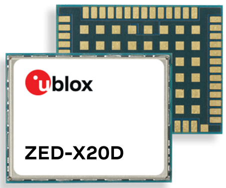
ZED-X20D

All-band high precision GNSS heading module
Professional grade

Integration manual



Abstract

This Integration manual describes the ZED-X20D high precision module with all-band GNSS receiver. The module is designed to provide the best possible heading information for applications for which precise attitude is of utmost importance. It is suitable for precision agriculture (including heavy machinery), unmanned autonomous vehicles (UAVs), and other industrial applications requiring robust positioning and accurate GNSS-based heading.

UBXDOC-304424225-21476 - R01
C1-Public

www.u-blox.com

Document information

Title	ZED-X20D	
Subtitle	All-band high precision GNSS heading module	
Document type	Integration manual	
Document number	UBXDOC-304424225-21476	
Revision and date	R01	07-Jul-2026
Disclosure restriction	C1-Public	

This document applies to the following products:

Product name	Type number	FW version	IN/PCN reference	RN reference
ZED-X20D	ZED-X20D-00B-00	HDG 2.00	UBXDOC-304424225-21473	UBXDOC-304424225-21402

Contents

1 System description

This document is an important source of information for all aspects of ZED-X20D software and hardware design. The purpose of this document is to provide guidelines for a successful integration of the receiver with the customer's end product.

1.1 Overview

Based on the u-blox X20 all-band high precision GNSS technology, the ZED-X20D module is designed for dual-antenna applications requiring RTK-based positioning and precise GNSS-derived heading. It supports all major GNSS constellations and frequency bands, including L1, L2, L5, and L6, to improve signal availability and maintain positioning and heading performance in environments with limited satellite visibility.

ZED-X20D integrates an all-band GNSS engine with support for real-time kinematics (RTK), precise point positioning (PPP), and PPP-RTK operation. It provides access to raw measurement data, including carrier phase and pseudorange observations, intended for users who require direct GNSS measurements for advanced processing or system integration.

ZED-X20D includes built-in mechanisms to support system integrity, such as secure boot with Root of Trust, GNSS jamming and spoofing detection, and authentication of Galileo navigation messages using OSNMA. The module is intended for use in applications such as precision agriculture (including heavy machinery), unmanned and autonomous platforms, and industrial systems that require GNSS-based positioning and heading within a compact hardware footprint.

1.2 Real time kinematic and heading

u-blox ZED-X20D high precision receiver takes GNSS precision and heading to the next level:

- Delivers heading accuracy down to 0.1 degrees (RMS).
- Delivers position accuracy down to the millimeter level: 0.006 m + 1 ppm CEP.
- Fast time to first fix and robust performance with all-band, multi-constellation reception.
- Compatible with leading correction services for global coverage and versatility.

Figure 1 presents typical use cases for ZED-X20D:

Figure 1: Typical applications for the ZED-X20D

1.2.1 Modes of operation

ZED-X20D supports the following modes of operation:

1. **Stand-alone mode:** Computes precise heading independently.
2. **Rover mode for precise position:**
    - It can receive RTCM correction data from a ZED-X20P operating as a base, or from a VRS service provider operating a network of base receivers.
    - It can receive SPARTN correction data via internet from the service provider.

- It can receive SPARTN correction data via L-band satellite channel (NEO-D9S can be used for this)
- It can receive CLAS correction data transmitted from Japan's QZSS constellation (from NEO-D9C message)

3. **Combined mode:** Operates in combination of the two above operation modes, for precise position and precise heading solution.

1.2.2 Networked transport of RTCM via internet protocol (NTRIP)

NTRIP is an open standard protocol for streaming differential data and other kinds of GNSS streaming data over the internet in accordance with specifications published by RTCM.

The NTRIP protocol is also used by SSR correction service providers to stream SSR correction data over the internet (e.g. SPARTN corrections).

There are three major parts to the NTRIP system: The NTRIP client, the NTRIP server, and the NTRIP caster:

1. The NTRIP server is a PC or an on-board computer running NTRIP server software communicating directly with a GNSS reference station. The NTRIP server serves as the intermediary between the GNSS receiver (NTRIP Source) streaming correction data and the NTRIP caster.
2. The NTRIP caster is an HTTP server which receives streaming correction data from one or more NTRIP servers and in turn streams the correction data to one or more NTRIP clients via the internet.
3. The NTRIP client receives streaming correction data from the NTRIP caster to apply as real-time corrections to a GNSS receiver.

u-center 2 GNSS evaluation software provides an NTRIP client and server application that can be used to easily evaluate a ZED-X20D as base or rover. Typically, a u-center 2 NTRIP client connects to an NTRIP service provider over the internet. The u-center 2 NTRIP client then provides the corrections to a ZED-X20D rover connected to the local u-center 2 application. VRS service is also supported by the u-center 2 NTRIP client.

1.3 Typical ZED-X20D application setups

Three application examples are illustrated in Figure 2 and Figure 3 as typical system implementations. These are representative of ZED-X20D usage as positioning and heading receiver. In Figure 2 and Figure 3, ZED-X20P is used as a base station providing corrections to a ZED-X20D receiver for precise positioning and heading. In Figure 4, ZED-X20D is used as a stand-alone solution for vehicle orientation. Mounting the two antennas on the X-axis provides heading and roll information.

Alternatively, the rover can use corrections provided over longer baselines from a correction stream distributed as a subscription service. This method can use a single fixed reference source which is local to the rover receiver or via a VRS service in which corrections are synthesized based on the rover's location.

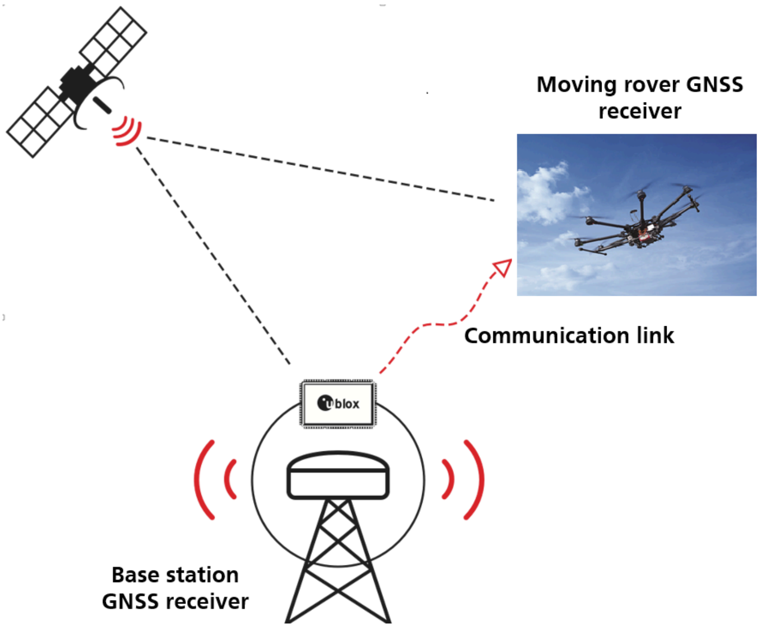


Figure 2: ZED-X20P base and ZED-X20D rover in a drone application for precise positioning and attitude determination

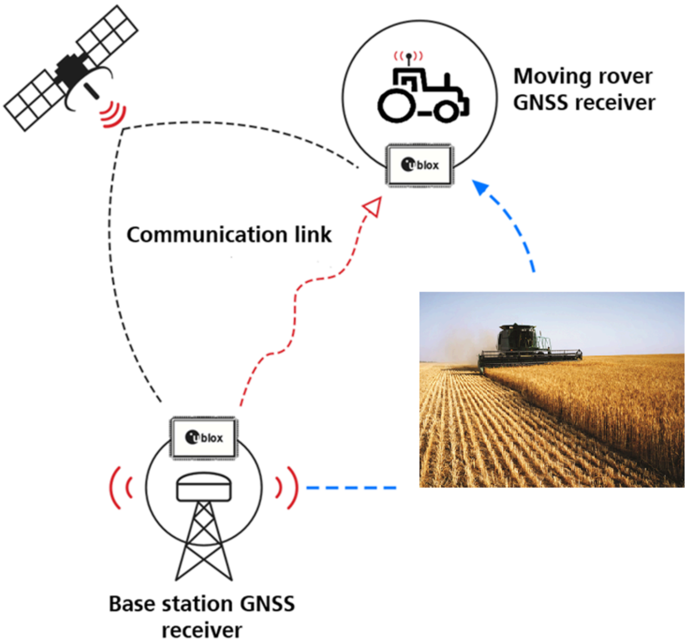


Figure 3: ZED-X20P base and ZED-X20D rover in a farming application for precise positioning and heading

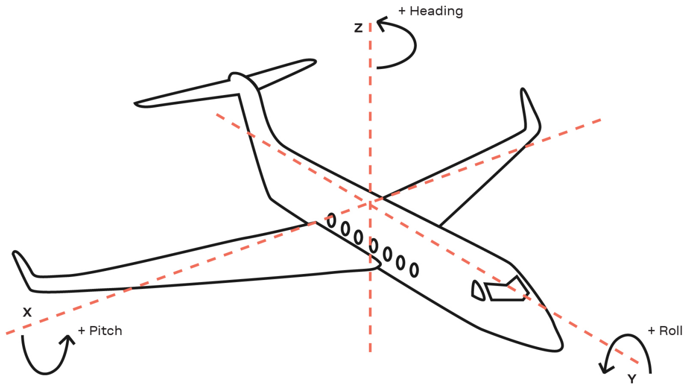


Figure 4: ZED-X20D used for a vehicle orientation in space application

1.4 Block diagram

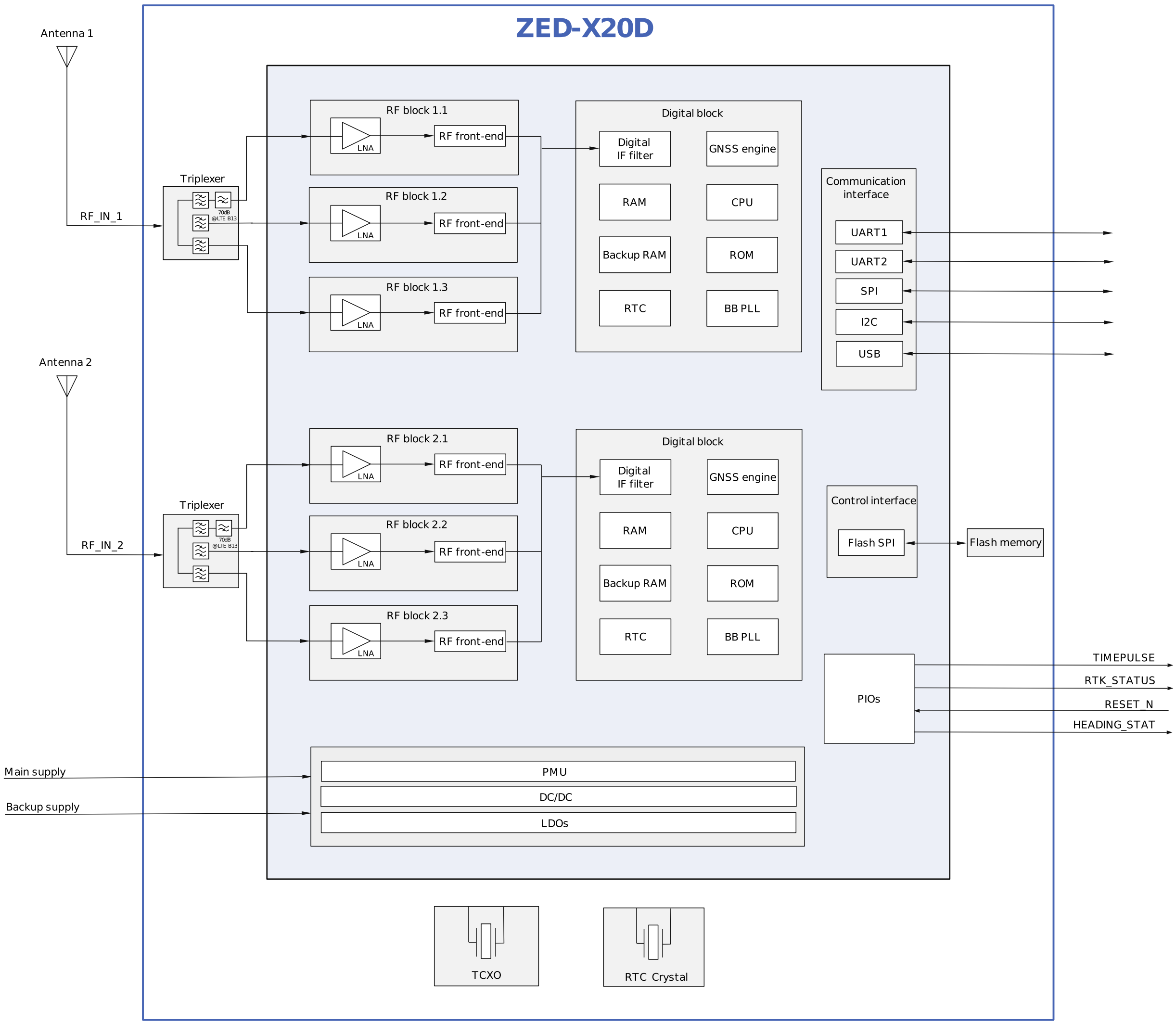


Figure 5: ZED-X20D block diagram

1.5 Pin assignment

The pin assignment of the ZED-X20D module is shown in Figure 6. The defined configuration of the programmable input/outputs (PIOs) is listed in Table 1.

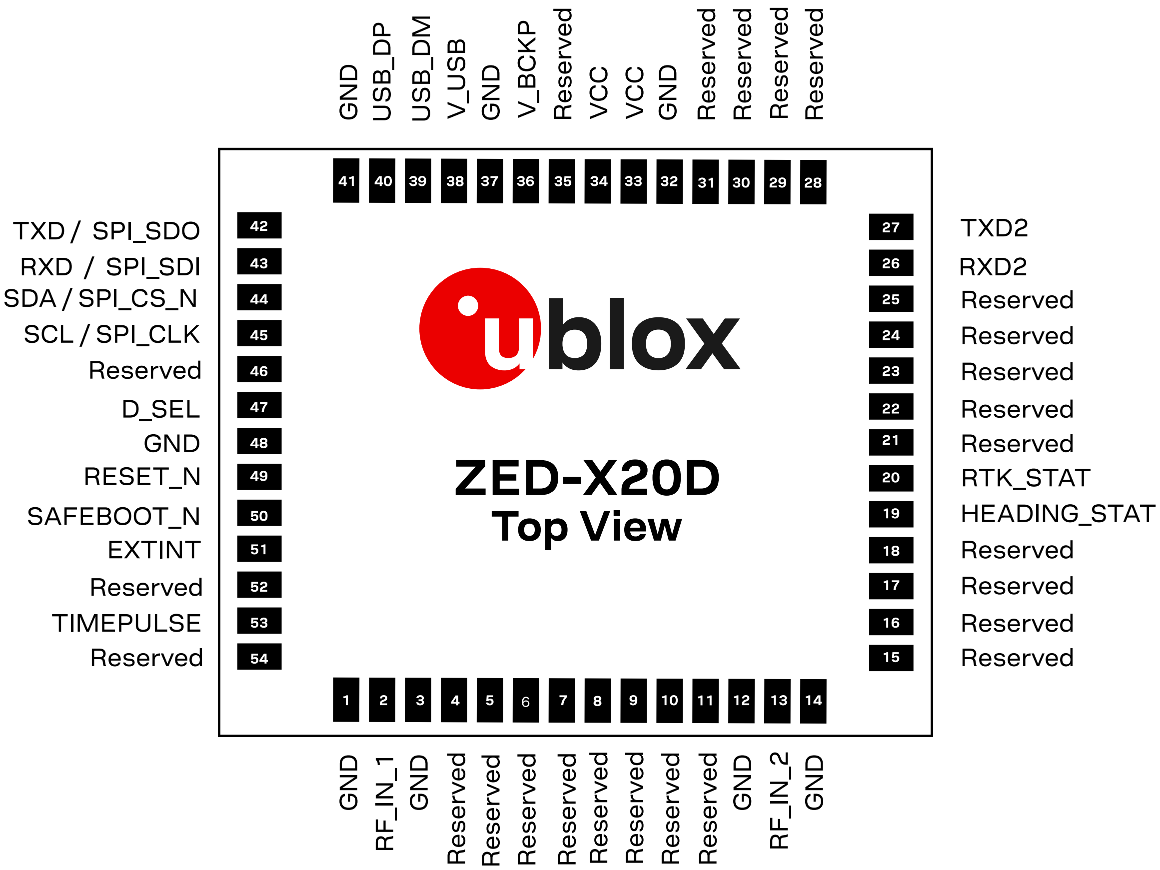


Figure 6: ZED-X20D pin assignment

Pin no.	Name	I/O	Description	Remarks
1	GND	-	Ground	Connect to GND
2	RF_IN_1	I	GNSS RF signal input	RF input gain is configurable with the help of three internal LNAs, one in each RF path. For more information about RF signal input considerations, see section RF front-end.
3	GND	-	Ground	Connect to GND
4	Reserved	-	Reserved pin	Leave open
5	Reserved	-	Reserved pin	Leave open
6	Reserved	-	Reserved pin	Leave open
7	Reserved	-	Reserved pin	Leave open
8	Reserved	-	Reserved pin	Leave open
9	Reserved	-	Reserved pin	Leave open

Pin no.	Name	I/O	Description	Remarks
10	Reserved	-	Reserved pin	Leave open
11	Reserved	-	Reserved pin	Leave open
12	GND	-	Ground	Connect to GND
13	RF_IN_2	I	GNSS RF signal input	RF input gain is configurable with the help of three internal LNAs, one in each RF path. For more information about RF signal input considerations, see section RF front-end.
14	GND	-	Ground	Connect to GND
15	Reserved	-	Reserved pin	Leave open
16	Reserved	-	Reserved pin	Leave open
17	Reserved	-	Reserved pin	Leave open
18	Reserved	-	Reserved pin	Leave open
19	HEADING_STAT	O	Indicates valid heading status; user configurable output	0 = Invalid heading 1 = Valid heading For more information, see section Heading status pin (HEADING_STAT).
20	RTK_STAT	O	RTK status pin	The RTK_STAT pin indicates the RTK positioning status. 0 = RTK/PPP-RTK fixed Toggling = receiving and using corrections 1 = no corrections For more information, see section RTK status pin (RTK_STAT).
21	Reserved	-	Reserved pin	Leave open
22	Reserved	-	Reserved pin	Leave open
23	Reserved	-	Reserved pin	Leave open
24	Reserved	-	Reserved pin	Leave open
25	Reserved	-	Reserved pin	Leave open
26	RXD2	I	UART2 input	UART2 interface input. For more information, see Communication interface configuration and UART.
27	TXD2	O	UART2 output[1]	UART2 interface output. For more information, see Communication interface configuration and UART.
28	Reserved	-	Reserved pin	Leave open
29	Reserved	-	Reserved pin	Leave open
30	Reserved	-	Reserved pin	Leave open
31	Reserved	-	Reserved pin	Leave open
32	GND	-	Ground	Connect to GND
33	VCC	I	Power supply input	Do not add any series resistance greater than 0.2 Ω to the VCC supply. For more information, see Power supply input (VCC).

[1] The UART2 output (TXD2) is reserved for internal system use and is not available for external communication.

Pin no.	Name	I/O	Description	Remarks
34	VCC	I	Power supply input	Do not add any series resistance greater than 0.2 Ω to the VCC supply. For more information, see Power supply input (VCC).
35	Reserved	-	Reserved pin	Leave open
36	V_BCKP	I	Backup supply input	If no backup supply voltage is available, connect the V_BCKP pin to GND. For more information, see Backup supply input (V_BCKP).
37	GND	-	Ground	Connect to GND
38	V_USB	I	USB supply	It is important to connect this pin to ground when USB interface is not used in an application. For more information, see USB.
39	USB_DM	I/O	USB data	Leave this pin open when USB interface is not used in an application. For more information, see USB.
40	USB_DP	I/O	USB data	Leave this pin open when USB interface is not used in an application. For more information, see USB.
41	GND	-	Ground	Connect to GND
42	TXD / SPI_SDO	O	UART1 output or SPI data output	UART1 output if D_SEL = 1(or open). SPI_SDO if D_SEL = 0. For more information, see Interface configuration pin (D_SEL), UART and SPI.
43	RXD / SPI_SDI	I	UART1 input or SPI data input	UART1 input if D_SEL = 1(or open). SPI_SDI if D_SEL = 0. For more information, see Interface configuration pin (D_SEL), UART and SPI.
44	SDA / SPI_CS_N	I/O	I2C data or SPI chip select	I2C serial data if D_SEL = 1 (or open). SPI chip Select if D_SEL = 0. For more information, see Interface configuration pin (D_SEL), I2C and SPI.
45	SCL / SPI_CLK	I/O	I2C clock or SPI clock	I2C clock if D_SEL = 1(or open). SPI clock if D_SEL = 0. For more information, see Interface configuration pin (D_SEL), I2C and SPI.
46	Reserved	-	Reserved pin	Leave open
47	D_SEL	I	Interface select for pins 42-45	Select the interface between UART/ I2C/SPI. For more information, see Interface configuration pin (D_SEL).
48	GND	-	Ground	Connect to GND
49	RESET_N	I	RESET_N	Has to be low for at least 1 ms to trigger a reset. For more information, see Reset pin (RESET_N).
50	SAFEBOOT_N	I	Safeboot pin	If held low during power-up, the receiver enters safeboot mode. To enable future service, updates and reconfiguration, provide a means to pull the line LOW. For more information, see Safeboot pin (SAFEBOOT_N).
51	EXTINT	I	External interrupt pin	Can be used for time aiding, wake up, and time mark. For more information, see External interrupt pin (EXTINT).

Pin no.	Name	I/O	Description	Remarks
52	Reserved	-	Reserved pin	Leave open
53	TIMEPULSE	O	Time pulse output	This pin outputs the time pulse signal. For more information, see Timepulse pin (TIMEPULSE).
54	Reserved	-	Reserved pin	Leave open

Table 1: ZED-X20D pin assignment

2 Receiver configuration

The ZED-X20D receiver is highly customizable using the UBX configuration interface. Its settings are stored in a configuration database located in the receiver's RAM, which is loaded during startup from multiple sources as discussed in section *Configuration layers* in the Interface description [2]. These settings are applied during operation and can be adjusted as needed.

The configuration interface settings are stored in a database. Each item is made up of a configuration key ID and value pair. Related items are grouped together and identified under a common group name: `CFG-GROUP`; a convention used in u-center 2 and within this document.

☞ In the u-center 2 *Device configuration* window, the configuration group is identified as *Group name* and the configuration item as the *Item name*.

The UBX messages available to change or poll the configurations are the `UBX-CFG-VALSET`, `UBX-CFG-VALGET`, and `UBX-CFG-VALDEL` messages. For more information about these messages and the configuration keys, see the *Configuration interface* section in the Interface description [2].

2.1 Storing configuration in different memory layers

Store the basic receiver configuration and the navigation configuration in the memory layers described in Table 2. For further details, see the Interface description section *Configuration layers* [2]. For more details of the permanence of the RAM and BBR layer configurations, see section Receiver reset and startup.

Memory	Remarks
RAM	• Contains the current runtime configuration. • Receiver power-down or entering backup mode clears the configuration in RAM.
Battery-backed RAM (BBR)	• Retains the settings as long as the backup power supply remains. • Can also be cleared with the `UBX-CFG-CFG` message.
Flash	• Permanent storage of the configuration settings. • Can be cleared with the `UBX-CFG-CFG` message. • **Recommended** to be written only once during production and not at every start-up. Infrequent updates during operation are permitted.

Table 2: Applicable memory storage layers

☞ To ensure persistent settings across power cycles, it is recommended to apply the runtime configuration to BBR or flash memory layers as appropriate. To preserve memory longevity, avoid frequent writes to the flash memory.

2.2 Basic receiver configuration

This section summarizes the most commonly used, basic receiver configurations.

2.2.1 Basic hardware configuration

The ZED-X20D receiver is configured with the default settings during the module production. The receiver starts up and is fully operational as soon as proper power supply, communication interfaces and antenna signal from the host application device are connected.

2.2.2 Interface configuration pin (D_SEL)

Use the **D_SEL** pin to configure the functionality of the combined UART1, I2C, and SPI pins as shown in Table 3. It is possible to configure the pins as UART1 + I2C, or as SPI.

Pin no.	D_SEL = GND	D_SEL = open
42	SPI_SDO	UART1 TXD
43	SPI_SDI	UART1 RXD
44	SPI_CS_N	I2C SDA
45	SPI_CLK	I2C SCL

Table 3: D_SEL configuration

2.2.3 Internal LNA mode configuration

ZED-X20D provides three independently configurable internal LNAs, one for each RF block. The internal LNA modes are configurable in all memory layers of the receiver. Configure the internal LNA modes with the configuration keys in Table 4 and apply a suitable reset to activate the changes.

Configuration key	Normal gain (default)	Low gain	Description
CFG-HW-RF1_LNA_MODE_LOWGAIN	0	1	Internal LNA mode of RF block 1
CFG-HW-RF2_LNA_MODE_LOWGAIN	0	1	Internal LNA mode of RF block 2
CFG-HW-RF3_LNA_MODE_LOWGAIN	0	1	Internal LNA mode of RF block 3

Table 4: Internal LNA mode configuration keys

2.2.4 GNSS signal configuration

ZED-X20D can concurrently receive signals from all supported GNSS bands. Each GNSS constellation can be enabled or disabled independently except for QZSS[2] and SBAS[3]. However, for all constellations, L1 band is always mandatory.

Configure the GNSS constellations and signal bands using the CFG-SIGNAL configuration group. ZED-X20D only supports certain combinations of constellations and bands, and it rejects unsupported combinations with the UBX-ACK-NAK message. It also sends the "inv sig cfg" warning via the UBX-INF and NMEA-TXT messages if they are enabled.

A GNSS constellation is considered as enabled when the constellation enable key is set and at least one of the constellation's band keys is enabled. See Table 5 for an example of the possible configuration key combinations for the Galileo constellation.

Constellation key **CFG-SIGNAL-GAL_ENA**	Band key **CFG-SIGNAL-GAL_E1_ENA**	Band key **CFG-SIGNAL-GAL_E5A_ENA**	Band key **CFG-SIGNAL-GAL_E6_ENA**	Constellation enabled?
true (1)	true (1)	true (1)	true (1)	**yes**
true (1)	true (1)	true (1)	false (0)	**yes**
true (1)	true (1)	false (0)	true (1)	**yes**
true (1)	true (1)	false (0)	false (0)	**yes**
true (1)	false (0)	true (1)	true (1)	**no**
true (1)	false (0)	false (0)	true (1)	**no**
true (1)	false (0)	true (1)	false (0)	**no**
true (1)	false (0)	false (0)	false (0)	**no**
false (0)	true (1)	true (1)	true (1)	**no**
false (0)	true (1)	true (1)	false (0)	**no**

2 QZSS can be enabled only if GPS is selected

3 SBAS can only be enabled with at least one of GPS, GAL and BDS

Constellation key CFG-SIGNAL-GAL_ENA	Band key CFG-SIGNAL-GAL_E1_ENA	Band key CFG-SIGNAL-GAL_E5A_ENA	Band key CFG-SIGNAL-GAL_E6_ENA	Constellation enabled?
false (0)	true (1)	false (0)	true (1)	**no**
false (0)	false (0)	true (1)	true (1)	**no**
false (0)	false (0)	false (0)	true (1)	**no**
false (0)	false (0)	true (1)	false (0)	**no**
false (0)	true (1)	false (0)	false (0)	**no**
false (0)	false (0)	false (0)	false (0)	**no**

Table 5: Examples of possible values of configuration items for the Galileo constellation

2.2.4.1 GNSS signal plan configuration

ZED-X20D offers GNSS signal plan options, as detailed in Table 6. The signal plan can be configured using the `CFG-SIGNAL-PLAN` configuration key as shown in Table 7.

GNSS signal plan	GPS	GAL	GLO [4]	BDS	QZSS[5]	NAVIC[6]	SBAS	Remarks
SP1	L1C/A L2C L5	E1B/C E5a E6	-	B1I B1C B2a B3I	L1C/A L1C/B L2C L5 L1S	L5	L1C/A	Available for specific use cases, not suitable as the default configuration.
SP2	L1C/A L2C L5	E1B/C E5a E6	L1OF L2OF	B1C B2a B3I	L1C/A L1C/B L2C L5 L1S	L5	L1C/A	Default and recommended GNSS signal plan.
SP6	L1C/A L2C L5	E1B/C E5a	L1OF L2OF	B1I B1C B2a	L1C/A L1C/B L2C L5 L1S	L5	L1C/A	Recommended to use only when using PointPerfect Flex over IP with SPARTN to benefit from B1I navigation data[7].

Table 6: List of available GNSS signal plans for ZED-X20D

☞ By default, GLONASS is not available in all regions. For more details on GLONASS availability, refer to GLONASS Geoblocking.

GNSS signal plan	Configuration key	Value
SP1	`CFG-SIGNAL-PLAN`	1
SP2	`CFG-SIGNAL-PLAN`	2

4 GLONASS generally available, restricted in some geographical areas.

5 QZSS is disabled by default in all signal plans. Enable it if required.

6 NAVIC is disabled by default in all signal plans. Enable it if required.

7 Set configuration item `CFG-BDS-D1D2_NAVDATA` = 1 to use B1I navigation data.

GNSS signal plan	Configuration key	Value
SP6	`CFG-SIGNAL-PLAN`	6

Table 7: GNSS signal plan configuration

2.2.5 GPS L5 signal health status configuration

Broadcasting of Civil Navigation (CNAV) messages on the L5 signal began in April 2014. However, at the time of writing, GPS L5 signals remain pre-operational and they are set unhealthy until sufficient monitoring capability is established.

To evaluate GPS L5 signals before they become fully operational, use the configuration strings in Table 8 to ignore the GPS L5 signal health status and override it with the respective GPS L1 signal health status. To revert to the default configuration, use the configuration strings in Table 9. Configuration in the RAM layer is applied immediately, if the receiver returns the `UBX-ACK-ACK` message. Applying the configuration stored in the BBR and flash layers requires a receiver reset.

⚠ Do not use unhealthy, pre-operational GPS L5 signals for safety-of-life or other critical purposes. This is an operational issue concerning the satellites / space segment and not a limitation or specific configuration of u-blox products.

⚠ Ignoring the GPS L5 signal health status in your production system may introduce operational risks. Ensure you're fully aware of the potential consequences before proceeding. Ensure that your system also includes a mechanism to revert the L5 signal health status monitoring to default when the GPS Operational Control System (OCX) upgrade is complete.

Configuration layer	Configuration string
RAM	B5 62 06 8A 09 00 01 01 00 00 01 00 32 10 01 DF F6
BBR	B5 62 06 8A 09 00 01 02 00 00 01 00 32 10 01 E0 FE
FLASH	B5 62 06 8A 09 00 01 04 00 00 01 00 32 10 01 E2 0E

Table 8: UBX binary string to override GPS L5 signal health status with GPS L1 health status

Configuration layer	Configuration string
RAM	B5 62 06 8A 09 00 01 01 00 00 01 00 32 10 00 DE F5
BBR	B5 62 06 8A 09 00 01 02 00 00 01 00 32 10 00 DF FD
FLASH	B5 62 06 8A 09 00 01 04 00 00 01 00 32 10 00 E1 0D

Table 9: UBX binary strings to revert the GPS L5 signal health status monitoring to default

2.2.6 Communication interface configuration

This section describes how to configure the available communication interfaces. The configuration groups listed in Table 10 define the interface parameters, such as data framing and transfer rate, and control which input and output protocols are enabled.

Each protocol, such as industry-standard NMEA and u-blox UBX, can be enabled or disabled independently for each communication interface. As a result, message output configuration applies only when the corresponding protocol is enabled for output on the interface.

Interface	Configuration groups	Description

UART1	`CFG-UART1`
	`CFG-UART1INPROT`
	`CFG-UART1OUTPROT`
		Configuration of the UART1 interface
		Input protocol configuration of the UART1 interface
		Output protocol configuration of the UART1 interface

UART2	`CFG-UART2`
	`CFG-UART2INPROT`
	`CFG-UART2OUTPROT`
		Configuration of the UART2 interface
		Input protocol configuration of the UART2 interface
		Output protocol configuration of the UART2 interface

Interface	Configuration groups	Description
USB	CFG-USB CFG-USBINPROT CFG-USBOUTPROT	Configuration of the USB interface Input protocol configuration of the USB interface Output protocol configuration of the USB interface
I2C	CFG-I2C CFG-I2CINPROT CFG-I2COUTPROT	Configuration of the I2C interface Input protocol configuration of the I2C interface Output protocol configuration of the I2C interface
SPI	CFG-SPI CFG-SPIINPROT CFG-SPIOUTPROT	Configuration of the SPI interface Input protocol configuration of the SPI interface Output protocol configuration of the SPI interface

Table 10: Interface configurations

2.2.7 Message output configuration

To enable or disable message output, or to configure the output rate of each periodic message, use the CFG-MSGOUT configuration group. The receiver generates output messages when specific events occur. For periodic events, the receiver outputs the corresponding messages at regular intervals defined by the event frequency.

As an example, the UBX-NAV-PVT message is associated with the navigation event, which produces a navigation solution. The output rate of this message depends on the configured navigation rate, as discussed in section Measurement and navigation rate configuration. Table 11 shows message output configuration examples for the UBX-NAV-PVT message.

Configuration	Description
CFG-MSGOUT-UBX_NAV_PVT_UART1 = 0	The UBX-NAV-PVT message output via UART1 is disabled.
CFG-MSGOUT-UBX_NAV_PVT_UART1 = 1	The UBX-NAV-PVT message is output via UART1 on every navigation solution.
CFG-MSGOUT-UBX_NAV_PVT_UART1 = 2	The UBX-NAV-PVT message is output on every second navigation solution.

Table 11: Message output configuration examples

☞ Some non-periodic messages, such as UBX-MON-VER, are only output in response to a poll request. Furthermore, the UBX-INF and NMEA-Standard-TXT non-periodic information messages can be configured with the CFG-INFMSG configuration group.

2.2.8 Measurement and navigation rate configuration

The measurement and navigation rate configuration defines the rate of measurement and navigation events. Therefore, it has a direct impact on the output rates of the related messages as discussed in section Message output configuration. Configure the measurement and navigation rate with the CFG-RATE-MEAS and CFG-RATE-NAV configuration keys. See Table 12 for examples.

☞ To optimize the use of processing resources, set the navigation rate value higher than one (1) only if the raw measurement data output is needed at a higher rate than the navigation data.

CFG-RATE-MEAS	Measurement rate	CFG-RATE-NAV	Navigation rate	Remarks
1000	1 Hz	1	1 Hz	Default configuration, suitable for generic use cases.
500	2 Hz	1	2 Hz	Ideal configuration for 2 Hz navigation rate.
100	10 Hz	5	2 Hz	Use only if raw measurements are enabled and needed at higher rate than navigation solutions.
100	10 Hz	1	10 Hz	Ideal configuration for 10 Hz navigation rate.

Table 12: Measurement and navigation rate configuration examples

The ZED-X20D heading module supports dual-antenna operation. For optimal performance, both antennas should use the same update rate.

If different update rates are required, this configuration is supported with technical assistance from u-blox. For reliable operation, the update rate of antenna 1 should be an integer multiple of the update rate of antenna 2. With HDG 2.00 firmware, this configuration can only be implemented through internal messages. For example:

- Antenna 1: 20 Hz navigation update rate; Antenna 2: 10 Hz or 5 Hz heading update rate.
- Antenna 1: 25 Hz navigation update rate; Antenna 2: 12.5 Hz or 5 Hz heading update rate.

For further information and guideline, contact u-blox local technical support.

2.3 Navigation configuration

This section presents various configuration options related to the navigation engine. These options can be configured with the `CFG-NAVSPG` configuration group.

2.3.1 Dynamic platform

Configure the dynamic platform model for the application with the `CFG-NAVSPG-DYNMODEL` configuration item. For the supported dynamic platform models and their details, see Table 13 and Table 14.

The receiver checks the sanity of the navigation solution against the dynamic platform model limits as described in Table 14. If the sanity check fails, the receiver sets the navigation solution invalid.

Platform	Description
Portable	Applications with low acceleration, e.g. portable devices. Suitable for most situations.
Stationary	Used in timing applications (antenna must be stationary) or other stationary applications. Velocity restricted to 0 m/s. Zero dynamics assumed.
Pedestrian	Applications with low acceleration and speed, e.g. how a pedestrian would move. Low acceleration assumed.
Automotive	Used for applications with equivalent dynamics to those of a passenger car. Low vertical acceleration assumed.
At sea	Recommended for applications at sea. Zero vertical velocity and sea level assumed.
Airborne <1g	Used for applications with a higher dynamic range and greater vertical acceleration than a passenger car. No 2D position fix supported.
Airborne <2g	Recommended for typical airborne environments. No 2D position fix supported.
Airborne <4g	Only recommended for extremely dynamic environments. No 2D position fix supported.
Wrist	Only recommended for wrist-worn applications. Receiver filters out arm motion.

Table 13: Dynamic platform models

Platform	Max altitude [m]	Max horizontal velocity [m/s]	Max vertical velocity [m/s]	Sanity check type	Max position deviation
Portable	12,000	310	50	Altitude and velocity	Medium
Stationary	9,000	10	6	Altitude and velocity	Small
Pedestrian	9,000	30	20	Altitude and velocity	Small
Automotive	6,000	100	15	Altitude and velocity	Medium
At sea	500	25	5	Altitude and velocity	Medium
Airborne <1g	80,000	100	6,400	Altitude	Large
Airborne <2g	80,000	250	10,000	Altitude	Large
Airborne <4g	80,000	500	20,000	Altitude	Large

Platform	Max altitude [m]	Max horizontal velocity [m/s]	Max vertical velocity [m/s]	Sanity check type	Max position deviation
Wrist	9,000	30	20	Altitude and velocity	Medium

Table 14: Dynamic platform model details

☞ Applying dynamic platform models designed for high acceleration systems, such as airborne <2g, can result in a higher standard deviation in the reported position.

2.3.2 Navigation input filters

The navigation input filters control how the navigation engine handles the input data that comes from the satellite signal. For the applicable navigation input filter configurations, see Table 15.

If the receiver has only three satellites for calculating a position, the navigation algorithm uses a constant altitude to compensate for the missing fourth satellite. This is called a 2D fix. The constant altitude value is taken from the last successful 3D fix using a minimum of four available satellites.

Configuration item	Description
`CFG-NAVSPG-FIXMODE`	By default, the receiver calculates only 3D position fix. The receiver can calculate 2D or 3D positions if configured to auto (2D/3D).
`CFG-NAVSPG-CONSTR_ALT` `CFG-NAVSPG-CONSTR_ALTVAR`	The fixed altitude is used if fixMode is set to 2D only. Supply a variance greater than zero.
`CFG-NAVSPG-INFIL_MINELEV`	The minimum elevation of a satellite above the horizon to be used in the navigation solution. Low-elevation satellites may provide degraded accuracy due to the long signal path through the atmosphere.
`CFG-NAVSPG-INFIL_MINSVS` `CFG-NAVSPG-INFIL_MAXSVS`	The minimum and maximum number of satellites to use in the navigation solution. There is an absolute maximum limit of 32 satellites that can be used for navigation.
`CFG-NAVSPG-INFIL_NCNOTHRS` `CFG-NAVSPG-INFIL_CNOTHRS`	A navigation solution will only be attempted if there is at least the given number of satellites with signals at least as strong as the given threshold.

Table 15: Navigation input filter parameters

2.3.3 Navigation output filters

The receiver initially classifies the navigation solution by the fix type, as in the `fixType` field of the `UBX-NAV-PVT` message. However, the fix type doesn't provide any validity information. Therefore, the receiver checks the validity of every position fix with the navigation output filters. That is, the receiver sets the fix as valid if the navigation solution is above all the navigation output filter masks (thresholds) described in Table 16. The receiver reports the fix validity in the message fields listed in Table 17.

☞ Don't use fixes that are not marked valid.

Configuration item	Description
`CFG-NAVSPG-OUTFIL_PDOP`	The position dilution of precision (PDOP) mask (threshold)
`CFG-NAVSPG-OUTFIL_TDOP`	The time dilution of precision (TDOP) mask (threshold)
`CFG-NAVSPG-OUTFIL_PACC`	Output filter position accuracy mask (threshold)
`CFG-NAVSPG-OUTFIL_TACC`	Output filter time accuracy mask (threshold)
`CFG-NAVSPG-OUTFIL_FACC`	Output filter frequency accuracy mask (threshold)

Table 16: Navigation output filter parameters

Message	Field	Description and remarks
`UBX-NAV-PVT`	`gnssFixOK`	1 = valid fix

Message	Field	Description and remarks
`UBX-NAV-STATUS`	`gpsFixOK`	This message is only retained for backwards compatibility, and it is recommended to use the `UBX-NAV-PVT` message instead.
`NMEA-GLL`	`status`	Data validity status
`NMEA-RMC`	`status`	Data validity status

Table 17: Messages and fields providing the fix validity

2.4 RTK configuration

RTK technology introduces the concept of a base[8] and a rover. In such a setup, the base sends corrections (complying with the RTCM 3.4 protocol) to the rover via a communication link. This enables the rover to compute its position relative to the base with high accuracy.

Operating as a rover, ZED-X20D can receive RTCM 3.4 corrections from another compatible GNSS receiver, such as ZED-X20P, operating as a base, or via NTRIP from a VRS service provider that operates a network of base receivers. For more information, refer to the Reference frames section in the Appendix.

After describing the RTCM protocol and corresponding supported message types, this section describes how to configure the ZED-X20D high precision receiver as a base or rover receiver.

☞ PointPerfect Live is a u-blox service that provides real-time, regional-scale positioning accuracy using Internet Protocol (IP)-based network RTK correction data. It supports GNSS RTK hardware that uses RTCM standards, allowing flexible integration across different receiver types. The service operation is continuously monitored using u-blox receivers.

2.4.1 RTCM corrections

RTCM is a standard-based binary protocol for the communication of GNSS correction information. ZED-X20D supports RTCM as specified by *RTCM 10403.4, Differential GNSS (Global Navigation Satellite Systems) Services – Version 3 (December 1, 2023)*.

The RTCM specification is currently at version 3.4 and RTCM version 2 messages are not supported by this standard.

To modify the RTCM input/output settings, see the configuration section in the applicable Interface description [2].

Users should be aware of the datum used by the correction source. The rover's reported position is in a coordinate system based on the correction service provider's reference frame. This may need to be taken into account when using the RTK rover position depending on the application. See the Reference frames section in the Appendix for more information.

2.4.2 List of supported RTCM input messages

Message type	Description
RTCM 1001	L1-only GPS RTK observables
RTCM 1002	Extended L1-only GPS RTK observables
RTCM 1003	L1/L2 GPS RTK observables
RTCM 1004	Extended L1/L2 GPS RTK observables
RTCM 1005	Stationary RTK reference station Antenna Reference Point (ARP)
RTCM 1006	Stationary RTK reference station ARP with antenna height

8 The terms base, base station, reference and reference station can be used interchangeably

Message type	Description
RTCM 1007	Antenna descriptor
RTCM 1009	L1-only GLONASS RTK observables
RTCM 1010	Extended L1-only GLONASS RTK observables
RTCM 1011	L1/L2 GLONASS RTK observables
RTCM 1012	Extended L1/L2 GLONASS RTK observables
RTCM 1033	Receiver and antenna description
RTCM 1074	GPS Multiple Signal Message (MSM) 4
RTCM 1075	GPS MSM5
RTCM 1077	GPS MSM7
RTCM 1084	GLONASS MSM4
RTCM 1085	GLONASS MSM5
RTCM 1087	GLONASS MSM7
RTCM 1094	Galileo MSM4
RTCM 1095	Galileo MSM5
RTCM 1097	Galileo MSM7
RTCM 1124	BeiDou MSM4
RTCM 1125	BeiDou MSM5
RTCM 1127	BeiDou MSM7
RTCM 1230	GLONASS code-phase biases
RTCM 4072.0	Reference station PVT (u-blox proprietary RTCM Message)

Table 18: ZED-X20D supported input RTCM version 3.4 messages

2.4.3 Rover operation

In its default configuration, ZED-X20D attempts to provide the best positioning accuracy depending on the received correction data. It enters RTK float mode shortly after it starts receiving an input stream of RTCM correction messages. Once the rover has resolved the carrier phase ambiguities, it enters the RTK fixed mode. When in this mode, the relative position accuracy between the base and the rover is expected to be at centimeter-level accuracy. The time period between the RTK float and RTK fixed operations is referred to as the convergence time. Note that the convergence time is affected by the baseline length as well as multipath and satellite visibility at both rover and base station.

To function optimally ZED-X20D has to receive RTCM corrections matching its GNSS signal configuration. The rover requires both base station observation (MSM4 or MSM7 messages) and position message (RTCM 1005 or RTCM 1006) to attempt ambiguity fixes. The rover attempts to provide RTK fixed operation when sufficient number of ambiguities is resolved. If phase lock on sufficient number of signals cannot be maintained, the rover drops back to the RTK float mode. Once the minimum number of signals has been restored, the rover continues attempting to resolve carrier ambiguities and to revert to the RTK fixed mode.

The RTK mode that an RTK rover operates in can be configured through the `CFG-NAVHPG-DGNSSMODE` configuration item. The following two RTK modes are available:

- RTK fixed: The rover attempts to fix ambiguities whenever possible.
- RTK float: The rover estimates the ambiguities as float but makes no attempts at fixing them.

The rover stops using RTCM corrections that are older than 60 s (default value) and drops back to the 3D or 3D/DGNSS mode. This is meant to prevent the computation of grossly misleading differential solutions. If desired, this value can be changed through the CFG-NAVSPG-CONSTR_DGNSSTO and CFG-NAVSPG-CONSTR_DGNSSTO_SCALE configuration items.

The received correction messages stream should comply with the following:

- The reference station ID in the reference station message (RTCM 1005 or RTCM 1006) must match that used in the MSM observation messages. Otherwise, the rover cannot compute the RTK fixed position.

CFG-RTCM-DF003_IN can be used to configure the desired reference station ID and CFG-RTCM-DF003_IN_FILTER can be used to configure how strict the filtering should be (RELAXED is the recommended setting).

2.4.3.1 Message output in RTK mode

When operating in RTK rover mode, note the modified information within the following NMEA and UBX messages:

- NMEA-GGA: The quality field is 4 for RTK fixed and 5 for RTK float (see NMEA position fix flags in interface description). The age of differential corrections and base station ID is set.
- NMEA-GLL, NMEA-VTG: The posMode indicator is D for RTK float and RTK fixed (see NMEA position fix flags in interface description).
- NMEA-RMC, NMEA-GNS: The posMode indicator is F for RTK float and R for RTK fixed (see NMEA position fix flags in interface description).
- UBX-NAV-PVT: The carrSoln flag is set to 1 for RTK float and 2 for RTK fixed. The age of differential corrections are reported.
- UBX-NAV-RELPOSNED
  - The diffSoln and relPosValid flags are set
  - The carrSoln flag is set to 1 for RTK float and 2 for RTK fixed
- UBX-NAV-SAT
  - The diffCorr flag is set for satellites with valid RTCM data
  - The rtcmCorrUsed, prCorrUsed, and crCorrUsed flags are set for satellites for which the RTCM corrections have been applied
- UBX-NAV-SIG
  - For signals to which the RTCM corrections have been applied, the correction source is set to RTCM3 OSR and the crUsed, prCorrUsed, and crCorrUsed flags are set
- UBX-NAV-STATUS
  - The diffSoln flag and the diffCorr flag is set
  - The carrSoln flag is set to 1 for RTK float and 2 for RTK fixed
- If the baseline exceeds 100 km, a UBX-INF-WARNING will be output, e.g. "WARNING: DGNSS long baseline: 102.7 km"

2.4.4 Moving base RTK operation

The moving base mode differs from the standard RTK operation in that the base station is no longer stationary at a predetermined location. Both the reference station and rover receivers are allowed to move while computing an accurate vector between the receiver antennas. This mode enables the calculation of heading on dynamic or static platforms, and provides a centimeter-level accurate 3D vector for use in dynamic positioning applications, for example in UAV follow-me use cases.

In the moving base RTK mode, the base and rover receivers are referred to as moving base and moving base rover respectively.

2.4.4.1 Configuring rover in moving base RTK mode

Operate the rover in the moving base RTK mode to estimate the relative position between receivers with centimeter level accuracy. Unless the base receiver applies RTCM 3.4 corrections, the absolute position accuracy remains at standard GNSS levels of a few meters.

In addition to the rules described in the rover operation section, follow the moving base-specific rules:

- A moving base receiver typically experiences worse GNSS tracking than a static base receiver in an open-sky environment and therefore the moving base RTK performance may be degraded.
- The moving base rover delays the navigation solution computation, and lowers the navigation update rate down to 1 Hz while waiting for time-matched observations. If observations are not received in time, the receiver flags the relative position as invalid.
- Minimize communication link latency. Reduce the delay between the transmission of RTCM messages from the base and reception by the rover to support higher navigation update rate.
- As a rule of thumb, keep latency below the configured navigation update period minus 50 ms.
- If the communication link latency prevents the configured navigation update rate, the receiver reduces the navigation update rate down to 1 Hz.
- If the communication link latency is too high for 1 Hz rover operation, the receiver declares the relative position as invalid.
- To ensure that the moving base processing works, configure the rover to use the same navigation update rate and measurement rate as the moving base.

UBX-NAV-RELPOSNED output reflects the moving base operation as follows:

- The isMoving flag is set
- The relPosValid flag is set when time-matched observations are processed successfully
- The length of the relative position vector and its accuracy are output
- The heading for the relative position vector and its accuracy are output
- The relPosHeadingValid flag is set unless the length of the relative position vector and/or its accuracy are not sufficient to reliably derive the heading information

2.4.5 RTK status pin (RTK_STAT)

ZED-X20D includes the **RTK_STAT** pin that provides an indication of the RTK positioning status. It can be used to confirm if a valid stream of correction messages is being received. As valid correction messages, we only consider the correction messages that are supported and used by the receiver.

The **RTK_STAT** pin status can be mapped to the `carrSoln` field of the `UBX-NAV-PVT` and interpreted as in Table 19:

Pin level	RTK status
Active low	RTK fixed mode has been achieved
Alternating (toggling)	A valid stream of correction messages is being received and utilized, but RTK fixed mode has not been achieved
Active high	No carrier phase solution is available

Table 19: RTK_STAT pin status interpretation

2.5 PPP-RTK configuration

2.5.1 SPARTN corrections

Operating as a rover, ZED-X20D can receive SPARTN corrections:

- via the internet from a service provider

- via a host application that receives L-band satellite data (NEO-D9S can be used for this). For more information on supported SPARTN corrections, see section Multiple SPARTN sources.

☞ PointPerfect Flex is a u-blox service offering flexible plans and usage models on a continental scale through IP-based network and in some locations L-band satellite link. It offers wide uniform coverage and 3-6 cm accuracy and convergence in seconds. The service is continuously monitored with u-blox receivers.

2.5.2 SPARTN protocol

SPARTN is a binary protocol for the communication of SSR correction information.

ZED-X20D supports SPARTN as specified by SPARTN Interface Control Document – Version 2.0.2 (February, 2022).

To modify the SPARTN input/output settings, see the configuration section in the applicable Interface description [2].

2.5.3 List of supported SPARTN 2.0.2 input messages

Message type-subtype	Description
SM 0-0	GPS orbit, clock, bias (OCB)
SM 0-1	GLONASS orbit, clock, bias (OCB)
SM 0-2	Galileo orbit, clock, bias (OCB)
SM 0-3	BeiDou orbit, clock, bias (OCB)
SM 1-0	GPS high-precision atmosphere correction (HPAC)
SM 1-1	GLONASS high-precision atmosphere correction (HPAC)
SM 1-2	Galileo high-precision atmosphere correction (HPAC)
SM 1-3	BeiDou high-precision atmosphere correction (HPAC)
SM 2-0	Geographic area definition (GAD)

Table 20: ZED-X20D supported input SPARTN version 2.0.2 messages

- Only the messages in Table 20 are supported. The implementation recognizes unsupported correction messages but they are not applied for the RTK solution such as QZSS correction messages, for instance.
- Group and embedded authentication messages are not supported.
- SM1 messages must contain tropospheric model for the receiver to reach an RTK fixed solution.

Application designs using ZED-X20D and SPARTN correction streams should provide firmware upgrade capability; upcoming firmware versions will implement further SPARTN messages and functionalities.

☞ Some SPARTN correction service providers broadcast different sets of messages in different regions and support different signals or satellites. These variations may affect the accuracy of ZED-X20D.

2.5.4 Multiple SPARTN sources

ZED-X20D supports multiple SPARTN correction stream sources. It can support a SPARTN correction stream received over the internet (SPARTN message formatted IP stream) or over L-band satellites (SPARTN L-band stream formatted as UBX-RXM-PMP messages).

Only one source can be configured to be used at a time by ZED-X20D. The configuration item `CFG-SPARTN-USE_SOURCE` can be configured to select which source will be used. Alternatively, the input protocol configuration items of a physical port can be configured to block input support for the UBX or the SPARTN protocols on the desired ports, for example CFG-UART1INPROT-UBX, CFG-USBINPROT-SPARTN, etc.

Source	Description	CFG-SPARTN-USE_SOURCE
SPARTN IP stream	This refers to corrections received in a SPARTN message format by any interface of the ZED-X20D. The SPARTN corrections must follow the SPARTN protocol specification and the source can be any SPARTN service provider.	IP (default)
SPARTN L-band stream	This refers to corrections received in a UBX-RXM-PMP message format by any interface of the ZED-X20D. UBX-RXM-PMP messages are provided by u-blox L-band NEO-D9S receivers and contain frames of SPARTN messages following the SPARTN protocol specification.	LBAND

Table 21: Supported SPARTN correction stream sources

☞ In case a host application receives a SPARTN L-band stream through other means and converts UBX-RXM-PMP messages to SPARTN messages, then ZED-X20D treats these corrections as a SPARTN IP stream

☞ When providing a SPARTN L-band stream formatted as UBX-RXM-PMP messages, it is recommended to enable both UBX and SPARTN input protocol support on the port where the UBX-RXM-PMP is received. For example, as the default configuration on UART2, where CFG-UART2INPROT-UBX = 1 (true) and CFG-UART2INPROT-SPARTN = 1 (true).

The host application is responsible for deciding which stream to use. This can be based, for example, on the current IP or L-band reception conditions, the needs of the host application, power/cost considerations etc. The ZED-X20D does not provide any intelligent or automatic stream selection.

ZED-X20D provides additional monitoring information in the form of UBX-RXM-COR messages. This helps to identify what the current stream status is to assist the host application in deciding which stream to use. Among other information, UBX-RXM-COR reports:

- The type/subtype of the received SPARTN messages.
- The source of the received SPARTN message (IP or L-band) and if it is used by ZED-X20D.

Additionally, some SPARTN input status information is also available in other UBX messages, such as UBX-MON-COMMS. For the full message specification, see ZED-X20D Interface description [2].

☞ If the selected SPARTN source contains encrypted SPARTN corrections, extra monitoring information is reported through the UBX-RXM-COR. This includes, for example, information if the message is encrypted and if it has been decrypted.

2.5.5 Encrypted SPARTN support

SPARTN messages may be encrypted as indicated by the TF004 SPARTN field (Encryption and authentication flag). ZED-X20D supports both encrypted and unencrypted SPARTN messages. The unencrypted SPARTN messages can be utilized by ZED-X20D as is without any special setup. Encrypted SPARTN messages can be decrypted and utilized by ZED-X20D once the appropriate dynamic keys have been set and the host application manages them.

☞ Different dynamic keys apply for the IP-only stream. The type of service available is specified by u-blox Terms and Services.

For information on enabling encrypted SPARTN support for the u-blox PointPerfect service, see Table 22.

Step	Description	Example/notes
Obtain PointPerfect dynamic key	Request a PointPerfect dynamic key lease. The keys come in a json structure containing two dynamic keys: the current key and the next key. The request can be postponed if the host application already holds a json structure obtained earlier and the current time falls within the current key validity time.	Current: • Key: current key in byte array format • Expires: current key expiring date Next: • Key: next key in byte array format • Expires: next key expiring date
Check if current and next dynamic keys are currently available	To see the current and next keys saved in ZED-X20D, poll the `UBX-RXM-SPARTNKEY` at every power cycle of or whenever the host application needs to decrypt the encrypted SPARTN messages for the first time. If no key is saved or both keys have expired, then no key is reported. If one key is available and/or one key has expired, then only one current key is reported. If two keys are available and no key has expired, then both current and next keys are reported.	See description of `UBX-RXM-SPARTNKEY` message in the applicable Interface description [2].
Set current and next dynamic keys	To set the current and next dynamic keys, convert the json structure into a `UBX-RXM-SPARTNKEY`. Repeat this at every power cycle, or whenever the host application needs to decrypt encrypted SPARTN messages for the first time, or when the dynamic keys are close to expiring (e.g. only one key is available and is close to expiring), or when no dynamic key has been saved.	This will load the current and next dynamic keys in this sequence. See the description of `UBX-RXM-SPARTNKEY` in the applicable interface description [2]. Although setting the current key only is sufficient, it is recommended that both current and next keys are set.
Forward or relay SPARTN corrections	Design the host application so that SPARTN corrections arrive to the ZED-X20D interfaces as SPARTN format messages (over an IP stream). If there are multiple SPARTN sources, the receiver only attempts to be decrypt/use the one selected by the `CFG-SPARTN-USE_SOURCE` configuration item. The other available SPARTN source will not be decrypted and will be reported as such.	
Monitor decryption status	`UBX-RXM-COR` reports information on the selected stream if has been encrypted and decryption has been performed. Further key status information are reported by the `UBX-RXM-SPARTNKEY` message.	Decryption success cannot be verified in SPARTN messages
Monitor key status	`UBX-RXM-SPARTNKEY` reports information on the current and next key and if both, one, or no key is available.	See description of UBX-RXM-SPARTNKEY message in the applicable Interface description [2].
Key switching from current to next	The host application does not need to handle the key switching form current to next as long as both keys have been saved in ZED-X20D. Once the current key expires, it gets removed and replaced by the next key (if available). In this case, only the next key is available and reported as the current one. If no next key is available to become current, the decryption stops and the above steps need to be repeated.	

Table 22: PointPerfect dynamic key handling

2.5.6 CLAS corrections

QZSS CLAS (centimeter-level augmentation service) is the satellite-based Japan's nationwide open service providing centimeter positioning accuracy. Corrections are transmitted on the QZSS L6 signal and encoded with Compact SSR (cSSR) protocol. Currently, the CLAS service provides corrections for GPS, Galileo, and QZSS satellites in view.

ZED-X20D supports CLAS corrections directly provided from NEO-D9C output in the form of UBX-RXM-QZSSL6. ZED-X20D can be directly connected to a NEO-D9C or the host application can forward the UBX-RXM-QZSSL6 message from NEO-D9C to ZED-X20D with no parsing needed.

For more information see the NEO-D9C integration manual and applicable interface description.

2.5.7 Rover operation

The rover operation and configuration, when using SPARTN corrections, is similar to the setup when using RTCM corrections (see RTCM rover operation).

The float/fix carrier phase ambiguities resolution concept is maintained and, where relevant, the NMEA and UBX output contents are updated accordingly. Small adjustments are made where necessary, for example the correction source field in UBX messages will be set to SPARTN instead of RTCM.

To verify that the rover is receiving and using SPARTN or corrections, observe the following messages:

- `UBX-MON-COMMS` message reports which data has been received on which port.
- `UBX-NAV-SIG` message reports which type of corrections are applied for each signal in the field "corrSource".
- `UBX-RXM-COR` message reports which SPARTN messages have been received and used.

For further details, see the applicable Interface description [2].

Users should be aware of the datum used by the correction source. The rover position provides coordinates in the correction source reference frame. This may need to be taken into account when using the PPP-RTK rover position.

☞ If the rover switches between different correction types (SPARTN or RTCM), it is recommended to reset the receiver before using a new type of correction.

2.6 PPP configuration

☞ For PPP solutions, the ambiguity resolution algorithm is disabled by default and not available on ZED-X20D.

2.6.1 Configuring Galileo HAS

ZED-X20D supports Galileo High Accuracy Service (HAS). This feature is disabled by default. It can be enabled with the following configuration keys as shown in Table 23.

Configuration key	Value	Description
`CFG-NAVCOR-ENABLE_HOST`	0	Enables or disables the corrections from RTCM/SPARTN. Default value 1.
`CFG-NAVCOR-ENABLE_GAL_HAS`	1	Enables or disables the corrections from Galileo HAS. Default value 0.

Table 23: Configuration keys to enable Galileo HAS

☞ If both `CFG-NAVCOR-ENABLE_HOST` and `CFG-NAVCOR-ENABLE_GAL_HAS` are set to True, RTCM or SPARTN corrections are prioritised over the corrections from Galileo HAS.

☞ ZED-X20D supports the corrections from Galileo HAS only over the Galileo E6-B signals.

2.7 OTP memory configuration

ZED-X20D contains a one-time programmable (OTP) memory. This is a non-volatile memory for storing configuration settings and ROM patches permanently in the device. The stored data cannot be modified after it has been initially programmed. The device applies the settings and ROM patches on startup.

As the space in the OTP memory is limited, it should be used only for storing essential system configuration settings. The total space used for device configuration and ROM patches in the OTP memory must not exceed 150 bytes. Other settings can be stored in the BBR or sent from the host to the device on each device startup.

☞ Ensure that the final configuration stored and optional ROM patches do not require more than 150 bytes of OTP memory space.

3 Receiver functionality

This chapter describes the ZED-X20D operational features and their configuration.

3.1 Heading

The ZED-X20D all-band GNSS module is designed for high precision heading applications.

The heading is defined as the angle between the baseline vector, connecting Antenna 1 and Antenna 2, and geographic true north in the North-East-Down (NED) coordinate system. As illustrated in Figure 7, the orientation of the baseline vector goes from Antenna 1 (connected to module pin **RF_IN_1**) to Antenna 2 (connected to module pin **RF_IN_2**).

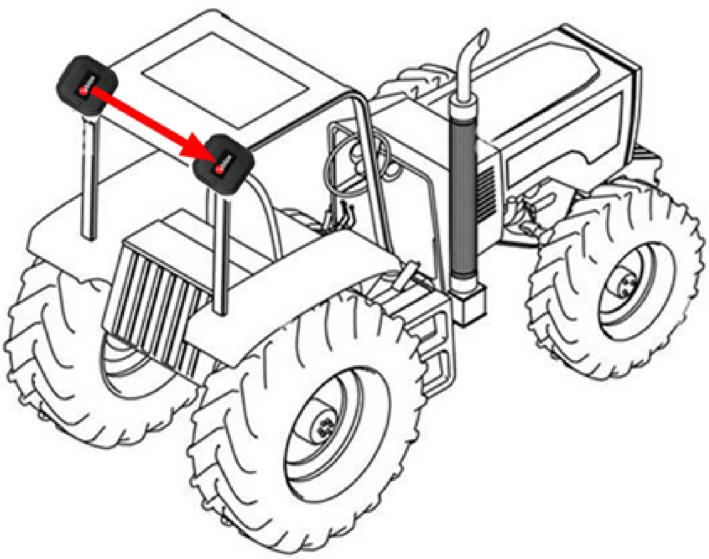


Figure 7: ZED-X20D Heading vector between RF_IN_1 and RF_IN_2 ports of ZED-X20D

The dual antenna installation has a direct impact on the heading performance. For example: the longer the baseline, the better the heading accuracy.

For more information on antenna selection and placement for a heading solution, see section Antenna selection and placement.

3.1.1 Heading status reporting

The `UBX-NAV-DAHEADING` message provides the relative position vector and heading from antenna 1 to antenna 2, along with the corresponding accuracy figures.

For detailed information on the `UBX-NAV-DAHEADING` message, refer to the Interface description [2].

The application can use the `UBX-NAV-DAHEADING` message to read the heading value, monitor the baseline, and check whether the heading solution is valid.

The heading solution is considered valid only if the `relPosHeadingValid` flag is set to 1.

If the heading solution is invalid, the application should discard the heading value until a valid heading solution is reported.

3.1.2 Heading status pin (HEADING_STAT)

In parallel to the `UBX-NAV-DAHEADING` message, the **HEADING_STAT** pin provides a hardware indication of the heading validity. This indication may be used, for example, as an input to a host processor GPIO or for connection to an LED.

Pin output	Description
High	Heading indication is valid.
Low	Heading indication is invalid.

Table 24: HEADING_STAT pin functionality

3.2 Augmentation systems

3.2.1 Satellite Based Augmentation System (SBAS)

Satellite Based Augmentation System (SBAS) broadcasts augmentation data, such as ionosphere correction parameters, to improve the positioning accuracy of the receiver. SBAS systems generate these correction parameters from measurements collected by regional Ranging and Integrity Monitoring Stations (RIMS). The parameters are combined into a Total Electron Content (TEC) map and broadcast by SBAS satellites to reduce ionospheric effects in the received GNSS signals.

ZED-X20D automatically selects one SBAS satellite as the primary source for receiving correction data because the information broadcast by other SBAS satellites is redundant or may be inconsistent. The selection strategy depends on the satellite proximity, the services provided by the satellite, the signal link quality, and the SBAS configuration.

The supported SBAS message types are listed in Table 25, whereas the `UBX-NAV-SBAS` message provides detailed information about the availability and use of SBAS corrections. Refer also to SBAS status reporting.

Message type	Message content	Source
0(0/2)	Test mode	All
1	Pseudo-Random Noise (PRN) mask assignment	Primary
2, 3, 4, 5	Fast corrections	Primary
6	Integrity	Primary
7	Fast correction degradation	Primary
9	Satellite navigation (ephemeris)	All
10	Degradation	Primary
12	Time offset	Primary
17	Satellite almanac	All
18	Ionosphere grid point assignment	Primary
24	Mixed fast / long-term corrections	Primary
25	Long-term corrections	Primary
26	Ionosphere delays	Primary

Table 25: Supported SBAS messages

☞ When the receiver switches from a solution using correction data to a standard position solution, the reference frame of the output position switches as well. The reference frame of an SBAS solution is aligned within a few centimeters of World Geodetic System 1984 (WGS84) and modern International Terrestrial Reference Frame (ITRF) realizations.

☞ SBAS is only used if no correction service is available. If the connection stream is lost during operation, the receiver switches to using the SBAS corrections after the time set in `CFG-NAVSPG-CONSTR_DGNSSTO` has elapsed (60 s by default).

3.2.2 SBAS status reporting

SBAS status reporting indicates whether SBAS correction data is received and used in the navigation solution. Table 26 provides examples of UBX and NMEA messages and fields that show if SBAS differential corrections are applied. For full message details, refer to the Interface description [2].

Message	Field	Description
`UBX-NAV-PVT`, `UBX-NAV-STATUS`	`diffSoln`	Indicates whether a differential position is provided.
`UBX-NAV-SAT`	`sbasCorrUsed`	Shows, per satellite, if SBAS correction data was used in the solution.
`UBX-NAV-SIG`	`corrSource`	Shows, per signal, if SBAS correction data was used in the solution.
`NMEA-GGA`	`quality`	Indicates whether a differential position is provided.
`NMEA-GLL`, `NMEA-RMC`, `NMEA-GNS`	`status`	Indicates whether a differential position is provided.

Table 26: Examples of SBAS status reporting messages

3.2.3 SBAS configuration

SBAS configuration defines how the receiver uses SBAS correction and integrity information. To configure the SBAS functionality, use the SBAS configuration items described in Table 27.

Parameter	Description
`CFG-SIGNAL-SBAS_ENA`	Enables or disables the SBAS subsystem.
`CFG-SBAS-USE_TESTMODE`	Enables or disables the use of SBAS data from satellites operating in test mode.
`CFG-SBAS-USE_RANGING`	Enables or disables the use of SBAS satellites that provide ranging information for navigation.
`CFG-SBAS-USE_DIFFCORR`	Enables or disables fast, long-term, and ionospheric corrections.
`CFG-SBAS-USE_INTEGRITY`	Applies SBAS integrity information to prevent the navigation engine from using signals without integrity data.
`CFG-SBAS-USE_IONOONLY`	Enables or disables the use of SBAS ionospheric corrections only (enabled by default).
`CFG-SBAS-PRNSCANMASK`	Enables or disables individual SBAS satellites. Use this parameter to exclude unwanted SBAS satellites.
`CFG-SBAS-ACCEPT_NOT_IN_PRNMASK`	Enables or disables the use of SBAS data from satellites that are not included in the PRN scan mask.

Table 27: SBAS configuration parameters

SBAS integrity restricts the receiver to signals for which integrity information is available. Near the borders of SBAS service regions, this restriction may significantly reduce the number of usable GNSS signals, including all non-GPS signals. In addition, the receiver does not apply SBAS integrity if integrity information is not available for at least five GPS satellites.

Each SBAS satellite serves a specific region, and its correction data is only useful within that region. Therefore, planning is important in areas where multiple SBAS systems can be received. Configure the receiver to exclude SBAS satellites that are not relevant for the operational region by applying the PRN scan mask in `CFG-SBAS-PRNSCANMASK`, for example as follows:

- **In eastern North America**, disable EGNOS satellites to ensure that WAAS satellites are preferred.
- **In Europe**, disable all satellites, except for those from the EGNOS system, to ensure that WAAS satellites do not take preference in western regions and to avoid GAGAN satellites taking preference in other areas.

3.2.4 BeiDou SBAS configuration

⚠ BeiDou SBAS is still in testing mode and it has not been officially released for operational use. Do not use it for safety related applications.

BeiDou satellite based augmentation system (BDSBAS) provides SBAS services to China and surrounding regions. BDSBAS is integrated in the BeiDou system and uses BDS-3 type satellites to broadcast SBAS L1/L5 signal, providing augmentation for BeiDou and GPS systems.

BeiDou SBAS is in testing mode and it is not enabled by default. Enabling Beidou SBAS may improve navigation solution by its correction data. To enable the BeiDou SBAS functionality, apply or verify the configuration items in Table 28.

Configuration item	Value
`CFG-SBAS-ACCEPT_NOT_IN_PRNMASK`	BDSBAS
`CFG-SBAS-PRNSCANMASK`	0x0000000001800400
`CFG-SBAS-USE_DIFFCORR`	TRUE
`CFG-SBAS-USE_INTEGRITY`	FALSE
`CFG-SBAS-USE_IONOONLY`	FALSE
`CFG-SBAS-USE_RANGING`	FALSE
`CFG-SBAS-USE_TESTMODE`	TRUE

Table 28: BeiDou SBAS configuration item

☞ The `CFG-SBAS-PRNSCANMASK` in Table 28 includes only BeiDou SBAS PRNs. Alternatively, the BeiDou SBAS PRNs can be added to the default list of PRNs enabled in the firmware or modified list of PRNs that is configured. This allows other SBAS systems to be used if BeiDou SBAS is not available.

3.2.5 QZSS SLAS

Sub-meter Level Augmentation Service (QZSS SLAS) is an augmentation technology, which provides correction data for pseudoranges of GPS and QZSS satellites. The correction stream is transmitted on the L1S signal at the L1 frequency (1575.42 MHz).

For more information on QZSS SLAS, see qzss.go.jp/en/.

☞ QZSS SLAS is only used if no other correction service is available (e.g. RTCM, SPARTN). If the connection stream is lost during the operation, the receiver switches to using the SLAS corrections after the time set in the `CFG-NAVSPG-CONSTR_DGNSSTO` configuration message has elapsed (60 s by default).

3.2.5.1 Features

Multiple QZSS SLAS signals can be received simultaneously.

When receiving QZSS SLAS correction data, the ZED-X20D high precision receiver autonomously selects the best QZSS satellite. The selection strategy is determined by the quality of the QZSS L1S signals, the receiver configuration (test mode allowed or not), and the location of the receiver with respect to the QZSS SLAS coverage area. When outside of this coverage area, the receiver will likely fall back to using SBAS corrections.

If QZSS SLAS corrections are used in the navigation solution, the differential status is indicated in several output messages such as `UBX-NAV-PVT`, `UBX-NAV-STATUS`, `UBX-NAV-SAT`, `NMEA-GGA`, `NMEA-GLL`, `NMEA-RMC` and `NMEA-GNS` (see the applicable interface description [2]). The UBX-NAV-SLAS message provides detailed information about which corrections are available and applied.

Message type	Message content
0	Test mode
47	Monitoring station information
48	PRN mask
49	Data issue number
50	DGPS correction
51	Satellite health

Table 29: Supported QZSS L1S SLAS messages for enhancing navigation

3.2.5.2 Configuration

Enable support for the necessary QZSS L1S signal with the `CFG-SIGNAL-QZSS_L1S_ENA` configuration item. Configure further QZSS SLAS functionalities with the `CFG-QZSS-USE_SLAS*` configuration items.

Parameter	Description
`CFG-QZSS-USE_SLAS_DGNSS`	Apply QZSS SLAS corrections
`CFG-QZSS-USE_SLAS_TESTMODE`	Allow the correction provided by QZSS satellites that are in test mode
`CFG-QZSS-USE_SLAS_RAIM_UNCORR`	If this configuration is set, the receiver tries to estimate the position by using only the corrected measurements; if all corrected measurements are not available, it doesn't use any corrections. If this configuration is not set, the receiver uses both corrected and uncorrected measurements for the navigation solution.
`CFG-QZSS-SLAS_MAX_BASELINE`	Maximum baseline distance to the closest ground monitoring station (GMS). SLAS corrections are applied only when receiver is within the specified maximum distance from the nearest GMS (default is 350 km). Note that due to the nature of the service, the usefulness of corrections degrades with distance. When the receiver is far from GMS, SBAS may be a more reliable source of correction data.

Table 30: QZSS SLAS configuration parameters

☞ When the RAIM option is enabled, measurements can only observe the QZSS GNSS time system.

3.3 Galileo High Accuracy Service (HAS)

Galileo High Accuracy Service (HAS) is a free service provided by the European Union's Galileo satellite navigation system. Galileo HAS is designed to provide improved positioning accuracy for various applications, including navigation, surveying, and geospatial data collection.

The corrections of Galileo HAS are broadcast through the Galileo E6-B signal and through IP, in a format similar to Compact-State-Space Representation (CSSR).

Galileo HAS transmits only corrections for GPS and Galileo, but in principle this could be combined with any other global or regional PPP/PPP-RTK service for other GNSS constellations to accelerate the convergence and improve the accuracy of the solution.

The Galileo HAS Full Service will provide two different service levels:

1. **Service Level 1 (SL1):** Global coverage with high accuracy corrections (orbits, clocks, code and phase biases) for Galileo E1/E5b/E5a/E6 and E5AltBOC and GPS L1/L5/L2C signals.
2. **Service Level 2 (SL2):** SL1 corrections and atmospheric corrections over the European Coverage Area (ECA).

For more information about Galileo HAS, refer to the Galileo HAS Service Definition Document (SDD) and Galileo HAS Information Note.

To configure ZED-X20D to use corrections of Galileo HAS, refer to the Configuring Galileo HAS section.

☞ Although labelled as global, the current Galileo HAS coverage does not include China, Japan, Korea, and some other regions due to the lack of ground stations in those areas.

3.4 Communication interfaces

u-blox receivers provide communication interfaces that support multiple protocols on a single port. This capability allows assigning several protocols, such as `UBX` and `NMEA`, to the same interface at the same time. As a result, the interface ports can transmit GNSS measurement data, report status information, and configure the receiver concurrently.

ZED-X20D provides the communication interfaces listed in Table 31 for communication with a host CPU. The `UBX-MON-COMMS` message provides consolidated information about the communication ports, and the communication interfaces can be identified by the `portId` field.

Electrical interface	UBX-MON-COMMS portId
I2C	0x0000
UART1	0x0100
UART2	0x0200
USB	0x0300
SPI	0x0400

Table 31: Port number assignment

☞ When the **VCC** voltage is removed, it is important to isolate the communication interface pins. They can be allowed to float or they can be connected to a high impedance.

3.4.1 UART

ZED-X20D supports a Universal Asynchronous Receiver/Transmitter (UART) port with RX and TX lines that can be used as a host interface with configurable baud rate and protocol selection. The UART supports only the baud rates listed in Table 32 for transmission and reception.

☞ The UART interface does not support handshaking signals or hardware flow control signals.

☞ The UART RX interface is disabled when more than 100 frame errors are detected during a one-second period. This can happen if the wrong baud rate is used or the **UART RX** pin is grounded. An error message appears when the UART RX interface is re-enabled at the end of the one-second period.

Baud rate	Data bits	Parity	Stop bits
4800	8	none	1
9600	8	none	1
19200	8	none	1
38400	8	none	1
57600	8	none	1

Baud rate	Data bits	Parity	Stop bits
115200	8	none	1
230400	8	none	1
460800	8	none	1
921600	8	none	1
2000000	8	none	1
4000000	8	none	1
8000000	8	none	1

Table 32: Possible UART interface configurations

Allow a short time delay of typically 100 ms between sending a baud rate change message and providing input data at the new rate. Otherwise some input characters may be ignored or the port could be disabled until the interface is able to process the new baud rate.

If there is too much data for the interface's bandwidth, the output buffer may overflow. Once the buffer space is exceeded, new messages to be sent will be dropped. To prevent message loss, the baud rate and the number of enabled messages should be selected carefully.

3.4.2 I2C

ZED-X20D provides an I2C interface for communication with an external host CPU in the I2C standard mode, fast mode, and fast mode plus. The interface can only operate in the peripheral mode, with the maximum bit rate of 1000 kbit/s. Refer to the ZED-X20D Data sheet for I2C peripheral timings and specifications [1].

ZED-X20D can make use of clock stretching by holding the Serial Clock (**SCL**) line LOW to temporarily pause data transfer. During the clock stretching, the effective bit transfer rate is reduced. The maximum clock stretching duration is 20 ms.

The **SCL** and Serial Data (**SDA**) pins include internal pull-up resistors, which are sufficient for most applications. For detailed design guidelines, refer to I2C Design Recommendations.

Read or set the I2C address with the `CFG-I2C-ADDRESS` configuration item (see Interface description [2]). This configuration item is an 8-bit value, in which the 7 most significant bits (MSB) represent the I2C address, and the least significant bit (LSB) is fixed to 0. The default I2C address is 0x84 (1000 0100b).

☞ When multiple peripherals share the I2C bus, configure each peripheral's I2C address to a different value to prevent conflicts.

The I2C interface uses three registers for communication between the controller and the peripheral as described in Table 33.

Register address	Description
0xFF	Actual data stream. If no data is available, reading from this register returns the value 0xFF.
0xFD	MSB of available data length.
0xFE	LSB of available data length.

Table 33: I2C Interface registers

3.4.2.1 I2C read access

To read data, the controller first queries the receiver for the available byte count (registers 0xFD and 0xFE), then polls register 0xFF to retrieve each byte of the data stream.

The register pointer:

- Auto-increments after each byte read.
- Stops incrementing at the highest valid register address (0xFF).

Figure 8 illustrates the read access format.

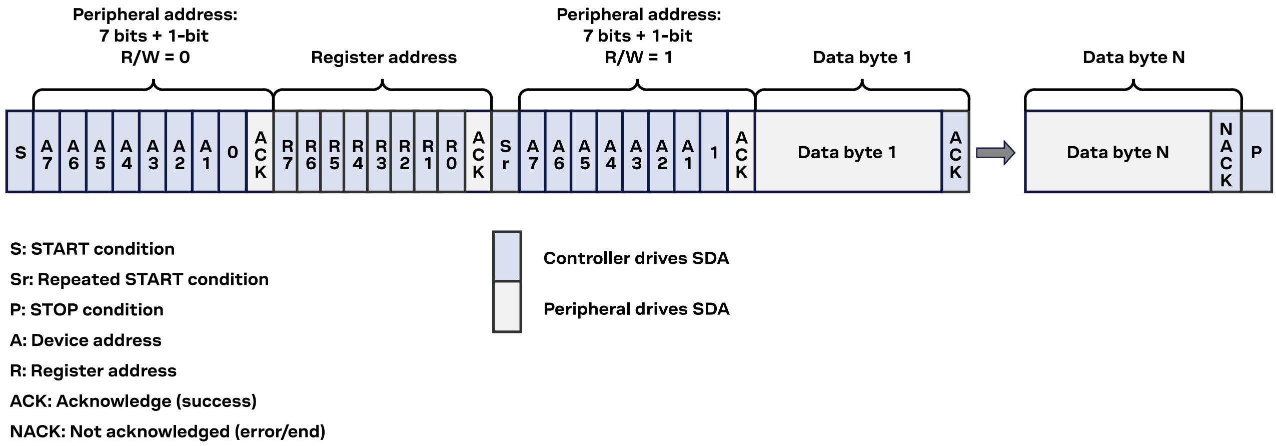


Figure 8: I2C data read

To perform a read operation on the I2C bus, follow these steps:

1. Initiate a START (S) condition on the I2C bus to signal the beginning of the communication.
2. Transmit the 7-bit receiver address followed by the R/W bit set to 0 (write).
   - The receiver responds with an ACK (logic low) to confirm recognition.
3. Write the 8-bit register address from which the reading will start (0xFD).
   - This sets the internal register pointer in the receiver.
   - The receiver acknowledges the receipt.
4. Issue a REPEATED START (Sr) condition to switch from the write mode to the read mode without releasing the bus.
5. Transmit the 7-bit receiver address again, this time with the R/W bit set to 1 (read mode).
   - The receiver acknowledges the address.
6. Read one or more bytes from the receiver acknowledging each byte except the last.
   - The first two bytes correspond to:
     - 0xFD → MSB of available data length
     - 0xFE → LSB of available data length
   - After reading these, the controller knows how many bytes are available at 0xFF (data register).
   - Continue reading from 0xFF to retrieve the actual data stream.
7. To terminate the transfer:
   - Send a NACK after the final byte to signal the end of reading.
   - Issue a STOP (P) condition to release the bus.

The data stream starts only after the controller has addressed the peripheral. If the controller does not read any data within a set timeout, 1.5 seconds by default, the receiver stops sending data to avoid overflowing its buffer. If necessary, consider disabling the I2C timeout by setting the `CFG-I2C-EXTENDEDTIMEOUT` configuration flag. For detailed information, refer to the Interface description [2].

☞ Disabling the timeout allows the receiver to continue buffering data for an extended period. It may lead to buffer overflow and potential data loss if the host controller does not read data frequently enough.

3.4.2.2 I2C write access

The receiver allows write access only for sending messages in supported protocols, such as UBX. The write access is intended for sending configuration commands, and aiding data.

☞ Do not write fewer than two bytes as the receiver interprets the operation as a pointer update, not a valid message write.

Figure 9 illustrates the write access format.

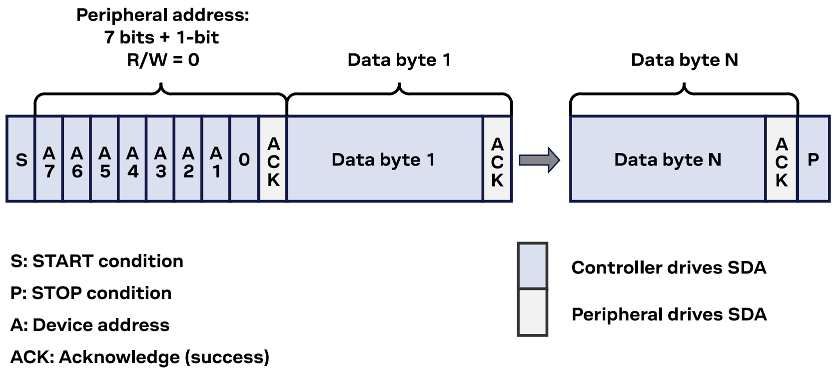


Figure 9: I2C data write

To perform a write operation on the I2C bus, follow these steps:

1. Initiate a START condition from the controller to begin communication on the I2C bus.
2. Transmit the 7-bit receiver address along with the R/W bit set to 0 (write).
   - This combination indicates a write operation.
   - The receiver responds with an ACK (logic low) to confirm address recognition.
3. Send the data (N bytes) to the receiver.
   - A minimum of two bytes is required to differentiate this operation from a register pointer write used for random read access.
4. To complete the write operation, issue a STOP condition after the final byte has been sent.

3.4.3 SPI

The ZED-X20D has an SPI peripheral interface that can be selected by setting **D_SEL** = LOW. The SPI peripheral interface is shared with UART1 and I2C port, the physical pins are same. The SPI pins available are:

- **SPI_SDO (TXD)**
- **SPI_SDI (RXD)**
- **SPI_CS_N**
- **SPI_CLK**

For more information about the communication interface selection, see Interface configuration pin (D_SEL).

☞ The SPI interface is designed to allow communication to a host CPU and thus, the interface can only be operated in peripheral mode.

☞ The SPI interface transmits data in Most Significant Bit (MSB) first order.

3.4.3.1 SPI read access

The register mode is not implemented for the SPI interface and thus, the NMEA and UBX message stream is accessible using the back-to-back read and write access implementation. When no data is available to be written to the receiver, **SDI** should be held logic high, i.e., all bytes written to the receiver are set to 0xFF.

To prevent the receiver from being busy parsing incoming data, the parsing process is stopped after 50 subsequent bytes containing 0xFF. The parsing process is re-enabled with the first byte not equal to 0xFF.

If the receiver has no more data to send, it sets **SDO** to logic high, i.e. all bytes transmitted decode to 0xFF. An efficient parser in the host will ignore all 0xFF bytes which are not part of a message and will resume data processing as soon as the first byte not equal to 0xFF is received.

3.4.3.2 SPI back-to-back read and write access

The receiver does not provide any write access except for writing UBX and NMEA messages to the receiver, such as configuration or aiding data. For every byte written to the receiver, a byte will simultaneously be read from the receiver. While the controller writes to **SDI** of the peripheral, at the same time it needs to read from **SDO** of the peripheral, as any pending data will be output by the receiver with this access. The data on **SDO** represents the results from a current address read, returning 0xFF when no more data is available. Figure 10 illustrates the SPI back-to-back read and write access.

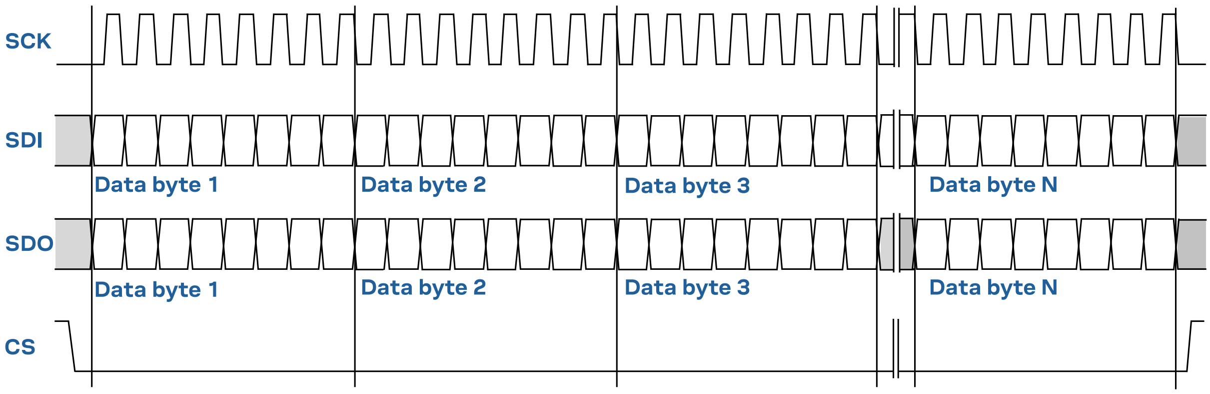


Figure 10: SPI back-to-back read/write access

3.4.4 USB

The Universal Serial Bus (USB) 2.0 full speed (12 Mbit/s) interface can be used for host communication. ZED-X20D is a USB device and requires a connection to a USB host.

ZED-X20D operates as a self-powered USB device and is supplied from its own power supply. The operation as a bus-powered USB device is not supported. For hardware implementation details, refer to the section USB circuit.

The receiver detects an active USB connection from the supply voltage at **V_USB**. After USB enumeration, the receiver retransmits the boot screen over the USB interface. The messages generated between the receiver startup and the completion of the USB enumeration are not available over USB.

☞ The USB suspend mode is not supported.

☞ The USB interface is disabled in the safeboot mode.

3.5 Receiver reset and startup

Forcing the receiver reset and defining its startup mode can be used to control the receiver's startup performance and behavior.

3.5.1 Reset types

Forcing receiver resets can help observe the effects of maintaining or losing data stored in RAM and/or BBR between restarts. Use the `UBX-CFG-RST` message to trigger a reset, specifying the type with the `resetMode` field to either clear or maintain navigation data in RAM and clear the RTC. Additionally, you can use the `navBbrMask` to initiate a cold, warm, or hot start configuration, or to define specific BBR data sections to be cleared, as detailed in the Interface description [2]. Table 34 outlines all the available reset types, detailing how each one affects the RTC and the data stored in BBR and RAM.

Reset type	Description	Clears RAM	Clears BBR	Clears RTC
0x00	**Immediate hardware reset (watchdog):** Uses the on-chip watchdog to electrically reset the chip as an immediate asynchronous reset without generating stop events.	All	All	Yes
0x04	**Hardware reset (watchdog) after shutdown:** Uses the on-chip watchdog to reset the receiver after shutdown.	All	All	Yes
0x01	**Controlled Software reset:** Terminates all running processes and restarts the receiver.	All	Selection	No
0x02	**Controlled Software reset (GNSS only):** Restarts only the GNSS-related processing and clears the navigation data in RAM without reinitializing the full system.	Navigation	Selection	No
0x08	**Controlled GNSS stop:** Stops only the GNSS-related processing and clears the navigation data in RAM without reinitializing the full system.	Navigation	Selection	No
0x09	**Controlled GNSS start:** Starts only the GNSS-related processing and clears the navigation data in RAM without reinitializing the full system.	Navigation	Selection	No
RESET_N	**Hardware reset by the RESET_N pin:** Immediately resets the chip as discussed in section Reset pin (RESET_N).	All	All	Yes

Table 34: Available reset types

☞ A receiver reset doesn't clear data or configurations stored in the flash memory.

3.5.2 Startup modes

GNSS receivers typically make a distinction between cold, warm and hot start modes based on the valid information the receiver has during the restart. Thus, the startup modes differ by means of TTFF and accuracy as the receiver can calculate the position and velocity data only when it receives enough signals from satellites with a valid ephemeris. Table 35 describes the different startup modes. Refer to the Data sheet for the startup performance specifications [1].

Startup mode	Description
Cold start	• The receiver starts in a cold start mode if it has no information about the last position, time, velocity, frequency and the currently available satellites (almanac or ephemeris). • In a cold start, the receiver must search through the full time and frequency space for all supported satellite signals to find and track satellite signals. • Once the receiver has found and started tracking a signal, it usually takes 18-36 seconds to decode the satellite's ephemeris under strong signal conditions. • Some GNSS receiver manufacturers call the cold start mode a factory startup mode.
Warm start	• The receiver starts in the warm start mode if it has approximate information for time, position and satellite position (almanac). • The receiver needs to download the ephemeris from the satellites prior calculating a PVT solution.
Hot start	• The receiver starts in the hot start mode if it has a valid ephemeris, RTC and the last position available. • A hot start is achievable after any controlled software reset or when restarting from the backup mode as the satellite ephemeris and RTC are maintained in the receiver's backup domain. • From the backup mode, hot starts are possible for up to 4 hours until the ephemeris data expires.
Aided start	• The receiver starts in the aided start mode if it is assisted upon the startup as described in section AssistNow GNSS assistance. • The startup performance depends on the quality and the latency of the assistance data.

Table 35: Receiver startup modes

3.5.3 Reset pin (RESET_N)

ZED-X20D provides a **RESET_N** pin as described in section pin assignment. To trigger a reset of the receiver, drive the **RESET_N** pin LOW for at least 1 ms. The pin voltage complies with the **VCC** level and can be actively driven HIGH. The **RESET_N** pin is input-only with an internal pull-up resistor and can be left open for normal operation.

☞ Do not drive the PIOs externally when the **VCC** is not supplied. If external driving of PIOs cannot be avoided, use isolation buffers.

☞ Receiver reset by the **RESET_N** pin will delete all information and trigger a cold start as discussed in sections Reset types and Startup modes. Use it only as a recovery option.

☞ Don't place a capacitor at **RESET_N** to GND, as it could trigger a reset on every startup.

3.6 Power management

Power management refers to controlling the receiver's power mode between the high-power continuous mode and the low-power backup modes to optimize its power consumption. In the continuous mode, the module operates normally, whereas in the backup mode, the receiver only maintains the critical navigation data and time information in the backup domain. Thus, in contrast to complete shutdown, the backup modes allow warm and hot starts at the next receiver restart as discussed in section Receiver reset and startup.

3.6.1 Continuous mode

The continuous mode is an active state where the receiver uses dedicated signal processing engines optimized for signal acquisition and tracking. The acquisition engine actively searches for and acquires signals during cold starts and whenever insufficient signals are available during navigation. Conversely, the tracking engine continuously tracks and downloads all the satellite data and acquires new signals as they become available.

3.6.2 Backup modes

☞ The software standby mode feature is not functional with the HDG 2.00 firmware.

A backup mode is an inactive state where the power consumption is reduced to a fraction of that of the continuous mode. Entering a backup mode always turns off the core domain, and therefore clears the RAM including the receiver configuration in RAM. To ensure data is preserved during the backup mode, save all the critical configuration data in the BBR or flash. By maintaining the BBR, the receiver can perform hot and warm starts at the next restart.

Table 36 provides an overview of the supported backup modes. The receiver automatically enters hardware-controlled backup mode and restarts in continuous mode according to the power supply status. Conversely, the software standby is controlled over the software interface as discussed in section Software standby mode.

	Power supply status		
Backup mode	**VCC**	**V_BCKP**	**Remarks**
Hardware backup mode	Removed	Supplied	• **V_BCKP** supplies the backup domain (BBR and RTC). • It's not allowed to drive the PIOs externally. • Use isolating buffers if external driving of the PIOs can't be avoided by other means.
Software standby mode	Supplied	N/A	• **VCC** supplies the backup domain (BBR and RTC) and PIOs. • Isolating the PIOs with buffers is not required.

Table 36: Supported backup modes

3.6.2.1 Hardware backup mode

In the hardware backup mode, the **V_BCKP** supply maintains the BBR and RTC while the **VCC** supply is switched off as described in Table 36. Therefore, the hardware backup mode requires an independent supply as discussed in section Backup supply input (V_BCKP). The **V_BCKP** supply is always internally disconnected when the **VCC** is supplied.

☞ Do not drive the PIOs externally when the **VCC** is not supplied. If external driving of PIOs cannot be avoided, use isolation buffers.

The recommended isolation options are:

- **Bus switches / analog switches:** Use FET-based switches to disconnect PIO lines when **VCC** is off.
- **Level shifters with enable control:** Select devices that can tri-state outputs when **VCC** is absent.
- **Dedicated buffer ICs:** Use buffers with OE pins tied to **VCC** for automatic disabling when power is off.

3.6.2.2 Software standby mode

Use the `UBX-RXM-PMREQ` message to control the standby mode as a power management request as described in the Interface description [2]. Configure the standby mode for a specific duration or until the receiver is woken up by an applicable wakeup source as in Table 37.

Wakeup source	Wakeup type	Description
RTC	Internal	The configured duration expires
RXD	PIO	Rising edge on the **RXD** pin
EXTINT	PIO	Rising edge on the **EXTINT** pin
SPI_CS_N	PIO	Rising edge on the **SPI_CS_N** pin

Table 37: Supported wakeup sources

☞ Leave the **V_BCKP** pin open if the hardware backup mode is not used in the design.

3.7 Time

Maintaining receiver local time and keeping it synchronized with GNSS time is essential for proper timing and positioning functionality. This section explains how the receiver maintains local time and introduces the supported GNSS time bases.

3.7.1 Receiver local time

The receiver is dependent on a local oscillator for both the operation of its radio parts and also for timing within its signal processing. No matter what nominal frequency the local oscillator has, u-blox receivers subdivide the oscillator signal to provide a 1-kHz reference clock signal, which is used to drive many of the receiver's processes. In particular, the measurement of satellite signals is arranged to be synchronized with the "ticking" of this 1-kHz clock signal.

When the receiver first starts, it has no information about how these clock ticks relate to other time systems; it can only count time in 1 millisecond steps. However, as the receiver derives information from the satellites it is tracking or from aiding messages, it estimates the time that each 1-kHz clock tick takes in the time base of the chosen GNSS system. This estimate of GNSS time based on the local 1-kHz clock is called receiver local time.

As receiver local time is a mapping of the local 1-kHz reference onto a GNSS time base, it may experience occasional discontinuities, especially when the receiver first starts up and the information it has about the time base is changing. Indeed, after a cold start, the receiver local time initially indicates the length of time that the receiver has been running. However, when the receiver obtains some credible timing information from a satellite or an aiding message, it jumps to an estimate of GNSS time.

3.7.2 GNSS time bases

GNSS receivers must handle a variety of different time bases as each GNSS has its own reference system time. What is more, although each GNSS provides a model for converting their system time into UTC, they all support a slightly different variant of UTC. So, for example, GPS supports a variant of UTC as defined by the US National Observatory, while BeiDou uses UTC from the National Time Service Center (NTSC) of China. While the different UTC variants are normally closely aligned, they can differ by as much as a few hundreds of nanoseconds.

Although u-blox receivers can combine a variety of different GNSS times internally, the user must choose a single source of GNSS time and, separately, a single type of UTC for input (on **EXTINT** pins) and output (via the **TIMEPULSE** pin) and the parameters reported in corresponding messages.

The `CFG-TP-TIMEGRID_TP` configuration item allows the user to choose between any of the supported GNSS (GPS, BeiDou, etc.) time bases and UTC. Also, the `CFG-NAVSPG-UTCSTANDARD` configuration item allows the user to select which variant of UTC the receiver should use. This includes an "automatic" option which causes the receiver to select an appropriate UTC version itself, based on the GNSS configuration, using, in order of preference, USNO if GPS is enabled, NTSC if BeiDou is enabled,

The receiver assumes that an input time pulse uses the same GNSS time base as specified for the time pulse output. Where UTC is selected for time pulse output, any GNSS time pulse input will be assumed to be aligned to GPS time.

☞ The receiver allows users to independently choose GNSS signals used in the receiver (using the `CFG-SIGNAL` configuration group) and the input/output time base (using the `CFG-TP` configuration group). For example it is possible to instruct the receiver to use GPS satellite signals to generate BeiDou time. This practice compromises time pulse accuracy if the receiver cannot measure the timing difference between the constellations directly and is therefore not recommended.

☞ The information that allows GNSS times to be converted to the associated UTC times is only transmitted by the GNSS at relatively infrequent periods. For example GPS transmits UTC(USNO) information only once every 12.5 minutes. Therefore, if a time pulse is configured to use a variant of UTC time, after a cold start, substantial delays before the receiver has sufficient information to start outputting the time pulse can be expected.

Each GNSS has its own time reference for which detailed and reliable information is provided in the messages listed in the table below.

Time reference	Message
GPS time	`UBX-NAV-TIMEGPS`
BeiDou time	`UBX-NAV-TIMEBDS`
Galileo time	`UBX-NAV-TIMEGAL`
QZSS time	`UBX-NAV-TIMEQZSS`
UTC time	`UBX-NAV-TIMEUTC`

Table 38: GNSS time messages

3.7.3 Navigation epochs

Each navigation solution is triggered by the tick of the 1 kHz clock nearest to the desired navigation solution time. This tick is referred to as a navigation epoch. If the navigation solution attempt is successful, one of the results is an accurate measurement of time in the time base of the chosen GNSS system, called GNSS system time. The difference between the calculated GNSS system time and receiver local time is called the clock bias (and the clock drift is the rate at which this bias is changing).

In practice the receiver's local oscillator is not as stable as the atomic clocks to which GNSS systems are referenced and consequently clock bias tends to accumulate. However, when selecting the next navigation epoch, the receiver always tries to use the 1 kHz clock tick which it estimates to be closest to the desired fix period as measured in GNSS system time. Consequently, the number of 1 kHz clock ticks between fixes occasionally varies. This means that when producing one fix per second, there are normally 1000 clock ticks between fixes, but sometimes, to correct drift away from the GNSS system time, there are 999 or 1001 ticks.

The GNSS system time calculated in the navigation solution is always converted to a time in both the GPS and UTC time bases for output.

Clearly when the receiver has chosen to use the GPS time base for its GNSS system time, conversion to GPS time requires no work at all, but conversion to UTC requires knowledge of the number of leap seconds since GPS time started (and other minor correction terms). The relevant GPS-to-UTC conversion parameters are transmitted periodically (every 12.5 minutes) by GPS satellites, but can also be supplied to the receiver via the `UBX-MGA-GPS-UTC` aiding message.

When insufficient information is available for the receiver to perform any of these time base conversions precisely, predefined default offsets are used. Consequently, plausible times are nearly always generated, but they may be wrong by a few seconds (especially shortly after receiver start).

Depending on the configuration of the receiver, such "invalid" times may well be output, but with flags indicating their state (e.g. the "valid" flags in `UBX-NAV-PVT`).

3.7.4 iTOW timestamps

All the main UBX-NAV messages (and some other messages) contain an iTOW field which indicates the GPS time at which the navigation epoch occurred. Messages with the same iTOW value can be assumed to have come from the same navigation solution.

Note that iTOW values may not be valid (i.e. they may have been generated with insufficient conversion data) and therefore it is not recommended to use the iTOW field for any other purpose.

☞ The original designers of GPS chose to express time/date as an integer week number (starting with the first full week in January 1980) and a time of week (often abbreviated to TOW) expressed in seconds. Manipulating time/date in this form is far easier for digital systems than the more conventional year/month/day, hour/minute/second representation. Consequently, most GNSS receivers use this representation internally, only converting to a more conventional form at external interfaces. The iTOW field is the most obvious externally visible consequence of this internal representation.

If reliable absolute time information is required, it is recommended to use the `UBX-NAV-PVT` navigation solution message which also contains additional fields that indicate the validity (and accuracy in `UBX-NAV-PVT`) of the calculated times (see also the GNSS times section below for further messages containing time information).

3.7.5 Time validity

Information about the validity of the time solution is given in the following form:

- **Time validity**: Information about time validity is provided in the `valid` flags (e.g. `validDate` and `validTime` flags in the `UBX-NAV-PVT` message). If these flags are set, the time is known and considered valid for use. These flags are shown in table GNSS times in section GNSS times above as well as in the `UBX-NAV-PVT` message.
- **Time validity confirmation**: Information about confirmed validity is provided in the `confirmedDate` and `confirmedTime` flags in the `UBX-NAV-PVT` message. If these flags are set, the time validity can be confirmed by using an additional independent source, meaning that the probability of the time to be correct is very high. Note that information about time validity confirmation is only available if the `confirmedAvai` bit in the `UBX-NAV-PVT` message is set.

☞ `validDate` means that the receiver has knowledge of the current date. However, it must be noted that this date might be wrong for various reasons. Only when the `confirmedDate` flag is set, the probability of the incorrect date information drops significantly.

☞ `validTime` means that the receiver has knowledge of the current time. However, it must be noted that this time might be wrong for various reasons. Only when the `confirmedTime` flag is set, the probability of incorrect time information drops significantly.

☞ `fullyResolved` means that the UTC time is known without full seconds ambiguity. When deriving UTC time from GNSS time the number of leap seconds must be known. It might take several minutes to obtain such information from the GNSS payload. When the one second ambiguity has not been resolved, the time accuracy is usually in the range of ~20s.

3.7.6 UTC representation

UTC time is used in many NMEA and UBX messages. In NMEA messages, time is always rounded to the nearest hundredth of a second and it is normally reported with two decimal places (e.g.

124923.52). When using NMEA compatibility mode (selected using CFG-NMEA-COMPAT) where the output must have three decimal places, the third digit is always zero since the underlying time is rounded to the nearest hundredth of a second.

UTC time is also reported within some UBX messages, such as UBX-NAV-TIMEUTC and UBX-NAV-PVT. In these messages date and time are separated into seven distinct integer fields. Six of these (year, month, day, hour, min. and sec.) have fairly obvious meanings and are all guaranteed to match the corresponding values in NMEA messages generated by the same navigation epoch. This facilitates simple synchronization between associated UBX and NMEA messages.

The seventh field is called nano and it contains the number of nanoseconds by which the rest of the time and date fields need to be corrected to get the precise time. So, for example, the UTC time 12:49:23.521 would be reported as: hour: 12, min: 49, sec: 23, nano: 521000000.

It is however important to note that the first six fields are the result of rounding to the nearest hundredth of a second. Consequently the nano value can range from -5000000 (i.e. -5 ms) to +994999999 (i.e. nearly 995 ms).

When the nano field is negative, the number of seconds (and maybe minutes, hours, days, months or even years) have been rounded up. Therefore, some or all of them must be adjusted to get the correct time and date. Thus in an extreme example, the UTC time 23:59:59.9993 on 31st December 2011 would be reported as: year: 2012, month: 1, day: 1, hour: 0, min: 0, sec: 0, nano: -700000.

If a resolution of one hundredth of a second is adequate, negative nano values can simply be rounded up to 0 and effectively ignored.

The UBX-NAV-TIMEUTC message gives information about the UTC time reference clock.

The preferred variant of UTC time can be specified using the CFG-NAVSPG-UTCSTANDARD configuration item. The UTC time variant configured must correspond to a GNSS that is currently enabled. Otherwise the reported UTC time is inaccurate.

3.7.7 Leap seconds

Due to the slightly uneven spin rate of the Earth, UTC time gradually moves out of alignment with the mean solar time (that is, the sun no longer appears directly overhead at 0 longitude at midday). Occasionally, a "leap second" is announced to bring UTC back into close alignment with the mean solar time. Usually this means adding an extra second to the last minute of the year, but this can also happen on 30th June. When this happens, UTC clocks are expected to go from 23:59:59 to 23:59:60, and only then on to 00:00:00.

It is also possible to have a negative leap second, in which case there will only be 59 seconds in a minute and 23:59:58 will be followed by 00:00:00.

u-blox receivers are designed to handle leap seconds in their UTC output and consequently applications processing UTC times from either NMEA or UBX messages should be prepared to handle minutes that are either 59 or 61 seconds long.

Leap second information can be polled from the receiver with the message UBX-NAV-TIMELS.

3.7.8 Date ambiguity

Each navigation satellite transmits information about the current date and time in the data message. The time of week (TOW) indicates the elapsed number of seconds since the start of the week (midnight Saturday/Sunday). The week number (WN) indicates the elapsed number of weeks since the particular GNSS system was started. By combining these two values the current date and time can be known. Modern GPS satellites use a 13-bit value for the week number. As GPS system was started in 1980, it allows the week number to represent dates up to year 2137. Unfortunately, at the time when the commonly used GPS L1C/A data message was designed the signal had only 10 bits available for the week number. The top bits of the full week number had to be left out. The 10 bottom bits of the week number are not sufficient to yield a completely unambiguous date as every 1024 weeks (a bit less than 20 years), the transmitted week number value "rolls over" back to zero. Consequently, the information in GPS L1 message does not differentiate between, for example, 1980, 1999, or 2019. GPS L1 receivers must thus use additional methods to calculate the full week number.

Although BeiDou and Galileo have similar representations of time, they still transmit sufficient bits for the week number to be unambiguous for the foreseeable future (the first ambiguity will be in 2078 for Galileo, and not until 2163 for BeiDou). Therefore, the receiver regards the date information transmitted by BeiDou, and Galileo to be unambiguous and, where necessary, uses this information to resolve any ambiguity in the GPS date.

☞ If the receiver is connected to a simulator, note that GPS time is referenced to 6th January 1980, Galileo to 22 August 1999 and BeiDou to 1 January 2006. The receiver doesn't work reliably with signals simulated before these dates.

3.7.8.1 GPS-only date resolution

If only GPS L1C/A signals are available, the receiver establishes the date by assuming that all week numbers must be at least as large as the reference rollover week number. The default value for the reference rollover week number is selected at the compile time of the receiver firmware and is normally set to a value of a few weeks before the software is completed. The value can be overridden by `CFG-NAVSPG-WKNROLLOVER` configuration item.

The following example illustrates how this works:

Assume that the reference rollover week number set in the firmware at compile time is 2148 (which corresponds to a week in calendar year 2021, but is transmitted by the satellites as 100). In this case, if the receiver sees transmissions containing week numbers in the range of 100 ... 1023, they are interpreted as week numbers 2148 ... 3071 (calendar years 2021 ... 2038), whereas transmissions with week numbers from 0 to 99 are interpreted as week numbers 3072 ... 3171 (calendar years 2038 ... 2040).

☞ It is important to set the reference rollover week number correctly when supplying the receiver with simulated signals, especially when the scenarios are in the past.

3.8 Time maintenance

3.8.1 Real-time clock

The receiver contains a real-time clock (RTC). The RTC section is located in the backup domain and can keep time while the receiver is otherwise powered off. When the receiver powers up, it attempts to use the RTC to initialize receiver local time and in most cases this leads to considerably faster and more accurate first fixes.

3.8.2 Time assistance

The host can deliver time assistance to the receiver using `UBX-MGA-INI-TIME_UTC` or `UBX-MGA-INI-TIME_GNSS` for better startup performance.

The current GNSS time can be supplied to the receiver as a coarse value via the standard communication interfaces. This method suffers from communication latency and unpredictable delays so the accuracy of the supplied time is poor. Accuracy of the supplied time can be improved greatly if the host system has a very good sense of the current time and can deliver an exactly timed pulse to the **EXTINT** pin. This pulse informs the receiver when the supplied time assistance data is to be applied.

UTC time leap seconds and GPS-to-UTC conversion parameters are transmitted periodically by GPS satellites, but that happens only every 12.5 minutes. The receiver can normally calculate the correct leap seconds value from other GNSS systems immediately, but in some situations that is not possible. If the leap seconds information or the difference of time between GPS and UTC system is important for the host application, the information can be supplied to the receiver via the `UBX-MGA-GPS-UTC` aiding message.

3.9 Time mark

The receiver can be used to provide an accurate measurement of the time at which a pulse was detected on the external interrupt pin. The reference time can be chosen by setting the time source parameter to UTC, GPS, BeiDou, Galileo, NAVIC or local time in the `CFG-TP` configuration group. The UTC standard can be set in the `CFG-NAVSPG` configuration group. The delay figures defined with `CFG-TP` are also applied to the results output in the `UBX-TIM-TM2` message.

A `UBX-TIM-TM2` message is output at the next epoch if

- The `UBX-TIM-TM2` message is enabled, and
- a rising or falling edge was triggered since last epoch on the **EXTINT** pin.

The `UBX-TIM-TM2` messages includes the time of the last time mark, new rising/falling edge indicator, time source, validity, number of marks and an accuracy estimate.

☞ Only the last rising and falling edge detected between two epochs is reported since the output rate of the `UBX-TIM-TM2` message corresponds to the measurement rate configured with `CFG-RATE-MEAS` (see Figure 11 below).

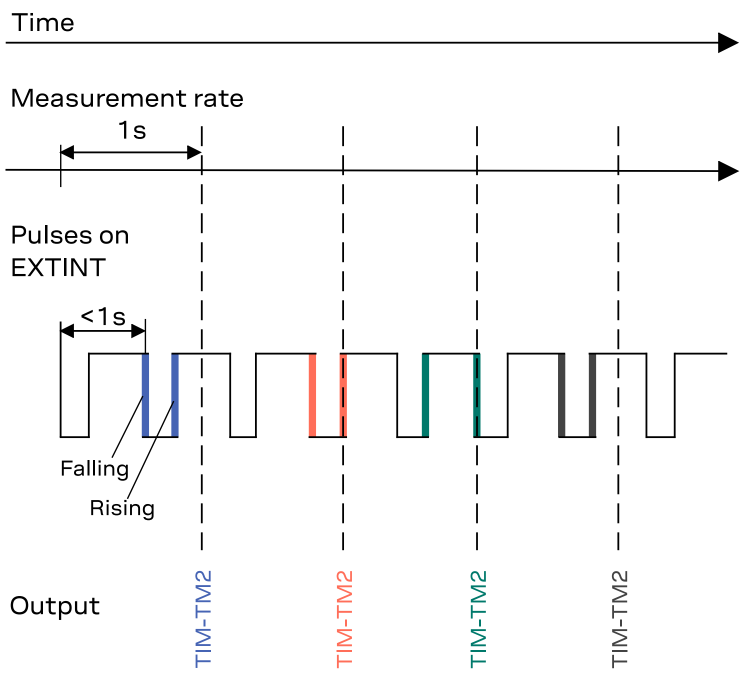


Figure 11: Time mark

3.10 Time pulse

The receiver includes a time pulse feature providing clock pulses with configurable duration and frequency. This function can be configured using the `CFG-TP` configuration group. The `UBX-TIM-TP` message provides time information for the next pulse and the time source. Time pulse signal output is available at Timepulse pin (TIMEPULSE). For more information about the feature and its configuration, see sections Time pulse recommendations and Time pulse configuration.

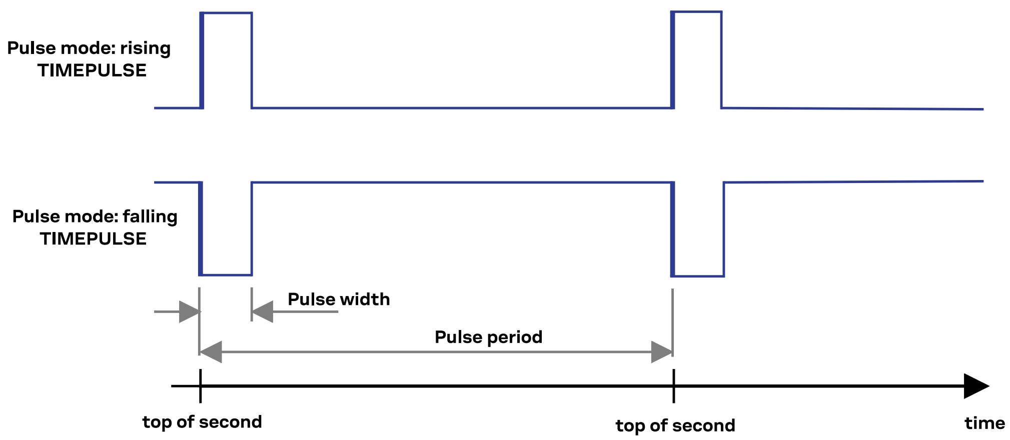


Figure 12: Time pulse

3.10.1 Timepulse pin (TIMEPULSE)

ZED-X20D features one time pulse output at the **TIMEPULSE** pin as described in section pin assignment. The output voltage is fixed with respect to the **VCC** voltage.

3.10.2 Time pulse recommendations

- The time pulse can be aligned to a wide variety of GNSS times or to variants of UTC derived from them. For further information, see GNSS time bases. However, it is strongly recommended that the choice of time base is aligned with the available GNSS signals (for example, to produce GPS time or UTC(USNO), ensure GPS signals are available). This involves coordinating the setting of `CFG-SIGNAL` configuration group with the choice of time pulse time base.
- When using time pulse for precision timing applications it is recommended to calibrate the antenna cable delay against a reference timing source.
- To get the best timing accuracy with the antenna, a fixed and accurate position is needed.
- If relative time accuracy between multiple receivers is required, do not mix receivers of different product families. If this is required, the receivers must be calibrated accordingly, by setting cable delay and user delay.
- The recommended configuration when using the `UBX-TIM-TP` message is to set both the measurement rate (`CFG-RATE-MEAS`) and the time pulse frequency (`CFG-TP`) to 1 Hz.

The sequential order of the signal present at the **TIMEPULSE** pin and the respective output message for the simple case of 1 pulse per second (1PPS) is shown in the following figure.

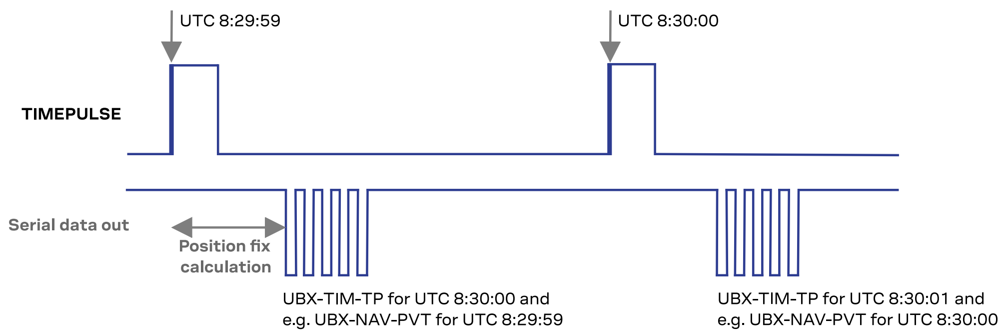


Figure 13: Time pulse and TIM-TP

3.10.3 Time pulse configuration

The time pulse (**TIMEPULSE**) signal has configurable pulse period, length and polarity (rising or falling edge).

It is possible to define different signal behavior (i.e. output frequency and pulse length) depending on whether or not the receiver is locked to reliable time source.

The `CFG-TP` configuration group can be used to change the time pulse settings, and includes the following parameters defining the pulse:

- **time pulse enable** - If this item is set, the time pulse is active.
- **frequency/period type** - Determines whether the time pulse is interpreted as frequency or period.
- **length/ratio type** - Determines whether the time pulse length is interpreted as length [us] or pulse ratio [%].
- **antenna cable delay** - Signal delay due to the cable between the antenna and the receiver.
- **pulse frequency/period** - Frequency or pulse time period when locked mode is not configured or not active.
- **pulse frequency/period lock** - Frequency or pulse time period for locked mode. In use as soon as the receiver has calculated a valid time from a received signal. Only used if the corresponding item is set to use another setting in locked mode.
- **pulse length/ratio** - Length or duty cycle of the generated pulse, specifies either time or ratio for the pulse to be on/off.
- **pulse length/ratio lock** - Length or duty cycle of the generated pulse for locked mode. In use as soon as the receiver has calculated a valid time from a received signal. Only used if the corresponding item is set to use another setting in locked mode.
- **user delay** - The cable delay from the receiver to the user device plus signal delay of any user application.
- **lock to GNSS freq** - If this item is set, uses the frequency gained from the GNSS signal information rather than the local oscillator's frequency.
- **locked other setting** - If this item is set, the alternative setting is used as soon as the receiver can calculate a valid time. This mode can be used, for example, to disable time pulse if the time is not locked, or to indicate a lock with different duty cycles.
- **align to TOW** - If this item is set, pulses are aligned to the top of a second.
- **polarity** - If set, the first edge of the pulse is a rising edge (pulse polarity: rising).
- **grid UTC/GNSS** - Selection between UTC (0), GPS (1), BeiDou (3), (4) Galileo and NAVIC (5) time grid. Also affects the time output by `UBX-TIM-TP` message.

☞ The maximum pulse length cannot exceed the pulse period.

☞ The high and the low period of the output cannot be less than 50 ns, otherwise pulses can be lost.

3.10.4 Time pulse example

The example below shows the 1PPS **TIMEPULSE** signal generated on the time pulse output according to the specific parameters of the `CFG-TP` configuration group:

- `CFG-TP-TP2_ENA` = 1
- `CFG-TP-PERIOD_TP2` = 1,000,000 μs
- `CFG-TP-LEN_TP2` = 100,000 μs
- `CFG-TP-TIMEGRID_TP2` = 1 (GPS)
- `CFG-TP-PULSE_LENGTH_DEF` = 0 (Period)
- `CFG-TP-ALIGN_TO_TOW_TP2` = 1
- `CFG-TP-USE_LOCKED_TP2` = 1
- `CFG-TP-POL_TP2` = 1
- `CFG-TP-PERIOD_LOCK_TP2` = 1,000,000 μs
- `CFG-TP-LEN_LOCK_TP2` = 100,000 μs

The 1 Hz output is maintained whether or not the receiver is locked to GPS time. The alignment to TOW can only be maintained when the GPS time is locked.

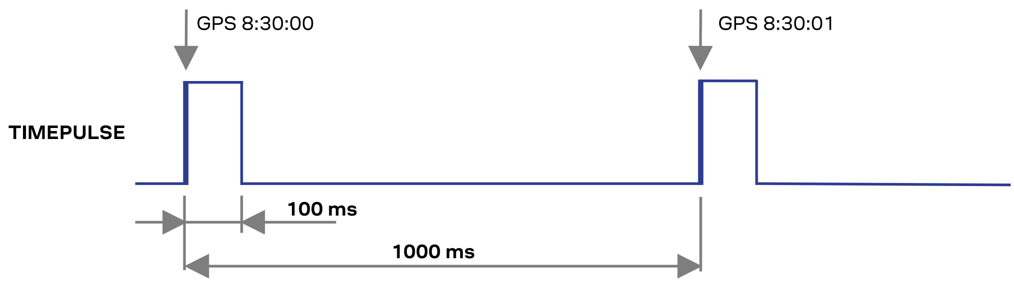


Figure 14: Time pulse signal with the example parameters

3.11 External interrupt

ZED-X20D provides an external interrupt input that can be used for the functions described in Table 39. By default, the functions are disabled. For more details, see section External interrupt pin (EXTINT).

Function	Remarks
Time mark	Use external interrupt to get an accurate measurement of time as discussed in section Time mark.
Wake up signal	Use the external interrupt to wake up the receiver from the software standby mode.

Table 39: External interrupt functions

3.11.1 External interrupt pin (EXTINT)

ZED-X20D provides an external interrupt pin **EXTINT** as described in section pin assignment. For applicable functions, see section External interrupt. The input voltage thresholds are fixed with respect to **VCC**. Leave the external interrupt pin open if unused.

3.12 Security

The security concept of ZED-X20D covers:

- **Over-the-air signal integrity and security** monitors and detects threats such as spoofing and jamming in the communication between the receiver and GNSS satellites, ensuring accurate and reliable data.
- **GNSS receiver integrity and security** protects the receiver from unauthorized firmware and configuration changes, ensuring secure operation and maintaining the integrity of the data.

Some security functions monitor and detect threats and report them to the host system. Other functions mitigate threats and allow the receiver to operate normally.

Table 40 outlines security domains and their threat detection and mitigation functions.

Security domain	u-blox solution
Over-the-air signal integrity and security	Spoofing detection and monitoring Jamming/interference detection and monitoring Compliance with DHS allow list
GNSS receiver integrity and security	Secure boot Secure firmware update Receiver configuration lock

Table 40: u-blox security solutions

3.12.1 Over-the-air signal integrity and security

3.12.1.1 Jamming/interference detection and monitoring

Intentional and/or unintentional jamming of GNSS receivers can degrade the quality of GNSS signals and receiver performance. All u-blox receivers can detect and monitor jamming and report it to the user. The monitoring function is always enabled to inform the user about interference in the GNSS RF bands.

☞ In case of excessive false jamming alerts, the jamming detector sensitivity can be configured with the `CFG-SEC-JAMDET_SENSITIVITY_HI` configuration message.

3.12.1.2 Spoofing detection and monitoring

Spoofing is the process where a counterfeit GNSS signal is transmitted locally to deceive the receiver/user and produce an erroneous position fix and/or time solution. The detection algorithm monitors GNSS signals for implausible changes or inconsistencies. These are evaluated with regards to spoofing.

Spoofing detection is typically successful when a signal transitions from an initially genuine state to a spoofed version. The detection algorithms benefit from having signals from multiple GNSS constellations, enhancing the spoofing detection capabilities. Additionally, depending on the spoofing detection mechanisms implemented in the firmware, it may also be possible to detect spoofing if the receiver starts under spoofing conditions.

3.12.1.3 Messages related to jamming, RF interference, and spoofing

ZED-X20D has the capability to both detect and monitor jamming, RF interference and spoofing and to report it to the user.

The information about jamming, RF interference and spoofing detection are reported in two messages:

- `UBX-SEC-SIG`: signal security status
- `UBX-SEC-SIGLOG`: signal security logfile

For more information, see the Interface description [2].

Signal security status (UBX-SEC-SIG)

The UBX-SEC-SIG message provides information related to the security of the signals, in particular about their integrity. It provides information about the jamming/interference and spoofing detection mechanisms at each navigation epoch, information useful to alert the host about potential jamming/RF interference or spoofing events.

Fields related to jamming and spoofing states in the UBX-SEC-SIG message are described in Table 41.

Message fields	Jamming/spoofing state	Description
jamDetEnabled	0/1	Flag indicates whether jamming, RF interference detection is enabled or not. If 0, it is disabled and if 1, it is enabled.
jamState	0: Unknown	Monitor is not enabled, monitor is uninitialized, or the antenna is disconnected
	1: No jamming indicated	No jamming or RF interference is detected
	2: Warning; jamming indicated	Position OK but jamming or RF interference is visible (above the thresholds)
spfDetEnabled	0/1	Flag indicates whether spoofing detection is enabled or not. If 0, it is disabled and if 1, it is enabled.
spfState / SpoofingState[9]	0: Unknown or deactivated	Monitor is not enabled, monitor is uninitialized, or the antenna is disconnected.
	1: No spoofing indicated	All spoofing detectors are active and report normal behavior.
	2: Spoofing suspected / Spoofing indicated[10]	Spoofing detectors report suspicion of a spoofing attack.
	3: Spoofing detected / Spoofing affirmed[10]	Spoofing detectors confirm the presence of a spoofing

Table 41: Fields related to jamming and spoofing states in the UBX-SEC-SIG message

☞ The spfState value reflects the detector result only for the UBX-SEC-SIGLOG epoch.

Signal security logfile (UBX-SEC-SIGLOG)

The UBX-SEC-SIGLOG message provides a log of past events triggered by jamming/interference or spoofing detection.

Each event consists of a detection type and an event type. The event types indication started and indication stopped form one pair, while indication triggered and indication timeout form another.

The receiver logs up to 16 events and new events take precedence over the past events in the log. Power cycles and restarts of the receiver reset the log, deleting its content.

Fields related to jamming and spoofing detection states in the UBX-SEC-SIGLOG message are described in Table 42.

Message fields	Signal security log state	Description
ttag		Shows the time tag in millisecond.
detectionType		Type of the spoofing or jamming detection:
	0 = simulated signal	Signal from simulator with changed navigation data
	1 = abnormal signal	Not supported
	2 = INS/GNSS mismatch	Not supported

[9] For UBX-SEC-SIG message version 0x03, use the field spfState; for message version 0x02, use spoofingState.

[10] Terms Spoofing suspected and detected are used in message version 0x03, terms spoofing indicated and affirmed are used in message version 0x02.

Message fields	Signal security log state	Description
	3 = abrupt changes in GNSS signal	Abrupt changes in GNSS signal level and time offset
	4 = jamming indicated	Jamming indicated in the GNSS signal environment
	5 = authentication failed	Authentication of GNSS signal failed
	6 = replayed signals	GNSS signals identified as replayed
`eventType`		Type of the event:
	0 = indication started	
	1 = indication stopped	
	2 = indication triggered	
	3 = indication timed-out	

Table 42: Fields related to jamming and spoofing detection states in the `UBX-SEC-SIGLOG` message

☞ Single epoch events, caused by abrupt changes due to switching from the real to the spoofing signal or vice versa are handled as time-out events. This means that the time-out event is reported after a certain cool off period which is not related to any observations in the signal. The other detection types make use of 'start' and 'stop' event types.

3.12.1.4 Compliance with DHS allow list

The GPS allow list is a set of validation checks implemented in the ZED-X20D receiver firmware to ensure the reliability of LNAV navigation data received from the GPS satellites. These checks help improve the receiver's performance by blocking unreliable data from affecting the navigation solution or alerting the user about issues in the navigation message.

The DHS - GPS Receiver Allow List Development Guide provides an example of an allow list and offers guidelines for creating validation rules. To enhance security and reduce vulnerabilities, the ZED-X20D firmware includes a comprehensive set of these checks.

3.12.2 GNSS receiver integrity and security

3.12.2.1 Secure boot

The ZED-X20D boots only with firmware images that are signed by u-blox. This prevents the execution of non-genuine firmware images on the receiver.

3.12.2.2 Secure firmware update

The firmware image is signed by u-blox. The ZED-X20D verifies the signature during the firmware update.

3.12.2.3 Receiver configuration lock

The receiver configuration lock feature ensures that no configuration changes are possible once the feature is enabled. The configuration lock is enabled by setting the configuration item `CFG-SEC-CFG_LOCK` to "true".

The configuration lock can be applied to different configuration layers including the RAM, BBR, and flash memory. At startup, the receiver constructs the configuration database from different configuration layers and maintains it in the run-time RAM memory. When the configuration lock is set in the run-time RAM, the receiver configuration cannot be changed on any configuration layer.

☞ For more information on the configuration layers including the order of priority they are applied in, see the applicable Interface description [2].

The configuration lock set on a configuration layer in volatile memory (RAM, BBR) is removed when the memory is cleared. However, the configuration lock set in non-volatile memory (flash memory) is permanent apart from one exception: during firmware upload to flash memory, the flash is erased during the process causing the configuration lock to be cleared. Refer to Firmware update for more information on firmware update.

To test the lock functionality, set it on the RAM configuration layer. After a power cycle, the information on RAM layer is cleared and the lock is no longer set.

☞ It is recommended to apply the configuration lock on the same layer the configuration is stored.

An example of use case is that the host application locks the receiver configuration. A user communicating with the ZED-X20D through any of the available interfaces can poll, enable or send messages, but cannot change the configuration by sending UBX configuration messages.

3.12.3 Galileo Open Service Navigation Message Authentication (OSNMA)

Open Service Navigation Message Authentication (OSNMA) is a free data authentication service for Galileo Open Service users worldwide. It allows users to confirm that the received Galileo OS navigation data originates from the Galileo system itself and has not been modified. It serves as a strong layer of protection in detecting various spoofing attacks and delayed attacks, also known as meaconing or record-and-replay attacks.

The OSNMA protocol data is transmitted in the previously reserved fields of the Galileo I/NAV message broadcasted on the E1B signal component. As the OSNMA data uses previously reserved fields of the I/NAV message, it is fully backwards compatible. Legacy receivers function with the same performance by simply ignoring the OSNMA fields of I/NAV message.

The ZED-X20D also supports cross-authentication. This means that the receiver can authenticate navigation messages from both the Galileo satellites which transmit and don't transmit the OSNMA protocol data, the receiver utilizes the data retrieved from the satellites transmitting OSNMA data.

3.12.3.1 Cryptographic keys

The cryptographic keys which the OSNMA security relies on, namely the Public Key and the Merkle tree root, are not factory installed. They need to be provisioned securely to the receiver and it is crucial to protect the integrity and authenticity of the these keys.

Public Key:

The Public Key is used to verify the TESLA chain provided within the Digital Signature Message of the OSNMA protocol data. The Public Key is transmitted in the INAV data of the E1B signal every 6 hours for 30 minutes starting at 00:00 GST. Alternatively, the Public Key can be retrieved as an xml file from the GSC web portal. The host system can provide it to the receiver.

Merkle tree root:

The Merkle tree root is used to verify the alert messages and Public Keys transmitted over the signal in space. It is only available as a Merkle tree xml file from the GSC web portal, not as a signal in space.

3.12.3.2 Downloading the OSNMA cryptographic keys

To download the Public Key and Merkle tree root, register at the European GNSS Service Center (GSC) web portal (https://www.gsc-europa.eu). Subscribe to the OSNMA products and after that has been confirmed, download the Public Key and Merkle tree xml files from the GSC PRODUCTS menu.

☞ The interface to the GSC OSNMA Server is specified in the Galileo Open Service Navigation Message Authentication (OSNMA) Internet Data Distribution (IDD) Interface Control Document Galileo OS IDD ICD v.1.1.

3.12.3.3 Sending the OSNMA cryptographic keys to the receiver

See Table 43 for the cryptographic key messages related to the OSNMA feature. For more details, refer to the Interface description [2].

OSNMA Cryptographic keys	Description
`UBX-MGA-GAL-OSNMA_PUBKEY`	To avoid waiting for the Public Key to be transmitted in the signal, it can be sent to the receiver with the `UBX-MGA-GAL-OSNMA_PUBKEY` message. This message requires the corresponding Public Key ID (PKID), the hash function with which the Public Key is hashed (Example: SHA-256 or SHA-512), the actual hexadecimal Public Key point which can be found in the Public Key xml file downloaded from the GSC web portal. Refer to the example below.
`UBX-MGA-GAL-OSNMA_MERKLE`	Use this message to send the OSNMA Merkle tree root to the receiver. This message requires the applicability time of the Merkle tree root (current or future), and the hexadecimal Merkle tree root which can be found in the Merkle tree xml file. The current and future applicability time of the Merkle tree root is used during the Merkle tree renewal process. The future Merkle tree root will be published in the GSC web portal 2 years prior to the renewal.

Table 43: OSNMA cryptographic key messages

☞ The ZED-X20D does not contain factory installed cryptographic keys. It is the user's responsibility to ensure the receiver always has the current valid keys, even after a Public Key and/or Merkle tree renewal event.

☞ The Public Key and Merkle tree root are sent from the host to the receiver over the host communication interface and stored in the non-volatile storage. During this process both keys are unprotected. To protect the keys, the host system must prevent unauthorized access to the system.

3.12.3.4 Storing the cryptographic keys on the receiver

The cryptographic keys sent to the receiver are stored in the non-volatile storage (NVS) on the receiver and they are retained after a power-down event.

If the Public Key stored in the NVS has expired, it is replaced with the one retrieved from the Galileo signal if the Merkle tree root available on the receiver is still valid.

If both the Public Key and the Merkle tree root stored in the NVS have expired, both keys must be updated by the host.

3.12.3.5 Trusted time

To detect delayed attacks, an OSNMA-capable receiver cannot trust on the time decoded from the Galileo satellites. Therefore, the host needs to provide the trusted time. This is compared to the time which the receiver decodes from the Galileo satellites. If the difference between the time decoded from the satellites and the trusted time provided by the host is:

- < 15 sec: OSNMA uses fast MACs (Message Authentication Codes) which is the normal OSNMA operation.
- 15 – 165 sec: OSNMA uses slow MACs. It takes longer to authenticate Galileo navigation data than using fast MACs.
- >= 165 sec: OSNMA will not be performed.

3.12.3.6 Providing trusted time to the receiver

See Table 44 for the messages related to Trusted time. For more details, refer to the Interface description [2].

Trusted time messages	Description
UBX-MGA-INI-TIME_UTC UBX-MGA-INI_TIME_GNSS	These messages can be used to provide trusted time either in UTC or GNSS time, respectively. Both messages allow to provide a trusted flag to the time.

Table 44: Trusted time messages

To protect the integrity of the trusted time provided by the host, it is propagated by the receiver using an internal free-running TCXO. This ensures the trusted time is completely independent from the Galileo satellite data. Due to the imperfections of the TCXO, the propagated trusted time accuracy will degrade over time.

See Table 45 for the items related to Trusted time propagation. For more details, refer to the Interface description [2].

Trusted time propagation	Description
UBX-NAV-TIMETRUSTED	Provides information about the current propagated trusted time accuracy.

Table 45: Trusted time propagation messages

The host system must monitor the propagated trusted time accuracy from the UBX-NAV-TIMETRUSTED message and periodically provide the trusted time to the receiver to maintain the accuracy within 15 seconds to avoid fall back to slow MACs or even losing OSNMA operation altogether.

3.12.3.7 Configuring OSNMA

See Table 46 for the configuration messages related to the OSNMA feature. For more details, refer to the Interface description [2].

OSNMA Configuration	Description
CFG-GAL-USE_OSNMA	Enables the execution of OSNMA.
CFG-GAL-OSNMA_TIMESYNC	Enables trusted time synchronization requirement for the OSNMA. By default, set to true as instructed by the OSNMA Receiver Guidelines.
CFG-NAVSPG-ONLY_AUTHDATA CFG-NAV2-NAVSPG_ONLY_AUTHDATA	When enabled, navigation uses only signals with authenticated navigation data.
CFG-GAL-OSNMA_INAVPRIM	Use authenticated INAV as primary data source over non-authenticated FNAV in E1-E5a configuration.
CFG-GAL-OSNMA_MINTAGLENGTH	The minimum tag length that defines the number of times the data needs to be authenticated before declaring it authenticated.

Table 46: OSNMA configuration messages

3.12.3.8 Verifying OSNMA

See Table 47 for the messages that give information about the status of the OSNMA processing in the receiver. For more details, refer to the Interface description [2].

OSNMA Verification messages	Description
UBX-SEC-OSNMA	Provides information related to the status and execution of the OSNMA protocol. The latest authentication service status and configuration. The total number of satellites transmitting the OSNMA protocol data and the authentication results per satellite are reported periodically. The status of Digital Signature Message authentication. TESLA key authentication. Time synchronization. The difference between the propagated trusted time and the time decoded from the Galileo navigation data.
UBX-NAV-SIG	Includes an additional field to indicate the authentication status of the navigation data used to compute the satellite's position in the current epoch per signal.
UBX-NAV-PVT	Indicates if the PVT fix has been verified with the NMA data. The nmaFixStatus flag is set to 1, indicating the PVT fix has been verified. Indicates if the output time has been validated against the external trusted time source. If the difference between the receiver estimated time and the external trusted time provided by the host is smaller than the threshold configured with the CFG-NAVSPG-MAX_TIMETRUSTED_ACC message, the authTime flag is set to 1, meaning time has been authenticated.
UBX-NAV-TIMEUTC	Indicates if the parameters used to convert GNSS time into UTC time have been authenticated. As the Galileo OSNMA protocol provides the data authentication function only for the I/NAV message of the E1B signal, only UTC(EU) and UTC(USNO) can be authenticated.

Table 47: OSNMA verification messages

3.13 Geofencing

The geofencing feature allows for the configuration of up to four circular areas (geofences) on the Earth's surface. The receiver will then evaluate for each of these areas whether the current position lies within the area or not and signal the state via UBX messaging.

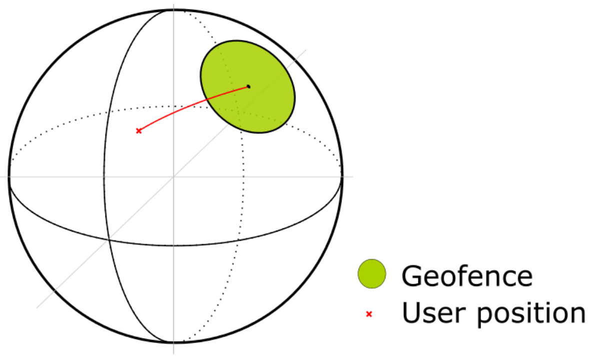


Figure 15: Geofence

3.13.1 Geofence interface

Geofencing can be configured using the CFG-GEOFENCE configuration group. The geofence evaluation is active whenever there is at least one geofence configured.

The current state of each geofence plus the combined state is output in `UBX-NAV-GEOFENCE` with every navigation epoch.

3.13.2 Geofence state evaluation

With every navigation epoch, the receiver evaluates the current solution's position versus the configured geofences.

The position solution uncertainty (standard deviation) is multiplied with the configured confidence sigma level and taken into account when evaluating the geofence state (red circle in Figure 16).

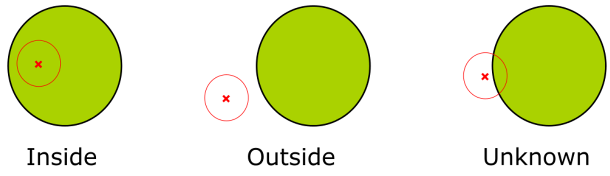


Figure 16: Geofence states

The combined state for all geofences is evaluated as the combination (Union) of all geofences:

- *Inside* - The position lies inside of at least one geofence
- *Outside* - The position lies outside of all geofences
- *Unknown* - All remaining states

3.14 GLONASS Geoblocking

GLONASS Geoblocking is a functionality that restricts the use of GLONASS signals when the receiver's calculated position is inside predefined geographic regions.

The Geoblocking functionality periodically examines the position output and applies the predefined restrictions if the receiver is inside a blocked region. Within the blocked area, the data from GLONASS satellites is not used in PVT calculation and no GLONASS data is presented in the RAW data output. When the receiver moves out of the area where the use GLONASS had been disabled, it restores the use of GLONASS data and operates normally.

The blocked area is predefined as polygons approximating the following area (the boundaries are always inside the area):

- The Russian federation
- Belarus
- North Korea
- Cuba
- Iran
- Sudan
- Ukraine

☞ This functionality is enabled by default in ZED-X20D. To use GLONASS signals globally, reach out to your local u-blox contact for support.

3.15 AssistNow GNSS assistance

GNSS receivers require information on the exact time as well as satellite orbits for several satellites to obtain a position fix. At start-up, the receiver finds the satellite signals and decodes the information from the signals. This typically takes 20–30 s under good signal conditions. Under adverse signal conditions, finding signals and decoding the data may take several minutes or even completely fail.

Assistance data enables the receiver to find satellites faster and even compute the position without the need to download data from satellites. This significantly reduces the time-to-first-fix (TTFF), improves fix accuracy, and increases satellite availability, even under poor signal conditions.

The AssistNow service is a u-blox proprietary assisted GNSS (A-GNSS) service compatible with the u-blox GNSS receivers. The AssistNow Live Orbits and the AssistNow Predicted Orbits services are accessed over the HTTP or HTTPS protocols.

☞ ZED-X20D supports AssistNow Live Orbits only.

3.15.1 Authorization

Using the AssistNow services requires an authorization token from u-blox. For further information on the service and obtaining access to it, see u-blox AssistNow Services page or contact your local technical support representative.

3.15.2 AssistNow Live Orbits

AssistNow Live Orbits is used in GNSS receiver systems with direct internet access. At start-up, the host downloads the satellite ephemerides, time aiding, and other optional data from the service and sends it to the receiver. The assistance data can reduce the TTFF down to 1–2 s under good signal conditions.

For the supported GNSS constellations and signals, refer to the ZED-X20D Data sheet [1].

3.15.3 Live Orbits data types

Fast signal acquisition requires time information as well as satellite and orbital data. Current time is also needed to determine the validity and use other assistance data.

The time assistance message UBX-MGA-INI-TIME_UTC contains the current time and the accuracy for the time provided. Time accuracy is set by default to 10 s to consider the network latency and any processing delay on the host. The ephemerides contain precise short-term satellite and orbital data. The ephemerides are valid approximately 2–4 hours depending on the GNSS system.

Almanac contains a reduced-precision subset of the clock and ephemeris parameters. It is valid for a few weeks and enables the receiver to find the currently visible satellites faster. AssistNow Live Orbits provides also auxiliary information on satellite health status, ionospheric corrections to improve position accuracy, and time information on different GNSS systems.

The total AssistNow Live Orbits data size is approximately 2–4 kB per GNSS constellation. For detailed information on the supported GNSS constellations and satellites, data types, validity period, data size, and the full list of messages, refer to the AssistNow service documentation [4].

Table 48 summarizes the AssistNow Live Orbits assistance data and the related messages.

Type of data	Message(s)	Description
Time assistance (TIME)	UBX-MGA-INI-TIME_UTC	Current time (coarse)
Ephemeris (EPH)[11]	UBX-MGA-XXX-EPH	Current satellite and orbital data for fix calculation
Almanac (ALM)[11]	UBX-MGA-XXX-ALM	Coarse orbital information

11 The string XXX stands for the GNSS constellations GPS, GAL, BDS, GLO, or QZSS. Almanac and auxiliary data are not available for all GNSS constellations.

Type of data	Message(s)	Description
Auxiliary data (AUX)[11]	UBX-MGA-XXX-IONO	Simplified ionospheric corrections (Klobuchar)
	UBX-MGA-XXX-HEALTH	Satellite health information
	UBX-MGA-XXX-UTC	UTC time information
	UBX-MGA-XXX-TIMEOFFSET	Time offset relative to the GPS time

Table 48: AssistNow Live Orbits assistance data

3.15.4 Host operation

The host operation consists of the following steps:

- Start up the receiver
- Download the AssistNow Live Orbits assistance data from the service
- Transfer the Assistance data to the receiver immediately at start-up

The AssistNow C Client Toolkit [4] helps implementing the AssistNow data download and transfer in the host application.

Downloading and storing assistance data

The host downloads the AssistNow Live Orbits assistance data from the service. The received data consists of UBX messages starting with time assistance followed by ephemerides, almanac, and auxiliary data.

The host can store the assistance data in the memory and use it for subsequent receiver start-ups until it expires. In addition, the receiver can maintain the assistance data and other information in its battery-backed RAM (BBR) memory.

Data download from the service is not required if valid assistance data is already available on the host system or on the receiver. However, it is recommended to replace ephemerides close to expiry with fresh data from the service.

For more information on maintaining data on the receiver, refer to the section Preserving AssistNow and operational data during power-off.

Transferring assistance data to the receiver

The assistance data must be sent to the receiver immediately at the receiver start-up. If downloading data from the service, send the messages directly after receiving them in the same order they were received: time assistance followed by ephemerides, almanac, and auxiliary data.

☞ Send the assistance data immediately at the receiver start-up

If valid assistance data stored on the host is used, the host must construct the UBX-MGA-INI-TIME_UTC message with current time and accuracy for it. The time accuracy provided must not be better than the actual accuracy of the host time.

☞ Do not provide too optimistic value for the time accuracy. This may degrade the start-up performance.

The internal time maintained in the receiver is generally significantly more accurate than the assisted time. If the receiver already has time information available, it therefore ignores the time assistance and continues to use its internal time. To force the receiver use the assisted time, clear the real-time-clock (RTC) time in the BBR memory before sending time assistance.

Apart from time assistance, sending new assistance data from the host clears the existing data in the receiver. Valid assistance data is stored in the receiver's BBR memory and used accordingly. However, expired assistance data is rejected resulting in a loss of assistance data.

☞ Do not send ephemerides close to expiring to the receiver. This may degrade the start-up performance.

3.15.5 Preserving AssistNow and operational data during power-off

The receiver stores the assistance data from the host in the navigation database. During operation, the receiver collects satellite broadcast data and updates the database when new data becomes available. Also time and position are continuously updated.

The receiver automatically copies the satellite data to the BBR to maintain it during the receiver power-off. Alternatively, the host can store satellite data on the host side or in the flash memory connected to the receiver.

The following mechanisms can be used instead or in parallel to the AssistNow feature. The maintained assistance data can be used for subsequent receiver start-ups until it expires.

☞ The quality of the assistance data degrades over time resulting in longer TTFF and reduced initial position accuracy. Provide fresh assistance data for best start-up performance.

Maintain BBR and RTC time

The recommended way to preserve satellite and operational data during power-off is to maintain the BBR and RTC time. The satellite data, last position, user configuration, and calibration data are all stored in the BBR. The RTC must be present to maintain an estimate of time. The receiver automatically applies the data at the next startup.

☞ The backup domain must be supplied to maintain BBR and RTC time.

Database dump

The database dump is used to store the receiver's navigation database on the host. Before power-off, the host reads the navigation database by polling the UBX-MGA-DBD message and stores the received UBX-MGA-DBD messages for later use. At the next startup, the host sends time assistance and the UBX-MGA-DBD messages back to the receiver. For more information on the UBX-MGA-DBD message, refer to the Interface description [2].

3.16 Safeboot mode

The safeboot mode can be used to recover from situations where the flash content has become corrupted and needs to be restored. In the safeboot mode, the GNSS operation is disabled. In the safeboot mode, ZED-X20D supports communication over UART1, I2C and SPI.

To enter the safeboot mode and establish communication, do as follows:

1. Enter the safeboot mode by either pulling the **SAFEBOOT_N** pin LOW or sending the `UBX-UPD-SAFE` message to the receiver.
2. If UART1 is used, initialize communication by sending the training sequence `0x55 0x55` as raw bytes only at 9600 baud. Note that the training sequence is not encapsulated in a UBX message.
3. After sending the training sequence, wait for at least 2 ms before sending any further messages to the receiver.

3.16.1 Safeboot pin (SAFEBOOT_N)

ZED-X20D provides the **SAFEBOOT_N** pin as discussed in section pin assignment. To initiate the receiver in the safeboot mode, pull this pin LOW during the power-up.

☞ u-blox recommends designing the application so that the SAFEBOOT_N pin can be pulled LOW either by an externally connected test point or through a host I/O port.

3.17 u-blox protocol feature descriptions

3.17.1 Broadcast navigation data

The receiver collects broadcast navigation data message for each tracked signal and reports it in the `UBX-RXM-SFRBX` message. When enabled, a separate message is generated each time the receiver decodes a complete subframe of data from a tracked signal. The data bits are reported as received, including preambles and error checking bits as appropriate. However, because there is considerable variation in the data structure of the different GNSS signals, the reported data also varies. This document uses the term "subframe", but other GNSS data structures might use different terms. For example Galileo uses the term "pages".

3.17.1.1 Parsing navigation data subframes

Each `UBX-RXM-SFRBX` message contains a subframe of data bits appropriate for the relevant GNSS, delivered in a number of 32-bit words, as indicated by the numWords field.

Due to the variation in data structure between different GNSS, the most important step in parsing the `UBX-RXM-SFRBX` message is to identify the form of the data. Do this by reading the gnssId field, which indicates the GNSS the data was decoded from. In almost all cases, this is sufficient to indicate the structure. Because of this, the following sections are organized by GNSS. However, in some cases the identity of the GNSS is not sufficient, and this is described, where appropriate, in the following sections.

In most cases, the data does not map perfectly into a number of 32-bit words and, consequently, some of the words reported in `UBX-RXM-SFRBX` messages contain fields marked as "Pad". These fields should be ignored and no assumption should be made about their contents.

`UBX-RXM-SFRBX` messages are only generated when complete subframes are detected by the receiver and all appropriate parity checks have passed.

For GNSS signals that require data inversion as part of the parity checking process (for example, GPS L1C/A), the receiver performs this inversion prior to the message output. As a result, users can process the reported data directly and do not need to apply any additional parity processing.

The interpretation of each subframe depends on the transmitting GNSS and is described in the relevant interface control documents (ICD).

3.17.1.2 Navigation data message formats

The following table gives a summary of the different data message formats reported by the `UBX-RXM-SFRBX` message. For more details, refer to corresponding signal ICD documents.

GNSS	Signal	gnssId	sigId	numWords	period	ICD
GPS	L1C/A	0	0	10	6 s	IS-GPS-200N
GPS	L2CL	0	3	10	12 s	IS-GPS-200N
GPS	L2CM	0	4	10	12 s	IS-GPS-200N
GPS	L5 I	0	6	10	6 s	IS-GPS-705J
SBAS	L1C/A	1	0	9	1 s	See SBAS system ICD
Galileo	E1	2	1	8	2 s	Galileo OS SIS ICD v.2.1

GNSS	Signal	gnssId	sigId	numWords	period	ICD
Galileo	E5a	2	3	8	10 s	Galileo OS SIS ICD v.2.1
Galileo	E6	2	8	16	1 s	Galileo OS SIS ICD v.2.1
BeiDou	B1C	3	6	variable (3,3,19)	18 s	BDS-SIS-ICD-B1C-1.0
BeiDou	B1I D1	3	0	10	6 s	Beidou SIS ICD B1I v.3.0
BeiDou	B1I D2	3	1	10	0.6 s	Beidou SIS ICD B1I v.3.0
BeiDou	B2a	3	8	9	3 s	BDS-SIS-ICD-B2a -1.0
BeiDou	B3ID1	3	4	10	6 s	BDS-SIS-ICD-B3I-1.0
BeiDou	B3ID2	3	10	10	0.6 s	BDS-SIS-ICD-B3I-1.0
QZSS	L1C/A	5	0	10	6 s	IS-QZSS-PNT-006
QZSS	L1S	5	1	9	1 s	IS-QZSS-L1S-007
QZSS	L2CM	5	4	10	12 s	IS-QZSS-PNT-006
QZSS	L2CL	5	5	10	12 s	IS-QZSS-PNT-006
QZSS	L5 I	5	8	10	6 s	IS-QZSS-PNT-006
NavIC	L5 A	7	0	10	12 s	ISRO-IRNSS-ICD-SPS-1.1

Table 49: Data message formats reported by `UBX-RXM-SFRBX`

3.18 Firmware update

ZED-X20D is supplied with firmware. u-blox may release updated images containing, for example, security fixes, enhancements, bug fixes, etc. Therefore, it is important to implement a firmware update mechanism in the system design.

The firmware update can be done with any of the following communication interfaces:

- UART1
- I2C
- SPI
- USB

☞ The ZED-X20D firmware update is possible only in the safeboot mode. Enable the safeboot option while initializing the firmware update process (not required if the firmware update is done over the USB interface).

A firmware image is a binary file containing the software to be run by the GNSS receiver. A firmware update is the process of transferring a firmware image to the receiver and storing it in non-volatile flash memory.

Contact u-blox for more information on firmware update.

3.19 Collecting debug log files: design-in guidance

The ability to collect log files with additional UBX protocol messages is essential throughout the ZED-X20D receiver's lifecycle: development, integration, validation, and field support. Enabling and collecting log files makes the integration and troubleshooting faster, more precise, and cost-effective, making it easier to resolve issues promptly, even if they occur in the field.

The additional messages offer deep insight into:

- Signal acquisition, tracking and navigation performance
- Protocol-level communication and interfaces
- Internal status and diagnostic data
- Unexpected behavior

To avoid support delays and ensure robust integration, incorporate log file collection in both the hardware interface design and host software capabilities during the design-in phase.

3.19.1 Checklist for designing debug log file collection

To ensure a successful and reliable integration of UBX message output within your system, follow the steps below. These cover both hardware and host configuration requirements.

Hardware interface

- Ensure at least one GNSS receiver interface is available for UBX message output.
- Provide access to an interface for external connection (for example to PC or data logger).
- Design the interface to handle the bandwidth required for UBX message output.
- Configure a baud rate that supports the expected debug message volume.

Host and configuration

- Enable the host to send UBX configuration strings to activate message output on the correct interface.
- Choose the message set based on the intended use case or guidance from u-blox technical support.
- Set up the host to store or stream the collected log files as needed.

Support and flexibility

- Request message definitions and estimated output payload sizes from u-blox technical support.
- Ensure updates or modifications to the message set are possible without firmware changes.

3.19.2 Hardware interface options for collecting debug log files

The receiver supports UBX message output over all available communication interfaces. When collecting log files, consider the scenarios in Table 50.

Scenario	Hardware design guidance
Logs collected by host	Use a communication interface (e.g. UART) connected to the host processor. The host enables messages and stores the log file locally.
Logs collected by external device	Expose a communication interface via a debug header or test points to allow connection to a PC or external logger.

Table 50: Logging interface options by scenario

Interfaces must be available and accessible at runtime. Messages are explicitly enabled per interface using configuration commands.

Enabling UBX output messages on a specific interface:

By default, the GNSS receiver does not output UBX messages used for in-depth analysis. Select the required messages based on the specific application or follow guidance from u-blox's technical support. Activate the messages on the appropriate interface using configuration messages.

- u-blox technical support provides a tailored set of binary CFG-MSGOUT configuration strings to enable the required messages on the selected interface.
- They also provide an estimated output payload size to help you assess the interface bandwidth requirements.
- These UBX configuration strings are sent to the ZED-X20D either by the host application or an external PC and the messages are output on the selected interface.

3.19.3 Host application and configuration requirements for collecting debug log files

The host must:

- Transmit the provided UBX configuration to the GNSS receiver
- Manage the interface on which the messages are enabled (host-connected or externally exposed)
- Log, buffer or stream the collected messages as required
- Provide a means to enter a debug mode and switch message sets based on a use case or support guidance
- Monitor interface health using UBX-MON-TXBUF to detect potential overflows

Message throughput depends on the message set and GNSS activity. Select appropriate baud rates and buffering strategies to avoid data loss.

3.19.4 Recommended baud rates for logging high-throughput UBX messages

Table 51 shows examples of recommended baud rates for transmitting high-throughput UBX messages at various navigation rates. Selecting the proper baud rate ensures reliable message delivery and helps prevent buffer overflows and data loss during logging.

Example applications	Navigation rate (Hz)	Recommended baud rate (Mbaud)
Full set of debug messages enabled for high precision applications, and raw data.	1 to 10	2
	10 to 20	4
	20 to 25	8

Table 51: Recommended baud rates for high-throughput message transmission based on navigation update rate

☞ Baud rates of 2 Mbaud or higher require host-side support for high-speed UART communication. If the host cannot handle these rates, message loss may occur. Always verify compatibility and monitor the UBX-MON-TXBUF message for buffer overflow warnings.

3.19.5 Recommended message groups by use case

Table 52 presents a preliminary set of a messages which can be enabled for log file collection. These messages can assist technical support during the initial troubleshooting and help refine the list of debug messages to be provided for more detailed analysis.

Use case	Purpose	Typical UBX message groups	Estimated interface load
General debug	OS-level issues, system exceptions	UBX-MON-HW, UBX-MON-COMMS, UBX-MON-SYS, UBX-MON-EXCEPT, UBX-INF	Low
RF / interference	Signal quality, jamming, spoofing analysis	UBX-SEC-SIG, UBX-SEC-SIGLOG, UBX-MON-RF, UBX-MON-SPAN, UBX-NAV-SIG	High

Use case	Purpose	Typical UBX message groups	Estimated interface load
Tracking	Satellite tracking and signal acquisition	UBX-RXM-RAWX, UBX-RXM-MEASX, UBX-RXM-SFRBX	High
Navigation	Standard precision GNSS positioning solution	UBX-NAV-PVT, UBX-NAV-STATUS, UBX-NAV-SIG, UBX-NAV-SAT, UBX-NAV-CLOCK	Medium
High precision	High precision solutions (RTK, PPP, base/rover, heading)	UBX-NAV-RELPOSNED, UBX-RXM-COR, UBX-NAV-SIG	Medium

Table 52: Recommended message groups per use case

☞ Only enable the message sets required for the specific use case. This keeps the system easier to manage and helps avoid unnecessary bandwidth usage. This is especially important in applications with limited buffer space or constrained network capacity. Selective message logging ensures optimal performance and cleaner diagnostic data.

4 Hardware integration

This chapter provides instructions for integrating the receiver into an application design.

4.1 Power supply

ZED-X20D has the following power supply pins: Power supply input (VCC) and Backup supply input (V_BCKP).

A power supply at **VCC** must be present for normal operation. A supply at **V_BCKP** is optional. If present, it enables the hardware backup mode when the **VCC** supply is off. For more information on hardware backup mode, see section Hardware backup mode.

For absolute maximum ratings, operating conditions, and power requirements, refer to the ZED-X20D Data sheet [1].

4.1.1 Power supply input (VCC)

VCC is the main power supply for the receiver. It is recommended to use a low-noise power source with low source impedance. The current drawn into **VCC** varies dynamically during normal operation. To minimize voltage ripple caused by the dynamic current variation, the series resistance on the **VCC** line must not exceed 0.2 Ω.

During start-up, internal capacitors at **VCC** charge resulting in a temporary high inrush current. The external power supply must be able to deliver the specified inrush current. For the power supply requirements, refer to the ZED-X20D Data sheet [1].

ZED-X20D integrates a DC/DC converter at **VCC** reducing the power consumption.

☞ When using a power source with a built-in current limiter, ensure that the current limit is set above the receiver's specified start-up current to avoid limiting the peak current during start-up.

☞ ZED-X20D must be supplied by an external limited power source in compliance with clause 2.5 of the IEC 60950-1 standard.

4.1.2 Backup supply input (V_BCKP)

Power supply at **V_BCKP** is optional and it only supplies the backup domain when the supply at **VCC** is interrupted. It allows the receiver to enter the hardware backup mode by maintaining the real-time clock (RTC) and battery-backed RAM (BBR). Supply the **V_BCKP** independently from the **VCC**.

If the hardware backup mode is not implemented in the design, it is recommended to connect **V_BCKP** to ground. Alternatively, **V_BCKP** can be left open.

Consider the current consumption at **V_BCKP** when supplying it from a power source with a limited capacity, such as a battery. For example, the **V_BCKP** is typically needed for up to 4 hours for maintaining the GNSS satellite ephemeris data for hot starts, and for up to a few days for warm starts. For more information on the current consumption at **V_BCKP**, refer to the Data sheet [1].

4.2 RF interference

The GNSS signal power received at the antenna is very low compared to other wireless communication signals. The received nominal –130 dBm GNSS signal strength makes the GNSS receiver susceptible to interference from many kinds of nearby RF sources.

As an example, cellular applications emit signals with power levels of approximately +30 dBm, while the GNSS signal is less than –130 dBm when reaching the antenna. By simply comparing these numbers, it is obvious that interference issues must be seriously considered during the design phase.

4.2.1 In-band interference

Although the radio communications standards prevent intentional RF signal sources from interfering the GNSS frequencies, many devices emit RF power into the GNSS band at levels much higher than the GNSS signal itself.

One reason is that the frequency band above 1 GHz is not well regulated with regards to EMI, and even if permitted, signal levels are much higher than the GNSS signal power. In particular, all types of digital equipment, such as PCs, digital cameras, LCD screens, etc. tend to emit a broad frequency spectrum up to several GHz of frequency. Also wireless transmitters may generate spurious emissions that fall into the GNSS band.

☞ ZED-X20D provides an integrated spectrum analyzer to detect in-band interference.

4.2.2 Out-of-band interference

Out-of-band interference is caused by signal frequencies that are different from the GNSS carrier frequencies. The main sources are wireless communication systems such as LTE, GSM, CDMA, WCDMA, Wi-Fi, BT, etc.

Typically, these systems may emit their specified maximum transmit power in close proximity to the GNSS receiving antenna, especially if such a system is integrated with the GNSS receiver. Even at reasonable antenna selectivity, destructive power levels may reach the RF input of the GNSS receiver. In addition, larger signal interferers may generate intermodulation products inside the GNSS receiver front-end that fall into the GNSS band and contribute to in-band interference.

Measures against out-of-band interference include maintaining a good grounding concept in the design and adding a GNSS band-pass filter into the receiver's antenna input line. For more information about the RF immunity and the mitigation of out-of-band interference, refer to sections Out-of-band blocking immunity and Interference coupling.

4.2.3 Spectrum analyzer

The ZED-X20D receiver includes an integrated spectrum analyzer. It outputs spectrum data using the `UBX-MON-SPAN` message, which helps identify in-band interference caused by the device environment or design. When visualized, the shape of the spectrum and visible peaks can indicate RF interference. For example, in-band interference appears directly in the spectrum whereas out-of-band interference may also be observed as a reduction in the Programmable Gain Amplifier (PGA) value.

The receiver adjusts the spectrum span based on the enabled GNSS constellations. Since the number of measurement bins is fixed at 256, adjusting the span affects the resolution of the spectrum. For details on frequency calculation and message structure, refer to the Interface description [2].

☞ A peak near the center frequency may originate internally from the receiver. This is normal and does not degrade performance.

4.2.3.1 Spectrum analyzer in u-center 2

u-center 2 visualizes the `UBX-MON-SPAN` message and provides three typical spectrum analyzer functions to support RF front-end design and jammer detection:

- **Hold**: Freezes the current spectrum for comparison with live data.

- **Average**: Displays a smoothed spectrum over time to reduce noise.
- **Max Hold**: Highlights the highest amplitude recorded at each frequency to detect persistent interference.

Figure 17 shows the `UBX-MON-SPAN` spectrum view in u-center 2 with hold, average, and max hold options enabled. Next to the chart, u-center 2 displays the center frequency, span, resolution, and PGA value. The vertical axis shows power levels in dB, helping to identify interference by comparing peaks to the noise floor. Vertical dashed lines indicate frequency offsets from the center in MHz, useful for estimating spurious emissions.

Figure 17: Spectrum analyzer view in u-center 2

4.3 RF front-end

GNSS receivers operate with very low signal levels, ranging from –130 dBm to approximately –167 dBm. This alone is a challenge for the GNSS application design. Out-of-band sources of interference such as GSM, CDMA, WCDMA, LTE, Wi-Fi, or Bluetooth wireless systems with a much higher signal level require additional specific measures. The goal of the RF front-end design is to receive the in-band signal with minimum loss and added noise while suppressing the out-of-band interference.

Refer to the Block diagram for an overview of the RF front-end.

4.3.1 Internal LNA modes

In addition to the integrated PGA gains in the RF front-end circuitry, ZED-X20D provides three independently configurable internal LNAs, one in each RF path. These configurable LNAs have two operating modes: normal gain and low gain as shown in Table 53.

Ensure the external gain is within the recommendations to provide the integrated PGAs with a sufficient dynamic range in all conditions. Exceeding the maximum external gain degrades the receiver's performance.

Internal LNA mode	Minimum external gain	Maximum external gain
Normal gain (default)	17 dB	40 dB
Low gain	20 dB	50 dB

Table 53: Overview of the internal LNA modes

☞ The external gain ratings listed in Table 53 for different internal LNA modes are not applicable for L-band.

4.3.2 Out-of-band blocking immunity

Out-of-band RF interference may degrade the quality and availability of the navigation solution. Out-of-band immunity limit describes the maximum power allowed at the receiver RF input with no degradation in performance.

Minor violation of the immunity limit may reduce C/N0 of the received signals but does not necessarily affect the overall receiver performance. However, a significant violation may reduce receiver sensitivity or cause a complete loss of signal reception. The severity of the interference depends on the repetition rate, frequency, signal level, modulation, and bandwidth of the signal.

Figure 18 and Figure 19 shows a typical out-of-band immunity level for the two internal LNA modes for the ZED-X20D RF input. The measurement was done at room temperature using a test signal with 64QAM modulation and 10 MHz bandwidth similar to an LTE signal.

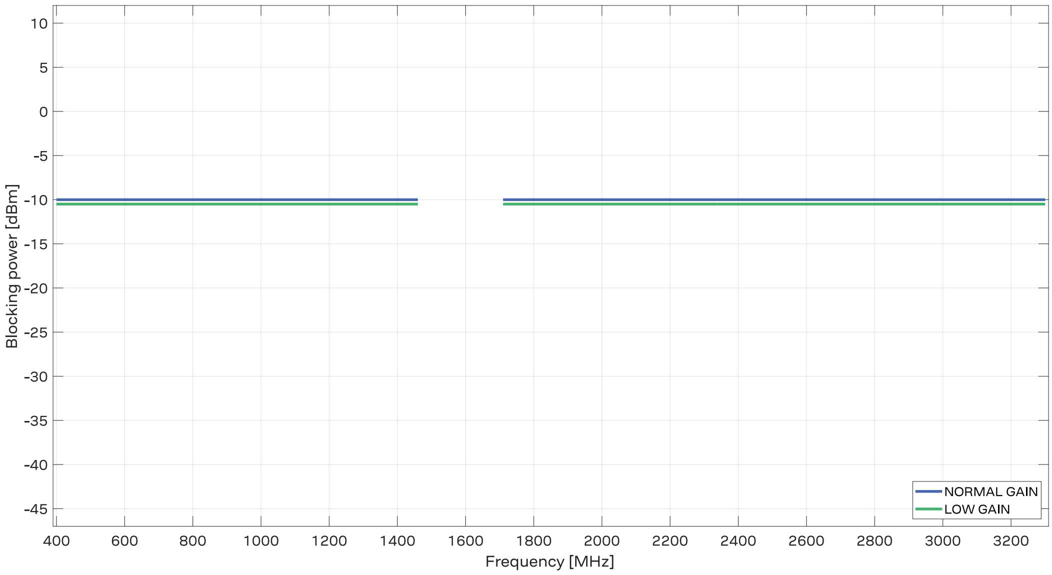


Figure 18: ZED-X20D out-of-band immunity level for L1 RF input at 400–1460 MHz and 1710–3300 MHz for normal gain and low gain

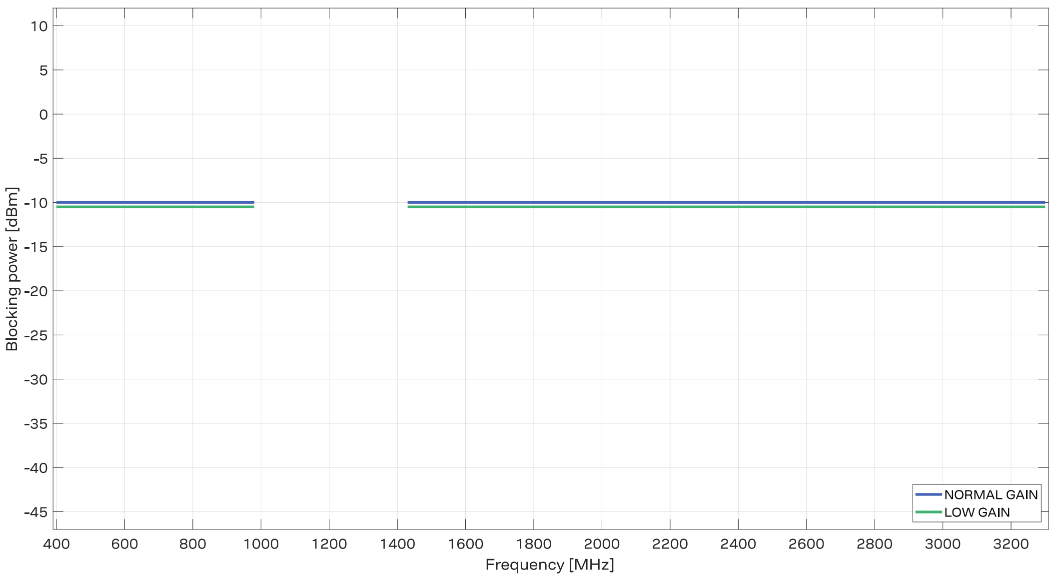


Figure 19: ZED-X20D out-of-band immunity level for L2 and L5 RF input at 400–980 MHz and 1430–3300 MHz for normal gain and low gain

☞ If the out-of-band immunity limit is exceeded, it is recommended to verify that the receiver performance is not affected or is at an acceptable level in the presence of interference.

4.3.3 Interference coupling

RF interference is typically first coupled into the antenna and subsequently conducted into the receiver input. Typical out-of-band interference sources include transmitting antennas of other radio systems. Estimation of the RF interference level coupled into the receiver antenna is a starting point for RF front-end design.

For designs with other radio systems, the maximum power coupled into the antenna can be estimated from the maximum transmission power and the isolation between the antennas. Practical values for antenna isolation can range from 15–20 dB down to 6–10 dB for very small devices. RF interference may also couple from external sources such as nearby mobile devices or base stations.

☞ A simplified test board can be used to estimate the isolation between two antennas. The size of the board and the placement of the antennas must match the final design. Connect the RF cables to the antenna inputs and measure S21 over the frequency band of interest with a vector network analyzer (VNA).

The required out-of-band rejection or isolation is the difference of the maximum power coupled into the antenna input terminal and the immunity level of the receiver RF input. The required isolation is realized with appropriate filtering, typically with one or two SAW filters. Amplification on the RF path reduces the out-of-band rejection and needs to be considered in filter selection. The type and number of filters are selected based on the estimated interference level and the immunity of the receiver.

An active antenna or an external LNA in the design must be protected from excessive RF power to avoid driving the internal LNA into compression.

The second harmonics of the LTE uplink bands 13 (777–787 MHz) and 14 (788–798 MHz) fall in the frequency ranges of 1554–1574 MHz and 1576–1596 MHz respectively, and overlap with the L1/E1/B1I GNSS bands. If the design is impacted by interference from LTE uplink bands 13 or 14, implement an additional narrow-band notch filter at the 777–798 MHz frequency range to attenuate the signal at the input of the external LNA or active antenna. This filter helps to prevent the generation of harmonic multiples falling in-band.

It is more difficult to estimate RF interference from other parts of the design. One option is to measure the interference level at the receiver input using a spectrum analyzer. Interference within the design is primarily a problem at the receiver in-band, where it cannot be addressed by filtering on the RF path. Outside the GNSS band, the required filtering is determined by the estimated interference level and the immunity of the receiver.

The maximum power coupled into the receiver RF input is compared against the immunity limit of the receiver defined in Out-of-band blocking immunity.

4.4 Antennas

The ZED-X20D heading module requires two all-band active antennas (one for each RF input port), each with an integrated Low Noise Amplifier (LNA) to ensure good performance under nominal signal reception.

When implementing a custom antenna installation, it is recommended to use an OEM active antenna module to meet the specification in Table 54. Implementing a custom active antenna design is an important exercise to meet the required bandwidths and group delay specifications compared to L1-only designs.

Figure 20 with information from u-blox ANN-MB2 active antenna provides an example of a typical all-band antenna design.

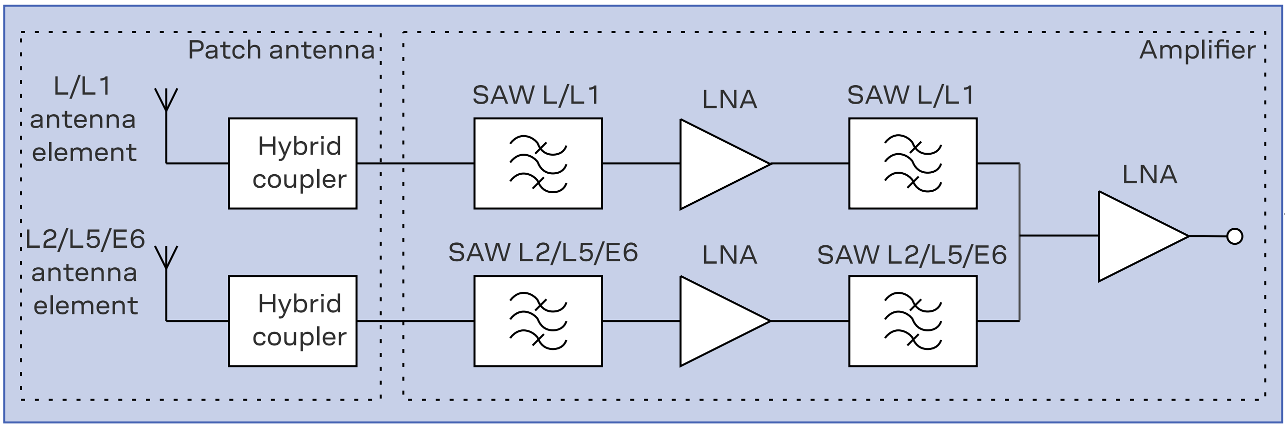


Figure 20: Internal structure of u-blox cost-efficent, high performance GNSS antenna

☞ A suitable ground plane is required for the antenna to achieve good performance.

☞ Location of the antenna is critical to reach the stated performance. Unsuitable locations within a vehicle could include, under vehicle dash, rear-view mirror location, etc.

Parameter	Specification	Rating	Units
Active antenna recommendations	Minimum gain[12]	17	dB
	Maximum gain[12]	50	dB
	Noise figure	<3.5	dB
Group delay variation in-band[13]		<10 typ.	ns
Out-of-band rejection		40 typ.	dB
Antenna element specification[14]	L-band antenna gain L1/L2/L5/E6 band antenna gain	4 typ. 3 typ.	dBic dBic
	L/L1 band (1535–1602 MHz) axial ratio at zenith	2 max	dB
	L5/L2/B3/E6 band (1166–1285 MHz) axial ratio at zenith	2.9 max	dB
	Polarization	RHCP	
	Phase center variation in all directions	<10	mm
EMI immunity out-of-band[15]		30	V/m
ESD circuit protection	Human body model air discharge	15	kV

Table 54: Antenna specifications for ZED-X20D modules

The antenna system should include filtering to ensure adequate protection from nearby transmitters. Take care in the selection of antennas placed close to cellular or Wi-Fi transmitting antennas.

☞ ZED-X20D provides three independently configurable internal LNAs, one for each RF block.

4.4.1 Active antenna power supply

The antenna power supply is typically used to power GNSS active antennas. To ensure optimal performance of ZED-X20D, make sure the power supply can provide the correct voltage and current to the antenna.

12 Including passive losses (filters, cables, connectors etc.)
13 GNSS system bandwidths: L,B1I,L1,E1,B1C 1535–1602 MHz; L2C 1223–1231 MHz; L5,E5a,E6,B2a,B3I 1166–1285 MHz
14 Measured with a ground plane d=120 mm
15 Exception GNSS system band +/- 200 MHz, emphasis on cellular bands

To power and limit the current to the antenna, you have the following options:

- External power supply
- External power supply and current limiting

Figure 21 shows the Z impedance of the antenna bias L4 inductor. This inductor is found in all the reference circuits mentioned in External power supply and External power supply and current limiting. It is important for the Z impedance to be greater than 500 Ω within the 1–1.8 GHz frequency range. This impedance ensures efficient blocking of RF signals from reaching the power supply.

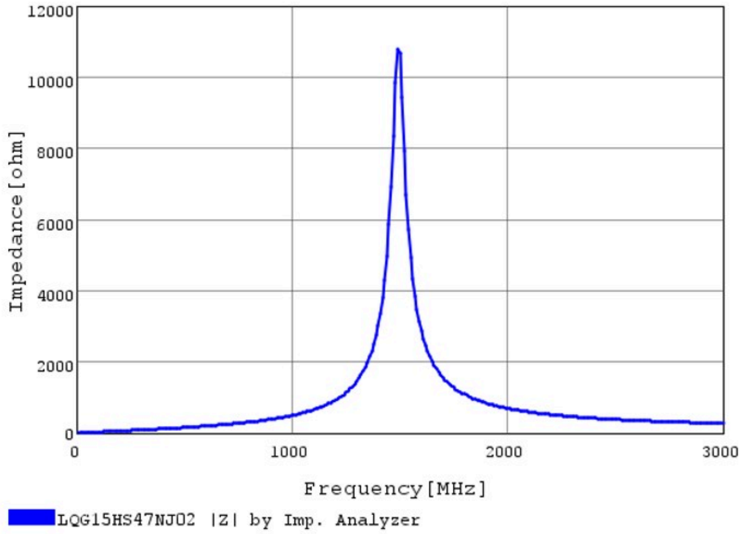


Figure 21: ZED-X20D antenna bias inductor impedance

In most cases, both active antennas can be powered from a shared low-noise main antenna supply rail, provided the supply is rated for the combined maximum current with suitable design margin for both antennas. Each antenna's bias branch should still remain independent, including the required filtering, current limiting, protection, and RF bias circuitry.

Consider separate main antenna supplies, **V_ANT_1** and **V_ANT_2**, when:

- The two antennas require different supply voltages.
- Each antenna requires independent enable/disable control.
- Each antenna requires separate current measurement, diagnostics, or supervision.
- A fault or short circuit on one antenna supply path must have minimal impact on the other antenna.

If both antennas are identical and the shared supply rail is clean and correctly dimensioned, a common upstream supply is usually sufficient. In all cases, the antenna bias and protection circuits should remain separated per RF input path.

4.4.2 External power supply

Figure 22 shows an example with external filtered supplies **V_ANT_1** and **V_ANT_2**. Consider the power dissipation in both the resistor and inductor based on the supply voltage and short circuit current. Calculate the current capacity of the bias-T inductor and the value of the bias resistor. Include the supply voltage and its current capacity for the bias-T in the calculation.

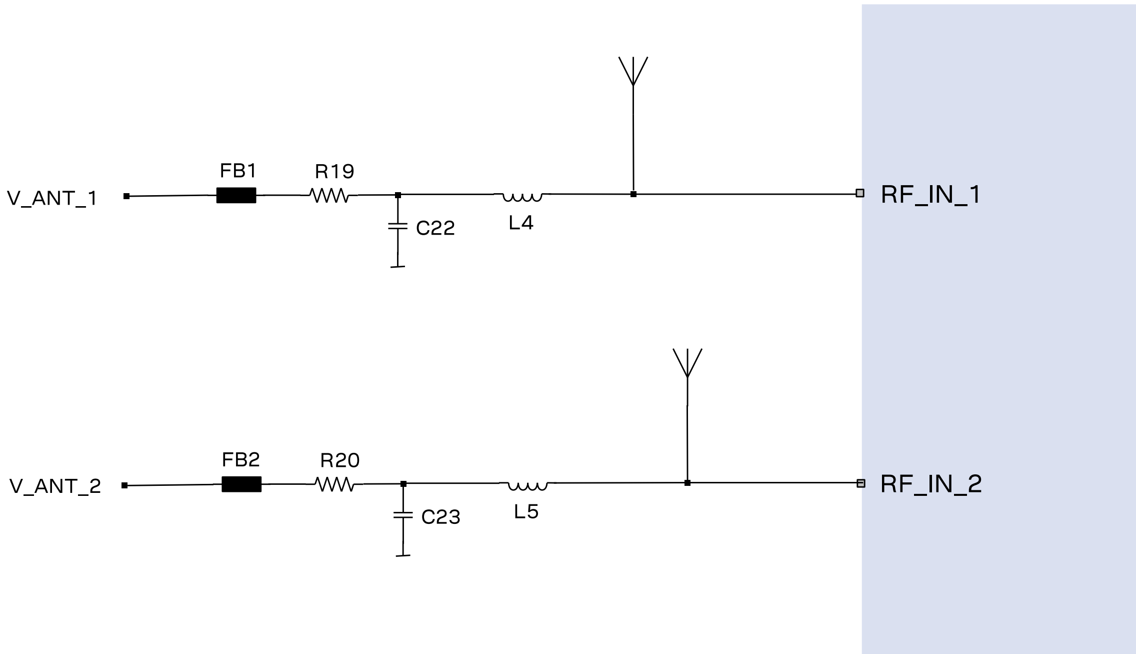


Figure 22: An external voltage antenna bias circuit used for ZED-X20D receiver RF inputs

Part	Specifications	Values
C22, C23	Filtering capacitor	100 nF, 16 V
FB1, FB2	Ferrite bead	BLM15HB121SH1
L4, L5	Minimum Current of 300 mA or more impedance >500 Ω at GNSS frequencies	LQG15HS47NJ02
R19, R20	Current limit resistor	10 Ω

Table 55: ZED-X20D external voltage antenna bias components

4.4.3 External power supply and current limiting

Figure 23 shows an example with external filtered supplies **V_ANT_1** and **V_ANT_2**. In this example, the current limiting threshold is set at 60 mA and the use of ferrite bead is recommended.

☞ Note that each active antenna typically draws 5–20 mA current, contributing to the overall power consumption of the system.

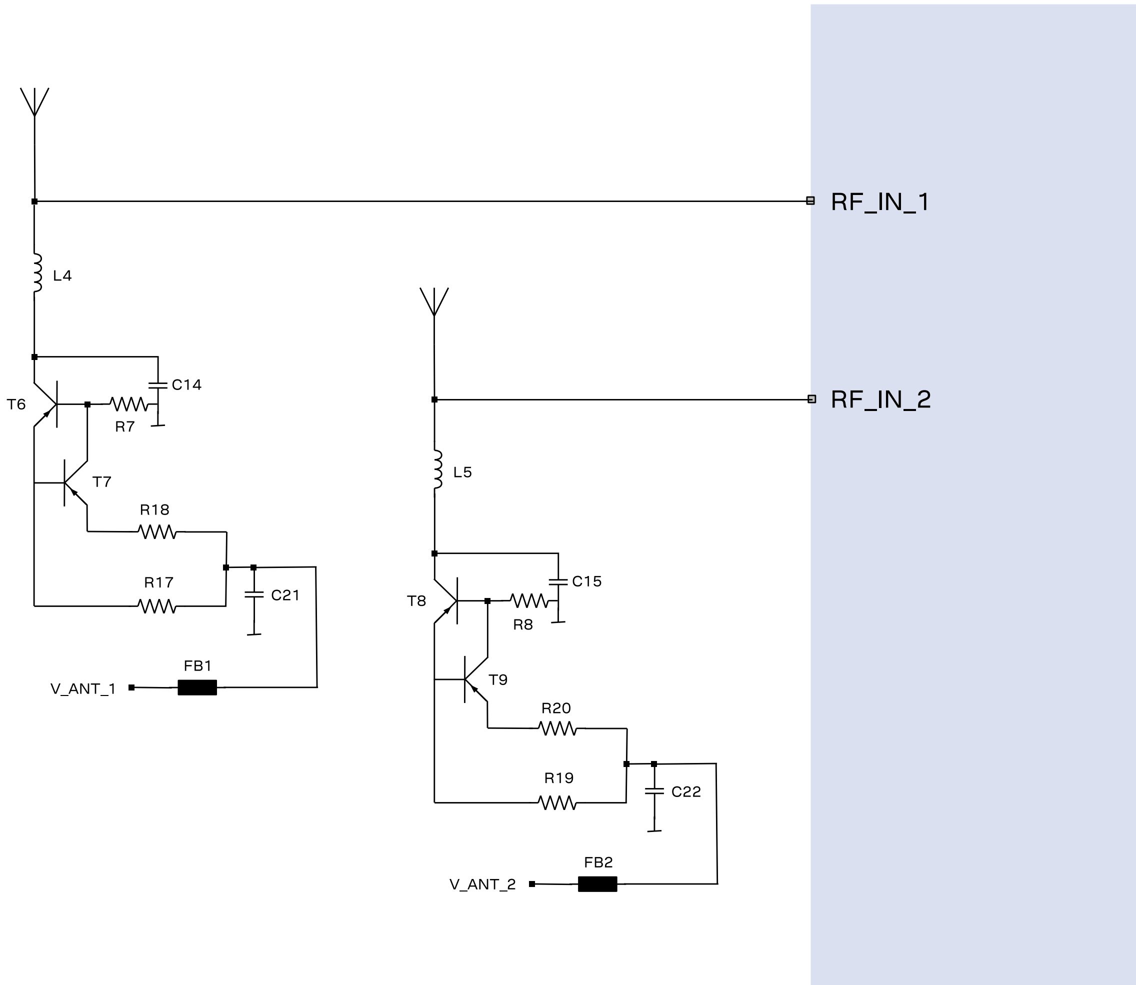


Figure 23: An external voltage antenna bias and current limit circuit for ZED-X20D receiver RF inputs

Part	Specifications	Values
C14, C15	Filtering capacitor	10n, Bias-T, X7R 10N 10% 16 V
C21, C22	Filtering capacitor	100 nF, 16 V
FB1, FB2	Ferrite bead	BLM15HB121SH1
L4, L5	Minimum Current of 300 mA or more impedance >500 Ω at GNSS frequencies	LQG15HS47NJ02
R7, R8	Passive pull-up to control T6	PNP off 2.2 kΩ
R18, R20	Defines the threshold of the comparator	220 Ω
R17, R19	Defines the threshold of the comparator	10 Ω
T6, T7, T8, T9	BJT PNP transistors	PNP

Table 56: ZED-X20D antenna bias components

4.4.4 Antenna selection and placement

The ZED-X20D receiver outputs both position and heading data. The selection and placement of antennas is important for both.

The antenna type, ground plane characteristics, and installation environment affect the GNSS accuracy and RTK performance. Table 57 summarizes the key antenna selection and placement requirements and their impact on the positioning and heading performance.

Topic	Description
Selection	• For optimal performance in dual-antenna designs, use identical antennas. • For a detailed antenna parameter specification, see Table 54.
Placement	• Place the antennas on an identical ground plane (size and shape). • Place the antennas on the same plane and with the same orientation as illustrated in Figure 24.
Ground plane	• A minimum ground plane size and uniform shape is required. • A non-uniform ground plane shape as in Figure 25 could distort the antenna phase center offset and create a position error. • The shorter the distance between the two antennas is, the more critical the ground plane becomes. • If a helical antenna is used, a ground plane is not required.
Distance between antennas	• The longer the distance is between the two antennas, the better the heading performance is. • For an illustration of the theoretical relationship between baseline length and heading accuracy, refer to the ZED-X20D Data sheet [1].
Multipath and obscuration	• Any surrounding structures may obscure the satellites and/or cause multipath that may lead to position errors. • Therefore, it is recommended to place GNSS antennas above any structures that may cause such issues.

Table 57: Antenna selection and placement recommendations

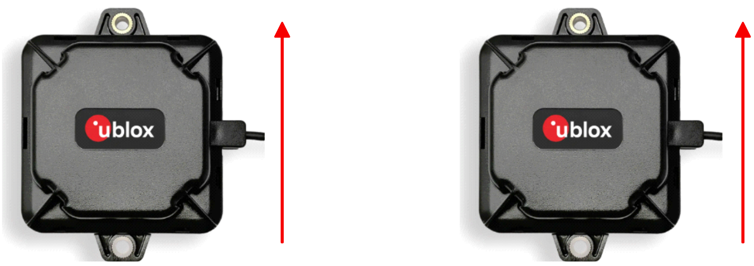


Figure 24: An example of an antenna placement with the same orientation

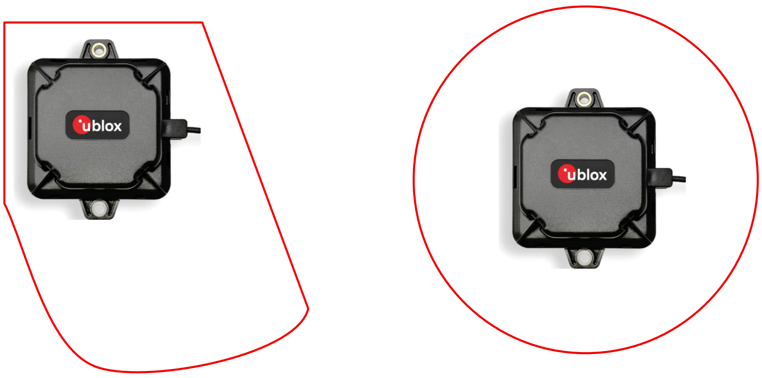


Figure 25: Non-uniform ground plane shape will offset the phase center (left). Uniform circular ground plane provides best accuracy and performance (right)

4.5 USB circuit

The USB interface is described in the section USB. Figure 26 shows the reference circuit for a self-powered USB device. Table 58 lists the components used in the reference.

Supply the **V_USB** from a 3.3 V LDO (U9, C21, C22) using the V_BUS from the USB host as the LDO input voltage. Derive the LDO enable signal from the receiver **VCC** supply. Add a pull-down resistor (R29) to ensure **V_USB** is pulled low when the LDO is unpowered or disabled.

Place the matching resistances (R13, R14) on the **USB_DP** and **USB_DM** signal lines. Include appropriate ESD protection (D1) on the USB interface.

☞ If the USB interface is not used in the design, connect the **V_USB** to ground and leave the data lines unconnected.

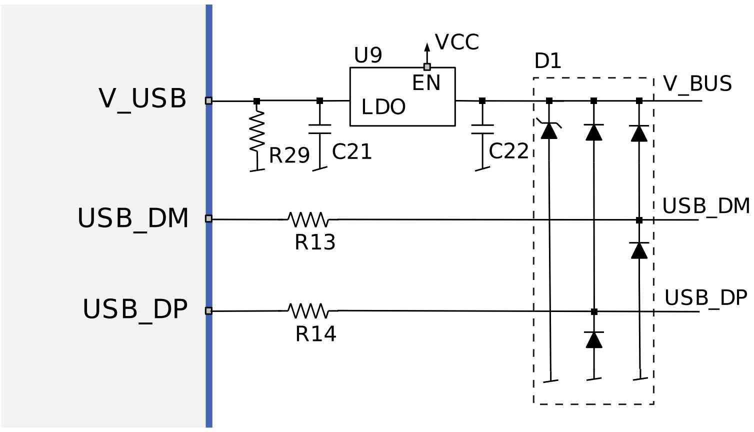


Figure 26: Reference circuit for the USB interface

Parameter	Specification	Type/value
U9	3.3 V LDO	
C21, C22	LDO decoupling capacitors for the USB power supply	1µF, 20%, 10V, X6S. Select values according to the LDO specifications.
R29	V_USB supply pull-down resistor	100 kΩ, 5%, 0.1 W
R13, R14	USB line termination resistor	27 Ω, 5%, 0.1 W
D1	ESD protection	Low-capacitance ESD protection diode

Table 58: USB reference circuit components

4.6 I2C design recommendations

The I2C communication bus is based on open-drain/open-collector ICs. Pull-up resistors must be connected from the I2C lines to the supply rails to pull the line high when it's not driven low by the open-drain interface.

The u-blox chip integrates internal pull-up resistors at the **SCL** and **SDA** pins. These resistors have a large value variation (chip to chip, over temperature, voltage), see product Data sheet [1]. To minimize timing variations, it is suggested adding external pull-up resistors with lower resistance at the **SCL** and **SDA** pins in parallel to the internal ones.

4.6.1 I2C pull up calculation

According to the I2C specification, the electrical input reference levels are set as 30% and 70% of the amplitude as illustrated in Figure 27. The rise time of the **SCL/SDA** lines is given by the pull-up resistors and the total bus capacitance.

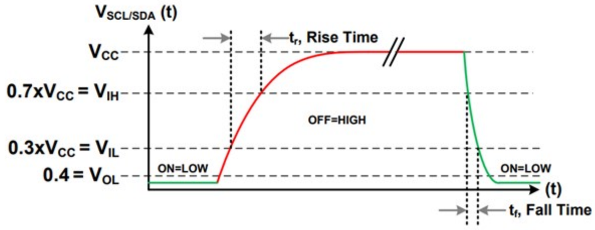


Figure 27: I2C bus signal rise and fall time

The minimum pull up $R_{p(min)}$ resistance is based on the bus voltage (V_{CC}), the maximum voltage that can be read as a logic-low (V_{OL}), and the maximum current that the pins can sink when at or below V_{OL} (I_{OL}).

$R_{p(min)} = (V_{CC} - V_{OL}) / I_{OL}$

The maximum pull-up resistance is based on the maximum rise-time (t_r) requirement (dependent on the I2C clock frequency) and the total capacitance (C_b) on the bus.

$R_{p(max)} = t_r / (0.8473 * C_b)$

Example:

For Fast-mode (400 kHz) I2C communication with t_r = 300 ns, bus voltage V_{CC} = 3.3 V, V_{OL} = 0.4 V, I_{OL} = 2 mA and assuming a total bus capacitance (input pad, line trace, filtering etc.) of max 100 pF (the I2C specification lists the maximum total bus capacitance with a pull-up resistor to be 200 pF):

$R_{p(min)} \approx 1.5\ k\Omega$ and $R_{p(max)} \approx 3.5\ k\Omega$

For an internal chip pull-up value between 8 kΩ to 40 kΩ, adding an external pull-up resistor of 3 kΩ between the **SCL/SDA** lines and the IO supply rail results in a total pull-up resistance in the range of 2.18 kΩ (3 kΩ||8 kΩ) to 2.79 kΩ (3 kΩ||40 kΩ).

4.6.2 EMI/EMC considerations for I2C bus

To minimize potential radiated emissions from the I2C lines near GNSS frequencies and address possible I2C timing issues, add filtering capacitors (typically 68 pF) to ground at the **SCL** and **SDA** pins or ensure placeholders for the capacitors are provided.

Route the I2C traces away from the PCB edges and connectors to further reduce radiated emissions.

4.7 Layout

This section details layout and placement requirements of the ZED-X20D high precision receiver.

4.7.1 Placement

GNSS signals at the surface of the Earth are below the thermal noise floor. A very important factor in achieving maximum GNSS performance is the placement of the receiver on the PCB. The placement used may affect RF signal loss from antenna to receiver input and enable interference into the sensitive parts of the receiver chain, including the antenna itself. When defining a GNSS receiver layout, the placement of the antenna with respect to the receiver, as well as grounding, shielding and interference from other digital devices are crucial issues and need to be considered very carefully.

Signal loss on the RF connection from antenna to receiver input must be minimized as much as possible. Hence, the connection to the antenna must be kept as short as possible.

Ensure that RF critical circuits are clearly separated from any other digital circuits on the system board. To achieve this, position digital part of the receiver close to the digital section of the system PCB and place the RF section and antenna as far away from the other digital circuits on the board as possible.

A proper GND concept shall be followed: the RF section shall not be subject to noisy digital supply currents running through its GND plane.

4.7.2 Thermal and mechanical considerations

Temperature-sensitive components, such as TCXOs and crystals, are highly susceptible to sudden changes in ambient temperature, which can negatively impact the GNSS signal tracking. Additionally, mechanical stress and vibration can further degrade performance. For best practices on thermal and mechanical design to enhance GNSS stability and accuracy, and ensure reliable performance in challenging conditions, refer to Table 59.

Topic	Description and design practices
Minimize temperature gradients	Avoid placing the receiver circuitry in the proximity of cooling fans or heat-emitting components, such as power devices. Shield the temperature-sensitive components to reduce air convection and improve thermal stability.
Thermal conduction via the PCB	Use a continuous ground (GND) plane to facilitate uniform heat dissipation and maintain thermal stability. Connect the receiver's ground to the common ground using an inner PCB layer to enhance heat distribution.
External vibration and mechanical stress	Position the receiver circuitry away from sources of vibration. Avoid mechanical stress that could affect TCXO or crystal stability. If necessary, use additional mechanical support points near the receiver or thicken the PCB.

Table 59: Thermal and mechanical considerations

4.7.3 Package footprint, copper and paste mask

This section provides recommendations for copper and solder mask dimensioning for the ZED-X20D module packages.

☞ These are recommendations only and not specifications. The exact copper, solder and paste mask geometries, distances, stencil thickness and solder paste volumes must be adapted to the specific production processes (e.g. soldering etc.).

⚠ PIN 1 indicator is the ground opening, do not route any signal below this pad.

Refer to the applicable Data sheet [1] for the mechanical dimensions.

4.7.3.1 Footprint

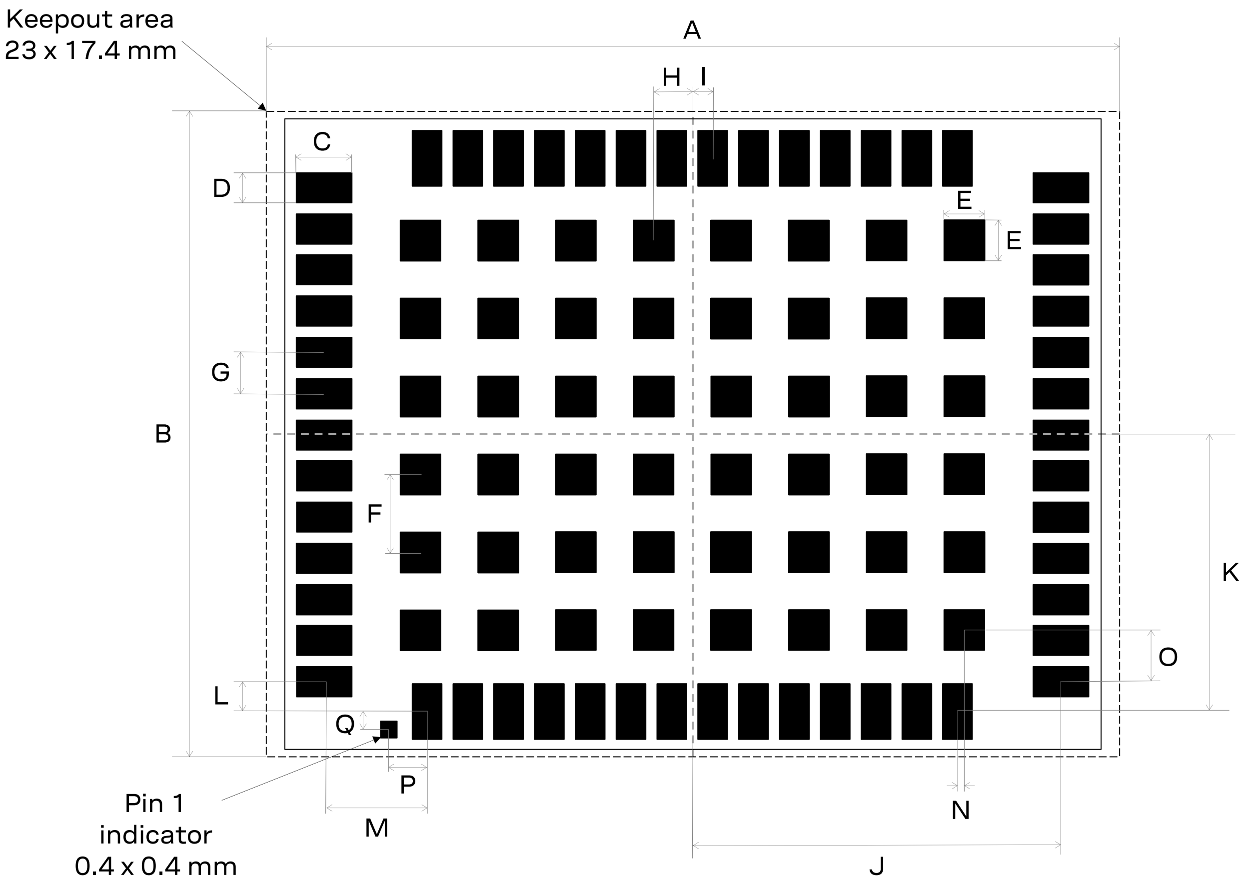


Figure 28: ZED-X20D suggested footprint (i.e. copper mask)

Symbol	Dimension (mm)
A	23.00
B	17.40
C	1.50
D	0.80
E	1.10
F	2.10
G	1.10
H	1.05
I	0.55
J	9.95
K	7.45
L	0.85
M	2.80
N	0.20
O	1.35
P	1.00
Q	0.50

Table 60: ZED-X20D footprint dimensions

4.7.3.2 Paste mask

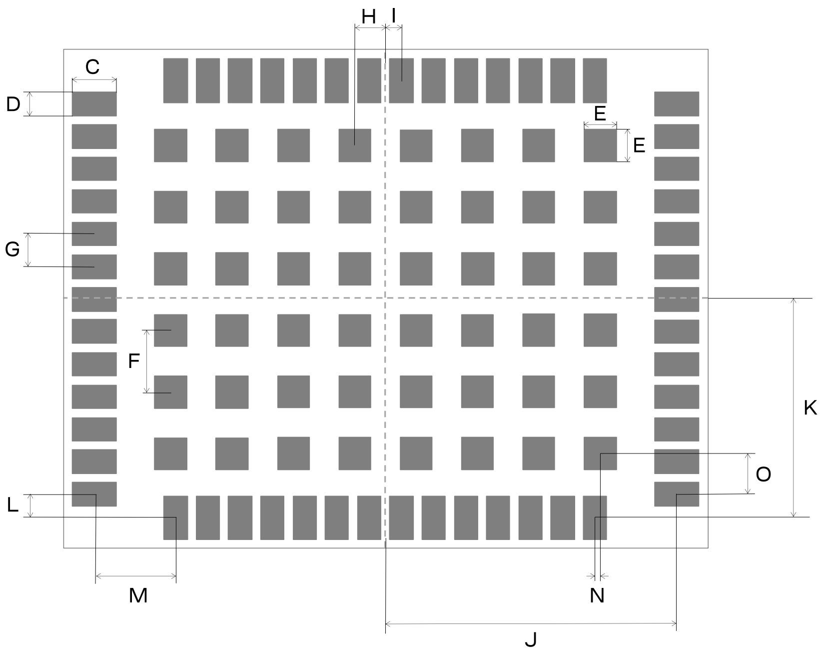


Figure 29: ZED-X20D suggested paste mask

Symbol	Dimension (mm)
C	1.55
D	0.75
E	1.05
F	2.10
G	1.10
H	1.05
I	0.55
J	10.00
K	7.50
L	0.90
M	2.85
N	0.20
O	1.35

Table 61: ZED-X20D paste mask dimensions

4.7.4 Layout guidance

The presented layout guidance reduces the risk of performance issues at design level.

4.7.4.1 RF In trace

The RF in trace has to work in the combined GNSS signal bands.

For FR-4 PCB material with a dielectric permittivity of for example 4.7, the trace width for the 50 Ω line impedance can be calculated.

A grounded co-planar RF trace is recommended as it provides the maximum shielding from noise with adequate vias to the ground layer.

The RF trace must be shielded by vias to ground along the entire length of the trace and the ZED-X20D **RF_IN** pad should be surrounded by vias as shown in the figure below.

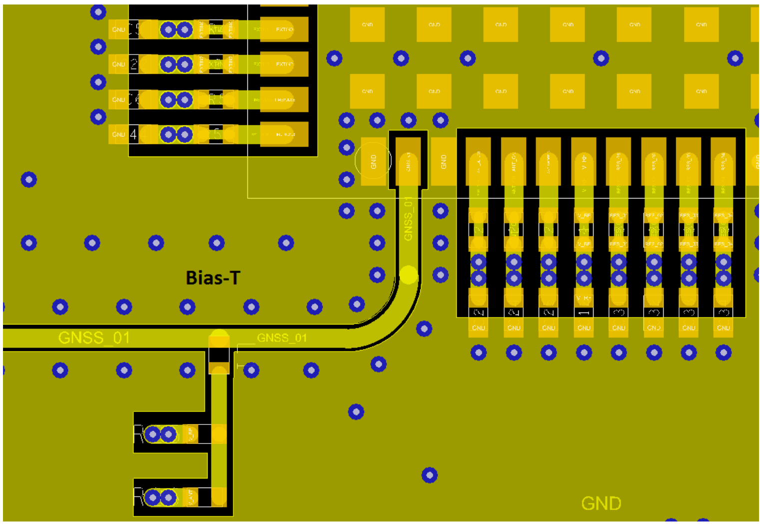


Figure 30: RF input trace

The **RF_IN** trace on the top layer should be referenced to a suitable ground layer.

4.7.4.2 Vias for the ground pads

The ground pads under the ZED-X20D high precision receiver need to be grounded with vias to the lower ground layer of the PCB. A solid ground layer fill on the top layer of the PCB is recommended. This is shown in the figure below.

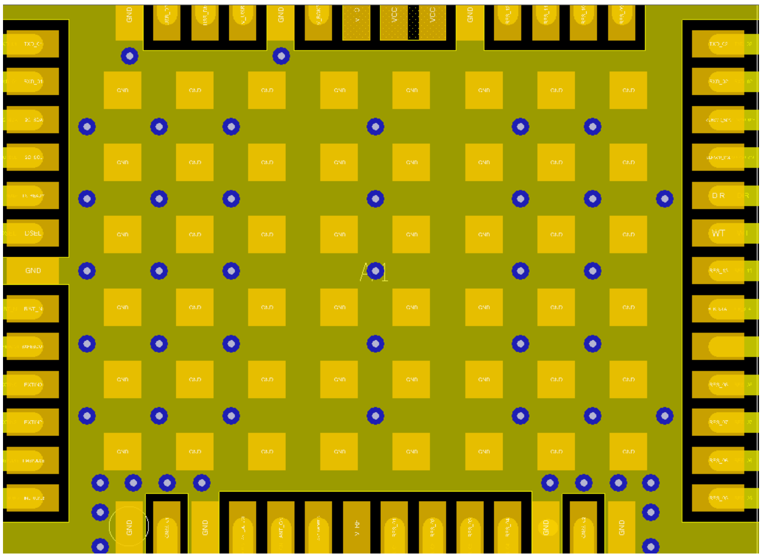


Figure 31: Top layer fill and vias

4.7.4.3 VCC pads

The **VCC** pads for the ZED-X20D high precision receiver must have as low impedance as possible with large vias to the lower power layer of the PCB. The **VCC** pads need a large combined pad and the de-coupling capacitors must be placed as close as possible. This is shown in the figure below.

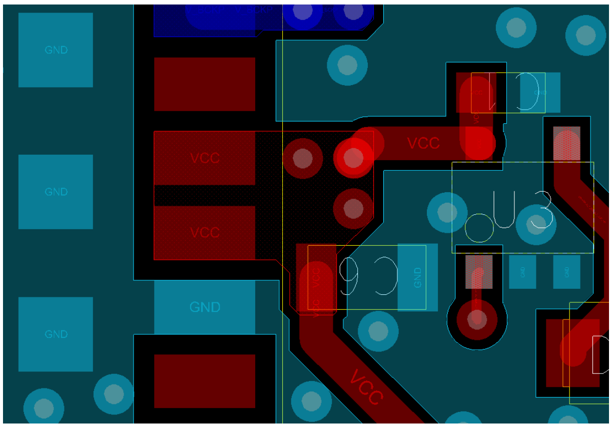


Figure 32: VCC pads

5 Production test

u-blox delivers products of the highest quality to its customers. To achieve this, we only supply fully tested units. At the end of the production process, every unit is tested. Defective units are analyzed in detail to continuously improve the production quality.

This is achieved with automatic test equipment, which delivers a detailed test report for each unit. The following measurements are done:

- Digital self-test (software download, verification of FLASH firmware, etc.)
- Measurement of voltages and currents
- Measurement of RF characteristics (e.g. C/N0)

Thanks to the 100 % test coverage done by u-blox, the OEM manufacturer doesn't need to repeat firmware tests or measurements of the GNSS parameters/characteristics (e.g. TTFF) in the production test.

The OEM manufacturer can focus on testing:

- Overall sensitivity of the device (including antenna, if applicable)
- Communication to a host controller

5.1 Connected sensitivity test

The best way to test the sensitivity of a positioning device is with the use of a GNSS simulator. It assures reliable and constant signals at every measurement.

Guidelines for sensitivity tests:

- Connect a GNSS simulator to the OEM product
- Choose the power level in a way that the "Golden Device" would report a C/N0 ratio of 38-40 dBHz
- Power up the DUT (Device Under Test) and allow enough time for the acquisition
- Read the C/N0 value from the NMEA GSV or the `UBX-NAV-SAT` message (e.g. with u-center)
- Compare the results to a "Golden Device", a u-blox Evaluation Kit or Application Board.

5.2 Go/no go tests for integrated devices

- For best results, place the device in an outdoor position with excellent sky view (HDOP < 3.0).
- Let the receiver acquire satellites and compare the signal strength with a "Golden Device". As the electro-magnetic field of a signal repeaters is not homogenous, indoor tests are not reliable in most cases.

These kinds of tests are useful as a go/no go test but not for sensitivity measurements.

6 Product handling

6.1 ESD precautions

⚠ CAUTION! Risk of electrostatic discharge (ESD) damage. u-blox chips and modules are electrostatic sensitive devices containing highly sensitive electronic circuitry. A discharge of static electricity may damage the device or reduce the life expectancy of the device. To avoid ESD damage, adhere to the standard guidelines for handling ESD devices.

Consider the following:

Preventing electrostatic discharge

- Keep components in their original packages during transport.
- Open the package within an ESD-protected area (EPA), as in Figure 33.
- At a workstation, store components in an EPA.
- Place ESD sensitive devices inside of shielding packaging or containers when transported outside of an EPA.
- Use protective clothing and proper personnel grounding at all necessary points when touching electrostatic sensitivedevice or assembly. For instance, wear ESD-safe clothing and shoes and wear an ESD wrist strap connected to a groundedworkstation. Use heel straps when standing on conductive floors or dissipating floor mats.
- Hold the devices by the edges and avoid touching component contacts, pins, or circuitry

Product handling

- When handling RF transceivers and patch antennas, work in an EPA.
- When connecting test equipment or any other electronics to the module (as a standalone or PCB-mounted device), the first point of contact must always be between the local ground and the PCB ground.
- Before mounting a ceramic patch antenna, connect the device to ground.
- When handling the RF pin, do not touch any charged capacitors. Be especially careful when handling materials likepatch antennas (~10 pF), coaxial cables (~50-80 pF/m), soldering irons, or any other materials that can develop charges.
- If there is any risk of touching an exposed antenna area in a non-ESD protected work area, implement proper ESDprotection measures in the design.
- When soldering RF connectors and patch antennas to the receiver's RF pin, use an ESD-safe soldering iron (tip)

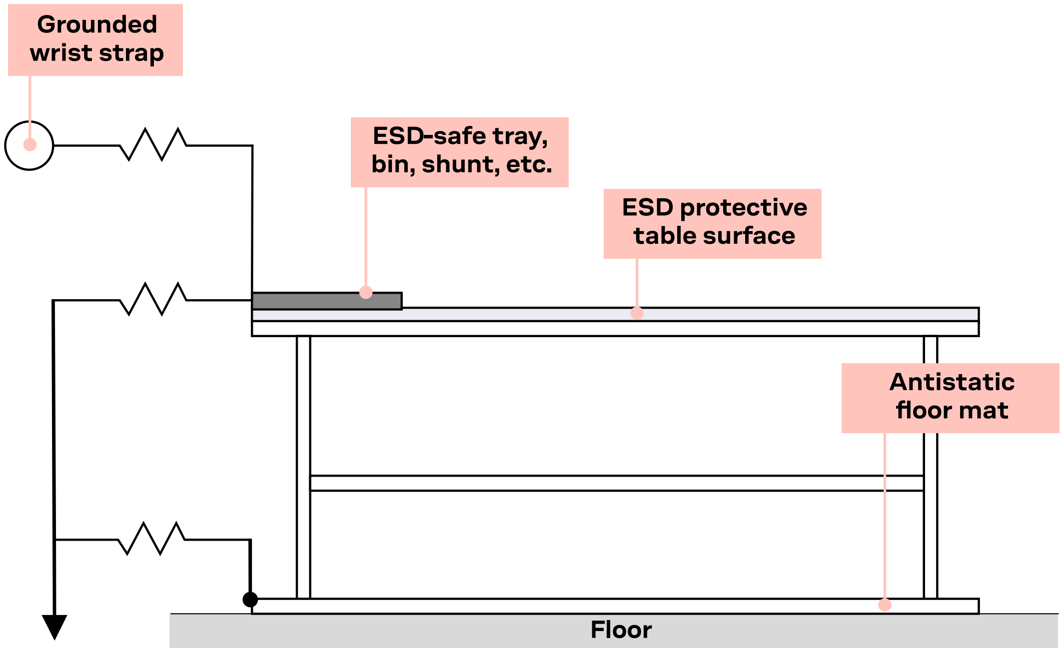


Figure 33: Standard workstation setup for safe handling of ESD-sensitive devices

6.2 Safety precautions

The ZED-X20D modules must be supplied by an external limited power source in compliance with the clause 2.5 of the standard IEC 60950-1. In addition to external limited power source, only Separated or Safety Extra-Low Voltage (SELV) circuits are to be connected to the module including interfaces and antennas.

☞ For more information about SELV circuits see section 2.2 in Safety standard IEC 60950-1.

6.3 Soldering

Reflow soldering procedures are described in the IPC/JEDEC J-STD-020 standard.

☞ When populating the modules, make sure that the pick and place machine is aligned to the copper pins of the module instead of the module edge.

Soldering paste

Use of “no clean” soldering paste is highly recommended, as it does not require cleaning after the soldering process. For instance, the following paste meets these criteria.

- Soldering paste: OM338 SAC405 / Nr.143714 (Cookson Electronics)
- Alloy specification: Sn 95.5/ Ag 4/ Cu 0.5 (95.5% tin/ 4% silver/ 0.5% copper)
- Melting temperature: 217 °C
- Stencil: The exact geometry, distances, stencil thicknesses and solder paste volumes must be adapted to the customer's specific production processes.

Reflow soldering

⚠ CAUTION. Risk of device damage. Exceeding the peak temperature of the recommended soldering profile may permanently damage the device.

The final soldering temperature chosen at the factory depends on additional external factors such as the choice of soldering paste, size, thickness and properties of the base board, etc.

As a reference, see “IPC-7530 Guidelines for temperature profiling for mass soldering (reflow and wave) processes”, published in 2001.

A convection-type soldering oven is highly recommended over the infrared-type radiation oven. Convection-heated ovens allow precise control of the temperature, and all parts will heat up evenly, regardless of material properties, thickness of components and surface color.

⚠ CAUTION. Risk of device damage. Modules must not be soldered with a damp heat process.

☞ To avoid falling off, the modules should be placed on the topside of the board during soldering.

For the recommended soldering profile and conditions, see Figure 34 and Table 62

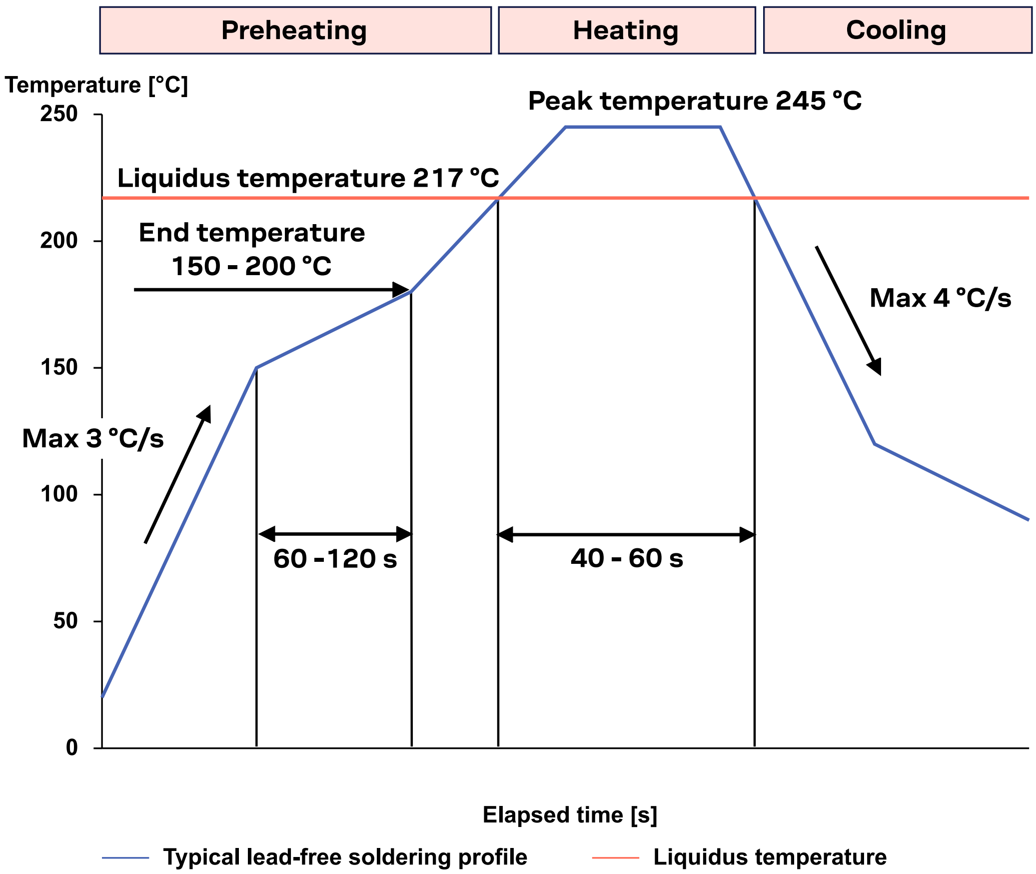


Figure 34: Recommended soldering profile

Phase	Value	Details
Preheating		During the initial heating of component leads and balls, residual humidity is dried out. Note that the preheating phase does not replace prior baking procedures.
Temperature rise rate	Max 3 °C/s	If the temperature rise is too rapid in the preheat phase, excessive slumping may be caused.
Time	60 – 120 s	If the preheating is insufficient, rather large solder balls tend to be generated. Conversely, if performed excessively, fine balls and large balls will be generated in clusters.
End temperature	150 – 200 °C	If the temperature is too low, non-melting tends to be caused in areas containing large heat capacity.
Heating - reflow		

Phase	Value	Details
Time limit above 217 °C liquidus temperature	40 – 60 s	The temperature rises above the liquidus temperature of 217 °C. Avoid a sudden rise in temperature as the slump of the paste could become worse.
Peak reflow temperature	245 °C	
Cooling		
Temperature fall rate	Max 4 °C/s	A controlled cooling prevents negative metallurgical effects of the solder (solder becomes more brittle) and possible mechanical tensions in the products. Controlled cooling helps to achieve bright solder fillets with a good shape and low contact angle.

Table 62: Recommended conditions for reflow soldering

Optical inspection

After soldering the module, consider optical inspection.

Wave soldering

Base boards with combined through-hole technology (THT) components and surface-mount technology (SMT) devices require wave soldering to solder the THT components. Only a single wave soldering process is encouraged for boards populated with modules.

6.4 Safe handling of modules

This section outlines safe practices of handling modules.

Cleaning

☞ Do not clean the module with water, solvent, or ultrasonic cleaner:

- Cleaning with water leads to capillary effects where water is absorbed into the gap between the baseboard and the module. The combination of residues of soldering flux and encapsulated water leads to short circuits or resistor-like interconnections between neighboring pins.
- Cleaning with alcohol or other organic solvents can result in soldering flux residues flowing underneath the module, into areas that are not accessible for post-cleaning inspections. The solvent also damages the sticker and the printed text on the module.

⚠ CAUTION. Risk of device damage. Ultrasonic cleaning permanently damages the module, in particular the quartz oscillators.

The best approach is to use a “no clean” soldering paste to eliminate the cleaning step after the soldering.

Repeated reflow soldering

☞ Repeated reflow soldering processes or soldering the module upside down are not recommended.

A board that is populated with components on both sides may require more than one reflow soldering cycle. In such a case, the process should ensure the module is only placed on the board submitted for a single final upright reflow cycle. A module placed on the underside of the board may detach during a reflow soldering cycle due to lack of adhesion.

The module can also tolerate an additional reflow cycle for rework purposes.

After the module is removed from the reflow oven, clean the pins before reapplying the solder paste, placing the module in the oven and proceeding with the reflow soldering of a new module.

Rework

⚠ CAUTION. Risk of device damage. Using a hot air gun is an uncontrolled process. It can lead to overheating and severely damage the module. Always avoid overheating the module.

☞ Never attempt to alter the module itself, e.g. by replacing individual components. Such actions immediately void the warranty.

Conformal coating

Certain applications employ a conformal coating of the PCB using HumiSeal® or other related coating products. These materials affect the RF properties of the GNSS. It is important to prevent them from flowing into the module. The RF shields do not provide 100% protection for the module from coating liquids with low viscosity. Apply the coating carefully.

☞ Conformal coating of the module voids the warranty.

Casting

If casting is required, use viscose or another type of silicon pottant. The OEM is strongly advised to qualify that such processes are suitable for the module before implementing them in the production.

☞ Casting voids the warranty.

Grounding metal covers

Attempts to improve grounding by soldering ground cables, wick or other forms of metal strips directly onto the EMI covers is done at the customer's own risk. The numerous ground pins should be sufficient to provide optimum immunity to interference and noise.

☞ u-blox provides no warranty for damages to the module caused by soldering metal cables or any other forms of metal strips directly onto the EMI covers.

Use of ultrasonic processes

Some components on the module are sensitive to ultrasonic waves.

⚠ CAUTION. Risk of device damage. Use of any ultrasonic processes (cleaning, welding etc.) may cause damage to the receiver.

☞ u-blox provides no warranty against damages to the module caused by ultrasonic processes.

Appendix

A Reference design

The key features of a typical ZED-X20D design include:

- **V_BCKP supply (optional):** If present, the hardware backup mode is supported. This mode maintains the RTC time and GNSS orbit data in the battery-backed RAM memory if the main supply is switched off.
- **UART communication interfaces:** UART1 and UART2 communication interfaces are available.
- **PIOs (EXTINT, TIMEPULSE):** For a typical design, these can be left open.
- **RESET_N and SAFEBOOT_N connections:** It is recommended to connect these to the host system to enable hardware reset and safe boot mode.

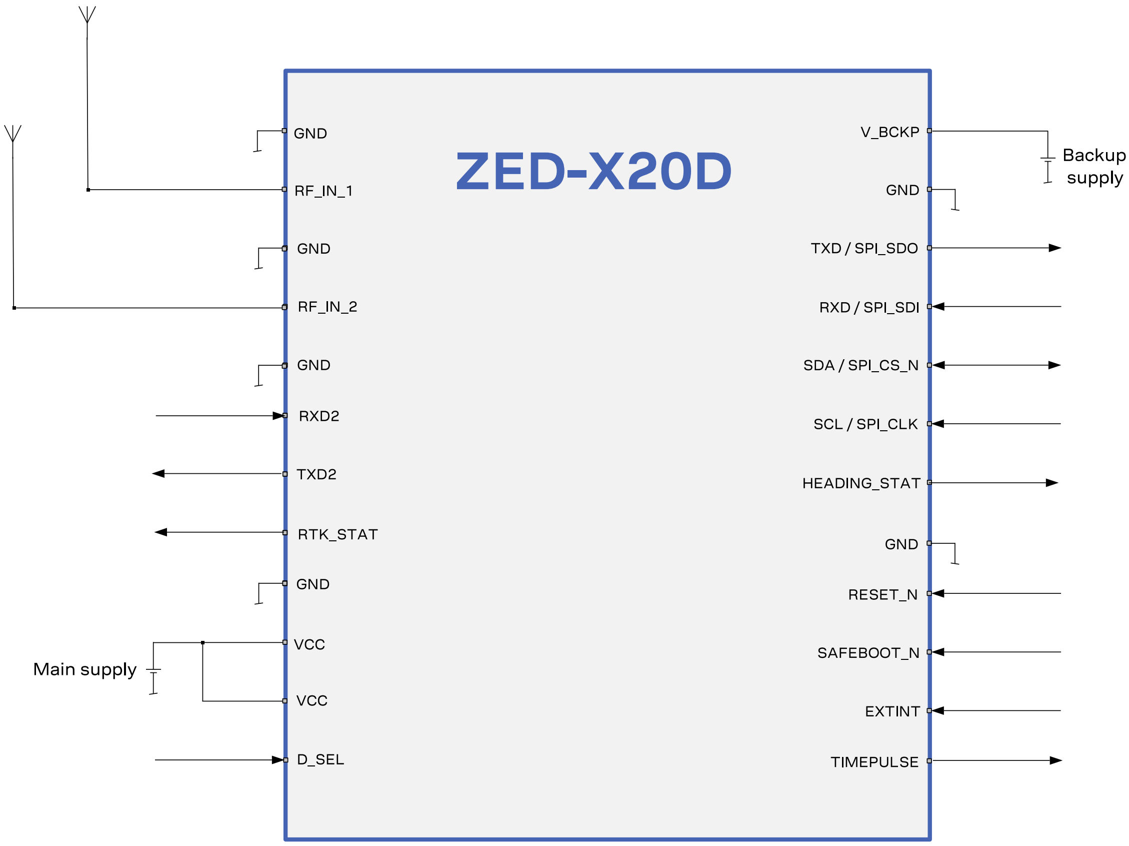


Figure 35: Typical ZED-X20D design

B Reference frames

Real time kinematic (RTK) is a differential system where the rover uses the corrections from a reference station or a reference station network. The rover receiver will calculate its position in the reference frame used by the service provider in its correction stream. If the output is required in a different reference frame, then a (custom) datum transformation is required.

For example, if an application requires the position in the International Terrestrial Reference Frame (ITRF) 14 reference frame but the correction service is using the European Terrestrial Reference System (ETRF) 14 reference frame - to which the RTK solution will also be referring - then this reference frame offset needs to be compensated. For example if utilizing a truth system which is using corrections referring to different reference frame, it is important to compensate for the reference frame offset to avoid systematic errors in the analysis.

Terrestrial reference system is a coordinate reference system which is rotating in space with the rotation of the Earth. The reference system is an abstract concept that is realized by obtaining coordinates for some points on the surface of the Earth. This kind of realization is called a reference frame. For more details, see for example the ITRF webpage. Commonly used reference systems include International Terrestrial Reference System (ITRS) and European Terrestrial Reference System 1989 (ETRS89).

Widely used reference frames include for example International Terrestrial Reference Frame (ITRF) and ETRF. ITRF is a realization of ITRS, done every few years. Latest realizations of ITRF are ITRF2008 and ITRF2014. ETRF is a realization of ETRS89, done every few years. Latest realizations are ITRF2005 and ETRF2014.

For example, the EUREF is used to realize the ETRS89. For information, see their homepage: EUREF.

See the ITRF website for more information and an online transform calculator: ITRF.

Another online tool for transformations is available on the EUREF network page: EUREF Transformation.

Reference frames can have constant offsets between each other but, in addition to that, they can also drift and rotate with respect to each other. One major reason for this is that the tectonic plates move constantly and the reference frames that are attached to the tectonic plates move along with the plates.

☞ ZED-X20D stores the EGM96 geoid model with limited resolution, which can reduce the precision of the reported mean sea level height and geoid separation. For applications requiring higher geoid separation accuracy, apply your own adjustment to the ellipsoidal height output from ZED-X20D.

Related documents

[1] ZED-X20D-00B Data sheet,UBXDOC-304424225-20103
[2] HDG 2.00 Interface description,UBXDOC-304424225-21470
[3] Product packaging reference guide UBX-14001652
[4] AssistNow service, https://support.thingstream.io/

☞ For regular updates to u-blox documentation and to receive product change notifications please register on our homepage https://www.u-blox.com.

Revision history

Revision	Date	Comments
R01	07-Jul-2026	Initial revision

Contact

u-blox AG

Address: Zürcherstrasse 68
8800 Thalwil
Switzerland

For further support and contact information, visit us at www.u-blox.com/support.