Article

Design and Performance Analysis of BDS-3 Integrity Concept

Cheng Liu [1], Yueling Cao [2], Gong Zhang [3], Weiguang Gao [1],*, Ying Chen [1], Jun Lu [1], Chonghua Liu [4], Haitao Zhao [4] and Fang Li [5]

[1] Beijing Institute of Tracking and Telecommunication Technology, Beijing 100094, China; liucheng@beidou.gov.cn (C.L.); cheny@beidou.gov.cn (Y.C.); lujun@beidou.gov.cn (J.L.)
[2] Shanghai Astronomical Observatory, Chinese Academy of Sciences, Shanghai 200030, China; caoyueling@shao.ac.cn
[3] Institute of Telecommunication and Navigation, CAST, Beijing 100094, China; zhanggong@cast.casc
[4] Beijing Institute of Spacecraft System Engineering, Beijing 100094, China; liuchonghua@cast.casc (C.L.); zhaohaitao@cast.casc (H.Z.)
[5] National Astronomical Observatories, Chinese Academy of Sciences, Beijing 100094, China; lifang@bao.ac.cn
* Correspondence: gaowg@beidou.gov.cn

Abstract: Compared to the BeiDou regional navigation satellite system (BDS-2), the BeiDou global navigation satellite system (BDS-3) carried out a brand new integrity concept design and construction work, which defines and achieves the integrity functions for major civil open services (OS) signals such as B1C, B2a, and B1I. The integrity definition and calculation method of BDS-3 are introduced. The fault tree model for satellite signal-in-space (SIS) is used, to decompose and obtain the integrity risk bottom events. In response to the weakness in the space and ground segments of the system, a variety of integrity monitoring measures have been taken. On this basis, the design values for the new B1C/B2a signal and the original B1I signal are proposed, which are 0.9×10^{-5} and 0.8×10^{-5}, respectively. The hybrid alarming mechanism of BDS-3, which has both the ground alarming approach and the satellite alarming approach, is explained. At last, an integrity risk analysis and verification work were carried out using the operating data of the system in 2019. The results show that the actual operation of the system is consistent with the conceptual design, which satisfies the integrity performance promised by BDS-3 in the ICAO SAPRs.

Keywords: BDS; BeiDou; integrity; risk tree; FMEA; satellite service failure; constellation service failure

1. Introduction

Accuracy, integrity, continuity, and availability are the four core performance indicators of satellite navigation systems. Among them, integrity refers to the ability of the system to alert users in time when the service is abnormal or experiences failure, and it characterizes the security and reliability of system services [1,2]. If there is an abnormality or failure in the service, but the system fails to detect it or fails to alarm in time, an "integrity event" has occurred. Once an integrity event occurs, it will have a security impact on the user, especially for civil aviation, maritime, railway, and other users related to life safety. System reliability is even more strategically important with the widespread use of low-cost sensors for various applications including personal positioning and autonomous navigation [3,4]. In addition, the integrity of the core constellation is also an important foundation for the construction of the satellite-based augmentation systems (SBAS) such as WASS (wide area augmentation system) [5,6], ENGOS (European geostationary navigation overlay system) [7,8], MSAS (multi-functional satellite augmentation system) [9,10], BDSBAS (BeiDou satellite-based augmentation system) [11], and airport ground-based augmentation systems (GBAS). These augmentation systems are constructed to further augment the global navigation satellite system (GNSS) constellation and provide higher integrity navigation services.

Satellite navigation systems in the world are paying more and more attention to the construction and improvement of their integrity capabilities. GPS and Galileo considered their integrity function at the beginning of the system design, defined the integrity parameters and algorithms, and planned its application scenarios [2,12–14]. China's BeiDou also attaches importance to the construction of integrity. China's BeiDou global navigation satellite system (BDS-3) carried out a brand new integrity concept design work, which defines and achieves the integrity functions for major civil open service (OS) signals such as B1C, B2a, and B1I. In addition to GNSSs, regional satellite navigation systems have also begun to upgrade their integrity capabilities. For example, Japan's QZSS not only defines and provides the integrity function for its basic positioning, navigation, and timing (PNT) service, but also for its sub-meter level augmentation service (SLAS) and centimeter-level augmentation service (CLAS) [15,16].

Due to the numerous components, functions, and processing operations of the system, it is not easy to ensure the integrity of satellite navigation systems, especially for global ones. On 13 July 2019, a mass outage occurred in Galileo—all 24 networking satellites in orbit entered an "unavailable" or "test" state, and the system was immediately paralyzed. After 48 h of full maintenance, the system did not return to normal until 8 o'clock on 18 July. During this period, the service was knocked offline for up to 117 h (about 5 days) [17]. Although the European GNSS Agency (GSA) issued a warning of service outage on the Galileo official website at 20:00 on 13 July [18], it still had a serious impact on users around the world. This incident also prompted countries to take measures to ensure the safe operations of satellite navigation systems. After this incident, Russia stated that it has set up a multi-level software detection system in the ground segment of GLONASS, with a redundant design and an autonomous control function to prevent such failures from occurring.

On 27 December 2018, BDS-3 completed the construction of the basic constellation (consisting of 18 MEOs) and began to provide the initial global service [19]. On 31 July 2020, BDS-3 completed all construction (consisting of 24 MEOs, 3 IGSOs, and 3 GEOs) tasks and officially opened the global service [20]. Since the initial service was provided, BDS-3 has been in a stable operation state, and there have been no integrity events affecting the system and user services. This benefits from the reasonable system design and effective risk monitoring and control measures. However, this does not mean that BDS-3 has completely eliminated the integrity hazards, especially considering that the system was built in such a short period of time (2012–2020). To ensure the safety and reliability of the service, it is necessary and valuable to carry out more in-depth research and evaluation.

This study focuses on the design and the performance analysis of BDS-3's integrity concept. In order to improve the reliability and safety of the service, BDS-3 upgraded and improved the conceptual design and function of integrity compared to BDS-2 and carried out standard development work in ICAO SARPs at the same time. The satellite service failure and constellation service failure concepts are clearly defined, and the integrity risk probability calculation method is designed for the three OS signals of B1I/B1C/B2a. The integrity fault tree model is studied and established, and the corresponding monitoring measures for weakness in the space segment and the ground segment of the system is proposed. In terms of alarms, BDS-3 is designed with a hybrid alarm mechanism of the ground alarm approach and the satellite alarm approach, to make up for the limitations for BDS's failure to deploy ground monitoring stations globally. Finally, the actual operation data of 2019 was used to verify the integrity performance of the system service. The results show that the actual operation of the system is consistent with the conceptual design, which proves the safety and reliability of the BDS-3 OS service.

The remainder of this paper is structured as follows. Section 2 defines the integrity of the BDS OS signals (B1I/B1C/B2a), introduces the alarm approach, and gives the calculation method of the satellite service failure probability (P_{sat}) and the constellation service failure probability (P_{const}). In Section 3, a fault tree model for the BDS satellite signal-in-space (SIS) is established, the bottom events from the space segment and the

ground segment are decomposed, and the system design values of P_{sat} and P_{const} are derived. In Section 4, the integrity prevention and control measures taken by BDS-3 in the space segment and the ground segment are introduced, respectively. Finally, Section 5 presents the integrity risk verification work on BDS-3 and the analyses of the results.

2. BDS Integrity Concept

This section first introduces the integrity definition of BDS-3 under the ICAO framework, which includes two concepts: P_{sat} and P_{const}. Secondly, the hybrid alarm mechanism of BDS-3, which has both the ground alarm approach and the satellite alarm approach, is explained. This hybrid design is mainly to make up for the limitations for BDS's failure to deploy ground monitoring stations globally.

2.1. Integrity Definition

Due to the high requirements for safety and reliability, the concept of navigation integrity first appeared in the field of civil aviation. In order to be approved for the application in the field of civil aviation, GNSSs need to carry out and complete their standard research and formulation work under the ICAO framework, and promise ICAO all necessary service performance indicators, including integrity.

According to the definition in the ICAO international standards and recommended practices (SARPs), integrity indicates the system's ability to detect faults and issue alerts. In order to make more detailed and accurate assessments, the integrity probability is further subdivided into the "satellite service failure probability" (denoted as P_{sat}) and the "constellation service failure probability" (denoted as P_{const}). Among them, the "satellite service failure" refers to the condition where the user range error (URE) of any single satellite exceeds the broadcast not-to-exceed (NTE) tolerance but the alarm cannot be achieved within the promised time. This type of failure will only affect itself and no other satellites. The "constellation service failure" refers to the condition where the UREs of more than two satellites exceed the corresponding NTEs at the same time, and the alarm cannot be achieved within the promised time. Once this type of failure appears, it means that some kind of common fault has occurred in the system.

ICAO allows the GNSS to develop its customized integrity technical content. See Table 1 for the integrity risk probability indicator of each GNSS in ICAO SARPs [19,21].

Table 1. GNSS integrity performance in ICAO SARPs.

	Items	GPS	GNLOASS	Galileo	BDS
P_{sat}	Error Tolerance	URE > 4.42 × IAURA	URE > 70 m	URE > 4.17 × URA	URE > 4.17 × URA for B1I; URE > 4.42 × SISA for B1C and B2a
	Time-to-Alert (TTA)	10 s	10 s	Not applicable	60 s for ground monitoring and alarming; 6 s/300 s for satellite and alarming
	Probability	$\leq 10^{-5}$	$\leq 10^{-4}$	$\leq 3 \times 10^{-5}$	$\leq 10^{-5}$
P_{const}	Error Tolerance	URE > 4.42 × IAURA	URE > 70 m	URE > 4.17 × URA	URE > 4.17 × URA for B1I; URE > 4.42 × SISA for B1C and B2a
	Time-to-Alert (TTA)	10 s	10 s	Not applicable	300 s for ground monitoring and alarming; 6 s for satellite monitoring and alarming
	Probability	10^{-8}	10^{-4}	$\leq 2 \times 10^{-5}$	$\leq 6 \times 10^{-5}$

It can be seen from Table 1 that the integrity functions of each GNSS are quite different. GPS has global ground monitoring and injection capabilities, so once the service is abnormal, the system can send an alert in real time. Specifically, there are several alarm approaches for GPS, including using the health status indicator in the message, setting the satellite pseudo random number (PRN) code to "37", or broadcasting non-standard PRN

codes. GLONASS indicates the operating status of the system to users through the health status indicator in the message. Galileo provides users with integrity information through the HS, DVS, SISA, and other parameters in the message; in addition, when the issue of data (IOD) of the message exceeds four hours, it also indicates that the system message is in an unhealthy state. BDS-3 is designed with two methods of ground integrity monitoring and satellite autonomous integrity monitoring (SAIM). Among them, the ground integrity monitoring approach provides users with integrity information through HS, SIF, DIF, SISA, and other parameters in the message; SAIM can provide users with integrity information through message parameters or non-standard PRN codes. In addition, the NTE tolerances of GPS, Galileo, and BDS are broadcasted to users as message parameters, while the NTE tolerance of GNLOASS is fixed to 70 m.

2.2. Alarming Approach

This section introduces the alarming mechanism of BDS-3. BDS-3 is designed with a hybrid alarming mechanism of the ground monitoring and alarm approach and the satellite monitoring and alarm approach, to make up for the limitations for BDS's failure to deploy ground monitoring stations globally.

2.2.1. Ground Monitoring and Alarming

The ground monitoring and alarm approach using the BDS ground segment facilities the monitoring of the signal quality and the URE of the satellite SIS. When the failure is detected, the user will be notified of the satellite SIS health status through the integrity parameters in the broadcast message. The designed TTA of the ground monitoring and alarming approach is better than 60 s, and the delay mainly comes from processes such as data transmission, information processing, and message update, etc. The new B1C and B2a signals and the original B1I signal of BDS have different integrity parameter designs and alarm mechanisms.

The B1I signal uses the "autonomous satellite health flag (SatH1)" parameter broadcast in the BDS D1 navigation message to indicate the satellite SIS health status, where "SatH1 = 0" indicates that the satellite SIS is available, and "SatH1 = 1" indicates that satellite SIS is not available (that is, URE > 4.17 × URA), which are shown in Table 2 [22,23].

Table 2. B1I SIS health status indications.

B1I SIS Health Status	SatH1
Healthy	0
Unhealthy	1

As a comparison, B1C and B2a signals use the "satellite health status (HS)" parameter to indicate the health status of the entire satellite, and the "signal integrity flag (SIF)" parameter to indicate the satellite SIS status. In addition, B1C and B2a signals use a "data integrity flag (DIF)" parameter to indicate the SIS accuracy (SISA) of satellites. This is mainly to take into account the differences in the sensitivity and tolerance of aviation and non-aviation users to satellite ranging errors. The integrity parameters of B1C and B2a signals are broadcast in sub-frame 3 of BDS B-CNAV1 and B-CNAV2 navigation messages, respectively [24,25]. As the update frequency of B-CNAV2 is higher, it is recommended to use the integrity parameters broadcast in B-CNAV2, for B1C/B2a dual-frequency users.

According to the above-mentioned integrity parameter design, B1C and B2a signals can take three different states as shown in Table 3, with the following meanings:

- "Healthy": The SIS of the satellite meets the minimum service performance specified in the "BeiDou Open Service Performance Specification" [22];
- "Unhealthy": The SIS of the satellite is not providing services or is under test;
- "Marginal": The signal is neither of the two previous states. For some types of users, it is acceptable and tolerable, but for others, it is not.

Table 3. B1C/B2a SIS health status indications.

B1C/B2a SIS Health Status	HS	SIF	DIF
Healthy	0	0	0
Marginal	0	0	1
	2/3	0	0
Unhealthy	Any value	1	0/1
	1	0/1	0/1

Further, the steps for the use of B1C and B2a signals can be described as following:

- Step 1: Confirm whether the entire satellite is healthy according to the HS parameter in the message. If HS = 1, it indicates that the satellite is currently unhealthy, and the user should stop using the satellite. If HS = 0, it indicates that the satellite is currently healthy, and proceed to step 2.
- Step 2: Confirm whether the satellite SIS is abnormal according to the SIF parameter in the message. If SIF = 1, it indicates that the satellite SIS has an anomaly affecting the pseudo-range, please stop using the satellite. If SIF = 0, it indicates that the satellite signal is normal, and proceed to step 3.
- Step 3: Access the DIF parameter in the message. If DIF = 1, it indicates that the SISA of the satellite exceed the NTE (that is, URE > 4.42 × SISA), and it is not recommended for users in the life safety field, such as aviation users. However, for the satellite, this is just that its SISA exceeds the limit at this time, not a failure. Other users who have less strict safety requirements can still choose to use it (for example, users in the mass consumer sector). If DIF = 0, it indicates that the SISA of the satellite does not exceed the NTE, and all users can use it with confidence.

Currently, this alarm approach has been implemented in B1C and B2a signals. Here, we want to further highlight the design significance of DIF. The introduction of DIF is mainly to take into account the differences in the sensitivity and tolerance of aviation and non-aviation users to satellite ranging errors. We hope that while ensuring integrity, the use of DIF will help improve the continuity and availability for non-aviation users.

2.2.2. Satellite Monitoring and Alarming

The satellite monitoring and alarming approach includes two mechanisms. One is that the satellite sends back the SIS quality monitoring information to the ground, and after the ground segment confirms the fault, the alert notification is sent to the satellite through the inter-satellite link (ISL). According to the topology of BDS ISL and the en-route operation performance requirements of ICAO, the TTA is designed to be 300 s.

Another mechanism is that the satellite uses the on-board SAIM equipment to monitor the satellite clock, SIS quality, and SIS-URE in real time without the need for ground confirmation. This mechanism can achieve a very fast alarm speed, and the expected TTA for it is 6 s. At present, this alarm approach is in the on-board testing stage, and BDS is working hard to implement this rapid alarm mechanism as soon as possible and has not ruled out the use of non-standard PRN codes and other alert notifications.

The use of the satellite monitoring and alarm approach is mainly to make up for the limitations for BDS's failure to deploy monitoring stations globally. When BDS satellites are located in China, the system will use the ground monitoring and alarm approach; when BDS satellites are located outside of China, it will mainly rely on the satellite monitoring and alarm approach to ensure the integrity of satellites.

2.3. P_{sat} and P_{const} Calculations

2.3.1. P_{sat} Calculation for B1I

For any satellite at any time t, the B1I SIS health status is determined as following:

$$\text{SatH1} = 0 \text{ (Health)} \tag{1}$$

where SatH1 is the integrity status parameter of B1I.

Using the precision satellite orbit product to calculate the along-track error (denoted as ΔT), cross-track error (denoted as ΔN), and radial error (denoted as ΔR) of the satellite orbit in the broadcast NAV message, and using the precision satellite clock product to calculate the satellite clock error (denoted as Δclk) in the broadcast NAV message. Their projection to the worst user location (WUL) position can be obtained by Equation (2) [26,27].

$$\text{SISURE} = \left| (\Delta R - \Delta clk) + C_1 \cdot sign(\Delta R - \Delta clk) \cdot \sqrt{(\Delta T^2 + \Delta N^2)} \right| \tag{2}$$

where C_1 is the projection factor at the WUL results from the approximation of the ratio $R_{earth}/a_{satellilte}$, with R_{earth} is the mean earth's radius and $a_{satellilte}$ is the semi major axis of the BDS satellites orbit. C_1 is given in Table 4 for MEOs and GEO/IGSOs, respectively.

Table 4. Values of C_1 for satellites of different orbit types.

Satellite	C_1
MEO	0.2285
GEO/IGSO	0.1512

The satellite service failure condition of the B1I signal is determined by the following logical function over the hour interval:

$$F_{P_{sat},\ B1I} = \begin{cases} 1, (\text{SISURE} \geq 4.42\ \text{URA, without a timely alert) and (SatH1} = 0) \\ 0, \text{other} \end{cases} \tag{3}$$

where the URA indicator of the B1I signal can be obtained via the user range accuracy index (URAI) broadcast in the D1 NAV message of B1I [23].

Faults have a finite duration before they are either corrected or before the user is notified. Here, we use the term mean time to notify (MTTN) in hours to denote the expected average fault duration [27,28]. On this basis, P_{sat} of a year is defined as the ratio of the MTTN duration of satellite failure conditions to the total hours of all satellites in the constellation, which can be expressed as follows:

$$P_{sat} = \frac{\sum_{N_{sat}} \sum_{MTTN}(F_{Psat,SV})}{N_{hours} \cdot N_{SV}} \tag{4}$$

where N_{sat} is the total number of failure satellites of a year, N_{hours} is the total hours of a year, and N_{SV} is the nominal number of satellites in the constellation (for BDS is 27 in ICAO SAPRs).

2.3.2. P_{sat} Calculation for B1C and B2a

For any satellite at any time t, the B1C/B2a SIS health status is determined by the integrity parameters as follows:

$$\text{HS} = 0, \text{SIF} = 0, \text{ and DIF} = 0 \text{ (Health)} \tag{5}$$

where HS, SIF, and DIF are the integrity status parameters of B1C/B2a.

The SISURE of the B1C/B2a signal is calculated using the same method as the B1I signal in Section 2.3.1, and the satellite service failure condition is determined as follows:

$$F_{P_{sat},B1C/B2a} = \begin{cases} 1, (SISURE \geq 4.42 \; SISA, \; without \; a \; timely \; alert) \; and \; (HS, SIF, DIF = 0) \\ 0, other \end{cases} \quad (6)$$

where the SISA indicators of B1C and B2a signals can be obtained by the SIS accuracy index (SISAI) broadcast in the B-CNAV1 [24] and B-CNAV2 [25] navigation messages, respectively.

More specifically, SISA can be calculated by the function as following [24,25,29]:

$$SISA = \sqrt{(SISA_{oe} \times \sin 14°)^2 + SISA_{oc}^2} \quad (7)$$

where $SISA_{oe}$ denotes the elevation-dependent component, and $SISA_{oc}$ denotes the non-elevation-dependent component. After that, Equation (4) is also suitable for calculating the P_{sat} of B1C and B2a signals.

2.3.3. P_{const} Calculation

P_{const} is obtained through statistics, which can be expressed as following:

$$P_{const} = \frac{N_{const} \cdot MTTN}{N_{hours}} \quad (8)$$

where N_{const} represents the total time in a year that two or more satellites fail due to a common cause at the same time.

3. Integrity Risk Probability Distribution

In this section, a fault tree model for the BDS satellite SIS is constructed, and the main integrity risk bottom events from the space segment and the ground segment are sorted out and decomposed. By analyzing them one by one, the design values of P_{sat} and P_{const} of the system are deduced and determined. At present, these technical indicators have been written into the latest draft of ICAO SARPs.

3.1. Integrity Risk Tree Model

The risk tree method is a graphical model of expressing the logical relationship between a particular failure condition and the causes or failures leading to this condition. It is an application of fault tree analysis being used in the aerospace industry [21].

The BDS satellite SIS integrity failure comes from the space segment and the ground segment. The bottom events of the space segment failure include the satellite clock anomaly, and the satellite signal and data anomaly (specifically, the transmitting power anomaly, the message data anomaly, the code-carrier inconsistency, and the signal distortion).

The bottom events of the ground segment failure include the satellite orbit processing anomaly, the satellite clock processing anomaly, the ephemeris fitting anomaly, the data input anomaly, the orbit and time synchronization processing equipment anomaly, the monitoring station (MS) data anomaly (including the transmission link failure between the MS and the master control station (MCS)), and the message upload anomaly (including the upload failure caused by control instruction faults and configuration faults).

Based on the above-mentioned bottom events, an integrity risk tree can be constructed to systematically analyze and evaluate the satellite service failure probability of BDS, as shown in Figure 1.
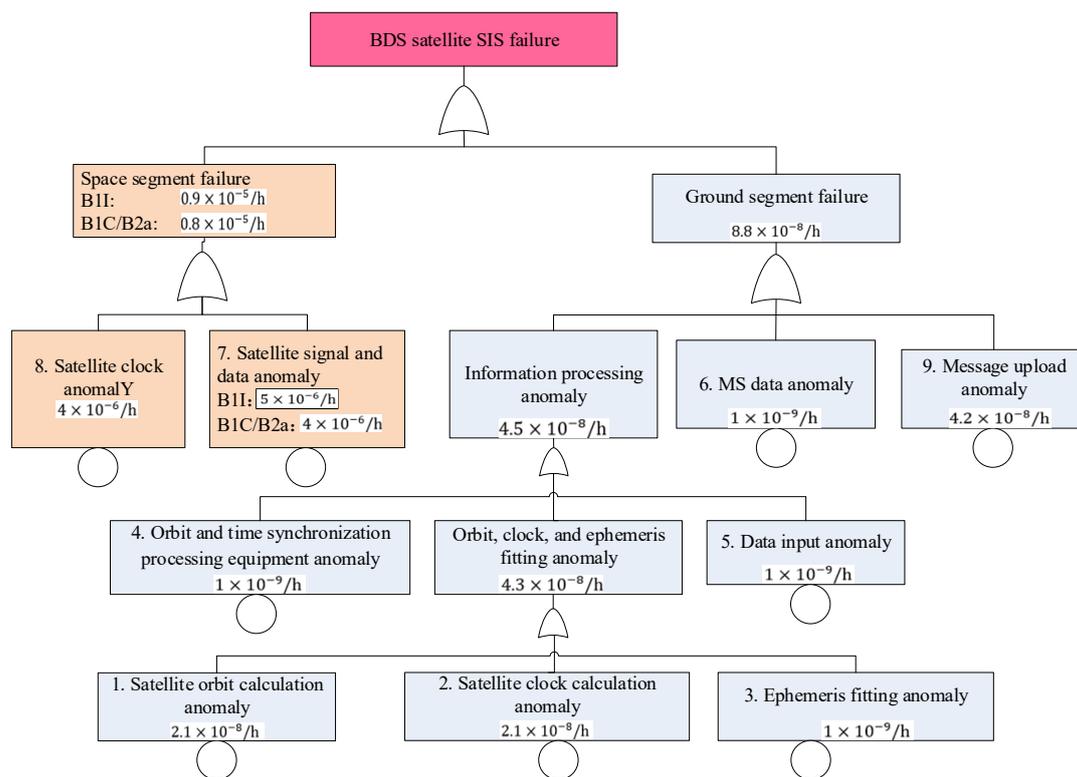
Figure 1. BDS SIS integrity risk tree.

There are a total of nine bottom events in Figure 1, including two in the space segment and seven in the ground segment. The probability of the top event is the known P_{sat}. The occurrence of each bottom event could lead to the occurrence of the top event. The relationship between them is a simple probability addition, which can be expressed as following:

$$P_{sat} = \sum_{i=1}^{9} P_{event_i} \tag{9}$$

where $P_{event_i} (i = 1, 2, \dots 9)$ denotes the probability of each bottom event in the integrity risk tree.

3.2. ModelBottom Event Probability

3.2.1. Bottom Event Probability for Space Segment

The failure probabilities of the two bottom events of the space segment are estimated as following:

1.　Satellite signal and data anomaly probability

For the B1I signal, the integrity failure mode and effect analysis (IFMEA) has been conducted on the operating status of the BDS-3 basic constellation (consisting of 18 BDS-3 satellites) since its completion on 27 December 2018, and no satellite signal and data anomaly events have been found during the assessment period. According to the design requirements of BDS-3, the probability of this anomaly is 5×10^{-6}/h, that is:

$$P_{event_{6,7}}^{B1I} = 5 \times 10^{-6}/h \tag{10}$$

where indices 6, 7 refer to the bottom events 6, 7 in the integrity risk tree.

For the B1C and B2a signals, there has also been no satellite signal and data anomaly events occurred since 27 December 2018. According to the design requirements of BDS-3, the probability of such anomaly is 4×10^{-6}/h, that is:

$$P_{event_{6,7}}^{B1C/B2a} = 4 \times 10^{-6}/h \tag{11}$$

where indices 6, 7 refer to the bottom events 6, 7 in the integrity risk tree.

2.　　Satellite clock anomaly probability

The IFMEA has been conducted and no satellite clock anomaly events have been found. According to the internal system design requirements of BDS-3, the probability of such an anomaly is $4 \times 10^{-6}/h$.

3.2.2. Bottom Event Probability for Ground Segment

The failure probabilities of the seven bottom events of the ground segment are estimated as following:

1.　　Satellite orbit calculation anomaly probability and satellite clock calculation anomaly probability

The IFMEA result shows that only one satellite orbit calculation anomaly event occurred since 27 December 2018, which was detected in time by the ground segment and did not affect the satellite SIS integrity. No satellite clock calculation anomaly event occurred during the assessment period.

Due to the similarities in the causes and mechanisms of these two types of bottom events, we assume that the average probability of each event is 0.5 times per year. Moreover, since the anomaly event can only affect the satellite SIS integrity when the system fails to detect it, we further assume that the missing alarm (MA) rate of the BDS-3 ground segment is 0.01. Thus, for the 24 MEOs and 3 IGSOs of BDS-3 (that is, the BDS-3 nominal constellation defined in ICAO SAPRs), the probabilities of these two anomalies can be determined as following:

$$P_{event_{1,2}} = \frac{0.5}{365 \times 24\,h \times 27} \times 0.01 = 2.1 \times 10^{-8}/h \tag{12}$$

where indices 1, 2 refer to the bottom events 1, 2 in the integrity risk tree.

2.　　Bottom events 3, 4, 5, and 6 anomaly probability

The IFMEA result shows that none of these four anomaly events occurred since 27 December 2018. According to the internal system design requirements of BDS-3, the probabilities of these four anomalies are all $1 \times 10^{-9}/h$, that is:

$$P_{event_{3,4,5,6}} = 1 \times 10^{-9}/h \tag{13}$$

where indices 3, 4, 5, 6 refer to the bottom events 3, 4, 5, 6 in the integrity risk tree.

3.　　Message upload anomaly

The IFMEA result shows that only one message upload anomaly event occurred since 27 December 2018, which was detected in time by the ground segment and did not affect the satellite SIS integrity. Therefore, the probability of occurrence of this anomaly can be assumed to be 1 time per year.

Still assuming that the MA rate of the BDS-3 ground segment is 0.01, the probability of such anomaly can be determined as following:

$$P_{event_9} = \frac{1}{365 \times 24\,h \times 27} \times 0.01 = 4.2 \times 10^{-8}/h \tag{14}$$

where index 9 refers to the bottom event 9 in Figure 1.

3.3. Design Values of P_{sat} and P_{const}

Table 5 shows the bottom event risk probability analysis results of the BDS satellite SIS integrity. The design value of P_{sat} is the sum of the design integrity risk probabilities of

all the bottom events in Table 3. For the B1I signal, the design P_{sat} is 0.9×10^{-5}/h; for the B1C and B2a signals, the design P_{sat} is 0.8×10^{-5}/h.

Table 5. Integrity risk of BDS SIS bottom event.

Bottom Events		Integrity Risk Probability
Satellite orbit calculation anomaly		2.1×10^{-8}/h
Satellite clock calculation anomaly		2.1×10^{-8}/h
Ephemeris fitting anomaly		1×10^{-9}/h
Orbit and time processing equipment anomaly		1×10^{-9}/h
Data input anomaly		1×10^{-9}/h
MS data anomaly		1×10^{-9}/h
Message upload anomalies		4.2×10^{-8}/h
Satellite clock anomaly	B1I	4×10^{-6}/h
	B1C, B2a	4×10^{-6}/h
Satellite signal and data	B1I	5×10^{-6}/h
anomaly	B1C, B2a	4×10^{-6}/h

For the BDS constellation service failure, the bottom events include the Earth orientation parameters (EOPs) determination or prediction abnormality, the MS antenna phase center deviation, the MS hardware/software failure, the MCS hardware/software failure, the satellite orbit and clock calculation parameter failure, and the satellite design defects, etc.

Investigating the operation status of BDS-3 in 2019 revealed that no constellation service failure event occurred. In this paper, we make assumptions and conservative estimates. Assuming that the system has 0.5 constellation service failure events since 27 December 2018, then P_{const} can be estimated according to Equation (8) as following [27,28]:

$$P_{const} = \frac{0.5 \cdot 1 \text{ h}}{365 \cdot 24 \text{ h}} = 5.7 \times 10^{-5} \approx 6 \times 10^{-5} \tag{15}$$

where 1 h is the assumed MTTN.

4. Risk Prevention and Control

In order to reduce the risk probability of the integrity bottom events, it is necessary to take corresponding preventive and control measures in the system. This section introduces the failure/risk prevention and control measures taken in BDS-3 satellites and ground facilities, which mainly focus on software/hardware redundancy backup and signal/information monitoring and verification.

4.1. Space Segment Measures

From the analysis in Section 3, it can be seen that the space segment is the part with the highest probability of BDS integrity risk. This is due to the complexity of the space environment in which the navigation satellite is located and the difficulty of operation caused by being far from the ground.

The BDS-3 satellite downlink navigation payload includes the time and frequency system, navigation signal generation, navigation signal broadcast, and antenna. In order to cope with possible integrity risks in the space segment, BDS-3 satellites have taken corresponding measures in various aspects.

To prevent the satellite clock anomaly (Event 8 in Figure 1), each satellite is equipped with multiple on-board atomic clocks, one of which is selected by the reference frequency synthesizer as the working clock, and the others as backups. The structure is shown in Figure 2, in which the 10 MHz signal is the standard output frequency of the atomic clock, and the 10.23 MHz signal for the working and standby circuits is generated by the frequency synthesizer. When an abnormality occurs in the working clock, the measurement and fault detection module of the reference frequency synthesizer detects the abnormality

in time and switches the output frequency to the hot standby circuit. To ensure a smooth signal transition before and after the switchover, the measurement and fault detection module synchronizes the frequency and phase of the 10.23 MHz signals of the hot standby and working circuits by means of a precision tracking algorithm, so that they remain synchronized at any time and the frequency and phase of the output signal can remain unchanged after the switchover.
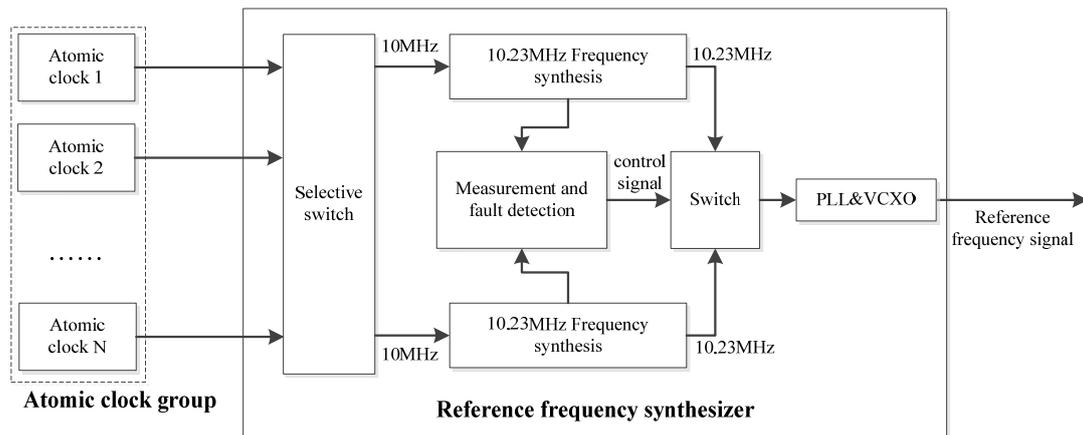

Figure 2. Anomaly monitoring and redundant switching structure of atomic clocks for BDS-3 satellites.

To prevent the satellite signal and data anomaly (Event-7 in Figure 1), each satellite has a fault-proof design for the navigation signal generation and broadcast process, as shown in Figure 3. In the digital intermediate frequency (IF) signal generation module, full triple modular redundancy (TMR) is designed for its look-up tables, registers, and processing modules, and a dedicated anti-fuse Field Programmable Gate Array (FPGA is used to refresh the TMR data at regular intervals to prevent single event upsets. For B1I, B1C, and B2a signals, the satellite has the ability to monitor and handle faults of relevant equipment on the broadcast channel, such as frequency modulators and power amplifiers, and switch to the other channel when a fault occurs in one path.
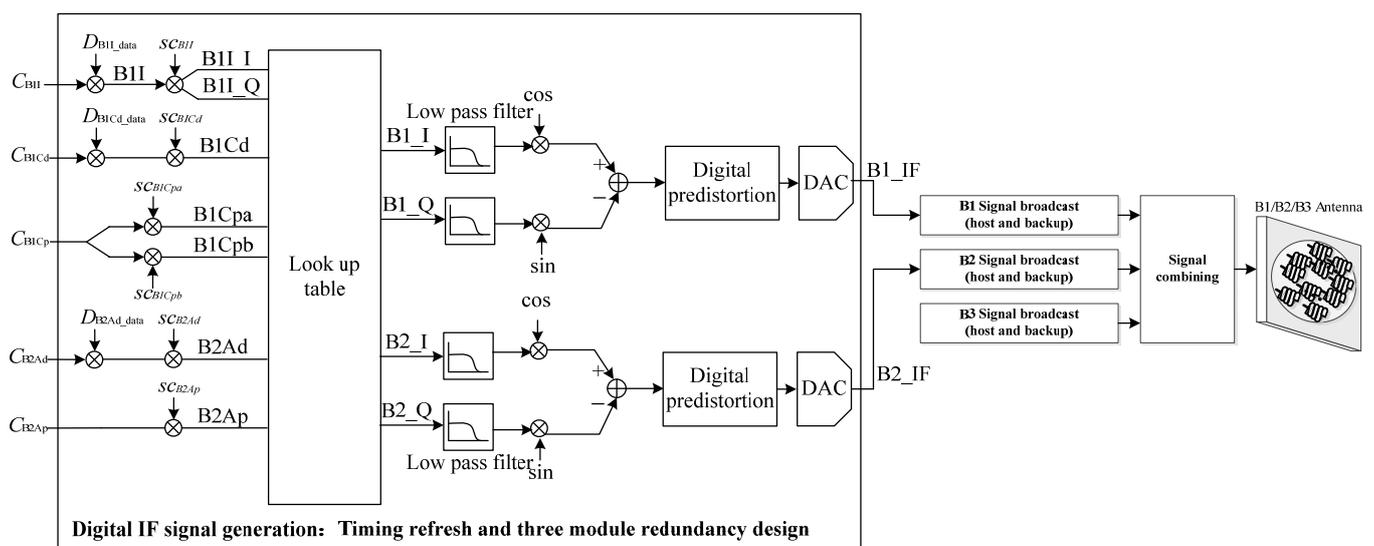

Figure 3. Fault prevention design of BDS-3 satellite signal generation and broadcasting.

4.2. Ground Segment Measures

Although the risk probability of the ground segment is very low, once it occurs, it easily causes serious consequences and becomes the "gray rhino" in system operation and service. For example, the Galileo offline event of 2019 mentioned above was precisely caused by the "ground technology failure" according to the EUROPEAN GNSS AGENCY (GAS). More specifically, it is confirmed to be related to the abnormal behavior of a ground atomic clock in the time determination function of the system [30,31]. Therefore, it is very necessary to strengthen the prevention and control on the ground section.

The composition of the BDS-3 ground segment and its processing flow can be simplified shown in Figure 4. In order to deal with possible integrity risks, BDS-3 has taken corresponding measures in each processing link:

- To prevent the MS data anomaly (Event 6 in Figure 1), each MS is equipped with multiple monitoring receivers and atomic clocks to achieve redundancy.
- To prevent the navigation message upload anomaly (Event-9 in Figure 1), one measure is to implement a mutual backup strategy for the uplink station (ULS) antennas to prevent hardware failures; the other is to set up the monitoring function points before uploading and retrieving the navigation messages, respectively (see point a and point *h* in Figure 4).
- To prevent the satellite orbit calculation anomaly, the satellite clock calculation anomaly, and the ephemeris fitting anomaly (Events 1–3 in Figure 1), one measure is that the data processing center (DPC) has multiple channels for data calculation and generation, and they are independent of each other; the other is that the master control station (MCS) will check the correctness and validity of the products sent from the DPC.
- To prevent the orbit and time processing equipment anomaly (Event 4 in Figure 1), one measure is that the system is running both the main DPC and the backup DPC online at the same time; the other is that each DPC is equipped with multiple processing equipment to achieve redundancy.
- To prevent the data input anomaly (Event 5 in Figure 1), for all the aspects of data transmission involved in ground segment facilities, the monitoring function points are set up before data transmission and after data reception (see point *b* to point *g* in Figure 4).
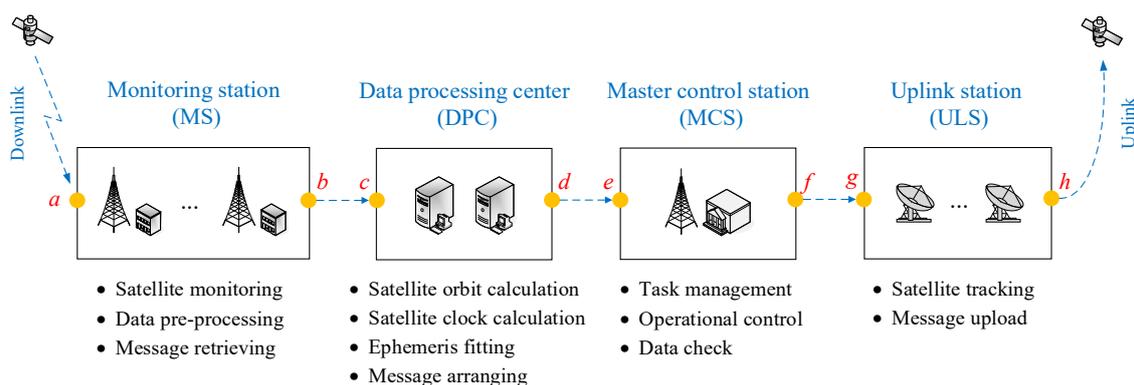

Figure 4. Information processing and fault monitoring of BDS-3 ground section. The yellow points a to h represent the fault monitoring function points in the ground segment.

In addition, BDS-3 also introduces a third-party external monitoring system independent of its own ground segment, such as the international GNSS monitoring and assessment system (iGMAS), commercial receivers, and FPGA verification terminals to conduct continuous and real-time monitoring and evaluation of satellite SIS and messages. When an anomaly is found, these external systems will notify the MCS via a rapid alarm mechanism (for example, a private network).

5. Results and Discussion

From 27 December 2018, BDS-3 has completed the construction of the basic constellation and started the initial open service (OS). The integrity risk requirements design and verification work completed by BDS-3 in the latest draft of ICAO SARPs is based on the actual operation of the system in 2019. Therefore, we correspondingly use the system data of 2019 for testing and analysis in this paper.

5.1. Test Results for B1I Signal

The SIS-URE of the B1I signal at the WUL is calculated based on the B1I broadcast message from 7 January 2019 to 31 July 2019, with a sampling interval of 30 s. The URE sequence of the 18 satellites of the basic BDS-3 constellation are shown in Figure 5, in which the red dots indicate the URE value. The x-axis is in units of days of the year, and the y-axis is in meters.

(a)

(b)

(c)
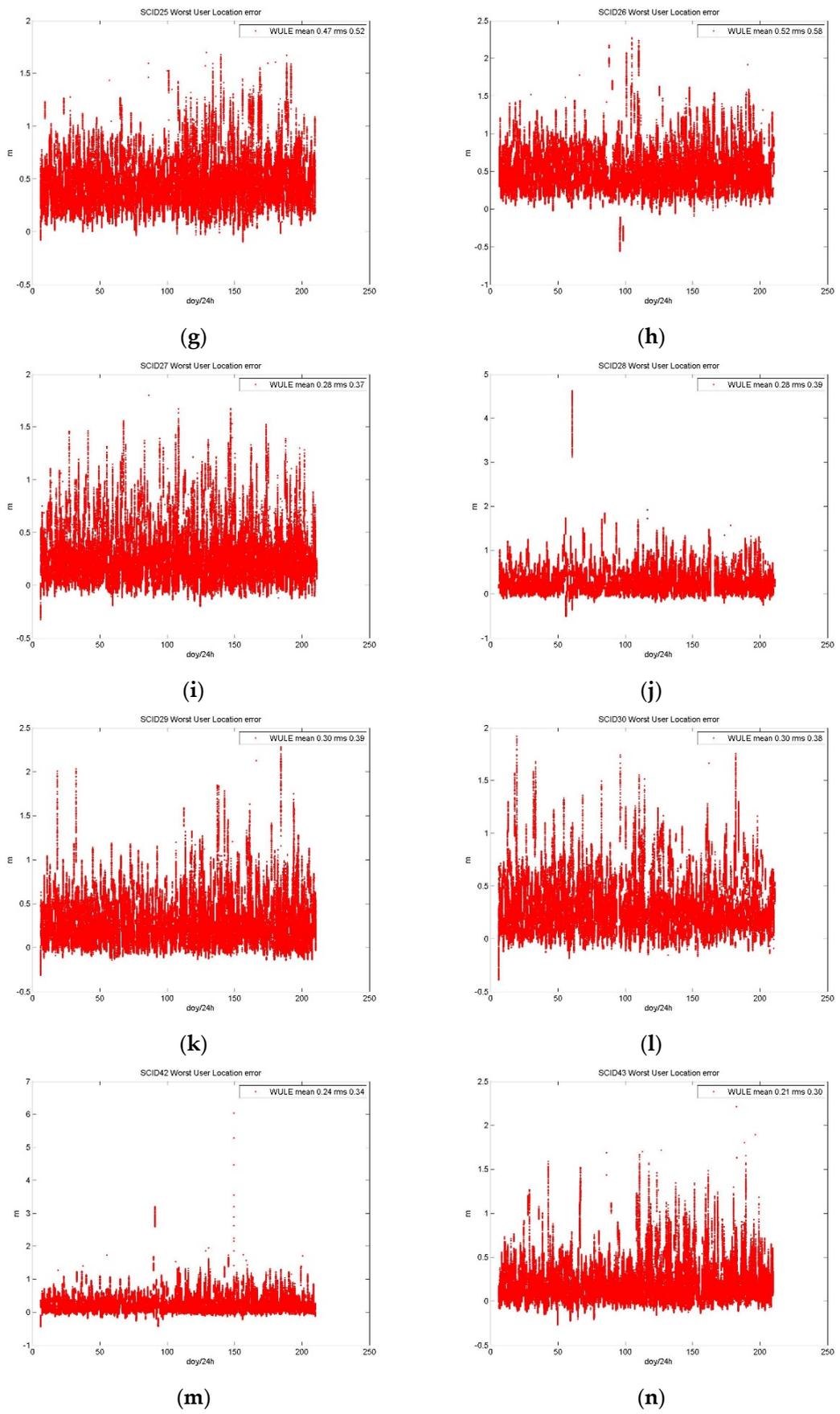
(d)

(e)

(f)

Figure 5. *Cont.*

(**g**)

(**h**)

(**i**)

(**j**)

(**k**)
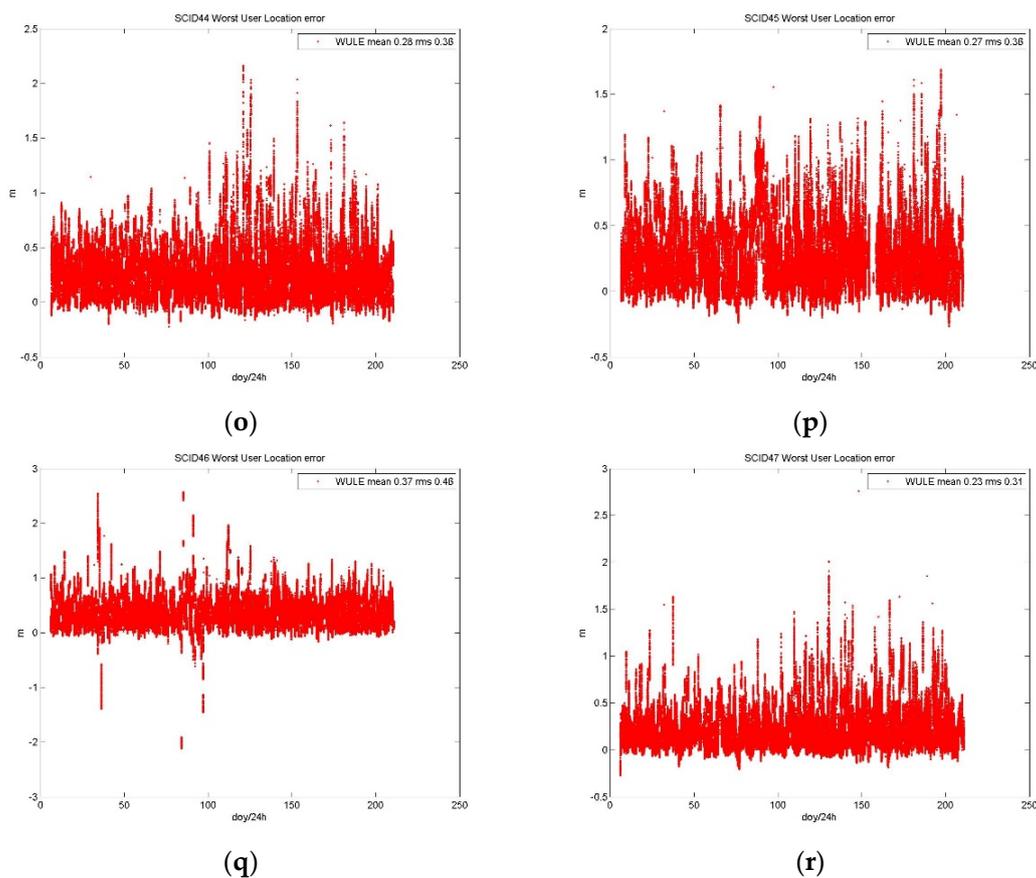

(**l**)

(**m**)

(**n**)
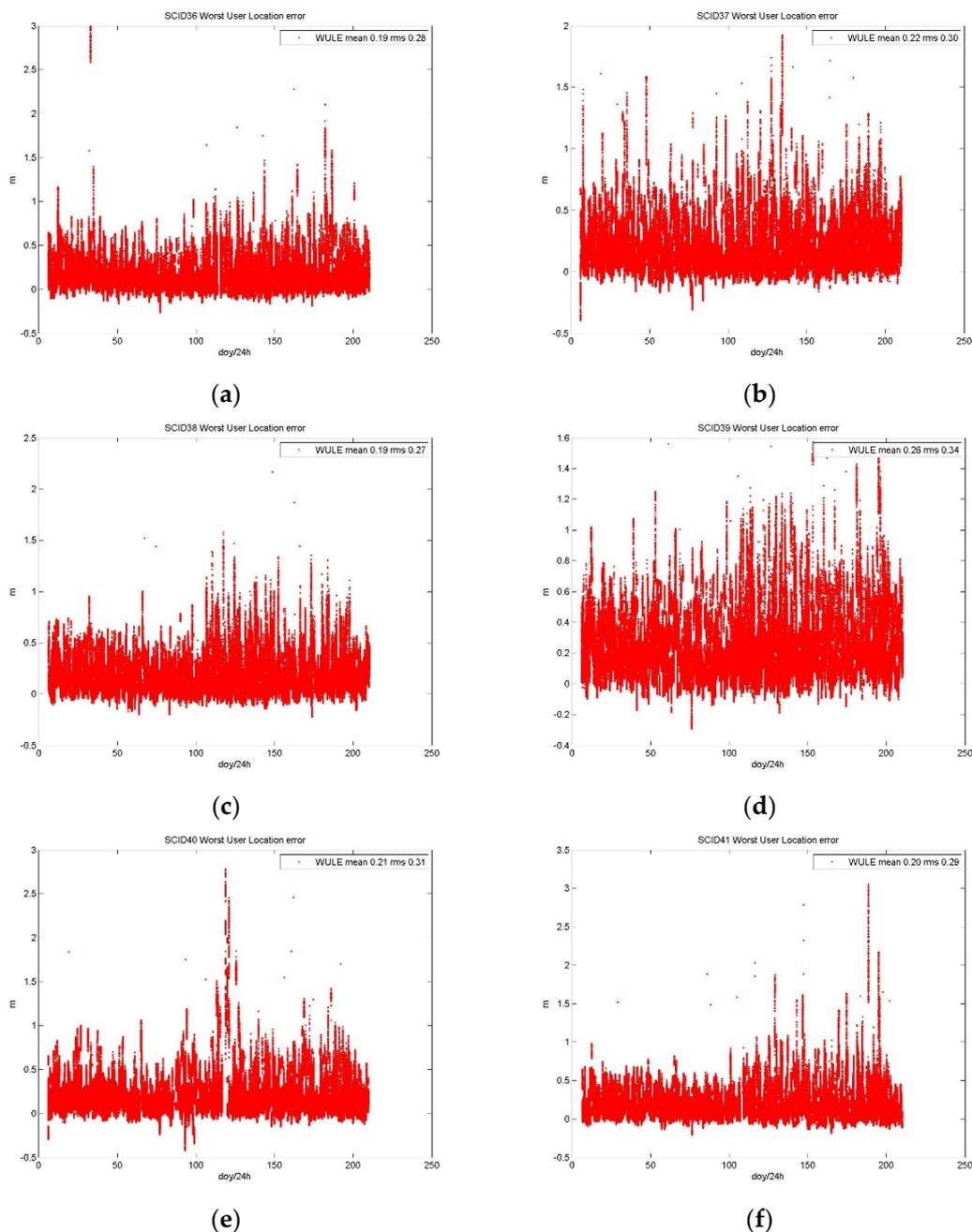
Figure 5. *Cont.*

Figure 5. URE and 4.42 × URA sequences of BDS-3 satellites form 1 January 2019 to 31 July 2019. (**a**) PRN 19; (**b**) PRN 20; (**c**) PRN 21; (**d**) PRN 22; (**e**) PRN 23; (**f**) PRN 24; (**g**) PRN 25; (**h**) PRN 26; (**i**) PRN 27; (**j**) PRN 28; (**k**) PRN 29; (**l**) PRN 30; (**m**) PRN 32; (**n**) PRN 33; (**o**) PRN 34; (**p**) PRN 35; (**q**) PRN 36; (**r**) PRN 37. SCID + Number in the titles of figures indicate the Satellite Configure Index used by the internal information processing system.

According to Section 2.3.1, the URE of B1I should be compared with the NTE, which is 4.42 times the URA. The URA can be obtained through the user range accuracy index (URAI) parameters broadcast in the D1 NAV message of B1I, and 4.42 times the URA is currently a fix value equal to 17.68 m. It can be seen from Figure 5 that the URE of all satellites are far less than 4.42 times the URA (among them, the largest URE appears in the satellite with a PRN code of 32, which is about 6 m). Therefore, there is no satellite service failure condition of the B1I signal during the test.

5.2. Test Results for B1C and B2a Signals

The SIS-URE of the B1C/B2a signal at the WUL is calculated based on the B1C/B2a broadcast message from 1 July 2019 to 25 September 2019, with a sampling interval of 30 s. The URE sequence of the 18 satellites of the basic BDS-3 constellation are shown in Figure 6, in which the red dots indicate the URE value and the black dots indicate the SISA value. The x-axis is in units of days of the year, and the y-axis is in meters.
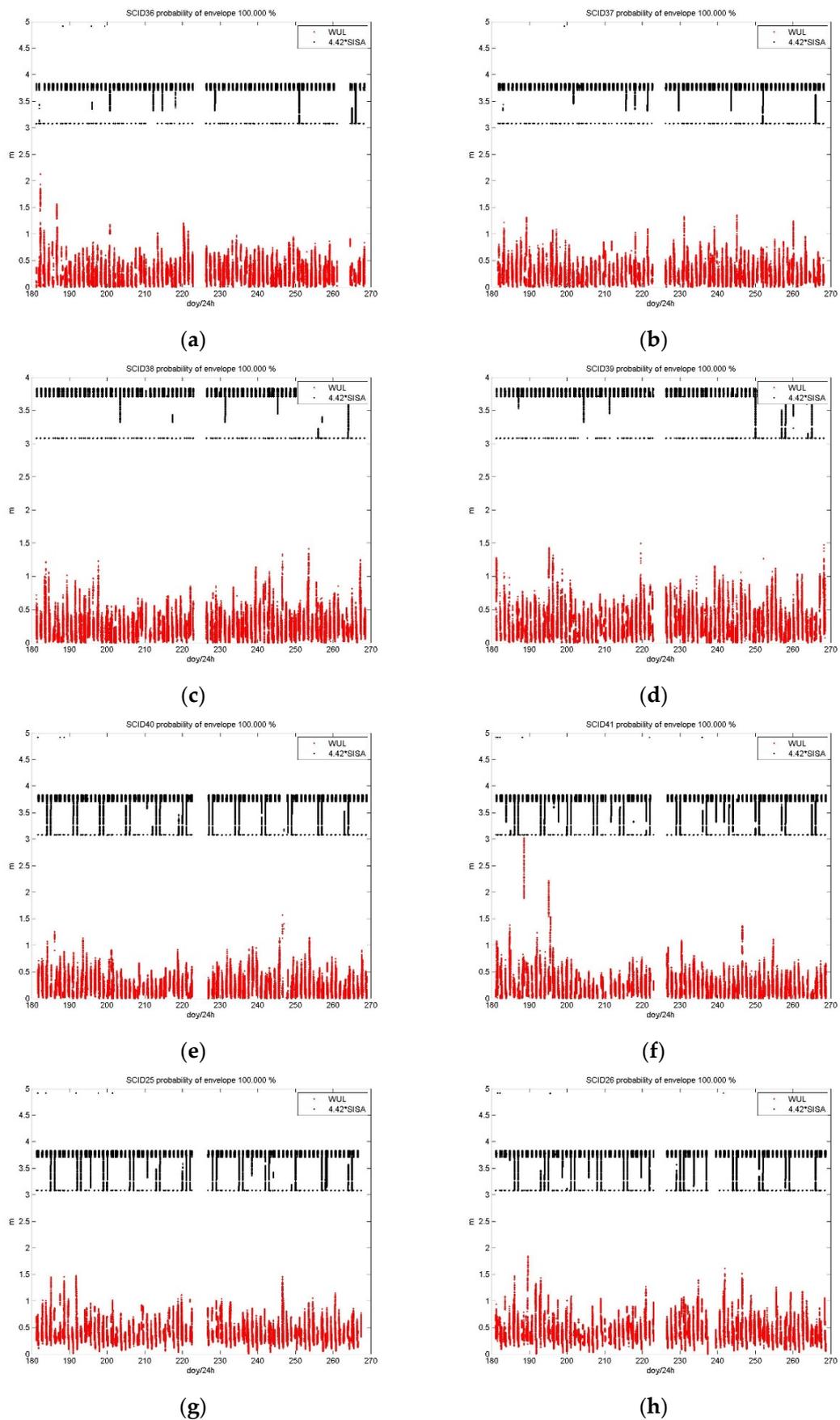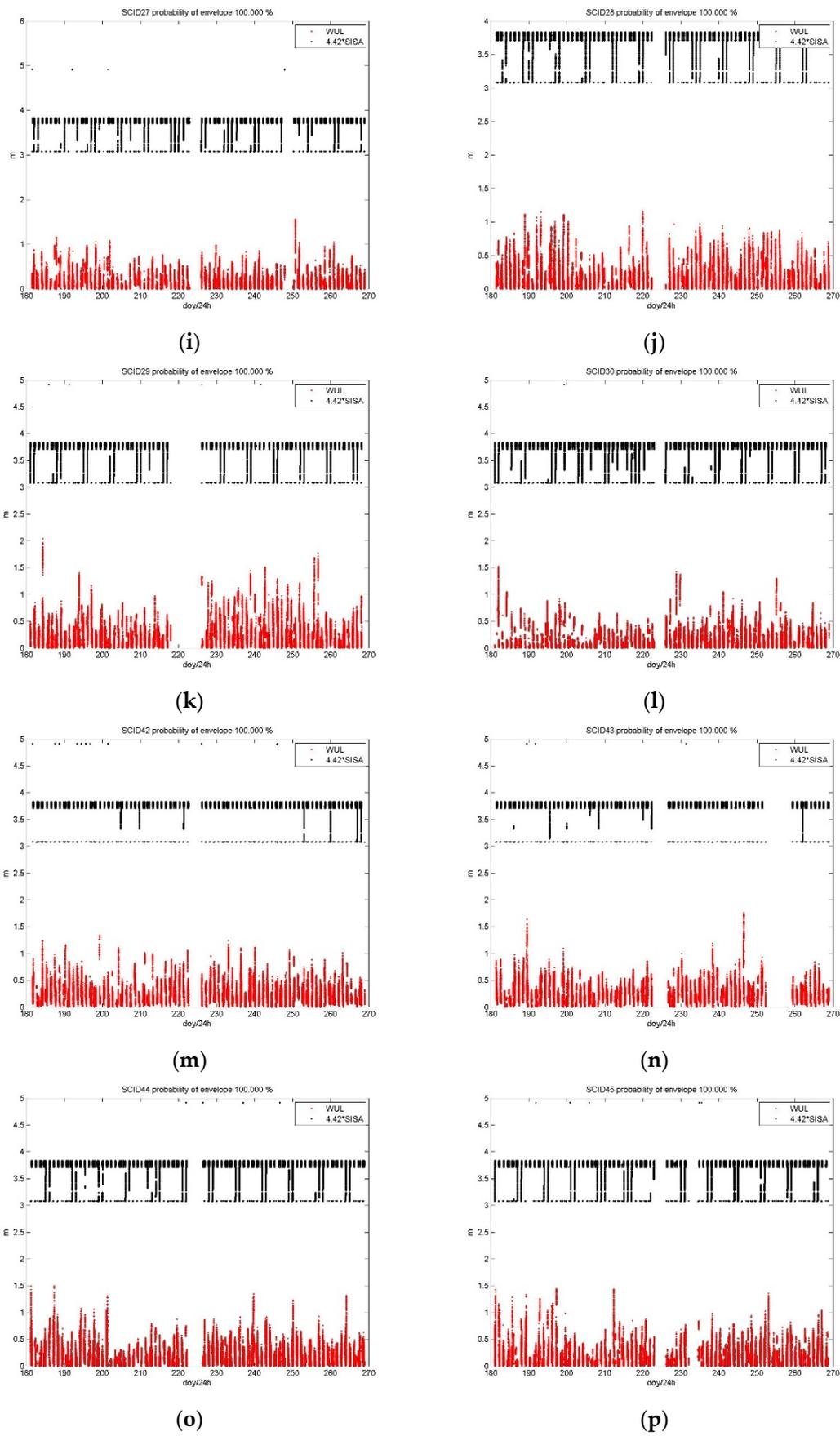
(**a**)

(**b**)

(**c**)

(**d**)

(**e**)

(**f**)

(**g**)

(**h**)

Figure 6. *Cont.*

(**i**)

(**j**)

(**k**)

(**l**)

(**m**)

(**n**)

(**o**)

(**p**)

Figure 6. *Cont.*

(q)   **(r)**
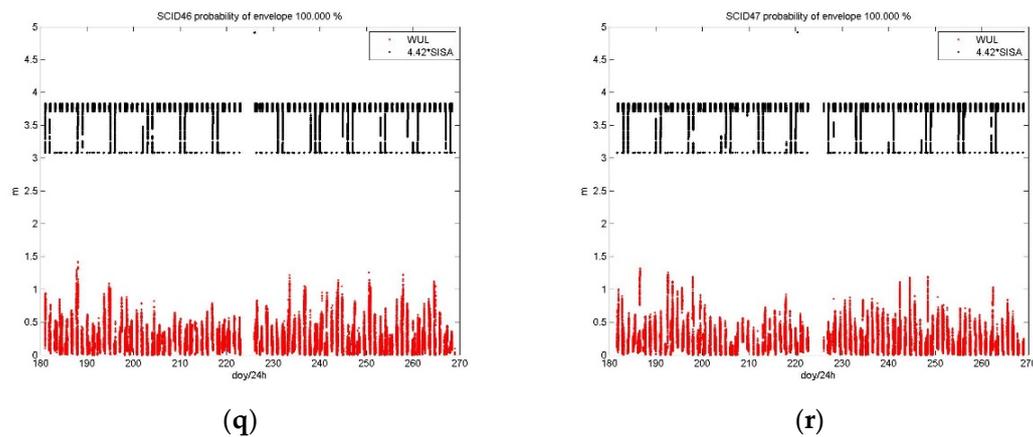
Figure 6. URE and 4.42 × SISA sequences of BDS-3 satellites from 1 July 2019 to 25 September 2019. (**a**) PRN 19; (**b**) PRN 20; (**c**) PRN 21; (**d**) PRN 22; (**e**) PRN 23; (**f**) PRN 24; (**g**) PRN 25; (**h**) PRN 26; (**i**) PRN 27; (**j**) PRN 28; (**k**) PRN 29; (**l**) PRN 30; (**m**) PRN 32; (**n**) PRN 33; (**o**) PRN 34; (**p**) PRN 35; (**q**) PRN 36; (**r**) PRN 37.

According to Section 2.3.1, the URE of B1C/B2a should be compared with the NTE, which is 4.42 times the SISA. The SISA can be obtained through the SISAI parameters broadcast in the B-CNAV1/B-CNAV2 navigation message, and its value may change with the change of the index parameters. It can be seen that the URE of all satellites are less than 4.42 times the SISA, and there is no satellite service failure condition of B1C and B2a signals during the test.

In fact, there have been satellite orbit calculation and message upload anomalies in the ground segment during the assessment period, but they are detected and disposed of by the ground segment monitoring measures. This indicates the effectiveness of the fault monitoring and processing functions of the BDS-3 ground segment. We also need to be aware that the assessment of GNSS service integrity is a long-term and elaborate process. As long as the time is long enough, any potential risks that seem to have a small probability might happen. Therefore, we will continuously evaluate and analyze the integrity of the BDS-3 OS signals, and release the information and status in time. In addition, we will also work to further improve the robustness of the BDS-3 satellite and ground segment to ensure the stable operation of the system and the safe and reliability of the service.

6. Conclusions

This contribution focuses on the integrity concept design and construction of China's BDS-3. Both the B1I signal and the B1C/B2a signal of BDS-3 have integrity functions. Among them, the B1I signal uses 4.42 times the URE as the NTE, and uses the SatH1 parameter in the D1 navigation message as the health status indicator; the B1C/B2a signal uses 4.42 times the SISA as the NTE, and uses the HS, SIF, and DIF parameters in the B-CNAV1/B- CVNV2 navigation message as the health status indicators. According to the nine integrity risk bottom events in the BDS-3 satellite SIS fault tree model, the P_{sat} design values of the B1I and B1C/B2a signals are analyzed and determined to be 0.9×10^{-5} and 0.8×10^{-5}, respectively, which both meet the ICAO's performance requirement for the en-route flight operation (less than 1×10^{-5}). The P_{const} design value of BDS-3 is 6×10^{-5}.

The integrity function of BDS-3 has two approaches, the ground monitoring and alarm, and the satellite monitoring and alarm, and the design TTA can reach 60 s and 6 s/300 s, respectively. Among them, the 6s rapid alert mechanism relies on the SAIM function, and BDS is still working hard to realize this capability as soon as possible.

The integrity risk analysis and verification results show that the actual operation of the system is consistent with the conceptual design requirement, and it satisfies the integrity performance promised by BDS-3 in the ICAO SAPRs. The performance of the system in actual operation and service proved the effectiveness of the BDS-3 integrity concept design and system prevention and control measures.

References

1. Blomenhofer, H.; Ehret, W.; Blomenhofer, E. Performance Analysis of GNSS Global and Regional Integrity Concepts. In Proceedings of the ION GPS/GNSS 2003, Portland, OR, USA, 9–12 September 2003; pp. 991–1001.
2. Hernández, C.; Catalán, C.; Martínez, M.A. Galileo Integrity Concept and its Applications to the Maritime Sector. *Int. J. Mar. Navig. Saf. Sea Transp.* **2009**, *3*, 287–291.
3. Robustelli, U.; Baiocchi, V.; Pugliano, G. Assessment of Dual Frequency GNSS Observations from a Xiaomi Mi 8 Android Smartphone and Positioning Performance Analysis. *Electronics* **2019**, *8*, 91. [CrossRef]
4. Jiménez-Martínez, M.J.; Farjas-Abadia, M.; Quesada-Olmo, N. An Approach to Improving GNSS Positioning Accuracy Using Several GNSS Devices. *Remote Sens.* **2021**, *13*, 1149. [CrossRef]
5. GPS. WAAS, Resiliency and Outreach. Available online: https://www.gps.gov/multimedia/presentations/2018/10/APEC/alexander-2.pdf (accessed on 15 June 2021).
6. ICAO. WAAS Development Changes since Commissioning. Available online: https://www.icao.int/APAC/APAC-RSO/GBASSBAS%20Implementation%20Workshop/1-4_WAAS_Development_Changes_Since_Commissioning_final%20(T%20Schemmp).pdf (accessed on 15 June 2021).
7. ICAO. EGNOS Status 3 June 2019. Available online: https://www.icao.int/APAC/APAC-RSO/GBASSBAS%20Implementation%20Workshop/1-5_EGNOS%20Status_final%20(G%20COMELLI).pdf (accessed on 15 June 2021).
8. ICAO. EGNOS Status and Plans. Available online: https://www.icao.int/MID/Documents/2016/ACAC-ICAO%20GNSS/EC%20Rabat%20EGNOS%20status%20and%20plans_final.pdf#search=EGNOS (accessed on 15 June 2021).
9. Sakai, T.; Tashiro, H. MSAS Status. In Proceedings of the ION GNSS+ 2013, Nashville, TN, USA, 16–17 September 2013; pp. 2343–2360.
10. ICAO. MSAS System Development. Available online: https://www.icao.int/APAC/APAC-RSO/GBASSBAS%20Implementation%20Workshop/1-6_MSAS%20System%20Development_Rev2%20(S%20Saito).pdf (accessed on 15 June 2021).
11. Liu, C.; Gao, W.; Shao, B.; Lu, J.; Wang, W.; Chen, Y.; Su, C.; Xiong, S.; Ding, Q. Development of BeiDou Satellite-Based Augmentation System. *Navigation* **2021**, *68*, 405–417. [CrossRef]
12. Medel, C.H.; Catalán, C.C.; Vidou, M.A.F.; Pérez, E.S. The Galileo Ground Segment Integrity Algorithms: Design and Performance. *Int. J. Navig. Obs.* **2008**, 1–16. [CrossRef]
13. Blomenhofer, H.; Ehret, W.; Leonard, A.; Blomenhofer, E. GNSS/Galileo Global and Regional Integrity Performance Analysis. In Proceedings of the ION GNSS 2004, Long Beach, CA, USA, 21–24 September 2004; pp. 2158–2168.
14. Werner, W.; Zink, T.; Lohnert, E.; Pielmeier, J. GALILEO Integrity Performance Assessment (GIPA). In Proceedings of the ION GPS 2001, Salt Lake City, UT, USA, 11–14 September 2001; pp. 1838–1849.
15. Cabinet Office. Quasi-Zenith Satellite System Performance Standard (PS-QZSS-001). Available online: https://qzss.go.jp/en/technical/download/pdf/ps-is-qzss/ps-qzss-001.pdf (accessed on 15 June 2021).
16. Cabinet Office. Quasi-Zenith Satellite System Interface Specification Centimeter Level Augmentation Service (IS-QZSS-L6-001). Available online: https://qzss.go.jp/en/technical/download/pdf/ps-is-qzss/is-qzss-l6-001.pdf (accessed on 15 June 2021).
17. GPS. Galileo and Its Outage in July 2019 from the IGS-MGEX Perspective. Available online: https://www.gps.gov/governance/advisory/meetings/2019-11/beutler.pdf (accessed on 15 June 2021).
18. GSA. Update on the Availability of Some Galileo Initial Services. Available online: https://www.gsc-europa.eu/news/update-on-the-availability-of-some-galileo-initial-services (accessed on 15 June 2021).
19. CSNO. The Application Service Architecture of BeiDou Navigation Satellite System (Version 1.0). Available online: http://en.beidou.gov.cn/SYSTEMS/Officialdocument/201812/P020181227424526837905.pdf (accessed on 15 June 2021).
20. Xinhua Net. Update: Xi Officially Announces Commissioning of BDS-3 Navigation System. Available online: http://www.xinhuanet.com/english/2020-07/31/c_139255481.htm (accessed on 15 June 2021).
21. ICAO. *International Standards and Recommended Practices (SARPs) Annex 10—Aeronautical Telecommunications*, 7th ed.; ICAO: Montreal, QC, Canada, 2018; Volume I.
22. CSNO. BeiDou Navigation Satellite System Open Service Performance Standard (Version 2.0). Available online: http://en.beidou.gov.cn/SYSTEMS/Officialdocument/ (accessed on 15 June 2021).

23. CSNO. BeiDou Navigation Satellite System Signal in Space Interface Control Document Open Service Signal B1I (Version 3.0). Available online: http://en.beidou.gov.cn/SYSTEMS/Officialdocument/201902/P020190227601370045731.pdf (accessed on 15 June 2021).

24. CSNO. BeiDou Navigation Satellite System Signal in Space Interface Control Document—Open Service Signal B1C (Version 1.0). Available online: http://en.beidou.gov.cn/SYSTEMS/Officialdocument/202008/P020200803544809266816.pdf (accessed on 15 June 2021).

25. CSNO. BeiDou Navigation Satellite System Signal in Space Interface Control Document—Open Service Signal B2a (Version 1.0). Available online: http://en.beidou.gov.cn/SYSTEMS/Officialdocument/201806/P020180608525870555377.pdf (accessed on 15 June 2021).

26. Brieden, P.; Wallner, S.; Canestri, E. Galileo Characterization as Input to H-ARAIM and SBAS DFMC. In Proceedings of the ION GNSS+ 2019, Miami, FL, USA, 16–20 September 2019; pp. 2819–2841.

27. Todd, W.; Juan, B.; Mathieu, J.; Boris, P. Determination of fault probabilities for ARAIM. In Proceedings of the IEEE/Institute Navigation Position, Location and Navigation Symposium, Savannah, GA, USA, 11–14 April 2016; pp. 451–461.

28. Todd, W.; Juan, B.; Kazuma, G.; Mathieu, J.; Boris, P. Determination of Fault Probabilities for ARAIM. *IEEE Trans. Aerosp. Electron. Syst.* **2019**, *55*, 3505–3516. [CrossRef]

29. Sun, S.; Wang, Z. Signal-In-Space Accuracy research of GPS/BDS in China region. In Proceedings of the CSNC 2016, Changsha, China, 18–20 May 2016; pp. 235–245. [CrossRef]

30. CNN. Europe's Version of GPS Suffers Major Outage. Available online: https://edition.cnn.com/2019/07/15/tech/galileo-gnss-outage-intl/index.html (accessed on 15 June 2021).

31. GSA. Further Information on the Event of 14th December. Available online: https://www.gsc-europa.eu/news/further-information-on-the-event-of-14th-december (accessed on 15 June 2021).