Secure Position Augmentation for Real-Time Navigation (SPARTN) Interface Control Document

Version 2.0.2

Scottsdale, February 2022

Table of Contents

1. Revision Control

Version	Date modified	Changes/updates
1.0	February 7 2018	- Initial version of ICD proposal including OCB messages only
1.1	March 23 2018	- Follow up of ICD proposal including atmospheric messages
1.2	August 1 2018	- Re-structuring of messages and document layout in accordance with feedback by all partners and collaborators in the SAPA format development
1.3	August 22 2018	- Incorporation of comments from technical board meeting; - Addition of several aspects of message interpretation and integration.
1.4	October 3 2018	- Adjust of HPAC atmosphere data field bounds - Added preface, introduction and carrier phase alignment sections
1.5	November 3 2018	- Added confidentially note in every page of document
1.6	December 7 2018	- Renamed HPAC Area definition message to Geographic Area Definition - Dropped Special Values representing invalid Satellite Corrections (SF020) and code bias correction (SF029). Range remains the same. - Decreased length of code bias masks by 1 to make them same length as phase bias masks. See SF027 and SF028 - Fixed inconsistency between Number of Grid Points Present (SF039) and Area Latitude Grid Node Count (SF034) and Area Longitude Grid Node Count (SF035). - Fixed Ionosphere Grid Residuals definition (table 6.22 and table 6.32) as data field referenced was incorrect. - Removed end-of-set from Geographic Area Definition Message as it is not required. - Minor spelling and grammar changes - Updated message size calculations due to changes described above
1.6.1	April 9, 2019	- Increased size of SF039 to 7 bits to support more than 63 grid points - Adjusted message size computations for change in SF039
1.6.2	May 15, 2019	- Added offset to large troposphere coefficient (SF048) to match the offset on the small troposphere coefficient (SF045).
1.7.0	June 29, 2019	- Renamed SF006/SF007 to Solution ID and Solution Processor ID respectively. - Restrict satellite reference datum to be consistent across all messages within a solution ID - Addition of 1 reserved bit to each message header - Specifically define bias track types - Add description on restricting the use of area definition related data to users located within the boundary of the area. - Merged message sub-types for OCB and HPAC messages

		- Replaced area continuity indicator with an Area Issue of Update to remove ambiguity of reference time - Added implementation details for troposphere height correction, phase windup, yaw attitude and GLONASS leap second handling - Removed unnecessary invalid field values. - Updated message size calculations - Added item to section 8.4 describing how the End-of-Set will exist in future OCB messages. - Fixed typo in polynomial coefficients
1.8.0	January 24,2020	- Added new message type to low precision ionosphere for sub-meter positioning. - Created a Payload Description Block that is part of the Transportation Layer and moved Message sub-type, Time-tag, Solution ID, and Solution Processor ID into that block to support encryption/authentication - Changed Small time tag from 12-bit (hourly time tag) to 16-bit (half day time tag) to support consistent byte alignment of frame/payload description for both encrypted and non-encrypted data - Added encryption and embedded/group authentication concept - Added additional acronym definitions and fix consistency issues with capitalization of data field names - Changed name to SPARTN - Moved Area IOU before reserved bit in HPAC message (SM-1) for consistency with GAD (SM-2) message. - Rename Low Precision Atmosphere Correction to Basic Precisions Atmosphere Correction - Added note to troposphere computation that ellipsoidal height to be used for mapping function computation - Added legal disclaimers
2.0.0	June 17, 2021	- Added support for Galileo, BeiDou and QZSS - Added additional signal support for GPS - Added proprietary message content - Clarified definition of Grid Node Present Mask (SF079) - Replaced Safe with Secure in name of SPARTN - Fixed payload length description in TF016
2.0.1	September 28, 2021	- Added note to indicate minimum implementation of the SPARTN format in section 6 - Other minor editorial changes
2.0.2	February 21, 2022	- Extended BDS signal types for code and phase biases with BeiDou 3 signals

2. Preface

The Secure Position Augmentation for Real Time Navigation (SPARTN) format was designed as an open standard to provide the data necessary to support high precision positioning applications using GNSS processing techniques in a secure manner. This document describes message formats, concepts behind field content, the types of data carried, what information various messages convey, as well as methods and algorithms that are necessary for fundamental use of such data.

3. Acronyms and abbreviations

AES – Advanced Encryption Standard

AIOU – Area Issue of Update

BDS – BeiDou

CAD – Computed Authentication Data

CCITT – Conservative Committee for Telephony and Telegraphy

CRC – Cyclic Redundancy Check

CTR – Counter

DNU – Do-not-use

EAF – Encryption and Authentication Flag

EAS – Encryption and Authentication Support

ECEF – Earth-Centered Earth-Fixed

ECI – Earth-Centered Inertial

EOS – End-of-set

GAD – Geographic Area Definition

GLONASS - GLObal NAvigation Satellite System

GNSS – Global Navigation Satellite Systems

GPS – Global Positioning System

HPAC – High-Precision Atmosphere Correction

IODE – Issue of Data Ephemeris

IOU – Issue Of Update

ITRF – International Terrestrial Reference Frame

IV – Initialization Vector

BPAC – Basic-Precision Atmosphere Correction

OCB – Orbits, Clocks, and Biases

PRN – Pseudo-Random Noise (used to denote a specific GNSS satellite)

QZSS – Quazi-Zenith Satellite System

SPARTN – Secure Position Augmentation for Real Time Navigation

SF – SPARTN field(s)

SHA – Secure Hash Algorithm

SIOU – Solution IOU

SM – SPARTN message(s)

TECU – Total Electron Content Unit

TF – Transport layer Field

URE – User Range Error

VTEC – Vertical Total Electron Content

4. Introduction

Global Navigation Satellite Systems (GNSS) are satellite-based positioning systems that are currently providing global service 24 hours each day. Systems within GNSS, include, the Global Positioning System (GPS), the GLObal NAvigation Satellite System (GLONASS), Galileo satellite system, the Quasi-Zenith Satellite System (QZSS), and the BeiDou Navigation Satellite System (BDS). Many types of correction services exist to improve the accuracy of these systems. Among these are techniques that emerged from precise positioning approaches that do not require that the end-user also set up some reference GNSS station or network. These systems rely on service providers to gather and process information from numerous real-time sources then broadcast the data to the end user to be used in connection with their own GNSS receiver for the purpose of accurate positioning/navigation realization.

To date there exists no open, industry recognized standard that supports low bandwidth requirements required by some delivery systems while, at the same time, providing standards for integrity for safety of life applications. The SPARTN message protocol has been developed with the goal of meeting these requirements.

5. Application Layer

The Application Layer defines how messages can be applied for different end-user applications. The messages provided in this document are for broadcasting (provider or sending) services, and they are not intended for two-way data links. As such, information is developed centrally by a Service Provider, who has an institutional or commercial interest in providing data that enables end-user applications for precise positioning or navigation.

The use of GNSS data for positioning and navigation has become an essential part of modern countries, their industries, their economy, and their people. Among these are techniques that emerged from precise positioning approaches that do not require that the end-user also set up some reference GNSS station or network. The initial offering of this standard is focused at the numerous applications that exploit such precise positioning approaches. Primarily the application layer for the use of these messages is within the systems exploiting GNSS receivers to produce precise positioning and navigation for real-time applications. The messages of this standard are focused at delivering the information which facilitates those end goals.

6. Presentation layer

The table below shows the existing message types in the SPARTN format design.

At least one Subtype of message Type 0 must be implemented to make proper use of the SPARTN format.

Table 6.1 – Messages types and subtypes in SPARTN

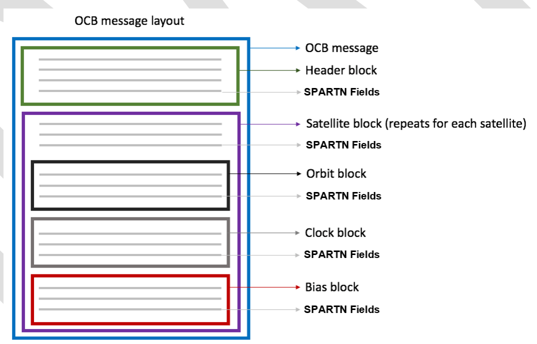
Type	Subtype	Message name	Description
0	0	GPS OCB	**GNSS Orbit, Clock, Bias (OCB) messages** These are the messages that carry data for satellite orbits, clocks, biases, and other auxiliary information. These messages are sufficient to allow global positioning modes that do not require the transmission of atmospheric data.
	1	GLONASS OCB	
	2	Galileo OCB	
	3	BeiDou OCB	
	4	QZSS OCB	
	5 to 15	TBD	
1	0	GPS HPAC	**High-precision atmosphere correction (HPAC) messages** These are the messages that contain high-precision atmosphere data, specifically ionospheric and tropospheric correction data. Both ionosphere and troposphere data are transmitted in the same message for each constellation.
	1	GLONASS HPAC	
	2	Galileo HPAC	
	3	BeiDou HPAC	
	4	QZSS HPAC	
	5 to 15	TBD	
2	0	GAD	**Geographic Area Definition (GAD) messages** These are the messages used to define geographic areas of data usage. The use of these messages can serve different purposes, including atmospheric data availability and other types of geographical/geometrical aspects of usage of data.
	1 to 15	TBD	
3	0	BPAC Polynomial	**Basic-precision atmosphere correction (BPAC) messages** These are the messages that contain basic-precision atmosphere data which prioritizes compression over accuracy. The messages may consider ionosphere and troposphere constituents.
	1 to 15	TBD	
4	0	Dynamic Key	**Encryption and Authentication Support (EAS) messages** These are the messages which are used to support encryption and authentication of message payload information.
	1	Group Authentication **(Deprecated – To be removed in future versions)**	
	2 to 15	TBD	
5 to 119	TBD	TBD	**TBD**
120	0	In-house proprietary test	**Proprietary messages** These messages are proprietary and are defined by the organization to whom they are assigned.
	1	u-Blox AG	
	2	Swift Navigation	
	2 to 15	TBD	
121 to 127	0 to 15	TBD	

6.1. General message layout

The SPARTN messages payload is structured as a composition of different elements. Those elements are listed below:

- SPARTN field – The SPARTN fields are the most basic element of every SPARTN message. They contain, in most cases, a single piece of information;
- Block – A block is a group of related SPARTN fields that are often repeated within a message, or simply used to cleanly separate different types of data within a message. In most cases the SPARTN fields within a block contain pieces of information that should be used in combination with each other. Blocks can contain other blocks;
- Header – SPARTN message headers contain general information about the message that applies to all blocks within that message;
- Message – The SPARTN messages (SM) are typically built with one header and one or more blocks, depending on the type of the message.

The figure below shows a representation of the OCB message (SM 0-0) layout as an example:



6.2. Continuity controls

The following is a list of existing continuity controls in the SPARTN message format, some of which are found in the Transportation layer:

- Solution ID (TF010) – Specifies a unique identifier of the current solution which consists of all instances of a correction streams that are generated for a given area of coverage. When a change in the Solution ID is encountered, no guarantee on continuity is provided;

- Solution Processor ID (TF011) – Specifies the instance of the processor being used for generating correction data. When a change in the Solution Processor ID is encountered, no guarantee on continuity is provided;
- Solution Issue of Update (SF005) – Controls when and if different parts of the correction that are sent in separate messages can be combined for processing;
- Continuity Indicator (SF015) – Indicates the time over which no discontinuities have occurred. Processor implementation must reset their current state when the time since the last processed (or received) data is greater than the continuity time indicated in this data field;
- IODE Continuity (SF022) - Indicates if there has been a change in the IODE (SF018,SF019, SF099, SF100 and SF101) currently in use for the correction data. In case of a change, users must wait to receive a new IODE, issued after the indicated change. A new IODE must be received before continuing combining correction and broadcast ephemeris data;
- Area Issue of Update (SF068) –Controls when and if area data from different messages can be combined for processing.

6.3. Floating-point numbers conversion

SPARTN achieves some of its compression by converting floating-point numbers to integer representations using range and resolution values. The following equation shows how to perform the conversion from encoded (unsigned integer) values to decoded (floating-point numbers) values:

$V_{decoded} = (V_{encoded} * Res) + Rng_{min}$,

where $V_{decoded}$ is the decoded value that is retrieved after converting the encoded value ($V_{encoded}$) from an integer to a floating-point number. Res is the field resolution, and Rng_{min} is the lower limit of the data field range.

The following equation shows how to perform the conversion from original (to be encoded floating-point numbers) values to encoded (unsigned integer) values:

$V_{encoded} = (V_{original} - Rng_{min}) / Res$,

where $V_{encoded}$ is the encoded integer value that is transmitted in the data field, and $V_{original}$ is the original value (floating-point number) that shall be encoded in the data field.

In the case of invalid or special values, encoders shall directly encode the special value as an unsigned integer. Decoders must check for special values prior to performing the conversion to a floating-point number.

6.4. SPARTN fields

The following table lists all data field definitions used in the SPARTN message format.

Table 6.2 – SPARTN fields

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF005	Solution issue of update (SIOU)	9	0 to 511	1	none	The SIOU controls when and if different parts of the correction that are sent in separate messages can be combined for processing. The SIOU can't change more than once per second. User must assume that SIOU has changed over outages of 510 secs or more even if the SIOU before/after an outage matches. SIOU is a solution-wide indicator and is not specific to any message type or subtype.
SF008	Yaw present flag	1	0 to 1	n/a	0 : SF021 not present 1 : SF021 present for all orbit blocks	The yaw present flag indicates whether the satellite orbit blocks will contain a yaw value. When set, all blocks will contain the yaw value field (SF021). When not set, none of the orbit will contain the yaw value field (SF021).
SF009	Satellite reference datum	1	0 to 1	1	0 : ITRF 1 : Provider defined	Reference datum indicator of the satellite orbits. When set to 0 the reference datum is ITRF current epoch, latest realization. When set to 1 the reference datum is defined by the provider. For practical purposes the evolution of current and future ITRFs is below the observable accuracy of real time GNSS systems. NOTE: Service providers must provide a consistent reference datum for a given Solution ID/Solution processor ID pair.
SF010	End of OCB set (EOS)	1	0 to 1	n/a	0 : more OCB subtype messages to follow 1 : All OCB subtype messages sent	The End of Orbit, Clock, Bias set indicates that all messages of the current type (including all subtypes) have been sent for a single epoch.
SF011	GPS satellite mask	34 to 66	Bitmask	Bitmask	Leftmost 2 bits indicate bitmask size to follow: 0 : 32 bits 1 : 44 bits 2 : 56 bits 3 : 64 bits	GPS satellite mask field is composed of two bits that indicate the bitmask size, followed by the bitmask. The bitmask after the 2-bit size defines the IDs and order of GPS satellites in the message. The bitmask position added by 1 is equal to the Pseudo-Random Noise (PRN) ID of a satellite. At least one satellite must be present in the bitmask. Bitmask position 0 is the leftmost bit of the satellite mask, excluding the 2-bits indicating the size of the bitmask.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF012	GLONASS satellite mask	26 to 65	Bitmask	Bitmask	Leftmost 2 bits indicate bitmask size to follow. 0 : 24 bits 1 : 36 bits 2 : 48 bits 3 : 63 bits	GLONASS satellite mask field is composed of two bits that indicate the bitmask size, followed by the bitmask. The bitmask after the 2-bit size defines the IDs and order of GLONASS satellites in the message. The bitmask position added by 1 is equal to the orbit slot of a satellite. At least one satellite must be present in the bitmask. Bitmask position 0 is the leftmost bit of the satellite mask, excluding the 2-bits indicating the size of the bitmask.
SF013	Do not use (DNU)	1	0 to 1	n/a	0 : Satellite fields present 1 : No fields in the associated satellite block will be present	The primary purpose of the DNU Flag, when set, is to indicate some negative health, negative integrity, poor quality, and other such negative aspects of the satellite and its data. When this flag is set, the remaining fields of this section for this satellite shall not be present. Users must immediately stop using any satellite that has been flagged with a DNU indicator.
SF014	OCB present flags	3	Bitmask	Bitmask	Bit 0 (leftmost) 0 : Orbit block no 1 : Orbit block yes Bit 1 (middle) 0 : Clock block no 1 : Clock block yes Bit 2 (rightmost) 0 : Bias block no 1 : Bias block yes	The OCB present flags field is a bitmask that is used to indicate which combination of orbits, clocks, or biases data blocks are present in the message.
SF015	Continuity indicator	3	0 to 7	n/a	0 : 0 secs 1 : 1 secs 2 : 5 secs 3 : 10 secs 4 : 30 secs 5 : 60 secs 6 : 120 secs 7 : 320 secs	Indicates if there has been a discontinuity in the data accompanied by the indicator. The time values provided here are to be read as: "The data has had no discontinuity within the last X seconds.", where X is the value provided in the special values list of this row. Processor implementation must consider resetting their current state when a data gap (i.e. last epoch processed or received) greater than the continuity time has occurred.
SF016	GPS ephemeris type	2	0 to 3	n/a	0 : GPS L1C/A 1 to 3 : TBD	Type of ephemeris being used for GPS corrections.
SF017	GLO ephemeris type	2	0 to 3	n/a	0 : GLO L1C/A 1 to 3 : TBD	Type of ephemeris being used for GLONASS corrections.
SF018	GPS IODE	8	0 to 255	1	none	Issue of data ephemeris (IODE) field that indicates to which GPS broadcast IODE the corrections must be combined with in order to be processed by the user.
SF019	GLO IODE	7	0 to 127	1	none	Issue of data ephemeris (IODE) field that indicates to which GLONASS broadcast IODE the corrections must be combined with in order to be processed by the user.
SF020	Satellite corrections	14	±16.382 m	0.002 m	none	Correction value in unit of meters.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF021	Satellite yaw	6	0 to 354°	6°	0x3F = invalid	Yaw attitude angle of satellite. The yaw correction is with respect to the satellite frame described in section Satellite Frame Convention
SF022	IODE continuity	3	0 to 7	n/a	0 : 0 secs 1 : 1 secs 2 : 5 secs 3 : 10 secs 4 : 30 secs 5 : 60 secs 6 : 120 secs 7 : 320 secs	Indicates if there has been a change in the IODE (SF018/SF019/SF099/SF100/SF101) currently in use for the correction data. In case of a change, user must wait to receive a new IODE, issued after the indicated change. A new IODE must be received before continuing combining correction and broadcast ephemeris data. The time values provided here are to be read as: "The data has been generated using the same IODE over the last X seconds.", where X is the value provided in the special values list of this row.
SF023	Fix flag	1	0 to 1	n/a	0 : Float 1 : Fixed	Indicates if the clock solution, in combination with orbits and biases, has been generated using fixed ambiguities or float ambiguities.
SF024	User range error (URE)	3	0 to 7	n/a	0 : unknown 1 : 0.01m 2 : 0.02m 3 : 0.05m 4 : 0.1m 5 : 0.3m 6 : 1.0m 7 : > 1.0m	Indicates the expected range error of the combined OCB corrections. Value 0 means that there is no known value for this field. Value 7 means that the URE is greater than 1.0 m and corrections can still be used when proper considerations about the uncertainty of the corrections are made.
SF025	GPS phase bias mask	7 or 12	bitmask	bitmask	Leftmost bit indicates bitmask size to follow: 0 : 6 bits 1 : 11 bits Bit #'s left to right (excluding size bit) 0 : L1C phase bias 1 : L2W phase bias 2 : L2L phase bias 3: L5Q phase bias 4 to 10 : spare phase biases	Indicates which phase bias types are present in the GPS satellite bias corrections block.
SF026	GLONASS phase bias mask	6 or 10	bitmask	bitmask	Leftmost bit indicates bitmask size to follow: 0 : 5 bits 1 : 9 bits Bit #'s left to right (excluding size bit) 0 : L1C phase bias 1 : L2C phase bias 2 to 8 : spare phase biases	Indicates which phase bias types are present in the GLONASS satellite bias corrections block.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF027	GPS code bias mask	7 or 12	bitmask	bitmask	Leftmost bit indicates bitmask size to follow: 0 : 6 bits 1 : 11 bits Bit #'s left to right (excluding size bit) 0 : C1C code bias 1 : C2W code bias 2 : C2L code bias 3: C5Q code bias 4 to 10 : spare code biases	Indicates which code bias types are present in the GPS satellite bias corrections block.
SF028	GLONASS code bias mask	6 or 10	bitmask	bitmask	Leftmost bit indicates bitmask size to follow: 0 : 5 bits 1 : 9 bits Bit #'s left to right (excluding size bit) 0 : C1C code bias 1 : C2C code bias 2 to 8 : spare code biases	Indicates which code bias types are present in the GLONASS satellite bias corrections block.
SF029	Code bias correction	11	±20.46 m	0.02 m	none	Satellite bias correction value in unit of meters.
SF030	Area Count	5	1 to 32	1	none	Number of areas to follow in the data block section of the current message.
SF031	Area ID	8	0 to 255	1	none	Area identifier of the geographic area being defined, must be unique within a solution processor ID (TF011)
SF032	Area reference latitude	11	±90.00 north degrees	0.1 degrees	none	The northern most latitude of the area being defined
SF033	Area reference longitude	12	±180.00 east degrees	0.1 degrees	none	The western most longitude of the area being defined.
SF034	Area latitude grid node count	3	1 to 8	1	none	The number of grid points that exist in the north-south direction beginning at the reference latitude (SF032).
SF035	Area longitude grid node count	3	1 to 8	1	none	The number of grid points that exist in the west-east direction beginning at the reference longitude (SF033).
SF036	Area latitude grid node spacing	5	0.1 to 3.2 degrees	0.1 degrees	none	The spacing between the grid nodes in the north-south direction
SF037	Area longitude grid node spacing	5	0.1 to 3.2 degrees	0.1 degrees	none	The spacing between the grid nodes in the west-east direction
SF039	Number of grid points present	7	0 to 127	1	none	Number of grid points present in the grid blocks of the message. When grids not present as indicated by SF040 within the same message, this data field may be ignored.
SF040	Poly/Grid block present indicator	2	0 to 2	1	0 : None present 1 : Poly block present 2 : Poly/grid block present	Indicates the presence of the polynomial and grid blocks within the message. As the polynomial and grid blocks are cumulative, grids cannot be present without polynomials.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF041	Troposphere equation type	3	0 to 7	1	See notes	Indicates the residual zenith troposphere delay polynomial model used. The coefficients are stored in the same order as they appear below ($T_{00}, T_{01}, T_{10}, T_{11}$). Models for each SF041 value: 0 : T_{00} 1 : $T_{00} + T_{01}(\delta\phi_p) + T_{10}(\lambda - \lambda_0)$ 2 : $T_{00} + T_{01}(\delta\phi_p) + T_{10}(\lambda - \lambda_0) + T_{11}(\delta\phi_p)(\lambda - \lambda_0)$ 3 to 7 : TBD
SF042	Troposphere quality	3	0 to 7	1	0 : unknown 1 : <=0.010m 2 : <=0.020m 3 : <=0.040m 4 : <=0.080m 5 : <=0.160m 6 : <=0.320m 7 : > 0.320m	The field represents the quality of the complete interpolated troposphere model (average, polynomial, and grid when applicable) in units of meters at zenith (1σ).
SF043	Area average vertical hydrostatic delay	8	±0.508m	0.004 m	None	The average vertical hydrostatic delay (reduced to a reference height of 0 m on the ellipsoid) within the area offset from 2.3m
SF044	Troposphere polynomial coefficient size indicator	1	0 to 1	1	0 : Troposphere small coefficient block is used 1 : Troposphere large coefficient block is used	Indicates whether the small or large troposphere polynomial coefficients block is used
SF045	Small troposphere coefficient T00	7	±0.252 m	0.004 m	None	The small size coefficient of the troposphere zenith delay polynomial offset by 0.252m.
SF046	Small troposphere coefficient T10/T01	7	±0.063 m/degree	0.001 m / degree	None	The small size coefficient of the troposphere zenith delay polynomial.
SF047	Small troposphere coefficient T11	9	±0.0510 m/degree^2	0.0002 m /degree^2	None	The small size coefficient of the troposphere zenith delay polynomial.
SF048	Large troposphere coefficient T00	9	±1.020 m	0.004 m	None	The large size coefficient of the troposphere zenith delay polynomial offset by 0.252m
SF049	Large troposphere coefficient T10/T01	9	±0.255 m/degree	0.001 m / degree	None	The large size coefficient of the troposphere zenith delay polynomial.
SF050	Large troposphere coefficient T11	11	±0.2046 m/degree^2	0.0002 m / degree^2	None	The large size coefficient of the troposphere zenith delay polynomial.
SF051	Troposphere residual field size	1	0 to 1	1	0 : Troposphere small residual is used 1 : Troposphere large residual is used	Troposphere residual field size indicator.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF052	Small troposphere residual zenith delay	6	±0.124 m	0.004 m	0x3F = invalid	The small size troposphere residual zenith delay.
SF053	Large troposphere residual zenith delay	8	±0.508 m	0.004 m	0xFF = invalid	The large size troposphere residual zenith delay.
SF054	Ionosphere equation type	3	0 to 7	1	See notes	Indicates the slant ionosphere delay polynomial model used. The coefficients are stored in the same order as they appear below ($C_{00}, C_{01}, C_{10}, C_{11}$). Models for each SF054 value: 0 : C_{00} 1 : $C_{00} + C_{01}(\delta\phi_p) + C_{10}(\delta\lambda_p)$ 2 : $C_{00} + C_{01}(\delta\phi_p) + C_{10}(\delta\lambda_p) + C_{11}(\delta\phi_p)(\delta\lambda_p)$ 3 - 7 : TBD
SF055	Ionosphere quality	4	0 to 15	1	0 : Unknown 1 : <=0.03 TECU 2 : <=0.05 TECU 3 : <=0.07 TECU 4 : <=0.14 TECU 5 : <=0.28 TECU 6 : <=0.56 TECU 7 : <=1.12 TECU 8 : <=2.24 TECU 9 : <=4.48 TECU 10 : <=8.96 TECU 11 : <=17.92 TECU 12 : <=35.84 TECU 13 : <=71.68 TECU 14 : <=143.36 TECU 15 : >143.36 TECU	The model quality of the interpolated ionosphere model (1σ). The indicator represents the combined accuracy of the polynomial, and when present, grid model.
SF056	Ionosphere polynomial coefficient size indicator	1	0 to 1	1	0 : Ionosphere small coefficient block is used 1 : Ionosphere large coefficient block is used	Indicates whether the small or large ionosphere polynomial coefficients block is used
SF057	Small ionosphere coefficient C00	12	±81.88 TECU	0.04 TECU	None	The small size coefficient of the ionosphere slant delay polynomial.
SF058	Small ionosphere coefficient C10/C01	12	±16.376 TECU/degree	0.008 TECU / degree	None	The small size coefficient of the ionosphere slant delay polynomial.
SF059	Small ionosphere coefficient C11	13	±8.190 TECU/degree^2	0.002 TECU / degree^2	None	The small size coefficient of the ionosphere slant delay polynomial.
SF060	Large ionosphere coefficient C00	14	±327.64 TECU	0.04 TECU	None	The large size coefficient of the ionosphere slant delay polynomial.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF061	Large ionosphere coefficient C10/C01	14	±65.528 TECU/degree	0.008 TECU / degree	None	The large size coefficient of the ionosphere slant delay polynomial.
SF062	Large ionosphere coefficient C11	15	±32.766 TECU/degree^2	0.002 TECU / degree^2	None	The large size coefficient of the ionosphere slant delay polynomial.
SF063	Ionosphere residual field size	2	0 to 3	1	0: Ionosphere small residual is used 1: Ionosphere medium residual is used 2: Ionosphere large residual is used 3: Ionosphere extra-large residual is used	Ionosphere residual field size indicator.
SF064	Small ionosphere residual slant delay	4	±0.28 TECU	0.04 TECU	0xF = invalid	The small size ionosphere residual slant delay.
SF065	Medium ionosphere residual slant delay	7	±2.52 TECU	0.04 TECU	0x7F = invalid	The medium size ionosphere residual slant delay.
SF066	Large ionosphere residual slant delay	10	±20.44 TECU	0.04 TECU	0x3FF = invalid	The large size ionosphere residual slant delay.
SF067	Extra-large ionosphere residual slant delay	14	±327.64TECU	0.04 TECU	0x3FFF = invalid	The extra-large size ionosphere residual slant delay.
SF068	Area Issue of Update (AIOU)	4	0 to 15	1	None	The AIOU controls when and if messages may be combined with the GAD messages described in SM 2. The AIOU cannot change more than once per 30 seconds. User must assume that an AIOU has changed over outages of 450 seconds or more even if the AIOU before and after the outage matches.
SF069	Reserved	N	N/A	N/A	N/A	Reserved bits may be used to extend existing messages in the future. Reserved bits should be set to zero, until defined in future versions of the ICD.
SF070	Ionosphere shell height	2	0-3	1	0 : 350 km 1 : 400 km 2 : 450 km 3 : 500 km	The height of the ionosphere shell used to compute the pierce point of the satellite observation
SF071	BPAC area count	2	1 to 4	1	None	Number of areas to follow in the data block section of the current message.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF072	BPAC area ID	2	0 to 3	1	None	Area identifier of the BPAC data contained within the message. Must be unique within a solution processor ID (TF011). NOTE: This parameter does not need to be unique from the Area ID (SF031).
SF073	BPAC area reference latitude	8	±85.00 north degrees	1.0 degrees	None	The northern most latitude of the area being defined
SF074	BPAC area reference longitude	9	±180.00 east degrees	1.0 degrees	None	The western most longitude of the area being defined.
SF075	BPAC area latitude grid node count	4	1 to 16	1	None	The number of grid points that exist in the north-south direction beginning at the reference latitude (SF073).
SF076	BPAC area longitude grid node count	4	1 to 16	1	None	The number of grid points that exist in the west-east direction beginning at the reference longitude (SF076).
SF077	BPAC area latitude grid node spacing	2	0-3	1	0 : 2.5 deg 1 : 5.0 deg 2 : 10.0 deg 3 : 15.0 deg	The spacing between the grid nodes in the north-south direction
SF078	BPAC area longitude grid node spacing	2	0-3	1	0 : 2.5 deg 1 : 5.0 deg 2 : 10.0 deg 3 : 15.0 deg	The spacing between the grid nodes in the west-east direction
SF079	Grid node present mask	N	Bitmask	Bitmask	None	Bit mask of length N (between 1 and 256 bits) indicating the presence of grid point data in the BPAC area VTEC block
SF080	Area average VTEC	12	±511.75 TECU	0.25 TECU	None	The average VTEC within the area
SF081	VTEC size indicator	1	0 to 1	1	0 : small 1 : large	Indicates the size of the VTEC bin
SF082	Small VTEC residual	7	±15.75 TECU	0.25 TECU	0x7F = invalid	VTEC residual at the specified location in units of TECU
SF083	Large VTEC residual	11	±255.75 TECU	0.25 TECU	0x7FF = invalid	VTEC residual at the specified location in units of TECU
SF084	Customer Key ID	20	0 to 1,048,576	1	None	Identification number used by a customer to determine if the dynamic key contained in the message can be decoded by their customer key.

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF085	Encryption Type	4	0 to 15	1	0 : AES 1 : ChaCha12 2 : ChaCha20 3 to 15 : TBD	The type of encryption
SF086	Week of Applicability	6	0 to 52	1	0x3F = Currently active	Indicates the week at which the dynamic key becomes active. Week 0 of current year always begins on Jan 1 at 00:00 UTC. A half year ambiguity is present and therefore the key cannot be sent out more than 6 months in advance. When special value of 0x3F is set, u64SatMask the key is currently active. NOTE: It is not required for a service provider to change the Week of Applicability once a key is active.
SF087	Key length	4	0 to 15	1	0 : 96 bits 1 : 128 bits 2 : 192 bits 3 : 256 bits 4 : 512 bits 5 to 15 : TBD	The length of the key in bits.
SF088	Cryptographic Key	Key length (SF087)	96 to 2^(Key length)-1	1	None	The cryptographic key.
SF089	Count of Message IDs	5	0 to 31	1	None	Count of message IDs in this message
SF090	Group Authentication Type	4	0 to 15	1	0 : none 1 : Ed25519 2 : SHA-2 2 : SHA-3 4 to 15 : TBD	Identifies authentication algorithm type
SF091	Computed Authentication Data (CAD) Length	4	0 to 15	1	0 : 32 bits 1 : 64 bits 2 : 96 bits 3 : 128 bits 4 : 192 bits 5 : 256 bits 6 : 512 bits 7 to 15 : TBD	The length of the CAD stored in the message (NOTE: the CAD is computed according to algorithm selected may be shorter or longer: i.e., meaning the CAD is either padded or truncated, respectively).
SF092	Computed Authentication Data (CAD)	CAD length	0 to 2^(CAD length) - 1	1	None	The CAD that is padded or truncated in accordance with CAD Length. The size, even zero, depends upon the Group Authentication Type (SF090). The CAD is computed from TF002 through TF016, where TF016 is encrypted before computation.
SF093	Galileo satellite mask	38 to 66	Bitmask	Bitmask	Leftmost 2 bits indicate bitmask size to follow: 0 : 36 bits 1 : 45 bits 2 : 54 bits 3 : 64 bits	Galileo satellite mask field is composed of two bits that indicate the bitmask size, followed by the bitmask. The bitmask after the 2-bit size defines the IDs and order of Galileo satellites in the message. The bitmask position added by 1 is equal to the Pseudo-Random Noise (PRN) ID of a satellite. At least one satellite must be present in the bitmask. Bitmask position 0 is the leftmost bit of the

ID	Name	# Bits	Range	Resolution	Special values	Notes
						satellite mask, excluding the 2-bits indicating the size of the bitmask.
SF094	BDS satellite mask	39 to 66	Bitmask	Bitmask	Leftmost 2 bits indicate bitmask size to follow. 0 : 37 bits 1 : 46 bits 2 : 55 bits 3 : 64 bits	BDS satellite mask field is composed of two bits that indicate the bitmask size, followed by the bitmask. The bitmask after the 2-bit size defines the IDs and order of BDS satellites in the message. The bitmask position added by 1 is equal to the Pseudo-Random Noise (PRN) ID of a satellite. At least one satellite must be present in the bitmask. Bitmask position 0 is the leftmost bit of the satellite mask, excluding the 2-bits indicating the size of the bitmask.
SF095	QZSS satellite mask	12 to 66	Bitmask	Bitmask	Leftmost 2 bits indicate bitmask size to follow. 0 : 10 bits 1 : 40 bits 2 : 48 bits 3 : 64 bits	QZSS satellite mask field is composed of two bits that indicate the bitmask size, followed by the bitmask. The bitmask after the 2-bit size defines the IDs and order of QZSS satellites in the message. The bitmask position added by 193 is equal to the Pseudo-Random Noise (PRN) ID of a satellite. At least one satellite must be present in the bitmask. Bitmask position 0 is the leftmost bit of the satellite mask, excluding the 2-bits indicating the size of the bitmask. L1-SAIF satellite mapping is not defined as part of the QZSS satellite mask.
SF096	Galileo ephemeris type	3	0 to 7	n/a	0: Galileo F/NAV 1: Galileo I/NAV 2: Galileo C/NAV 3 to 7: TBD	Type of ephemeris being used for Galileo corrections.
SF097	BDS ephemeris type	4	0 to 15	n/a	0 :D1 Nav (B1I) 1 : D2 Nav (B1I) 2 :D1 Nav (B3I) 3 : D2 Nav (B3I) 4: B-CNAV1 5: B-CNAV2 6 to 15 TBD	Type of ephemeris being used for BDS corrections.
SF098	QZSS ephemeris type	3	0 to 7	n/a	0 :LNAV (L1C/A) 1 : CNAV2(L1C) 2: CNAV (L2C,L5) 3 to 7 TBD	Type of ephemeris being used for QZSS corrections.
SF099	Galileo IOD_{nav}	10	0 to 1023	1	none	Issue of data (IOD_{nav}) field that indicates to which Galileo broadcast ephemeris (identified by its IOD_{nav}) the corrections must be combined with in order to be processed by the user.
SF100	BDS IODE/IODC	8	0 to 255	1	none	Issue of Data Ephemeris (IODE) or issue of Data Clock (IODC), field that indicates to which BDS broadcast ephemeris the corrections must be combined with in order to be processed by the user. The IODE/IODC choice depends upon the ephemeris type. That is, the IODE of the ephemeris is used when SF097 indicates either B-CNAV1 or B-CNAV2. When SF097 indicates either the D1 or D2 Nav type then one computes the IODC value in

ID	Name	# Bits	Range	Resolution	Special values	Notes
						accordance with the RTCM/CSNO agreed algorithm (which produces and 8-bit value): BDS IODC=mod (toc / 720, 240).
SF101	QZSS IODE	8	0 to 255	1	none	Issue of data ephemeris (IODE) field that indicates to which QZSS broadcast ephemeris (identified by its IODE) the corrections must be combined with in order to be processed by the user.
SF102	Galileo phase bias mask	9 or 16	Bitmask	Bitmask	Leftmost bit indicates bitmask size to follow: 0 : 8 bits 1 : 15 bits Bit #'s left to right (excluding size bit) 0 : L1C phase bias 1 : L5Q phase bias 2 : L7Q phase bias 3 to 14 : spare phase biases	Indicates which phase bias types are present in the Galileo satellite bias corrections block. For Galileo observation codes, see Table 6 of RINEX 3.04 (Nov 23, 2018).
SF103	BDS phase bias mask	9 or 16	Bitmask	Bitmask	Leftmost bit indicates bitmask size to follow: 0 : 8 bits 1 : 15 bits Bit #'s left to right (excluding size bit) 0 : L2I phase bias 1 : L5P phase bias 2 : L7I phase bias 3 : L6I phase bias 4 : L1P phase bias 5 : L7P phase bias 6 : L8P phase bias 7 to 14 : spare phase biases	Indicates which phase bias types are present in the BDS satellite bias corrections block. For BDS observation codes, see Table 9 of RINEX 3.04 (Nov 23, 2018).
SF104	QZSS phase bias mask	7 or 12	Bitmask	Bitmask	Leftmost bit indicates bitmask size to follow: 0 : 6 bits 1 : 11 bits Bit #'s left to right (excluding size bit) 0 : L1C phase bias 1 : L2L phase bias 2 : L5Q phase bias 3 to 10 : spare phase biases	Indicates which phase bias types are present in the QZSS satellite bias corrections block. For QZSS observation codes, see Table 8 of RINEX 3.04 (Nov 23, 2018).
SF105	Galileo code bias mask	9 or 16	Bitmask	Bitmask	Leftmost bit indicates bitmask size to follow: 0 : 8 bits 1 : 15 bits Bit #'s left to right (excluding size bit) 0 : C1C code bias 1 : C5Q code bias 2 : C7Q code bias 3 to 14 : spare code biases	Indicates which code bias types are present in the Galileo satellite bias corrections block. For Galileo observation codes, see Table 6 of RINEX 3.04 (Nov 23, 2018).

ID	Name	# Bits	Range	Resolution	Special values	Notes
SF106	BDS code bias mask	9 or 16	Bitmask	Bitmask	Leftmost bit indicates bitmask size to follow: 0 : 8 bits 1 : 15 bits Bit #'s left to right (excluding size bit) 0 : C2I code bias 1 : C5P code bias 2 : C7I code bias 3 : C6I code bias 4 : C1P code bias 5 : C7P code bias 6 : C8P code bias 7 to 14 : spare code biases	Indicates which code bias types are present in the BDS satellite bias corrections block. For BDS observation codes, see Table 9 of RINEX 3.04 (Nov 23, 2018).
SF107	QZSS code bias mask	7 or 12	Bitmask	Bitmask	Leftmost bit indicates bitmask size to follow: 0 : 6 bits 1 : 11 bits Bit #'s left to right (excluding size bit) 0 : C1C code bias 1 : C2L code bias 2 : C5Q code bias 3 to 10 : spare code biases	Indicates which code bias types are present in the QZSS satellite bias corrections block. For QZSS observation codes, see Table 9 of RINEX 3.04 (Nov 23, 2018).

6.5. SPARTN Messages

Many SPARTN Messages are provided on a per constellation basis. For each constellation data field definitions which are a function of constellation are marked with a **. These data fields must be treated consistently throughout the message. All other data fields are consistent across all constellations.

6.5.1. Orbit, Clock, Bias (OCB) messages - SM 0-0 to SM 0-4

The following table describes the overall layout of the SM 0-0 to SM 0-4:

Table 6.3 – Overall layout of SPARTN message 0-0 to 0-4

Block	Name	Definition	Size (bits)
Header block (SM 0-0 to SM 0-4)	**Solution issue of update (SIOU)**	SF005	9
	End of set	SF010	1
	Reserved	SF069	1
	Yaw present flag	SF008	1
	Satellite reference datum	SF009	1
	Ephemeris type**	SF016 or SF017 or SF096 or SF097 or SF098	2, 3, or 4
	Satellite mask**	SF011 or SF012 or SF093 or SF094 or SF095	12 to 66

Block	Name	Definition	Size (bits)
Satellite block (SM 0-0 to SM 0-4)	Satellite block	Table 6.4	Variable (Repeated for each satellite)

The following tables describe the satellite, clock, and bias blocks present in SM 0-0 to SM 0-4. The satellite block repeats for every satellite present in the satellite mask (SF011/SF012/SF093/SF094/SF095).

Table 6.4 – Message 0-0 to 0-4 satellite block

Block	Name	Definition	Size (bits)
Satellite block (SM 0-0 to SM 0-4)	Do not use (DNU)	SF013	1
	OCB present flags	SF014	3
	Continuity indicator	SF015	3
	Orbit block	Table 6.5	49, 50, 52, 55, 56, or 58
	Clock block	Table 6.6	20
	Bias block**	Table 6.7 or Table 6.8 or Table 6.9 or Table 6.10 or Table 6.11	Variable size

Table 6.5 – Message 0-0 to 0-4 orbit block

Block	Name	Definition	Size (bits)
Orbit block (SM 0-0 to SM 0-4)	IODE**	SF018 or SF019 or SF099 or SF100 or SF101	8 or 7 or 10
	Orbit radial correction	SF020	14
	Orbit along-track correction	SF020	14
	Orbit cross-track correction	SF020	14
	Satellite yaw	SF021	0 or 6

Table 6.6 – Message 0-0 to 0-4 clock block

Block	Name	Definition	Size (bits)
Clock block (SM 0-0 to SM 0-4)	IODE continuity	SF022	3
	Clock correction	SF020	14
	User range error	SF024	3

Table 6.7 – Message 0-0 GPS bias block

Block	Name	Definition	Size (bits)
Bias block (SM 0-0)	GPS phase bias mask	SF025	7 or 12
	Phase bias block	Table 6.12	18 per phase bias type (Repeated for each bias)
	GPS code bias mask	SF027	7 or 12
	Code bias correction	SF029	11 per code bias type (Repeated for each bias)

Table 6.8 – Message 0-1 GLONASS bias block

Block	Name	Definition	Size (bits)
Bias block (SM 0-1)	GLONASS phase bias mask	SF026	6 or 10
	Phase bias block	Table 6.12	18 per phase bias type (Repeated for each bias)
	GLONASS code bias mask	SF028	6 or 10
	Code bias correction	SF029	11 per code bias type (Repeated for each bias)

Table 6.9 – Message 0-2 Galileo bias block

Block	Name	Definition	Size (bits)
Bias block (SM 0-2)	Galileo phase bias mask	SF102	9 or 16
	Phase bias block	Table 6.12	18 per phase bias type (Repeated for each bias)
	Galileo code bias mask	SF105	9 or 16
	Code bias correction	SF029	11 per code bias type (Repeated for each bias)

Table 6.10 – Message 0-3 BeiDou bias block

Block	Name	Definition	Size (bits)
Bias block (SM 0-3)	BeiDou phase bias mask	SF103	9 or 16
	Phase bias block	Table 6.12	18 per phase bias type (Repeated for each bias)
	BeiDou code bias mask	SF106	9 or 16
	Code bias correction	SF029	11 per code bias type (Repeated for each bias)

Table 6.11 – Message 0-4 QZSS bias block

Block	Name	Definition	Size (bits)
Bias block (SM 0-4)	QZSS phase bias mask	SF104	7 or 12
	Phase bias block	Table 6.12	18 per phase bias type (Repeated for each bias)
	QZSS code bias mask	SF107	7 or 12
	Code bias correction	SF029	11 per code bias type (Repeated for each bias)

Table 6.12 – Message 0-0 to 0-4 phase bias block

Block	Name	Definition	Size (bits)
Phase bias block (SM 0-0 to SM 0-1)	Fix flag	SF023	1
	Continuity indicator	SF015	3
	Phase bias correction	SF020	14 per phase bias type

6.5.2. High Precision Atmosphere Correction (HPAC) message - SM 1-0 to 1-4

The following table describes the overall layout of the SM 1-0 to SM 1-4:

Table 6.13 – Overall layout of SPARTN message 1-0 to 1-4

Block	Name	Definition	Size (bits)
Header block (SM 1-0 to SM 1-4)	Solution issue of update (SIOU)	SF005	9
	Area issue of update (AIOU)	SF068	4
	Reserved	SF069	1
	Area count	SF030	5
Atmosphere block (SM 1-0 to SM 1-4)	Atmosphere block	Table 6.14	Variable (Repeated for each area)

Table 6.14 – Message 1-0 to 1-4 HPAC atmosphere data block

Block	Name	Definition	Size (bits)
Atmosphere block (SM 1-0 to SM 1-4)	Area data block	Table 6.15	19
	Troposphere data block	Table 6.16	Variable
	Ionosphere data block	Table 6.19	Variable

The following tables describe the HPAC area data block, troposphere and ionosphere blocks present in SM 1-0 to 1-4 The blocks repeat for every area present in SM 1-0 to 1-4.

Table 6.15 – Message 1-0 to 1-4 HPAC area data block

Block	Name	Definition	Size (bits)
Area data block (SM 1-0 to SM 1-4)	Area ID	SF031	8
	Number of grid points present	SF039	7
	Tropo blocks indicator	SF040	2
	Iono blocks indicator	SF040	2

The HPAC troposphere data blocks are only present if one or both Tropo blocks indicator bits are turned on. It is made up of the troposphere block, troposphere polynomial coefficient block and troposphere grid block.

Table 6.16 – Message 1-0 to 1-4 HPAC troposphere data block

Block	Name	Definition	Size (bits)
Troposphere polynomial coefficient block (SM 1-0 to SM 1-4) (Present if tropo blocks indicator = 1 or 2)	Troposphere equation type	SF041	3
	Troposphere quality	SF042	3
	Area average vertical hydrostatic delay	SF043	8
	Troposphere polynomial coefficient size indicator	SF044	1
	Troposphere polynomial coefficients	SF044 = 0 see table 6.17 SF044 = 1 see table 6.18	Variable
Troposphere grid block (SM 1-0 to SM 1-4)	Troposphere residual field size	SF051	1
	Troposphere grid residuals	SF051 = 0 : SF052 SF051 = 1 : SF053	SF051 = 0: NGridPts * 6 SF051 = 1: NGridPts * 8

Block	Name	Definition	Size (bits)
(Present if tropo blocks indicator = 2)			

The HPAC troposphere small coefficient blocks are only present if the Troposphere polynomial coefficient size indicator is set to 0. The equation type is defined from SF041 – Troposphere Equation Type.

Table 6.17 – Message 1-0 to 1-4 HPAC troposphere small coefficient block

Block	Name	Definition	Size (bits)
Troposphere small coefficients block (SM 1-0 to SM 1-4)	Troposphere coefficient T00 (SF041 models 0, 1 or 2)	SF045	7
	Troposphere coefficient T01 (SF041 models 1 or 2)	SF046	0 or 7
	Troposphere coefficient T10 (SF041 models 1 or 2)	SF046	0 or 7
	Troposphere coefficient T11 (SF041 model 2)	SF047	0 or 9

The HPAC troposphere large coefficient blocks are only present if the Troposphere polynomial coefficient size indicator is set to 1. The equation type is defined from SF041 – Troposphere Equation Type.

Table 6.18 – Message 1-0 to 1-4 HPAC troposphere large coefficient block

Block	Name	Definition	Size (bits)
Troposphere large coefficients block (SM 1-0 to SM 1-4)	Troposphere coefficient T00 (SF041 models 0, 1 or 2)	SF048	9
	Troposphere coefficient T01 (SF041 models 1 or 2)	SF049	0 or 9
	Troposphere coefficient T10 (SF041 models 1 or 2)	SF049	0 or 9
	Troposphere coefficient T11 (SF041 model 2)	SF050	0 or 11

The HPAC ionosphere data blocks are only present if one or both Iono blocks indicator bits are turned on. It is made up of the ionosphere block and the ionosphere satellite block.

Table 6.19 – Message 1-0 to 1-4 HPAC ionosphere data block

Block	Name	Definition	Size (bits)
Ionosphere block (SM 1-0 to SM 1-4) (Present if iono blocks indicator = 1 or 2)	Ionosphere equation type	SF054	3
	Satellite mask**	SF011 or SF012 or SF093 or SF094 or SF095	12 to 66
Ionosphere satellite block (SM 1-0 to SM 1-4) (Present if iono blocks indicator = 1 or 2)	Ionosphere satellite block	Table 6.20	Variable (Repeated for all satellites)

The HPAC ionosphere satellite block consists of the satellite polynomial block, the satellite coefficients block and ionosphere satellite grid block. The satellite block is repeated for all satellites enabled in the satellite Mask of SM 1-0 to 1-4.

Table 6.20 – Message 1-0 to 1-4 HPAC ionosphere satellite block

Block	Name	Definition	Size (bits)
Ionosphere satellite polynomial block (SM 1-0 to SM 1-4) **(Present if iono blocks indicator = 1 or 2)**	**Ionosphere quality**	SF055	4
	Ionosphere polynomial coefficient size indicator	SF056	1
Ionosphere satellite coefficient block (SM 1-0 to SM 1-4) **(Present if iono blocks indicator = 1 or 2)**	**Ionosphere satellite polynomial coefficients**	SF056 = 0 see table 6.21 SF056 = 1 see table 6.22	Variable
Ionosphere grid block (SM 1-0 to SM 1-4) **(Present if iono blocks indicator = 2)**	**Ionosphere residual field size**	SF063	2
	Ionosphere grid residuals	SF063 = 0 : SF064 SF063 = 1 : SF065 SF063 = 2 : SF066 SF063 = 3 : SF067	SF063 = 0: NGridPts * 4 SF063 = 1: NGridPts * 7 SF063 = 2: NGridPts * 10 SF063 = 3: NGridPts * 14

The HPAC ionosphere small coefficient blocks are only present if the Ionosphere polynomial coefficient size indicator is set to 0. The equation type is defined from SF054 – Ionosphere Equation Type.

Table 6.21 – Message 1-0 to 1-4 HPAC ionosphere small coefficient block

Block	Name	Definition	Size (bits)
Ionosphere small coefficients block (SM 1-0 to SM 1-4)	**Ionosphere coefficient C00 (SF054 models 0, 1 or 2)**	SF057	12
	Ionosphere coefficient C01 (SF054 models 1 or 2)	SF058	0 or 12
	Ionosphere coefficient C10 (SF054 models 1 or 2)	SF058	0 or 12
	Ionosphere coefficient C11 (SF054 model 2)	SF059	0 or 13

The HPAC ionosphere large coefficient blocks are only present if the Ionosphere polynomial coefficient size indicator is set to 1. The equation type is defined from SF054 – Ionosphere Equation Type.

Table 6.22 – Message 1-0 to 1-4 HPAC ionosphere large coefficient block

Block	Name	Definition	Size (bits)
Ionosphere large coefficients block (SM 1-0 to SM 1-4)	**Ionosphere coefficient C00 (SF054 models 0, 1 or 2)**	SF060	14
	Ionosphere coefficient C01 (SF054 models 1 or 2)	SF061	0 or 14
	Ionosphere coefficient C10 (SF054 models 1 or 2)	SF061	0 or 14

Block	Name	Definition	Size (bits)
	Ionosphere coefficient C11 (SF054 model 2)	SF062	0 or 15

6.5.3. Geographic Area Definition (GAD) message - SM 2-0

The following table describes the overall layout of the SM 2-0:

Table 6.23 – Overall layout of SPARTN message 2-0

Block	Name	Definition	Size (bits)
Header block (SM 2-0)	Solution issue of update (SIOU)	SF005	9
	Area issue of update (AIOU)	SF068	4
	Reserved	SF069	1
	Area count	SF030	5
Area definition block (SM 2-0)	Area definition block	Table 6.24	47 per area (Repeated for all areas)

The following table describe the area definition block present in SM 2-0. The area definition block repeats for every area present in a solution.

Table 6.24 – Overall layout of SPARTN message 2-0

Block	Name	Definition	Size (bits)
Area definition block (SM 2-0)	Area ID	SF031	8
	Area reference latitude	SF032	11
	Area reference longitude	SF033	12
	Area latitude grid node count	SF034	3
	Area longitude grid node count	SF035	3
	Area latitude grid node spacing	SF036	5
	Area longitude grid node spacing	SF037	5

6.5.4. Basic Precision Atmosphere Correction (BPAC) message - SM 3-0

The following table describes the overall layout of the SM 3-0:

Table 6.25 – Overall layout of SPARTN message 3-0

Block	Name	Definition	Size (bits)
Header block (SM 3-0)	Solution issue of update (SIOU)	SF005	9
	Reserved	SF069	1
	Ionosphere shell height	SF070	2
	BPAC area count	SF071	2
BPAC area block (SM 3-0)	BPAC area block	See table 6.26	Variable (Repeated for each area)

The table below defines the BPAC area block for SM 3-0. It is repeated for each area contained in the message:

Table 6.26 – BPAC area block definition

Block	Name	Definition	Size (bits)
BPAC area block (SM 3-0)	**BPAC area data block**	See table 6.27	Variable
	BPAC VTEC block	See table 6.28	12 or 16 (Repeated for each grid point)

Table 6.27 – BPAC area data block definition

Block	Name	Definition	Size (bits)
BPAC area data block (SM 3-0)	**BPAC area ID**	SF072	2
	BPAC area reference latitude	SF073	8
	BPAC area reference longitude	SF074	9
	BPAC area latitude grid node count	SF075	4
	BPAC area longitude grid node count	SF076	4
	BPAC area latitude grid node spacing	SF077	2
	BPAC area longitude grid node spacing	SF078	2
	Average area VTEC	SF080	12
	Grid node present mask	SF079	Num Grid Points

Table 6.28– BPAC grid node VTEC block for message 3-0

Block	Name	Definition	Size (bits)
BPAC grid node VTEC block (SM 3-0)	**VTEC quality**	SF055	4
	VTEC size indicator	SF081	1
	VTEC residual	SF081 = 0 : SF082 SF081 = 1 : SF083	7 or 11

6.5.5. Dynamic Key message - SM 4-0

The following table describes the overall layout of the SM 4-0 message. (^^) indicates data fields transmitted in plain text. Unlike other SPARTN messages, when the Dynamic Key message is encrypted (i.e., the EAF-TF004 is set to 1), the Customer Key ID and Dynamic Key Encryption Type is transmitted in clear-text of the SPARTN Payload (both are included in any authentication computation). See section 8.15 for more details.

Table 6.29 – Overall layout of SPARTN message 4-0

Block	Name	Definition	Size (bits)
Dynamic key encryption meta data block^^ (SM 4-0)	Customer key ID^^	SF084	20
	Dynamic key encryption type^^	SF085	4
Dynamic key payload block (SM 4-0)	Week of applicability	SF086	6
	Payload encryption type	SF085	4
	Dynamic key length	SF087	4
	Dynamic key	SF088	Variable

6.5.6. Group Authentication Message - SM 4-1(Deprecated – To be removed in future versions)

The group authentication message contains the authentication details pertaining to a group (or collection) of SPARTN messages for a given time tag. The following table describes the overall layout of SM 4-1:

Table 6.30 – Overall layout of SPARTN message 4-1

Block	Name	Definition	Size (bits)
Group authentication data block (SM 4-1)	Count of message IDs	SF089	5
	Group authentication type	SF090	4
	Computed authentication data length	SF091	4
	Message group IDs block	See Table 6.31	Variable

Table 6.31 – Message ID block layout of SPARTN message 4-1

Block	Name	Definition	Size (bits)
Message ID block (SM 4-1)	Message type	TF002	7
	Message sub-type	TF007	4
	Encryption sequence number	TF013	6
	Computed authentication data	SF092	Variable

6.5.7. Proprietary Message Support

SPARTN Proprietary messages are allocated to message types (TF002) in the range of 120 through 127. Each subtype (TF007) of these messages are assigned to different organizations. Their contents are defined by the organization assigned the proprietary TF002/TF007 pair.

The SPARTN Committee manages the assignments. Requests for proprietary message assignments are made through http://www.spartnformat.org. There is no fee associated with such requests.

Table 6.38 shows the Proprietary Message assignments at the time of this document publication.

Table 6.38 – Assigned Proprietary IDs

Proprietary Type & Subtype	Organization	Contact
SM 120-0	None	This message shall only be used for an organization's in-house development and testing (typically while awaiting a for a Proprietary Message assignment).
SM 120-1	U-Blox AG	https://www.u-blox.com/
SM 120-2	Swift Navigation Inc	https://www.swiftnav.com
SM 120-3 through SM 127-15	Reserved	

7. Transport layer

The transport layer defines the frame architecture for sending or receiving SPARTN messages. The purpose of defining this layer is to ensure that SPARTN messages can be properly ***decoded*** by applications.

The structure of the frame format is depicted below and described in the table that follows:

Figure 7.1 – Message frame layout

Frame Start (TF001-TF006)	Payload Description Block (TF007-TF015)	Payload (TF016)	Embedded Authentication Data (TF017)	Message CRC (TF018)

Table 7.1 – Message frame and payload description block format

ID	Name	# Bits	Range	Resolution	Special values	Notes
TF001	Preamble	8	n/a	n/a	115 : This is the only valid value that can be used for the SPARTN message frame preamble.	Various notations for the preamble value: Binary: 01110011_2 Decimal: 115_{10} Hexadecimal: 0x73
TF002	Message type	7	0 to 127	1	none	Types defined in table 6.1
TF003	Payload length	10	0 to 1023	1 byte	none	
TF004	Encryption and authentication flag (EAF)	1	0 to 1	n/a	0 : No encryption or authentication is applied to any portion of the message frame and/or payload 1: The message payload is encrypted and authenticated.	When applied, encryption and authentication is present in the message payload section (TF016).
TF005	Message CRC type	2	0 to 3	1	0: CRC-8-CCITT 1: CRC-16-CCITT 2: CRC-24-Radix-64 3: CRC-32-CCITT	This field indicates what type of CRC is used in the message. Table 7.2 describes details of each option.
TF006	Frame CRC	4	n/a	n/a	n/a	Byte-by-byte 4-bit CRC calculated from TF002 through TF005. A 4-bit 0x0 filler (4 bits) is added to the right of the rightmost bit of the TF002-TF005 bit sequence (20 bits). Therefore, a 24-bit sequence is used in the CRC computation. This is done in order to allow byte alignment of the buffer used for the CRC computation. The parameters of this CRC-4 are: a. Polynomial = 0x09 b. Initialized at zero c. Input is reflected. d. Output is reflected. e. Zero XOR on output.

ID	Name	# Bits	Range	Resolution	Special values	Notes
TF007	Message Subtype	4	0 to 15	1	none	Subtypes defined in table 6.1
TF008	Time tag type	1	0 to 1	n/a	0 : Half-day (16 bit) time tag to follow 1 : Full (32-bit) time tag to follow	Time tag type is used to define the size of the time tag to follow. Messages can carry time represented by either a 16-bit half day time tag or a full, 32-bit time tag. See field definitions described in TF009.
TF009	GNSS time tag	16 or 32	0 to 43,199 or 0 to 4,294,967,295	1	none	This field provides the time tag of the message in the system time of the GNSS constellation to which the message pertains: i.e., GPS message time tags are in GPS system time, while GLONASS message time tags are in GLONASS system time. For message which do not indicate a constellation (e.g., GAD message) or may contain data for multiple constellations simultaneously, the time tag is GPS. When Time tag type (TF008) is set to 0, the ambiguous, 16-bit GNSS time tag is used. When Time tag type (TF008) is set to 1, the full 32-bit time tag is used. The half-day must be resolved with the assistance of an unambiguous time tag, either received in the message through the full 32-bit time tag, or from another source. The reference time for the 32-bit time tag is seconds since January 1st 2010, 00:00:00.
TF010	Solution ID	7	0 to 127	1	none	The solution ID represents the unique identification of the current system, which consists of all instances of a solution that is being generated for a given area of coverage. The different instances of the solution are represented by unique solution processor IDs (TF011).
TF011	Solution processor ID	4	0 to 15	1	none	The solution processor ID indicates the unique ID of the processing instance that has generated the correction data in the message. Each processing instance of the solution must be associated with a unique solution processor ID by the corrections provider.
TF012	Encryption ID	4	0 to 15	1	None	When the EAF Flag of the Transportation Layer (TF004) is set to 1, this field is present. Otherwise it is not present. When present, it provides a unique identifier for the encryption instance to ensure a unique crypto initialization vector (IV).

ID	Name	# Bits	Range	Resolution	Special values	Notes
TF013	Encryption Sequence Number	6	0 to 63	1	None	When the EAF Flag of the Transportation Layer (TF004) is set to 1, this field is present. Otherwise it is not present. When present, the encryption sequence number gets incremented each time a sub-type gets sent. The encryption sequence number is tracked for each type & sub-type. Must not send more than 64 messages of a single type & sub-type in one second.
TF014	Authentication Indicator	3	0 to 7	1	0 : None 1 : Group authenticated 2 : Ed25519 3 to 7 : TBD	When the EAF Flag of the Transportation Layer (TF004) is set to 1, this field is present. Otherwise it is not present. When present, it is used to indicate where this message is authenticated: either by the Group Authentication message or an authentication that is part of the current message.
TF015	Embedded Authentication Length	3	0 to 7	1	0 : 64 bits 1 : 96 bits 2 : 128 bits 3 : 256 bits 4 : 512 bits 5 to 7 : TBD	Present only when the EAF Flag (TF004) is set to 1. When the Authentication Indicator (TF014) is less than or equal to 1 this field shall be ignored. It is used to indicate the length of the authentication data stored after the message payload (TF016).
TF016	Message payload	8 to 8192	n/a	n/a	n/a	Message payload, containing encoded message – supported messages are defined in the Presentation Layer section of this document. If the encoded message length is not byte-aligned, fill bits must be inserted to match the payload length declared in the message frame (TF003). When the EAF Flag of the Transportation Layer (TF004) is set to 1, this payload is encrypted.
TF017	Embedded Authentication Data	Size indicated by TF015	n/a	n/a	n/a	Present when the Authentication Indicator (TF014) is set greater than 1. Otherwise it is not present. Authentication is computed from TF002 through TF016, where TF016 is encrypted before authentication.
TF018	Message CRC	8 to 32	n/a	n/a	n/a	CRC computed using all bits from TF002 through TF017. The type and size of CRC used is defined in TF005. If EAF (TF004) is set to one, CRC computation is computed using the encrypted payload (TF016), and when present, includes the Embedded Authentication Data (TF017).

Table 7.2 – SPARTN message CRC types

TF005 value	CRC type	Notes
0	CRC-8-CCITT	An unsigned 8-bit CRC using a polynomial of 0x07U. Pre-computation initialization: None. Post-computation inclusion: None.
1	CRC-16-CCITT	An unsigned 16-bit CRC using a polynomial of 0x1021U. Pre-computation initialization: None. Post-computation inclusion: None.
2	CRC-24-Radix-64	An unsigned 24-bit CRC using a polynomial of 0x864CFBU. Pre-computation initialization: None. Post-computation inclusion: None.
3	CRC-32-CCITT	An unsigned 32-bit CRC using a polynomial of 0x04C11DB7U. Pre-computation initialization: 0xFFFFFFFFU. Post-computation inclusion: Result XORed with 0xFFFFFFFFU.

8. Implementation Details

General guidelines and notes about using and implementing the SPARTN message format are described below.

8.1. Numerical Constants

Table 8.0 – SPARTN numerical constants

Constant	Description	Value	Unit
c	Speed of light	299792458.0	m/s
π	Circular constant “pi”	3.1415926535898	unitless

8.2. Reference Datum

SF009 is used to define the datum of the satellite coordinates provided in SPARTN message. Over the past decades updates to ITRF have become stable at close to the mm level. Therefore, it is not necessary to define the exact realization of ITRF used in the SPARTN message format. The epoch of the positions computed using the SPARTN message format will always be in the current epoch as provided in the message.

Service providers may choose to broadcast SPARTN messages in non-ITRF datums. In this case users must consult the service providers to establish the reference datum.

8.3. Broadcast Ephemeris

All references to broadcast ephemeris refer to the following versions of interface documents:

Table 8.1 – SPARTN Constellation ICD

Constellation	Document
GPS	IS-GPS-200H
GLONASS	Version 5.1
Galileo	OS SIS ICD Issue 1.3
BeiDou	ICD SIS Version 2
QZSS	IS-QZSS-PNT-003

SPARTN OCB messages are combined with the corresponding value obtained from the satellite broadcast message. The IODE is used to uniquely identify the broadcast ephemeris used in the expansion. Any deviation from the standard broadcast ephemeris implementations described in the documents above will directly impact the final accuracy of the system.

8.4. Message Flexibility

This standard is designed to allow for flexibility in how service providers broadcast the messages to optimize bandwidth as well as support future growth. Below are several guidelines which should be followed:

1) GNSS OCB messages (SM 0) contain an OCB present indicator (SF014) which allows service providers to independently send clocks, biases and orbits if desired. This allows for data rates to be optimized based on the rate of change of each parameter.

2) HPAC Atmosphere correction messages (SM 1) should only broadcast troposphere parameters for a single constellation. Service providers can take advantage of the Troposphere blocks indicator field (SF040) to indicate whether the troposphere block is present in the SM 1 message. If multiple troposphere models are broadcast for a single epoch, it is expected that the user utilize the latest received troposphere model. Additional service providers can choose to send polynomial only, or grid plus polynomial corrections depending on accuracy requirements.

3) Geographic Area Definition Message (SM 2) provides flexibility to allow for optimizing area size based on service requirements.

4) Several messages include reserved bits which in the future may be used to extend message content at the end of the payload. Therefore, decoder implementations should not use payload length to indicate where they stop decoding.

5) For OCB messages, SF010 is used to mark the end of an epoch. In the future, additional OCB messages may be added to the standard (e.g., supporting other constellations) and providers may elect to mark the End-of-Set in any SM-0 message. Therefore, decoder implementations should be designed so as to decode the SF010 field of all current and future SM 0 message possibilities, even though they may not understand the data for certain OCB messages (i.e., the SF010 field will be at the exact same location for all current and future OCB message types).

8.5. Message Payload Size Calculations

Below are the computations for message payload lengths base upon message type and sub-type. For total message lengths, one should also include the Frame Start, the Payload Description Block, any Embedded Authentication Data, and the message CRC

Table 8.2 – SPARTN message payload size calculations

Type	Subtype	Message name	Nominal Size Calculation (bits)	
0	0-4	**OCB (SM 0-0 to SM 0-4)**	**HeaderBlock**	15 + MNsc
			OrbitBlock	Op * (Iod+42 +Yp * 6)
			ClockBlock	Cp * 20
			BiasBlock	Bp *(MNPb + Npb*18 + MNCb + Ncb * 11)
			Total	HeaderBlock + (7 + Dnu * (OrbitBlock + ClockBlock + BiasBlock)) * NSc
1	0-4	**HPAC (SM 1-0 to SM 1-4)**	**HeaderBlock**	19
			AreaDataBlock	19
			TropDataBlock	15 + Tpc + Tgp * (1 + Tgr * NGp)
			IonoDataBlock	3 + MNsc + (5 + Ipc + Igp * (2 + Igr * NGp)) * Nsa
			Total	HeaderBlock + NAreas * (AreaDataBlock + Tp * TropDataBlock + Ip * IonoDataBlock)
2	0	**Geographic Area Definition (SM 2-0)**	**Total**	19 + 47 * NAreas
3	0	**BPAC Message (SM 3-0)**	**HeaderBlock**	14
			AreaDataBlock	43 + NGp
			VTECBlock	(5+Vs) * NGpPrst
			Total	HeaderBlock + NAreas * (AreaDataBlock + VTECBlock)
4	0	**Dynamic Key Message (SM 4-0)**	**Dynamic Key Encryption Meta Data Block**	24
			Dynamic Key Payload Block	14 + DKL
			Total	DynKeyEncMetaDataBlock + DynKeyPayload
	1	**Group Authentication Message (SM 4-1)**	**Group Authentication Data Block**	13
			Message ID Block	17 + CADL
			Total	GroupAuthDataBlock + CGID * MessageIdBlock

MNsc Mask size as defined in SF011/SF012/SF093/SF094/SF095 for constellation (including expansion bits)
Iod Number of bits for the IODE. See SF018/SF019/SF099/SF100/SF101.
Op 0 when orbit block is not present, 1 when orbit block is present
Yp 0 when yaw is not present, 1 when yaw is present
Cp 0 when clock block is not present, 1 when clock block is present
Bp 0 when bias block is not present, 1 when bias block is present
MNpb Max Number of phase biases. See SF025/SF026/SF102/SF103/SF104.
Npb Number of phase biases present.
MNcb Max Number of code biases. See SF027/SF028/SF105/SF106/SF107.
Ncb Number of code biases present.
Dnu 0 when satellite should not be used, 1 otherwise
Nsc Number of satellites present for constellation within the solution
Tpc Number of bits for the troposphere polynomial coefficient block:

	Troposphere Eq Type		
	0	1	2
Troposphere Small Coefficients Block	7	21	30
Troposphere Large Coefficients Block	9	27	38

Tgp 0 when troposphere grid block is not present, 1 when troposphere grid block is present
Tgr Troposphere grid bits, 6 or 8 if "Troposphere residual field size" (SF051) is 0 or 1 respectively.
Ipc Number of bits for the ionosphere polynomial coefficient block:

	Ionosphere Eq Type		
	0	1	2
Ionosphere Small Coefficients Block	12	36	49
Ionosphere Large Coefficients Block	14	42	57

Igp 0 when ionosphere grid block is not present, 1 when ionosphere grid block is present
Igr Ionosphere grid bits, 4, 7, 10 or 14 if "Ionosphere residual field size" (SF064) is 0, 1, 2 or 3 respectively.
Tp 0 when troposphere data block is not present, 1 when troposphere data block present
Ip 0 when ionosphere data block is not present, 1 when ionosphere data block present
NAreas Number of areas within the solution
NSa Number of satellites visible in area
NGp Number of grid points in area
NGpPrst Number of grid points present
Vs VTEC bin size 7 or 11 if VTEC size indicator (SF081) is 0 or 1
DKL Dynamic key length
CADL Length of CAD
CGID The count of group message IDs

8.6. Satellite and User Dependent Biases

In order to facilitate ambiguity resolution, it is necessary that satellite biases are consistent between all satellites of a satellite system and a specific frequency. Parameters provided with the SPARTN message format must be free from satellite signal dependent biases other than those provided in the system dependent code and phase bias data fields.

Dependent on the user's hardware specifications, it may be necessary to model receiver dependent biases such as:

- Receiver quarter cycle carrier phase shifts
- GLONASS inter-frequency biases
- Inter-System clock biases

8.7. GNSS Satellite Clock Calculation

SPARTN OCB messages (SM 0) contains the parameters for clock correction δC. This correction is combined with the broadcast satellite clock t_b to form the corrected satellite clock t_s:

$$t_s = t_b - \frac{\delta C}{c}$$

where c is the speed of light constant.

Relativistic effects must be applied for all constellations, except for GLONASS, where relativistic effect is already accounted for in the broadcast clock parameter. The relativistic clock correction for GPS is:

$$\delta t_r = -\frac{2\,\boldsymbol{r}\cdot\dot{\boldsymbol{r}}}{c^2}$$

8.8. GNSS Satellite Orbit Calculation

SPARTN OCB message (SM 0) contains the parameters for orbit correction $\delta\boldsymbol{O}$ in radial, along-track and cross-track component. These corrections are transformed to a satellite position correction $\delta\boldsymbol{X}$ to be combined with the broadcast satellite position $\boldsymbol{X}_b$ to form the corrected satellite nominal antenna phase center position $\boldsymbol{X}_{orb}$:

$$\boldsymbol{X}_{orb} = \boldsymbol{X}_b - \delta\boldsymbol{X}$$

The satellite position correction $\delta\boldsymbol{X}$ is computed according to:

$$\boldsymbol{e}_{along} = \frac{\dot{\boldsymbol{r}}}{|\dot{\boldsymbol{r}}|}$$

$$\boldsymbol{e}_{cross} = \frac{\boldsymbol{r}\times\dot{\boldsymbol{r}}}{|\boldsymbol{r}\times\dot{\boldsymbol{r}}|}$$

$$\boldsymbol{e}_{radial} = \boldsymbol{e}_{along}\times\boldsymbol{e}_{cross}$$

$$\delta\boldsymbol{X} = \left[\boldsymbol{e}_{radial}\ \ \boldsymbol{e}_{along}\ \ \boldsymbol{e}_{cross}\right]\cdot\delta\boldsymbol{O}$$

$\boldsymbol{r} = \boldsymbol{X}_b$ satellite broadcast position vector

$\dot{\boldsymbol{r}} = \dot{\boldsymbol{X}}_b$ satellite broadcast velocity vector

$\boldsymbol{e}_i$ direction unit vector, $i = \{radial, along, cross\}$

Satellite orbits are in the reference frame defined in SF009. See section 8.2 for further details.

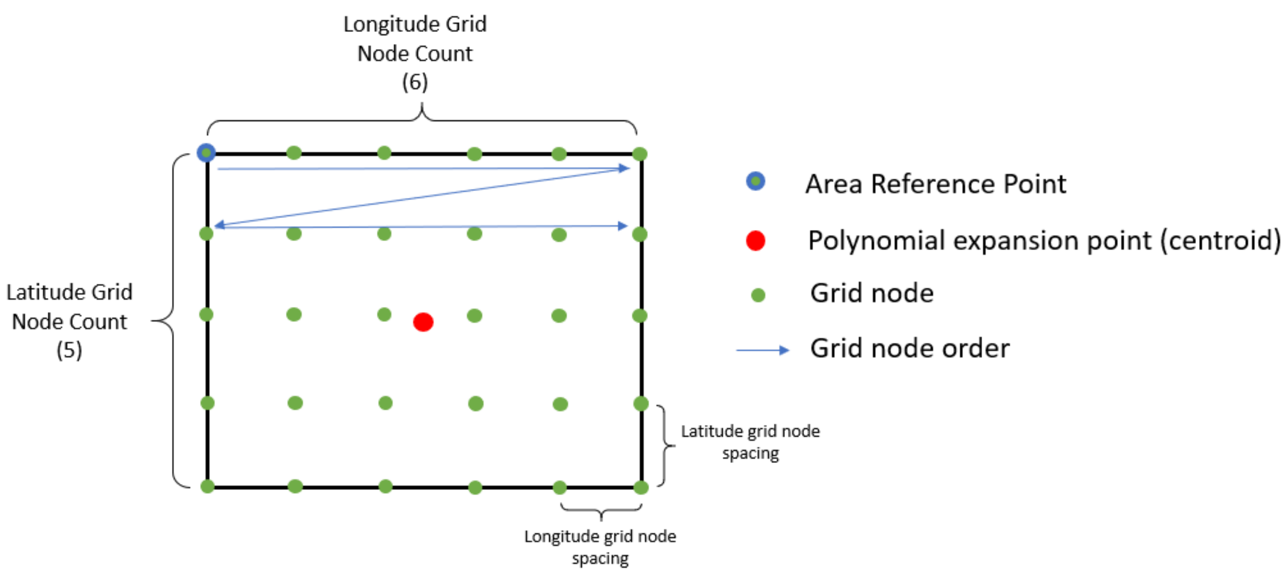
8.9. GNSS Satellite Bias Calculation

SPARTN OCB message (SM 0) contains parameters for bias correction for various track types. These biases shall be subtracted from the raw pseudorange and carrier phase measurements for the corresponding track types.

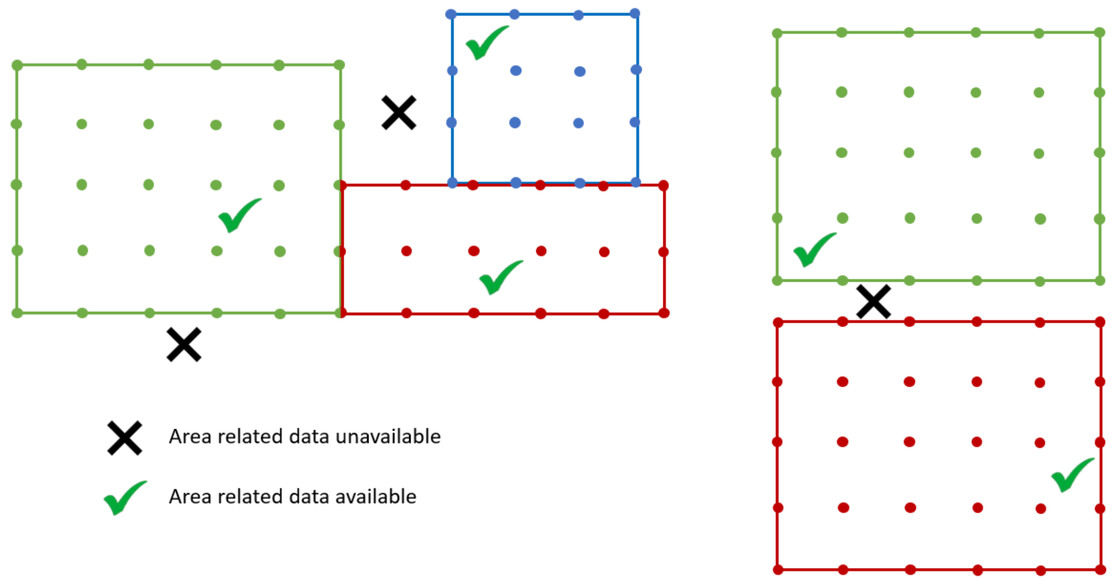
GLONASS biases are aligned to a theoretical zero bias receiver.

8.10. SPARTN Geographic Area Definition Message Implementation Details

The area definition message (SM 2) defines the geographic validity regions, grid layout and polynomial expansion point for the atmosphere model data (SM 1). These are shown in the figure below



Users select the appropriate geographic area based on approximate receiver position. The user position must be located inside of the area definition for the data to be used. This is to ensure safe and consistent interpolation of both polynomial and gridded data. Below are examples showing availability of atmosphere data with respect to various configurations.



Due to the curvature of the earth, the SM 2 area definition messages are not suited for arctic navigation and should not be used above +/- 85 degrees latitude.

8.11. HPAC Ionosphere Slant Delay Calculation

SM 1 contains parameters for correcting for the ionosphere slant delay for each signal frequency. The slant delay for a given satellite is computed as:

$$\delta I_{CP}^{i} = -40.3 \times \frac{10^{-16}}{f_j^2} \cdot (I_P^i + I_G^i)$$

$$\delta I_{PR}^{i} = 40.3 \times \frac{10^{-16}}{f_j^2} \cdot (I_P^i + I_G^i)$$

where

δI_{CP}^{i} slant ionosphere delay of satellite i, for the carrier phase measurement, in units of meters

δI_{PR}^{i} slant ionosphere delay of satellite i, for the pseudorange measurement, in units of meters

I_P^i slant ionosphere delay evaluated for the polynomial for satellite i, in units of TECU

I_G^i interpolated residual slant ionosphere delay interpolated from the gridded residuals for satellite i in units of TECU.

In the case where no grid information is present, I_G^i is assumed to be zero.

Grid Interpolation:

A bi-linear grid interpolation is used to interpolate the residual slant delay for the requested user position.

$$I_G^i = \sum_{k=1}^{4} W_k {I_G}_k^i$$

Where

W_k is the weight applied to the grid point k

${I_G}_k^i$ is the residual slant ionosphere delay for satellite i at grid point k in units of TECU.

Polynomial Evaluation:

The slant ionosphere delay is evaluated for the user location based on distance from the area's centroid latitude (ϕ_c)and longitude (λ_c) and approximate user latitude (ϕ_u) and longitude (λ_u):

$$I_P^i = f_p(\delta\phi, \delta\lambda)$$

where

$$\delta\phi_p = \phi_u - \phi_c$$

$$\delta\lambda_p = \lambda_u - \lambda_c$$

ϕ_u latitude of the user in units of degrees

ϕ_c area centroid latitude in units of degrees

λ_u longitude of the user in units of degrees

λ_c area centroid longitude in units of degrees

f_p is the polynomial representation of the ionosphere slant delay, as given by data field SF054:

0 : $I_P^i = C_{00}$
1 : $I_P^i = C_{00} + C_{01}(\delta\phi_p) + C_{10}(\delta\lambda_p)$
2 : $I_P^i = C_{00} + C_{01}(\delta\phi_p) + C_{10}(\delta\lambda_p) + C_{11}(\delta\phi_p)(\delta\lambda_p)$
3 - 7 : place holders for future polynomial representations

8.12. Troposphere Delay Calculation

SM 1 contains parameters for correcting for the troposphere zenith delay. The slant delay for a given satellite is computed as:

$$\delta T^i = \overline{T_h^z} \cdot m_h(\epsilon_i, h) + (T_P + T_G) \cdot m_{nh}(\epsilon_i)$$

Where

δT^i is the troposphere slant delay for satellite i at the user's location

$\overline{T_h^z}$ is the average zenith hydrostatic delay for the given area referenced to a zero ellipsoidal height (WGS-84)

$m_h(\epsilon_i, h)$ is the hydrostatic mapping function defined in Niell (1996) for the satellite elevation angle (ϵ_i) and ellipsoidal height (h) for the approximate user location.

$m_{nh}(\epsilon_i)$ is the non-hydrostatic mapping function defined in Niell (1996) for the satellite elevation angle (ϵ_i)

T_G is the residual troposphere zenith delay for station interpolated from the grid points, in units of meters.

T_P^i is the residual troposphere zenith delay for satellite i interpolated obtained from the polynomial expansion, in units of meters.

<u>Grid Interpolation:</u>

A bi-linear grid interpolation is used to interpolate the residual slant delay for the requested user position.

$$T_G = \sum_{k=1}^{4} W_k T_{G_k}$$

Where

W_k is the weight applied to the grid point k

T_{G_k} is the residual troposphere zenith delay for ionosphere delay at grid point k in units of TECU.

<u>Polynomial Evaluation:</u>

The troposphere zenith delay is evaluated for the user location based on distance from the area's centroid latitude $(\phi_c)$and longitude (λ_c) and approximate user latitude (ϕ_u) and longitude (λ_u):

$$T_P = f_p(\delta\phi, \delta\lambda)$$

where

$$\delta\phi_p = \phi_u - \phi_c$$

$$\delta\lambda_p = \lambda_u - \lambda_c$$

ϕ_u latitude of the user in units of degrees

ϕ_c area centroid latitude in units of degrees

λ_u longitude of the user in units of degrees

λ_c area centroid longitude in units of degrees

f_p is the polynomial representation of the troposphere residual zenith delay, as given by data fields SF041:

0 : $T_P = T_{00}$
1 : $T_P = T_{00} + T_{01}(\delta\phi_p) + T_{10}(\delta\lambda_p)$
2 : $T_P = T_{00} + T_{01}(\delta\phi_p) + T_{10}(\delta\lambda_p) + T_{11}(\delta\phi_p)(\delta\lambda_p)$
3 - 7 : place holders for future polynomial representations

8.13. BPAC Ionosphere Delay Evaluation

In the BPAC ionosphere message, the ionosphere is modelled as a vertical total electron content (VTEC) and a mapping function. An ionosphere shell model, is used to compute the ionosphere pierce point of the satellite's ray and can be computed using geometric relationships and a spherical earth assumption.

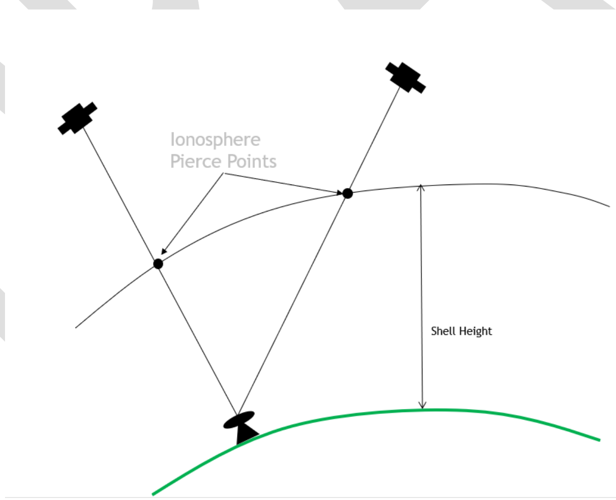


Figure 1 Description of the ionosphere shell model and satellite ray pierce points

The pierce point for a given satellites ray can be computed as follow:

$$\phi_{ipp} = \sin^{-1}(\sin(\phi_{usr}) \cdot \cos(\Psi) + \cos(\phi_{usr}) \cdot sin(\Psi) \cdot \cos(\alpha))$$

$$\lambda_{ipp} = \lambda_{usr} + \sin^{-1}\left(\frac{\sin(\Psi) \cdot \sin(\alpha)}{\cos(\phi_{ipp})}\right)$$

$$\Psi = \frac{\pi}{2} - \epsilon - \sin^{-1}\left(\frac{R}{R + h_i} \cdot \cos(\epsilon)\right)$$

where:

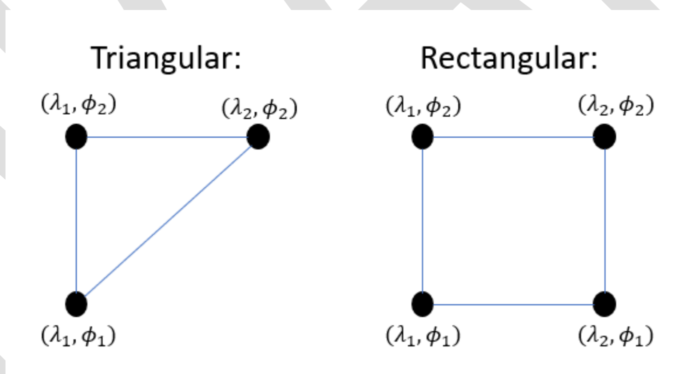
R = radius of the earth 6,378,000 m

h_i = ionosphere shell height in meters

α = azimuth of the satellite with respect to the user

ϵ = elevation angle of the satellite with respect to the user

End user implementations must be able to support two interpolation strategies. The triangular interpolation will additionally have different orientations which must be considered. Interpolation may only be performed within a defined area and it is not valid to interpolate between two adjacent areas.



The rectangular interpolation uses the following formula:

$$VTEC_{ipp} = \sum_{i=1}^{4} W_i(x_{pp}, y_{pp}) \cdot VTEC_i$$

$$x_{pp} = \frac{\delta\lambda_{ipp}}{\lambda_2 - \lambda_1}$$

$$y_{pp} = \frac{\delta\phi_{ipp}}{\phi_2 - \phi_1}$$

where

λ_1 = longitude of the grid point west of the ionosphere pierce point

λ_2 = longitude of the grid point east of the ionosphere pierce point

ϕ_1 = latitude of the grid point south of the ionosphere pierce point

ϕ_2 = latitude of the grid point north of the ionosphere pierce point

$VTEC_i = VTEC_{Avg} + VTEC_{Grid}$

$VTEC_{AVG}$ = area average VTEC as specified in SF080

$VTEC_{Grid}$ = area average VTEC as specified in SF082 or SF083

If the longitude cross +/- 180 degrees, then the computation must consider this discontinuity.

The weights are computed according to:

$$W_1 = x_{pp} y_{pp}$$

$$W_2 = (1 - x_{pp}) y_{pp}$$

$$W_3 = (1 - x_{pp})(1 - y_{pp})$$

$$W_4 = x_{pp}(1 - y_{pp})$$

The triangular interpolation uses the following formula:

$$VTEC_{ipp} = \sum_{i=1}^{3} W_i(x_{pp}, y_{pp}) \cdot VTEC_i$$

$$x_{pp} = \frac{\delta\lambda_{ipp}}{\lambda_2 - \lambda_1}$$

$$x_{pp} = \frac{\delta\phi_{ipp}}{\phi_2 - \phi_1}$$

where

λ_1 = longitude of the grid point west of the ionosphere pierce point

λ_2 = longitude of the grid point east of the ionosphere pierce point

ϕ_1 = latitude of the grid point south of the ionosphere pierce point

ϕ_2 = latitude of the grid point north of the ionosphere pierce point

If the longitude cross +/- 180 degrees, then the computation must consider this discontinuity.

The weights are computed according to:

$$W_1 = y_{pp}$$

$$W_2 = 1 - x_{pp} - y_{pp}$$

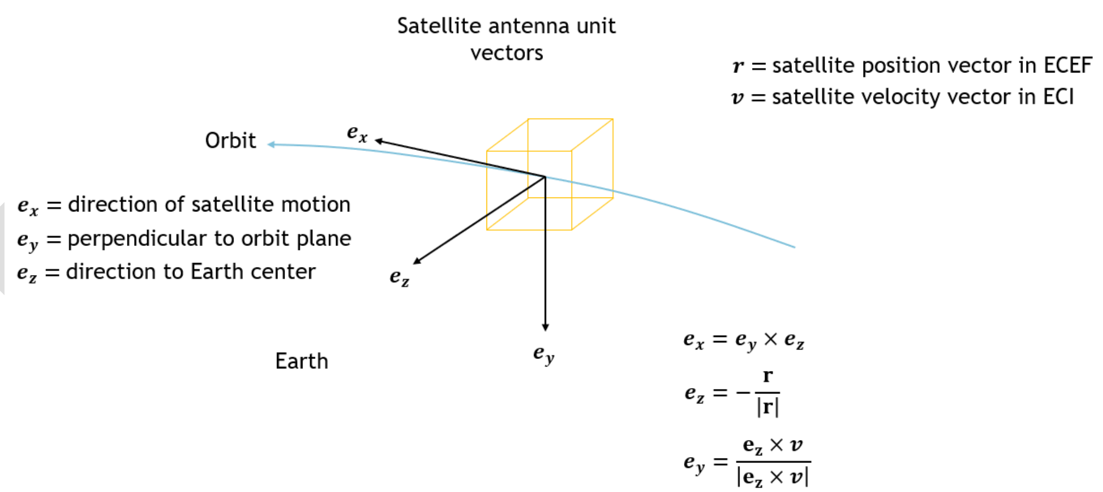
$$W_3 = x_{pp}$$

The VTEC can be mapped to the slant delay via a mapping function defined as:

$$mf(\epsilon) = \left(1 - \left(\frac{R \cdot \cos(\epsilon)}{R + h_i}\right)^2\right)^{-\frac{1}{2}}$$

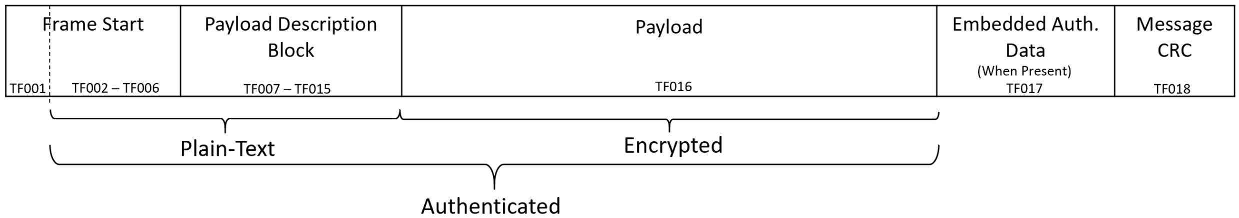
8.14. Satellite Frame Convention

If the yaw angle is not provided, the satellite yaw angle should be considered zero. The nominal satellite phase windup is computed according to Wu et al. (1993). The satellite frame used for yaw computations is a satellite fixed frame defined as follows:



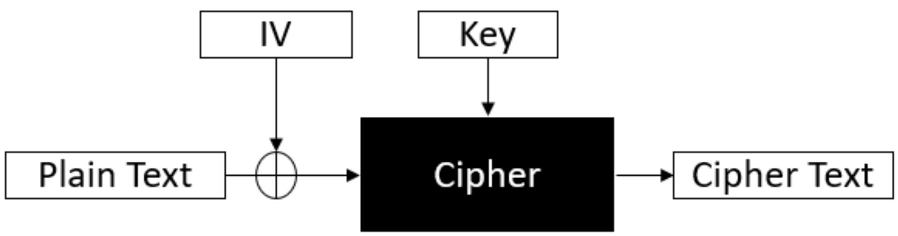
8.15. Encryption/Authentication Implementation

This section describes implementation details related to the encryption and authentication concept. For all messages, with the exception of the Dynamic Key Message (SM 4-0), the diagram below shows the portions of the message that are plain-text, that are encrypted and that are part of the authentication computation. In this case, the payload is encrypted using the dynamic key. All encryption and authentication algorithms describe within this ICD operate on byte-aligned input.



For the Dynamic Key Message, in addition to the Payload Description Block, the Dynamic Key Encryption Meta Data Block is also transmitted in plain text. This block contains the dynamic key encryption type which indicates the type of encryption performed on the dynamic key payload block. The payload encryption type present in the dynamic key payload block indicates the type of encryption performed on all other SPARTN messages.

A typical interface for the encryption function, referred to as a cipher is as follows:



Plain Text – Payload to be encrypted by the cipher

Cipher Text – Encrypted form of the payload

Key – Secret cryptographic value used for encrypting and decrypting the plain/cipher-text payload.

Cipher – Algorithm used for encrypting the plain-text and decrypting the cipher-text payload. Takes as input the secret key and initialization vector

Initialization Vector – Value used in an initial step for the encryption/decryption of plain/cipher-text. The IV does not need to be a secret however, the IV must be unique and not reused for encrypting different plain-text payloads.

8.15.1. Initialization Vector

The Initialization Vector (IV) for encryption is formed using the following (from left most position to right most position):

a. Message type (TF002)
b. Payload length (TF003)
c. Message sub-type (TF007)
d. 32-bit Time tag: i.e., when 16-bit form is present, it must be expanded to 32-bit form (TF009)
e. Solution ID (TF010)
f. Solution processor ID (TF011)
g. Encryption ID (TF012)
h. Encryption Sequence number (TF013)
i. Pad zeros (to right most position) to reach required length for encryption algorithm IV

Initialization Vector (IV)								
Msg type	Payload length	Msg sub-type	Time tag	Solution ID	Solution processor ID	Encryption ID	Encryption SN	Pad zeros

For AES-CTR and ChaCha encryption, the IV (e.g., counter for AES-CTR) will be constructed as described in RFC-3686 section 2.1 (Housley, 2004), with items a-i above forming the 96 most-significant bits, and the least-significant 32-bits of the counter set to one (i.e., 0x00000001).

8.16. Modeling Conventions

The table below lists references for the standard error models which must be applied at the rover in order to achieve full accuracy:

Error Source	Reference Document
Solid Earth Tides	IERS (2010)
Phase Windup	Wu et al. (1993)
Shapiro	Ashby (2003)
Sagnac	Ashby (2003)
Troposphere Mapping Function	Niell (1996)

9. References

Ashby, N. (2003) Relativity in the global positioning system. Living Rev. Relativity 6, 1–42 (2003).

Housley, R. (2004) Using Advanced Encryption Standard (AES) Counter Mode with IPsec Encapsulating Security Payload (ESP) Vigil Security, January 2004, https://tools.ietf.org/html/rfc4309

Niell, A. E. (1996) Global mapping functions for the atmosphere delay at radio wavelengths, J. Geophys Res, 101, 2337 - 3246

Petit, G. and Luzum, B. (2010) IERS Conventions (IERS Technical Note ; 36) Frankfurt am Main: Verlag des Bundesamts für Kartographie und Geodäsie, 2010. 179 pp., ISBN 3-89888-989-6

Wu, J. T., S. C. Wu, G. A. Hajj, W. I. Bertiger, and S. M. Lichten (1993), Effects of antenna orientation on GPS carrier phase, Manuscripta Geodaetica, 18 (2), 91–98.