cases, indicates new data being available.	(a) Effective range must be 604,784 (b) t_{oe} for at least first data set after new upload must be different from that prior to cutover (c) Must obey fixed relationships between fit interval/transmission interval and offset to toe. See Table 20-XIII	20.3.3.4.3	2	All	10	1-16
e - eccentricity	Eccentricity of SV orbit	Must be ≤ 0.03	20.3.3.4.3.1	2	All	6, 7	17-24, 1-24
Square root of the semi-major axis (almanac)	Square root of the orbital semi-major axis	Must be greater than the Earth's radius for all SVs, but can be on the order of the distance of Earth's surface from the Earth's center for a generic transmitter. Specifically, the ICD requires this value to be between 2530 and 8192.	20.3.3.5.1.2	ALM	ALM	6	1-24

Field Name	Field Description	Necessary Condition/Rule	IS GPS 200L References	SF	Page	Word	Bits
Almanac Own-SV Health	Indicates potential issues with portions of signals or entire signals, such as the NAV data or the power of the carrier. This is the 8 bit field that describes the NAV data health in the 3 most significant bits (MSBs) (Table 20-VII) and signal health in the 5 least significant bits (LSBs) (Table 20-VIII)	Must only take on values that make sense given the configuration code of the SV.	20.3.3.5.1.3	ALM	ALM	5	17 - 24
Almanac SV Health Summary (SF 4)	Indicates potential issues with portions of other SVs signals. This is the 6 bit field that describes NAV data health in its MSB and signal health in its 5 LSBs	Must only take on values that make sense given the block type of the SV.	20.3.3.5.1.3	4	25	8-10	See spec
Almanac SV Health Summary (SF 5)	Indicates potential issues with portions of other SVs signals. This is the 6 bit field that describes NAV data health in its MSB and signal health in its 5 LSBs	Must only take on values that make sense given the block type of the SV.	20.3.3.5.1 .3	5	25	4-9	See spec
Almanac A-S flags/SV config	Indicates SV block (i.e., capabilities), and anti-spoofing feature status. MSB indicates AS status. 3 LSBs indicate configuration of the SV.	Must only use defined bits as shown in 20.3.3.5.1.4; 000 is reserved	20.3.3.5.1.4	4	25	3-8	See spec
SV special message	Use reserved at discretion of Operating Command.	Do not use for integrity check. Use reserved at discretion of Operating Command.	20.3.3.5.1.8	4	17	3-10	See spec

Field Name	Field Description	Necessary Condition/Rule	IS GPS 200L References	SF	Page	Word	Bits
Reference Time: Almanac (t_{oa})	Reference time used to compute the almanac orbital parameters. It also serves as the almanac's version of the IODE field--a change in it indicates a change in the almanac data or the SV health.	(a) Effective range must be 602,112. (b) "...within an upload all t_{oa} values will be the same for a given almanac data set, and shall differ for successive data sets which contain changes in almanac parameters or SV health."	20.3.3.5.2.2, 20.3.3.5.2.3	ALM	ALM	4	1-8
Leap second day number	Day number within a GPS week at which the leap second should be applied	Must be between 1 and 7, inclusive	20.3.3.5.2.4	4	18	9	17-24
UTC reference week number (WN_t)	Truncated week number corresponding to the t_{ot} time	From the IS: "The CS shall manage these parameters such that the absolute value of the difference between the untruncated WN and [untruncated] WN_t values shall not exceed 127." The differences can be up to 127*2+1=255, which is one less than the total dynamic range of WN_t. Thus, there is always exactly one illegal value possible based on the current WN.	20.3.3.5.2.4	4	18	8	17-24
Leap second week number (WN_{LSF})	Reference week number of the scheduled/"future" leap second	From the IS: "When $delta\_t_{ls}$ and $delta\_t_{lsf}$ differ, the absolute value of the difference between the untruncated WN and [untruncated] WN_{LSF} values shall not exceed 127." The differences can be up to 127*2+1+255, which is one less than the total dynamic range of WN_{LSF}. Thus, there is always exactly one illegal value possible based on the current WN.	20.3.3.5.2.4	4	18	9	9-16
Reference Time: Time (t_{ot})	Reference time for UTC data	Maximum value is 602,112	20.3.3.5.2.4	4	18	8	9-16

Field Name	Field Description	Necessary Condition/Rule	IS GPS 200L References	SF	Page	Word	Bits
UTC offset: current	UTC time offset due to leap seconds	(a) Value should either be exactly the same or 1 second higher than previous value. (b) Value of field must always be at least 16 as of 1/2015	20.3.3.5.2.4	4	18	9	1-8
UTC offset: scheduled	UTC time offset due to leap seconds scheduled for future or recent past	(a) Value should either be exactly the same or 1 second higher than previous value. (b) Value of field must always be at least 16 as of 1/2015	20.3.3.5.2.4	4	18	10	1-9
Subframe ID	Indicates SF number, which is uniquely determined by time of week. Tells UE how to parse data within the SF.	(a) Must be in range [1,5] (b) Must increment by 1 sequentially within this range, wrapping around as necessary (c) Must start at 1 at the beginning of the week and cut back to 1 at week boundary (d) Must agree with the SF number computed from a correct TOW	20.3.4.1	All	All	2	20-22
Issue of Data, Clock (IODC)	Flag that indicates that new clock parameters are available in the data message. Can also be used to determine transmission interval and curve fit interval, which in turn determine reference time relationships.	(a) Must only take on specific ranges as a function of SV block (see Tables 20-XI and 20-XII) (b) 8 LSBs equal to IODE (c) Per 20.3.4.1, cutovers must occur on frame boundaries	20.3.4.4	All	All	3, 8	23-24, 1-8

Field Name	Field Description	Necessary Condition/Rule	IS GPS 200L References	SF	Page	Word	Bits
Issue of Data, Ephemeris (SF 2) (IODE)	Flag that indicates new ephemeris parameters available in message.	(a) Equals 8 LSBs of IODC of same data set (b) Changes to IODEs between SF2 and SF3 must be simultaneous (c) Must only take on specific ranges as a function of SV block (see Tables 20-XI and 20-XII) (d) Per 20.3.4.1, cutovers must occur on frame boundaries; thus, a new SF2 must be followed immediately by a new SF3	20.3.4.4, 20.3.3.4.1	2	All	3	1-8
Issue of Data, Ephemeris (SF 3)	Flag that indicates new ephemeris parameters available in message.	(a) Equals 8 LSBs of IODC of same data set. (b) Changes to IODEs between SF2 and SF3 must be simultaneous. (c) Must take on specific ranges as a function of SV block. (see Tables 20-XI and 20-XII) (d) Does not repeat over preceding 6 hours. (e) Per 20.3.4.1, cutovers must occur on frame boundaries	20.3.4.4, 20.3.3.4.1	3	All	10	1-8

The list of rules in Table 1 can be divided into four basic classes, to which we will refer in later sections. The simplest class is “value checking,” in which a field is verified to be a single, expected value (e.g., the rule for the Preamble field in Table 1). Only slightly more complex is the class of “range” or “bounds checking,” which is really the superset of value checking. Range checking, as exemplified by the test in Table 1 for eccentricity, confirms that a data field is within a prescribed range or a member of an allowed set. The class of “temporal checks,” e.g., rule (b) in Table 1 for the Week Number data field, uses information about the current time to verify that a data field exhibits a specific behavior as a function of real time, or at a specified moment in time. The “state history validation” class contains some of the most complex rules; it is similar to temporal checks in that the tests verify that a data field changes appropriately over time, but do not require a field to have an explicit dependence on real time. One example of state history validation is the criteria for checking the leap second week number field in Table 1.

2.2 Scope of Exemplar Allow List

The GPS LNAV allow list presented in Table 1 is intended to be a simple, straightforward example of the allow list concept. Moreover, data validation using the exemplar allow list is intended to have a minimal impact on a receiver’s processing and memory resources: all of the checks examine the information from a single satellite data stream only, over a short time horizon. Most of the checks operate on a single data field at a time, keeping memory

requirements low. The simplest of GPS receivers should be capable of implementing this allow list to validate, with high reliability, that inputs to the receiver software are within expected parameters. While many different hardware platforms could implement data validation as a software assurance measure, no special capabilities of these platforms are required to use any of the rules listed in Table 1; for example, any time information required for the tests can be provided by the clocks used to acquire and demodulate the RF signal.

Due to the desire for low computational requirements and high reliability, the example allow list in Table 1 cannot and should not be considered exhaustive. Many possibilities exist for extending the example allow list to make it more comprehensive. As the example allow list only addresses information within a single satellite's downlink message, one may add tests of data across multiple satellites or constellation-based cross-checks.[3] Additional tests incorporating data from multiple message data fields or longer time horizons are also available. For more capable systems, the opportunities for data validation expand greatly. In systems with high-accuracy clocks, checks based on absolute time become possible.[4]

3 Guidelines for a Customized GPS Allow list

One can implement data validation using allow lists in any type of system employing a GPS receiver, e.g., a complete receiver that processes from RF signal through to position and time solutions (a stand-alone handheld or car GPS) or systems which integrate or fuse inputs from a GPS receiver with other hardware, software, and sensors to output the position or time (such as a timing receiver with a disciplined clock, or vehicle systems with integrated sensors including inertial measurements). A stand-alone receiver will directly process the data message transmitted via the signal-in-space, to which allow list constraints similar to those in Table 1 can be applied. On the other hand, system integrations combining a GPS receiver with other hardware are usually built around a receiver card or module from some GPS receiver manufacturer which communicates via some protocol, open or proprietary, to some processing element in the receiver. These protocols, including National Marine Electronics Association (NMEA) and Receiver Independent Exchange Format (RINEX), usually convey information about the receiver position, the current time, health information about their fused measurements, and constellation health. The message streams can contain a variety of information that can be validated against an allow list. Often the protocols can provide almanacs and ephemeris used in the navigation solution, which can be checked against a portion of an allow list created for a stand-alone GPS receiver.

Allow list development combines deriving a set of rules from the GPS signal of interest's interface specification (also referred to as the "standard" or the "spec") and testing the validity of those rules against simulated and real messages transmitted by the appropriate satellite constellation to ensure the standard has been interpreted correctly. The following guidelines can be used to assemble a customized allow list which works with the data available to a particular system.

[3] For example, in the LNAV message, multiple almanac and UTC corrections exist on all the satellites at the same time and are all within their fit interval. This means the UTC corrections should all be consistent with the error bounds of the SPS.

[4] Time related checks have both an absolute and relative implementation. An incrementing counter such as TOW can be checked that it increments about once every six seconds, a relative check. The absolute check would make sure it is the right value for the current time of day.

3.1 Rule Development

Allow list rules are merely a set of tests. The first step in rule development is to list all the data fields from the navigation data message which are relevant to your receiver; or, if the receiver is part of an integrated system, list the message fields which are available for validation by cross-checking the standard and the interface specification for your system's receiver message protocol. Reserved and spare data fields should be ignored, as they are not publicly documented and cannot be checked. The special message field also should be ignored as its use is at the discretion of the Operating Command. Data fields in the navigation message which are not used in your particular receiver/system may also be ignored. However, some unused or "irrelevant" fields may contain valuable information against which "relevant" fields can be checked, so we recommend including as many data fields as possible in your list, as long as constraints on those fields are well understood and do not risk rejection of legitimate data messages in the future.

Second, derive requirements governing each data field in the list using the descriptions in the standard. Further insight into trends in and constraints on the data fields may be gleaned through analysis of archived navigation message data from the appropriate GPS.[5] However, we caution that signal standards for the various GPS constellations tend to be living documents and are frequently revised, so historical data may not represent the current standard employed by the system operators. For this reason, the most recent revision of the desired signal standard should be regarded as the authoritative information source. While working with the spec, the following questions may be of assistance in enumerating the requirements for each data field:

- What is the purpose of the data field? Does it describe a state, a parameter, or an alert?
- Can the data field be constrained? If so, what is the range, or set, of allowed values?
- How should the data field change as time progresses? Some potential responses are:
    - Static (single-valued)
    - Any value within a valid range
    - Increments by a specific value
    - Changes according to a rule
- Does the data field have a relationship to, or is it constrained by, another field in the message?
- Does the data field make provisions for special conditions?

When identifying the requirements for a particular data field, care should be exercised so as not to create *new* requirements for the field, i.e., ones which are not contained within, or supported by, the standard.

The next step is to create tests to determine if a receiver/system input meets the requirements identified in the second step. Multiple tests of different types may be created for a single field: test types to consider include value tests, bounds tests, state history validation, and temporal

[5] For example, the CORS network maintains a public archive of historical GPS LNAV message data in RINEX format at https://www.ngs.noaa.gov/CORS/.

tests. When creating the tests, note what information/inputs are necessary to perform each test, besides the data field itself, e.g.:

- Is another data field needed, and if so, should the field in question be checked in conjunction with the other field?
- Is the current time needed?
- Is a previous value of the data field needed?

The tests should be designed with flexibility to accommodate future changes to the standard, where possible, to avoid test failures when the standard is updated. It may not be possible to design useful, future-proof tests for all data fields; in such cases device software updates may be a more reasonable response to spec revisions.

Finally, prune the list of tests according to your system's capabilities. A particular test may not be suitable if it requires more information or resources than are available to your system. Tests which cannot accommodate special operational conditions or constellation changes may also require removal. The goal is to have as many tests as possible, which handle as many circumstances as possible, while simultaneously permitting uninterrupted operation of the receiver or system.

3.2 Implementation

Transforming an allow list on paper into functional input data validation software is a straightforward process. What requires special attention are the details associated with applying the allow list tests ("heuristics") efficiently, in real-time, under non-ideal conditions. In particular, the following points should be considered when designing and implementing GPS input data validation software using allow list constraints:

- the timing and frequency of data tests
- under what conditions data tests should be performed[6]
- the order in which various tests should be performed; the results of one test may be usable in multiple later tests, or more critical than another test
- handling of both regular (e.g., data set cutovers, satellite rise/set) and unpredictable (e.g., outages, interference, dropped messages) changes to data sets
- handling of GPS constellation configuration changes (e.g., satellite repositioning, satellite addition/removal) and special operational conditions (e.g., extended operations mode for GPS described in IS-GPS-200).

The action taken should data fail an allow list check, and the timing of that action, is also an important decision when implementing input data validation. Responses to failed tests should be tailored to a receiver or system based on how the system is used (CONOPs) and the system's capabilities. For simple receivers, acceptable responses may be restricted to dropping the message containing the failing data or power-cycling the device. Other potential responses

[6] From requirements listed in RTCA DO-229 [3], a C/N_0 in excess of approximately 30dB-Hz is recommended for demodulating data. We recommend applying this threshold prior to executing allow list tests for maximum reliability. Data below the threshold should be ignored.

include sounding an alarm, “coasting” a solution using older data, or re-computing a solution while excluding the failing data. Integrated navigation or timing systems have an additional option of relying on other sensor data, such as that from an inertial measurement unit or a backup clock, when navigation message data fails an allow list test.

3.3 Verification

Verification testing is essential to not only ensure proper implementation and integration of GPS data validation and allow lists in software, but also to demonstrate that the standard has been interpreted correctly when drafting the allow list rules. The testing stage must include unit and system-level tests of the software utilizing digital simulation, Radio Frequency (RF) simulation, and recordings of GPS signals received over-the-air. Live sky system tests, while helpful, are not sufficient to verify an implementation.

Standard unit tests of GPS navigation data validation software and extensive system tests should be carried out in a digital environment, such as a PC-based test bench or digital system simulation. Such environments offer the most flexibility and speed for testing a large number and wide variety of software inputs. System-level tests should present both allow list-compliant and non-allow list compliant inputs to the software to verify the system’s response to the outcome of the allow list tests. Depending on the capabilities of the digital test environment and system application, the system tests should employ either or both recordings of over-the-air GPS signals and archived navigation message data. Detailed logging of success and failure in detecting allow list-compliant inputs in such tests permits post-test effectiveness analysis via computation of probabilities of detection and misidentification of disallowed data (i.e., “false alarms”).

Because of the ease with which large numbers of test trials can be conducted, digital system-level testing is also the best opportunity to validate one’s interpretation of the GPS signal standard. Tests using recorded over-the-air GPS signals provide the most feedback on the interpretation since the recordings offer the opportunity to, in effect, “interact” with the GPS system’s operators in a wide variety of circumstances. Such tests may reveal unanticipated complexities of the navigation data message definitions and unintended consequences of some allow list rules.

Additional system-level verification testing should be conducted using RF signals received and processed in real time. To create controlled conditions for RF tests, GPS constellation simulators can be used in conjunction with other test equipment to generate RF waveforms, which can be injected directly into the system under test. Receiver/ system outputs recorded from such tests are useful in determining the impacts of input data validation on system performance.

4 Summary

Input data validation using allow list constraints is a simple and valuable tool by which a measure of software assurance can be introduced into systems which receive and process GPS signals. Although the allow list approach has tradeoffs, such as potential compatibility impacts with future signal specification changes, it is nonetheless an effective method to ensure that navigation data inputs conform with published specifications and the expectations of a GPS device’s software. We have presented here an example allow list for GPS LNAV message data, guidelines for GPS device developers to create and implement their own customized allow lists.

This information is provided to motivate navigation device developers to implement software assurance measures within their systems.

List of Acronyms

Acronym	Definition
CONOPs	Concept of Operations
CS	Control Segment
DHS	Department of Homeland Security
GPS	Global Positioning System
HEO	High Earth Orbit
ID	Identifier
IODC	Issue of Data, Clock
IODE	Issue of Data, Ephemeris
LEO	Low Earth Orbit
LNAV	Legacy Navigation
LSB	Least Significant Bit
MSB	Most Significant Bit
NAV	Navigation
NMEA	National Marine Electronics Association
RAIM	Receiver Autonomous Integrity Monitoring
RINEX	Receiver Independent Exchange Format
RF	Radio Frequency
RTCA	Radio Technical Commission for Aeronautics
SLOC	Source Lines of Code
SPS	Standard Positioning Service Performance Standard
SF	Subframe
SV	Satellite Vehicle
SVID	Space Vehicle Identifier
TOW	Time of Week
UE	User Equipment

Acronym	Definition
US	United States
UTC	Coordinated Universal Time
WAAS	Wide-Area Augmentation System
WN	Week Number
WN_{LSF}	Leap Second Week Number
WN_t	UTC Reference Week Number

List of References

[1] Global Positioning Systems Enterprise Space and Missile Systems Center, *Interface Specification IS-GPS-200: Navstar GPS Space Segment/Navigation User Segment Interfaces*, IS-GPS-200L, 14 May 2020

[2] *Global Positioning System Standard Positioning Service Performance Standard*, 5th Edition, April 2020

[3] RTCA, *DO-229 Operational Performance Standards for Global Positioning System Satellite-Based Augmentation System Airborne Equipment*, 15 Dec 2016