

Satellite Navigation Technology

Hui Yang
Haitao Zhao

Reliability Engineering of BeiDou Navigation Satellite



國防工業出版社
National Defense Industry Press



Springer

Satellite Navigation Technology

Series Editors

Yuanxi Yang, Beijing, China


Baoguo Yu, Anhui, China

The series focuses on the development of the Beidou Navigation Satellite System in China, summarizes the cutting-edge key technologies and engineering research achievements in the field of satellite navigation in China in recent years, absorbs the latest cutting-edge technologies in relevant fields at home and abroad, and strives to reflect new perspectives, new trends, and new academic levels in this field, as well as innovative achievements in the field of engineering technologies of Beidou Navigation Satellite System.

The series is divided into four series in terms of content: First, satellite navigation system technology, which focuses on the principles, signal design, precise orbit determination, timing, and verification of Beidou navigation satellite system; The second is satellite navigation equipment technology, which includes precise time transmission, integrated positioning and attitude determination, system reliability assurance, and digital multi beam measurement; The third is satellite navigation testing and evaluation technology, which mainly describes satellite navigation system engineering testing and receiver testing technology; Fourth, satellite navigation augmentation and application technology, including satellite navigation applications in land transportation, maritime navigation, air traffic management, and other aspects.

Hui Yang · Haitao Zhao

Reliability Engineering of BeiDou Navigation Satellite

 国防工业出版社
National Defense Industry Press

 Springer

Hui Yang
China Academy of Space Technology
Beijing, China

Haitao Zhao
China Academy of Space Technology
Beijing, China

ISSN 2948-2267

ISSN 2948-2275 (electronic)

Satellite Navigation Technology

ISBN 978-981-99-9129-7

ISBN 978-981-99-9130-3 (eBook)

<https://doi.org/10.1007/978-981-99-9130-3>

Jointly published with National Defense Industry Press

The print edition is not for sale in China (Mainland). Customers from China (Mainland) please order the print book from: National Defense Industry Press.

© National Defense Industry Press 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publishers, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publishers nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publishers remain neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.

The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Paper in this product is recyclable.

Preface

BeiDou Navigation Satellite System (BDS) is one of the four major navigation systems in the world today, including the Global Positioning System (GPS) of the USA, the Global Navigation Satellite System (GLONASS) of Russia, and the Galileo system of the European Union. Navigation satellite system can send all-time, all-weather, and high-accuracy positioning, navigation, and timing information. It is an indispensable important space infrastructure for today's national economy and national defense construction.

China's BDS has been implemented step by step according to the general idea of "first regional, then global, first active, and then passive", forming a distinctive BDS development path that highlights the region and faces the world. BDS-1 started construction in 1994 and was completed in 2003. BDS-2 started construction in August 2004 and was completed in December 2012. BDS-2 is compatible with BDS-1 radio determination satellite service (RDSS) and provides passive navigation and positioning services to China and surrounding areas. At present, China has completed the construction of BDS-3, which is composed of 30 hybrid orbit satellites and a ground system. Twenty-four medium earth orbit (MEO) satellites adopt the Walker 24/3/1 constellation configuration, three geostationary orbit (GEO) satellites, and three inclined geosynchronous orbit (IGSO) satellites.

The BDS project is the first large-scale networking satellite system in China. Compared with previous spacecraft development missions, navigation satellites have typical characteristics such as high reliability and availability requirements, difficulty in ensuring product consistency, and high risk of satellite batch launch. BeiDou navigation satellite is also the first batch production spacecraft project in China. Compared with the development of a single spacecraft, the batch production of navigation satellites has the characteristics of multi-satellite compatible design, multi-satellite parallel development, complex system state, large impact of technology change, cross-overlap of verification, and so on. These characteristics of the BeiDou navigation satellite project pose a great challenge to the development.

High reliability is of great significance for navigation satellites. On the one hand, the risk caused by the design and process defects of a single satellite has doubled. The

failure of a single satellite will lead to the change of all other navigation satellites and may delay the launch, which is an unacceptable risk for the constellation construction. On the other hand, during the on-orbit operation of the constellation, even if the failure lasts only a few minutes, it may lead to a decline in navigation performance or even an outage of service. Therefore, compared with other spacecraft, it also puts forward the requirements of “availability” and “continuity”, which raises new questions about the reliability work we previously knew. During the implementation of BeiDou navigation satellite project, the development team planned and performed a series of reliability work according to the basic methods of reliability engineering and closely combined with the characteristics of navigation satellites, created the reliability and availability evaluation indices of the BeiDou navigation satellite, expanded the reliability work items and connotation of spacecraft, proposed and implemented a set of effective reliability and availability design methods, and realized the goal of successful construction, continuous and stable operation of China’s regional navigation system. The indices and methods have been further verified and improved in the design and implementation of the BDS-3 space segment.

In recent decades, the research on reliability has developed rapidly. From reliability mathematics, failure physics to reliability tests and other fields, new technologies and methods continue to emerge, and a large number of theoretical and methodological books have been published. However, there are few reference books on the reliability engineering methods and practices based on engineering projects. How to apply the basic theory and method of reliability, effectively carry out reliability work according to the characteristics of the projects, and ensure that the requirements of long life and high reliability can be met “fast, well, and economically” is the key problem that every spacecraft project must face. Because it is difficult to carry out quantitative verification of the reliability indices with high confidence on the ground, qualitative means such as reliability design and analysis are usually used to ensure that satellite reliability meets the requirements, which poses a great challenge to the implementation of satellite reliability engineering. This book gives the effective ways and experience of the application of reliability theory and methods in satellite practical engineering, to promote the development of spacecraft reliability engineering and the related reliability work of other aerospace products.

This book covers the reliability and availability requirements, reliability management, reliability and availability design, reliability and availability analysis, reliability process control, reliability test and verification, and other aspects of the development process of BeiDou navigation satellites from project approval to satellite delivery. From the perspective of reliability in a broad sense, this book incorporates the work related to availability. At the same time, this book includes reliability indices and analysis work at the constellation level. There are 10 chapters in the book: Chap. 1 is the introduction, which introduces the characteristics of navigation satellite engineering and the particularity of navigation satellite reliability work; Chap. 2 describes the determination of the reliability and availability requirements of navigation satellites; Chap. 3 describes the methods and implementation cases of reliability modeling and prediction of navigation satellites; In Chap. 4, from the perspective of availability, according to the typical characteristics of high

requirements for continuity and availability of navigation satellites, the design methods and experience related to availability are described; Chap. 5 introduces the modeling and analysis of the availability of navigation satellites and constellation; Chap. 6 introduces the work of navigation satellite in redundancy design, environmental adaptability design, and other designs from the perspective of long life and high reliability; Chap. 7 introduces the reliability analysis of navigation satellite, including failure mode and effect analysis (FMEA), fault tree analysis (FTA), sneak circuit analysis (SCA), etc.; in Chap. 8, the methods and experience of reliability assurance in the batch production process are described; Chap. 9 describes the methods and implementation of reliability development test, life test, screening, and verification of navigation satellites; Chap. 10 introduces the reliability management work of navigation satellite, such as the planning, review, monitoring, etc.

This book is mainly written by Yang Hui and Zhao Haitao. Also participating in the writing of this book are Li Haisheng (Sects. 2.1 and 5.4), Xiong Xiao (Sects. 3.2, 4.3.3, 6.1 and 7.3), Zheng Yuzhan (Sects. 4.3.1 and 4.3.2), Zhu Jiantao (Sects. 6.3 and 9.3), Hu Yanqi (Sect. 6.5), Xu Hao (Sects. 7.4 and 7.5), Dong Fangcheng (Sects. 10.4 and 10.5). This book is mainly translated by the original author. Also participating in the translation of this book are Zhang Meng (Chap. 8) and Chen Lei (Sect. 2.1).

Thanks for the strong support given by Beijing Institute of Spacecraft System Engineering, China Academy of Aerospace Standardization and Product Assurance, and National Defense Industry Press during the preparation and publication of this book. Thank academician Yang Yuanxi for his guidance in this book. Thank research fellows Xie Jun, Yu Jin, Gu Yan, and Liu Zhiqian for their valuable comments and suggestions on this book. The book cites some examples from the BeiDou navigation satellite project, and we would like to thank the designers concerned.

The contents of this book inevitably have omissions or improprieties. We earnestly request experts, scholars in relevant fields, and readers to criticize and correct.

Beijing, China

Hui Yang
Haitao Zhao

Contents

1	Introduction	1
1.1	Reliability Engineering	1
1.2	BeiDou Navigation Satellite Engineering	4
1.2.1	BeiDou Navigation Satellite System	4
1.2.2	BeiDou Navigation Satellites	5
1.3	Reliability Engineering of BeiDou Navigation Satellite	7
1.3.1	Reliability Work Needs of BeiDou Navigation Satellite	7
1.3.2	Reliability Practice of BeiDou Navigation Satellite	9
1.4	Scope and Content of This Book	10
2	Reliability Requirements	15
2.1	Service Reliability of Navigation Constellation	15
2.1.1	Concept and Connotation of Service Reliability	15
2.1.2	Decomposition of Service Reliability	19
2.2	Quantitative Requirements for Navigation Satellite Reliability	25
2.2.1	General Reliability Parameters of Satellite	25
2.2.2	Reliability Parameters of BeiDou Satellite	27
2.2.3	Reliability Demonstration	32
2.3	Qualitative Requirements for Navigation Satellite Reliability	37
2.3.1	Qualitative Requirements for Satellite Reliability	37
2.3.2	Reliability Design Criteria for Satellite	38
2.4	Decomposition of Navigation Satellite Reliability Requirements	41
2.4.1	Approach to Decomposing Reliability Requirements	41
2.4.2	Reliability Allocation	44
2.4.3	Determination of Product Technical Requirements	51
	References	65

- 3 Reliability Modeling and Prediction** 67
 - 3.1 Reliability Modeling 67
 - 3.1.1 Reliability Model Classification 68
 - 3.1.2 Static Reliability Model 70
 - 3.1.3 Dynamic Reliability Model 75
 - 3.1.4 Process of System Reliability Modeling 81
 - 3.1.5 Reliability Modeling of Navigation Satellite 89
 - 3.2 Reliability Prediction 94
 - 3.2.1 Reliability Prediction Method 94
 - 3.2.2 Reliability Prediction of Navigation Satellite 97
- References 101
- 4 Availability Design** 103
 - 4.1 Availability Design Elements 104
 - 4.2 Redundancy and Maintenance Design of Constellation Configuration 107
 - 4.2.1 Constellation Configuration Index Related to Availability 107
 - 4.2.2 Redundancy Design of Constellation Configuration 110
 - 4.2.3 Constellation Configuration Maintenance Design 113
 - 4.3 Continuity Design of Satellite Operation 121
 - 4.3.1 Mitigation of Single Event Soft Error for Device and Equipment 121
 - 4.3.2 Mitigation of the Single Event Soft Error of Satellite System 128
 - 4.3.3 Software Robustness Design 132
 - 4.3.4 On-Orbit Scheduled Maintenance Design 144
 - 4.4 Rapid Recovery Design of Outage 144
 - 4.4.1 Rapid Replacement Design of Satellite 145
 - 4.4.2 Rapid Recovery Design of Orbit Control 146
 - 4.4.3 Fault Recovery Strategy Design 147
- 5 Availability Analysis** 149
 - 5.1 Outage Effect Analysis 149
 - 5.1.1 Method for Outage Effect Analysis 150
 - 5.1.2 Outage Effect Analysis for Navigation Satellite 157
 - 5.1.3 Outage Effect Evaluation of Navigation Satellite [2] 160
 - 5.2 Outage Index Analysis 167
 - 5.2.1 Frequency Analysis of Short-Term Unscheduled Outages 168
 - 5.2.2 MTTR Analysis of Short-Term Unscheduled Outages 170
 - 5.2.3 Analysis of Long-Term Unscheduled Outage Index [3] 171

- 5.3 Satellite Availability Analysis 177
 - 5.3.1 Availability Parameters 177
 - 5.3.2 Availability Analysis Method 178
 - 5.3.3 System Availability Analysis 182
- 5.4 Availability Analysis of Navigation Constellation 185
 - 5.4.1 Process of Constellation Availability Analysis 185
 - 5.4.2 Modeling and Analysis Methods 186
- References 191
- 6 Reliability Design 193**
 - 6.1 Redundancy Design 194
 - 6.1.1 Key Points of Redundancy Design 194
 - 6.1.2 Redundancy Design Process 196
 - 6.1.3 Redundancy Design of Navigation Satellites 199
 - 6.2 Derating Design 199
 - 6.2.1 Derating Design Points 201
 - 6.2.2 Implementation of Derating Design 203
 - 6.2.3 Output of Derating Design 207
 - 6.3 Mechanical Environmental Adaptability Design 208
 - 6.3.1 Mechanical Environment of Navigation Satellite 208
 - 6.3.2 Mechanical Environmental Adaptability Design Requirements 213
 - 6.3.3 Mechanical Environmental Adaptability Design of Satellite 215
 - 6.3.4 Mechanical Environmental Adaptability Design of Assembly 218
 - 6.4 Thermal Design 222
 - 6.4.1 Thermal Environment of Navigation Satellite 222
 - 6.4.2 Thermal Design Requirements 223
 - 6.4.3 System-Level Thermal Design 226
 - 6.4.4 Equipment-Level Thermal Design 227
 - 6.5 Space Environmental Adaptability Design 231
 - 6.5.1 Space Environment in Navigation Satellite Orbits 231
 - 6.5.2 Space Environmental Adaptability Design Requirements 234
 - 6.5.3 Space Environmental Adaptability Design for System Level 237
 - 6.5.4 Space Environmental Adaptability Design of Assembly 240
 - 6.6 EMC Design 246
 - 6.6.1 EMC Design Requirements 246
 - 6.6.2 EMC Design Method [1] 248
 - 6.6.3 EMC Design of Navigation Satellite 251

- 6.7 Reliability Design of Information Flow 253
 - 6.7.1 Reliability Design Requirements of Information Flow 253
 - 6.7.2 Reliability Design Elements of Information Flow 254
 - 6.7.3 Reliability Design of Navigation Satellite Information Flow 258
- 6.8 Reliability Design for Batch Production 260
 - 6.8.1 Characteristics of Reliability Design for Batch Production 260
 - 6.8.2 Inspection and Verification of Reliability Design 261
 - 6.8.3 Envelope of Reliability Design 261
 - 6.8.4 Reliability Redesign 268
- References 270
- 7 Reliability Analysis 271**
 - 7.1 Mission Profile Analysis 271
 - 7.1.1 Steps of Mission Profile Analysis 271
 - 7.1.2 Mission Profile Analysis for Navigation Satellite 272
 - 7.2 DFMEA 275
 - 7.2.1 Steps of DFMEA 276
 - 7.2.2 Analysis Method of DFMEA 279
 - 7.2.3 DFMEA for Navigation Satellite 289
 - 7.2.4 Practical Experience of DFMEA 293
 - 7.3 Fault Tree Analysis 298
 - 7.3.1 Establishment of Fault Tree 298
 - 7.3.2 Static FTA 302
 - 7.3.3 Dynamic FTA 307
 - 7.3.4 A Case of FTA for Navigation Satellite 310
 - 7.4 Worst Case Circuit Analysis 316
 - 7.4.1 Analysis Process of WCCA 317
 - 7.4.2 Analysis Method of WCCA 320
 - 7.4.3 Typical Cases of WCCA 324
 - 7.5 Sneak Circuit Analysis 330
 - 7.5.1 Sneak Circuit 330
 - 7.5.2 Analysis Method of Sneak Circuit 331
 - 7.5.3 SCA Clue Table 336
 - 7.5.4 Design Points for Preventing Sneak Circuit 337
 - 7.5.5 Application of SCA in Navigation Satellite 341
 - References 343
- 8 Reliability Assurance for Batch Production 345**
 - 8.1 Reliability Critical Items Control 346
 - 8.1.1 Determination of Reliability Critical Items 346
 - 8.1.2 Control Measures of Reliability Critical Items 349
 - 8.2 Process Reliability Assurance 350

- 8.2.1 Identification and Control of Critical Process Characteristics 352
- 8.2.2 Process Control of Navigation Satellite 356
- 8.2.3 Process Reliability Improvement of Navigation Satellite 358
- 8.3 PFMEA 361
 - 8.3.1 Implementation Process of PFMEA 361
 - 8.3.2 Analysis Method of PFMEA 363
 - 8.3.3 PFMEA of the Navigation Satellite 366
- 8.4 AIT Process Control 371
 - 8.4.1 On-Site ESD Protection Control 372
 - 8.4.2 Pollution Control 374
 - 8.4.3 Mandatory Inspection Points Control 375
- 8.5 Consistency Comparison of Test Data 376
 - 8.5.1 Contents of Data Consistency Comparison 376
 - 8.5.2 Method for Data Consistency Comparison 377
 - 8.5.3 Test Data Comparison System and Application 378
- 8.6 Backup Satellites Demonstration and Spare Support 379
 - 8.6.1 Analysis of the Number of Backup Satellites 379
 - 8.6.2 Application Strategy of Backup Satellites 385
 - 8.6.3 The Spares Support Strategy 386
- 8.7 Storage Reliability Assurance 388
 - 8.7.1 Effect of Storage Environment on Satellite Products [4] 388
 - 8.7.2 Satellite Storage 394
- References 397
- 9 Reliability Test and Verification 399**
 - 9.1 Reliability Development Test 400
 - 9.1.1 Test Method 400
 - 9.1.2 RDT of Navigation Satellites 405
 - 9.2 Life Test 408
 - 9.2.1 Test Method 408
 - 9.2.2 Life Test of Navigation Satellites 413
 - 9.3 Environmental Stress Screening 418
 - 9.3.1 Screening Method 418
 - 9.3.2 ESS for Navigation Satellites 422
 - 9.4 Reliability Verification 428
 - References 432
- 10 Reliability Management 433**
 - 10.1 Overview of Reliability Management 433
 - 10.1.1 Principles of Reliability Management 434
 - 10.1.2 Methods of Reliability Management 434
 - 10.1.3 Reliability Management at Different Phases 435
 - 10.2 Reliability Organization Management 438

- 10.3 Reliability Program Plan 440
 - 10.3.1 Development of Reliability Program Plan 440
 - 10.3.2 Selection of Reliability Work Items 443
 - 10.3.3 Experience in Reliability Program Planning 446
- 10.4 Reliability Review 447
- 10.5 Reliability Management of Subcontractor 449
 - 10.5.1 Management Requirements for Different Development Phases 449
 - 10.5.2 Contents of Reliability Management for Subcontractor’s Product 450
 - 10.5.3 Characteristics of Reliability Management for Subcontractor’s Product 452
- 10.6 Reliability Information Management 453
 - 10.6.1 Reliability Information 453
 - 10.6.2 Procedures and Methods of Reliability Information Management 454
 - 10.6.3 Application of Reliability Information Management 455

Chapter 1

Introduction



1.1 Reliability Engineering

Reliability engineering is a series of technical and management activities carried out to meet the reliability requirements of the product. Reliability engineering through the study of the occurrence, development, and prevention of product failure, through design, analysis, testing, and other means, to prevent and control the occurrence and development of failure, and improve the inherent reliability of products, to ensure the success of product missions and reduce life cycle costs. Reliability engineering is an important part of the whole system and life cycle management of spacecraft. It includes the determination of reliability requirements, reliability design and analysis, reliability tests, reliability management, and other aspects. It runs through the feasibility phase, preliminary definition phase, qualification and production phase, and on-orbit operation phase of the project, and is applied to spacecraft systems, subsystems, equipment, components and parts, as well as electronic, electromechanical, optoelectronic, mechanical, structural, software and other types of products.

The basic implementation approaches of spacecraft reliability engineering are:

- (1) According to the determined reliability work items, the reliability design, analysis, test, and other technologies or methods are used to ensure that the products meet the qualitative and quantitative requirements of reliability specified in the contract or assignment book.
- (2) Trade-off with the requirements of function/performance, safety, maintainability, testability, environmental adaptability, etc.
- (3) Identify and control technical risks, eliminate or reduce risks to an acceptable level, and achieve the best cost-effectiveness.
- (4) Integrate the reliability program plan into the development plan of the system, subsystem, or equipment, ensure the necessary resources (human, financial, material, etc.), and determine the progress requirements and management actions.

- (5) Determine the reliability critical items through reliability analysis and carry out effective control.
- (6) Formulate and carry out reliability design according to reliability design rules.
- (7) Through reliability analysis and reliability development/growth tests such as failure mode and effect analysis (FMEA), fault tree analysis (FTA), and worst case circuit analysis (WCCA), weaknesses in product design and manufacturing are found and improved.
- (8) Strictly control the production, testing, inspection, screening, and other processes of products and the application of technology, components, and materials to avoid reducing the inherent reliability of the design.
- (9) Evaluate the reliability of the system and its components through analysis, verification, and review.

In the reliability work of a certain project, the goal of reliability engineering is usually achieved by specifying and executing a series of reliability work items. The basic contents of spacecraft reliability engineering can be divided into five categories.

1. Reliability design

Reliability design is to meet the reliability needs of users as the goal, systematically consider various factors affecting reliability in product engineering design, and carry out targeted design, analysis, and evaluation of products, to ensure the inherent reliability of products. Reliability design is an organic part of engineering design. It is to comprehensively weigh the performance and reliability of products at different phases of development, to obtain the optimal design of products under certain constraints.

According to the experience of reliability design at home and abroad, combined with the characteristics of spacecraft products, reliability design mainly includes the following work items:

- (1) Reliability index demonstration and allocation;
- (2) Redundancy design;
- (3) Mechanical environmental adaptability design;
- (4) Space environmental protection design;
- (5) Thermal design;
- (6) Derating design;
- (7) Electromagnetic compatibility (EMC) design;
- (8) Margin design, etc.

2. Reliability analysis

Reliability analysis is to analyze and identify the weakness of product reliability or find out the failure cause and failure mechanism through engineering analysis, failure mechanism analysis, mathematical simulation analysis, and other methods. Reliability analysis and reliability design are closely related and carried out iteratively. The specific methods of reliability analysis include:

- (1) FMEA;
- (2) FTA;
- (3) Sneak circuit analysis (SCA);
- (4) WCCA;
- (5) Failure physical analysis;
- (6) Reliability modeling and prediction.

3. Reliability control of the production process

The reliability level of the product given by the design needs to be controlled through the production process to ensure that the inherent reliability is not reduced. The basic contents of reliability control in the production process include:

- (1) Process reliability control;
- (2) Process control of reliability critical items;
- (3) Stress screening (including thermal cycling, aging, running in, etc.).

4. Reliability test

Whether the reliability design is effective or not needs to be tested. The reliability test of spacecraft generally includes:

- (1) Reliability development test: it is used to verify the design and process of the product, and continuously improve and optimize the product through the process of “test, analysis, and improvement” to improve the inherent reliability of the product.
- (2) Environmental stress screening (ESS): by applying the specified environmental stress to the product, the quality defects introduced in the product manufacturing process can be found and eliminated, the early failure can be eliminated, and the operational reliability of the product can be improved.
- (3) Life test: accelerated test is usually used to verify whether the product life meets the requirements.

5. Reliability management

Reliability management is a series of activities to plan, organize, coordinate, and monitor the life cycle of products, various reliability technical work, and all contractors and personnel, to achieve the predetermined reliability objectives. Reliability management usually includes the formulation of a reliability program plan, reliability review, monitoring of supplier reliability work, etc.

The life cycle of a spacecraft is generally divided into five phases: feasibility phase, preliminary definition phase, detailed definition phase, qualification and production phase, and on-orbit operation phase. The process of spacecraft reliability work is shown in Fig. 1.1.

Compared with ground-based products, spacecraft usually has the characteristics of long life, high reliability, small sample size, and non-repairable in orbit. From launch to the end of its life, it will experience complex and harsh environmental conditions, including harsh overload, vibration, noise and impact environment during

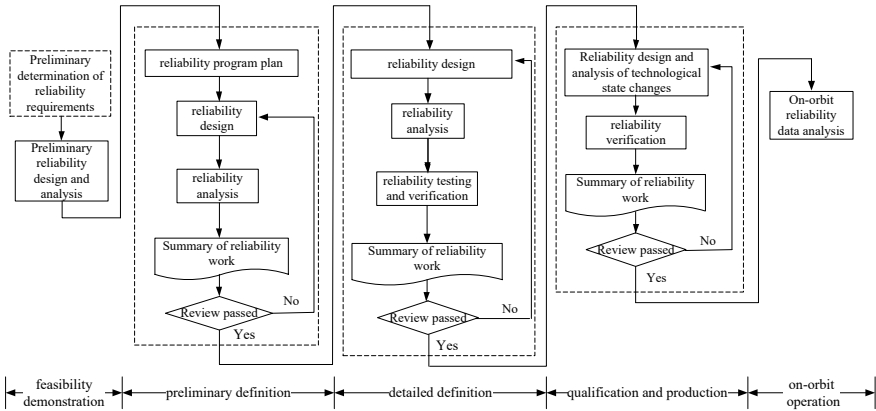


Fig. 1.1 Reliability workflow of spacecraft

launch, high vacuum, strong radiation, microgravity, ultra-low temperature and high temperature alternating, etc. Therefore, the reliability work of spacecraft has many significant characteristics, such as:

- (1) It emphasizes reliability design and verification of correctness and effectiveness of design, and seldom carries out reliability evaluation or reliability statistical test verification;
- (2) Carry out protection design for various space environments, paying special attention to single event effect protection design and total radiation dose protection design;
- (3) ESS is usually combined with an acceptance environmental test;
- (4) Carry out highly reliable design, for example, the use of components should meet the requirements of class I derating, and aerospace components should be selected.

1.2 BeiDou Navigation Satellite Engineering

1.2.1 BeiDou Navigation Satellite System

BeiDou Navigation Satellite System (BDS) is one of the four major navigation systems in the world today, including the Global Positioning System (GPS) of the United States, the Global Navigation Satellite System (GLONASS) of Russia, and the Galileo system of the European Union. Navigation satellite system provides all-time, all-weather, and high-accuracy positioning, navigation, and timing services to global users. It is a temporal-spatial infrastructure of national significance. The system is widely used in many fields of the national economy and has formed a huge navigation satellite industry.

In the late twentieth century, China started to explore a path to develop a navigation satellite system suitable for its national conditions, and gradually formulated a three-step development strategy: By 2000, the construction of BDS-1 was completed to provide services to China; by 2012, the construction of BDS-2 was completed to provide services to the Asia–Pacific region; the construction of BDS-3 was completed to provide services worldwide in 2020. BDS is mainly comprised of three segments: a space segment, a ground segment, and a user segment. The BDS space segment consists of many satellites located in the Geostationary Earth Orbit (GEO), Inclined Geo-Synchronous Orbit (IGSO), and Medium Earth Orbit (MEO).

1.2.2 BeiDou Navigation Satellites

BeiDou navigation satellites are the space segment of BDS. It constitutes a constellation system and includes three different types of satellites: MEO satellite, IGSO satellite, and GEO satellite. Its basic function is to receive the navigation message sent by the ground control system, store, process, and generate the navigation signal, and send it to the ground control system and users. The satellites are divided into payload and platform according to their functions. The basic composition of the payload includes a navigation subsystem and an antenna subsystem. The basic composition of the platform includes the attitude and orbit control subsystem, propulsion subsystem, integrated electronic subsystem, telemetry, tracking and command (TT&C) subsystem, power supply and distribution subsystem, thermal control subsystem, and structure subsystem. The BDS-3 navigation satellite is equipped with crosslinks, and some satellites are equipped with short message communication payload, search and rescue payload, etc.

1. Navigation subsystem

The navigation subsystem completes the functions of satellite time system establishment, uplink signal reception and ranging, navigation signal generation and transmission, and navigation signal integrity monitoring. The navigation subsystem is composed of an uplink signal unit, time–frequency unit, navigation processing unit, and signal broadcasting unit. The time–frequency unit is used to generate and maintain high-precision and reliable satellite reference frequency and time. The uplink signal unit completes the reception and processing of uplink signals. The navigation processing unit completes time management, navigation information processing, navigation signal generation, and integrity monitoring. The navigation signal broadcasting unit completes the frequency conversion, amplification, and filtering of the navigation signal.

2. Antenna subsystem

The antenna subsystem is used to receive the ground uplink signal and transmit the navigation signal to the user. The basic components of the antenna subsystem are the uplink antenna and downlink transmit antenna.

3. Attitude and orbit control subsystem

The task of the attitude and orbit control subsystem is to complete the attitude and orbit control of the satellite separated from the launch vehicle or upper stage to the operating orbit, overcome the influence of the satellite itself and environmental interference torque, and meet the control accuracy requirements. The attitude and orbit control subsystem is composed of a control computer, fault-tolerant control circuit, sensor, and actuator. The sensors include the sun sensor, the earth sensor, the gyro components, etc.

4. Propulsion subsystem

The task of the propulsion subsystem is to cooperate with the attitude and orbit control subsystem to provide the thrust and control torque required for phase acquisition, phase maintenance, phase adjustment, and attitude control for the satellite. The propulsion subsystem includes thruster components, propellant tanks, and various control valves and pipelines.

5. Integrated electronic subsystem

The integrated electronic subsystem cooperates with other subsystems to complete energy management, attitude and orbit control, power distribution, telemetry and remote control management, data bus management, software maintenance, and other functions. The integrated electronic subsystem is composed of a central management unit, integrated business unit, data bus network, etc.

6. TT&C subsystem

The TT&C subsystem receives the uplink TT&C signal sent by the ground TT&C station and sends the satellite telemetry signal to the ground TT&C station, and provides a tracking signal for the ground TT&C station. The TT&C subsystem is composed of the transponder, fixed amplifier, antenna, etc.

7. Power supply and distribution subsystem

The power supply and distribution subsystem provides the required energy for the satellite, which is generally composed of the solar array, battery pack, power controller, and overall circuit. The solar array supplies power for the satellite load during sunlight and charges the battery pack at the same time; The battery pack provides power for the satellite in the launch phase, power for the satellite during the shaded area of the transfer orbit and operating orbit, and power for the high current pulse load on the satellite.

8. Thermal control subsystem

The main task of the thermal control subsystem is to meet the requirements of each subsystem on the satellite for the thermal environment through the control of the internal and external heat exchange of the satellite, ensure that the temperature of all equipment during the mission is within the required range, and meet the temperature indices such as temperature change rate and control accuracy. The

thermal control subsystem is composed of a variety of thermal control materials and components, including thermal control coatings, multilayer thermal insulation material components, heat pipes, thermal conductive fillers, thermal insulation gaskets, electric heating devices, temperature sensors, etc.

9. Structural subsystem

The structural subsystem is used to maintain the integrity of the satellite, support the satellite and onboard equipment, and bear the effects of various external forces during the satellite flight and ground operation. According to the function, the structural subsystem is divided into three compartments: load compartment, propulsion compartment, and service compartment, which are composed of a truss structure and honeycomb sandwich structure plate connected to the truss.

10. Autonomous operation subsystem

The autonomous operation subsystem completes inter-satellite ranging and communication, which is the main part of the crosslinks of the BDS-3 system. The autonomous operation subsystem is mainly composed of the signal transceiver unit and phased array antenna.

1.3 Reliability Engineering of BeiDou Navigation Satellite

1.3.1 Reliability Work Needs of BeiDou Navigation Satellite

BeiDou navigation satellite project is the first large-scale networking satellite system in China. Compared with the previous space projects, the BeiDou navigation satellite project has the remarkable characteristics of high technical indices, high requirements for reliability and availability, batch parallel production, hybrid constellation configuration, and continuous launch, which not only put forward very high requirements for the management mode, development process, and support resources of the satellite project but also poses a major challenge to the method and implementation of reliability work. In terms of reliability, short-term failures of satellites that were not paid much attention to in the past may lead to the loss of navigation signals and service outages. In the past, the design or process defects of a single satellite not only increased the failure probability under the batch production of navigation satellites but also caused more serious consequences due to the wider impact of various quality problems. Therefore, the reliability of the BeiDou navigation satellite not only needs to meet the general requirements of spacecraft development but also presents many particularities.

1. The operational characteristics of the navigation system put forward high requirements for availability and continuity

To achieve all-time, all-weather, and high-accuracy positioning, navigation, and timing services, navigation satellite constellations must meet the strict requirements

of accuracy, availability, continuity, and integrity. The accuracy is the difference between the position coordinate parameters determined by the user equipment and the real coordinate parameters in the given service area or during a mission, which reflects the basic performance of the navigation system. Availability is the percentage of time that the system can be used for navigation in a period based on reliable information provided to users. Continuity refers to the probability that the system will maintain the specified performance during the operation phase, which can also be expressed as the probability that the healthy spatial signal can work continuously and healthily without unscheduled outage within the specified time interval.

Ensuring the continuity of navigation signals is a significant mission feature of navigation satellites, which is different from other spacecraft. If the navigation signal transmitted by the navigation system is frequently interrupted and unavailable due to various reasons, no matter how high the accuracy of the system is, it has no practical value. Therefore, availability and continuity determine the ability of navigation satellite system to provide services. The continuity and availability of space signals are closely related to the functional outage of navigation satellites. For this reason, BDS has put forward the availability index for the first time in China's spacecraft engineering, which puts forward very strict requirements for the reliability and availability of satellites. Accordingly, the BeiDou navigation satellite must carry out innovative work in availability design and analysis, on orbit short-term failure prevention and rapid recovery.

2. Batch production puts forward high requirements for the design and implementation of product reliability

BeiDou navigation satellite is the first spacecraft project produced in a batch in China. The so-called batch production in this book means that in the same engineering project, there are more than or equal to three spacecraft with basically the same technical state and the mission profile and operating conditions of each spacecraft are allowed to be different.

Under the background of batch production, the reliability design, production, and management of the BeiDou navigation satellite show particularity, which is mainly reflected in:

- (1) Due to the wider range of hazards caused by design defects, reliability design must be strictly required. Because the mission profiles, life cycle operating conditions, and equipment selection of multiple satellites are different, the reliability design and analysis must be carried out according to the maximum envelope principle. The focus of reliability analysis of the first and subsequent satellites is different, and the technical status may also be different due to different data sources. The characteristics of batch production and the constraints of the system also affect the final results of reliability design. For example, the crosslink should be considered in the design of information flow. These characteristics determine the particularity of batch production of BeiDou navigation satellites in reliability design and analysis.
- (2) Due to the wider range of hazards caused by process defects, process identification, and process control must be strictly required. Even if it is the same design

and technology, the implementation process of different satellites will inevitably have differences and fluctuations in details. The process control and verification work must match the development process of satellite parallel development and batch test, and cover all operation modes. Batch production has doubled the number of test data and in-orbit flight data, providing good conditions for data consistency comparison, trend analysis, and reliability verification. These characteristics determine the particularity of batch production of the BeiDou navigation satellite in reliability process control and verification.

- (3) The important changes in management mode, development process, and support resources brought by multi-satellite batch production directly affect the organizational form, planning, and implementation of various management elements of navigation satellite reliability. The difficulty of reliability management increases due to the increase of subcontractors. The quality problems in the development process involve a wide range and are difficult to handle. These characteristics determine the particularity of batch production of BeiDou navigation satellites in reliability management.
3. The operation of multi-satellite networking puts forward high requirements for launch success rate and long-term maintenance

The development of the BeiDou navigation satellite is a multi-satellite and multi-batch hybrid. Constellation requires a high degree of consistency of satellite products in batch production mode. According to the requirements of constellation networking and operation performances, a certain number of satellites must be launched into orbit within the specified time, and higher requirements are put forward for failure handling under the conditions of dense launch and “narrow window” on-time launch, and the success rate of multi-satellite launch with one launch vehicle.

BDS will provide long-term operational services to global users, with a large constellation scale, wide coverage area, and complex operational modes, posing great challenges to the operation and maintenance of the integrated network of satellite and ground segment.

1.3.2 Reliability Practice of BeiDou Navigation Satellite

During the development of reliability engineering, the concepts of maintainability, testability, and availability have been put forward and developed. Maintainability is the ability of a product to facilitate maintenance, rapid maintenance, and economic maintenance. Testability is a design feature of a product that can timely and accurately determine its state (operable, inoperable, or degraded performance) and isolate its internal faults. Availability describes the ability of the system to be put into use at any time and is a synthetical index of the reliability, maintainability, testability, and support resources of the product. Because the concepts of maintainability and testability are developed in reliability engineering, the generalized reliability concept includes maintainability and testability.

According to the analysis in Sect. 1.3.1, the most prominent characteristics of the BeiDou navigation satellite are high reliability and high availability. In the BDS reliability project, the concept of generalized reliability is applied. For the convenience of management and the close correlation of technology, the availability work is included in the reliability work, including the availability indices, availability design, and availability analysis. At the constellation level, the service reliability is proposed, which is decomposed into the on-orbit reliability, mean time between short-term unscheduled outages, mean recovery time of short-term unscheduled outages, and other indices from the availability and continuity. Compared with the reliability work of most satellite projects, the reliability work scope of the BeiDou navigation satellite is wider.

At present, more than 50 BeiDou navigation satellites have been produced in batches, and the satellite system has accumulated considerable experience in reliability implementation in many years of engineering development. According to the spacecraft development specifications and the significant characteristics of navigation satellites, the main contents of BDS reliability engineering include:

- (1) According to the requirements of constellation performance and service reliability, the reliability and availability indices of BDS and each system are demonstrated in-depth, and the simulation model is established and analyzed;
- (2) Carry out comprehensive, detailed, and focused reliability program planning and organize the implementation;
- (3) Facing the requirements of high availability and continuity, continuously deepen the availability design and verification, and carry out qualitative and quantitative analysis of availability;
- (4) To meet the requirements of long life and high reliability, the reliability design and verification are carried out in-depth, the reliability analysis is carried out from a multi-dimensional, and the analysis is integrated into the design process to ensure inherent reliability;
- (5) According to the characteristics of batch production and testing, carry out reliability assurance in process control, and strengthen the control of critical items and quantitative control of the production process;
- (6) Carry out special reliability tests and/or life tests for newly developed critical equipment;
- (7) Improve the technical support means for the constellation operation, realize intelligent operation and maintenance, collect and analyze flight data in real-time, and support the reliability improvement and growth of products at all levels.

1.4 Scope and Content of This Book

This book takes the BeiDou navigation satellite as the object, summarizes the experience of navigation satellite reliability engineering, and systematically expounds the theoretical methods applied in navigation satellite reliability practice from the

aspects of reliability requirements, reliability modeling, reliability design and analysis, reliability assurance for batch production, reliability test and verification, reliability management, and the availability design and analysis method. The engineering implementation experience or engineering examples are introduced, and the particularity and targeted work of navigation satellite reliability are described. As mentioned earlier, the availability of navigation satellites is included in the reliability work system, and this book also includes the work on availability.

The core of realizing the high availability of navigation services is the high reliability and high availability of every navigation satellite. However, the realization of navigation service needs to be completed through navigation constellation. The availability of navigation service has both requirements for navigation constellation and navigation satellite. In navigation satellite engineering, it is necessary to decompose the reliability and availability indices from the constellation level, conduct availability modeling and analysis, and support reliability and availability demonstration and constellation design optimization. Therefore, this book is aimed at the reliability engineering of the BeiDou navigation satellite, but it also includes the availability technology at the navigation constellation level.

The overall framework and content arrangement of this book not only considers the classification of reliability engineering activities but also corresponds to the development process of navigation satellites. This book is divided into 10 chapters, and the overall framework is shown in Fig. 1.2.

The main contents of each chapter are as follows:

This chapter, introduction. This chapter briefly describes the basic concept of reliability engineering and the general situation of BeiDou navigation satellite engineering, analyzes the characteristics of navigation satellite reliability engineering, and defines the scope of this book.

Chapter 2, reliability requirements. This chapter first introduces the concept of constellation service reliability and its indices decomposition and then expounds on the reliability indices and qualitative requirements of navigation satellites from both

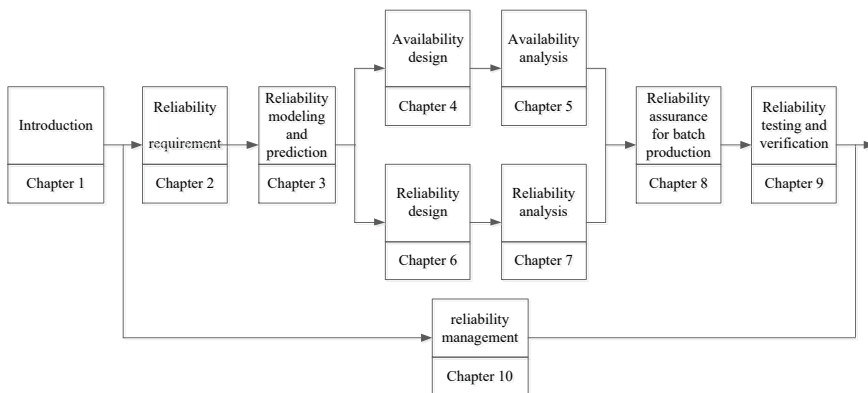


Fig. 1.2 Overall framework of the book

quantitative and qualitative aspects. Finally, for subsystems and equipment, the idea of satellite system level reliability indices decomposition, the method of allocation, and the process of how reliability forms product technical requirements as part of technical requirements are explained.

Chapter 3, reliability modeling and prediction. Based on the analysis of quantitative reliability requirements, this chapter introduces the static reliability model and dynamic reliability model related to navigation satellites, expounds on the process of system reliability modeling and navigation satellite reliability modeling, and introduces the basic methods and examples of navigation satellite reliability prediction.

Chapter 4, availability design. According to the high availability requirements of navigation satellites and constellations, this chapter first proposes four types of elements of availability design, then introduces the constellation configuration redundancy design method, constellation configuration maintenance design method, and engineering examples, and expounds on-orbit continuity design methods of the single satellite such as single event soft error protection design, software robustness design and on-orbit scheduled maintenance design, and the design methods of rapid recovery from outage, such as rapid replacement design of satellite, rapid recovery design of orbit control, and fault recovery strategy design.

Chapter 5, availability analysis. This chapter first introduces the outage analysis method from the perspective of availability weakness analysis, expounds on the implementation of outage analysis, and introduces how to identify critical soft faults through quantitative analysis of outage effects. Then, from the perspective of quantitative analysis of the availability indices, the method of availability analysis and the process of system availability analysis are described. Finally, the process and methods of constellation availability analysis are introduced.

Chapter 6, reliability design. This chapter introduces the reliability design work of navigation satellites, including redundancy design, derating design, mechanical environmental adaptability design, thermal design, EMC design, space environmental protection design, etc. For each design element, the basic design method or design requirements are usually described first, and then the implementation of the navigation satellite is introduced.

Chapter 7, reliability analysis. This chapter introduces the reliability analysis methods applied in the design process of navigation satellites and the specific analysis work carried out, including mission profile analysis, Design FMEA, FTA, WCCA, and SCA. Mission profile analysis is the basis of reliability and related critical characteristic analysis. FMEA and FTA are used to identify potential weaknesses and determine critical items. WCCA is used to find weaknesses in circuit design. SCA is used to identify potential states that cause non-expected functions or inhibit expected functions.

Chapter 8, reliability assurance for batch production. According to the characteristics of batch production and batch production process of navigation satellites, this chapter introduces the reliability-related work focused on and carried out in the production process of navigation satellites, including the control of reliability critical items to eliminate or control the technical risks of the satellite; Process reliability

assurance and Process FMEA to identify weakness in the batch production process and ensure process consistency and process stability; The assembly, integration, and test (AIT) process control focusing on electrostatic protection control, pollution control, and mandatory inspection; Test data consistency comparison to find the product weakness through data analysis; The backup satellite demand demonstration and spare parts guarantee for continuous launch and long-term operation risk, and the storage reliability guarantee for production tasks.

Chapter 9, reliability test and verification. This chapter focuses on the basic methods of reliability development tests, life tests, and implementation examples according to the characteristics of many newly critical equipment and high lifetime requirements of navigation satellites. This chapter also introduces the implementation method of ESS and reliability verification.

Chapter 10, reliability management. Reliability management runs through the whole process of navigation satellite development. This chapter first summarizes the basic methods and work contents of reliability management, then introduces the implementation of navigation satellite in the aspects of reliability program plan, reliability review, reliability management of subcontractors, and reliability information management.

Chapter 2

Reliability Requirements



Reliability requirements are the basis for reliability design, analysis, test, and verification. Reliability requirements can be divided into qualitative requirements and quantitative requirements. Qualitative requirements are to design, evaluate, and assure the reliability of products in a non-quantitative form. Quantitative requirements specify the reliability parameters, values, and verification methods of products, to evaluate or verify the reliability level of products with quantitative methods in the process of design, production, and use.

The reliability requirements of a navigation satellite system correspond to four levels: constellation, satellite, subsystem, and equipment. At the constellation level, the navigation system emphasizes the continuous availability of services and on-orbit maintainability, so the connotation of constellation reliability includes continuity, availability, and integrity. At the satellite level, the reliability indices includes not only the on-orbit reliability and on-orbit service life but also the availability-related indices such as mean time between outages (MTBO) and mean time to repair (MTTR).

2.1 Service Reliability of Navigation Constellation

2.1.1 *Concept and Connotation of Service Reliability*

2.1.1.1 Overview

The service performance parameters of navigation constellation mainly include service accuracy and service reliability. Service accuracy includes positioning accuracy, timing accuracy, and speed measurement accuracy, which refers to the difference between the position coordinate parameters determined by the user equipment and the real coordinate parameters in a given service area or during the navigation task. Service accuracy is the most basic performance parameter, and also the

basis and constraint of service reliability. Service reliability includes service availability, continuity, and integrity. It is an important parameter to measure the ability of the system to provide continuous, stable, and reliable services. Note that reliability here is a generalized concept. Service reliability is not only related to the operating environment conditions of the user segment but also closely related to constellation performance and satellite reliability, as well as the navigation operation control and satellite management capabilities of the ground segment. To build an available navigation satellite system, the satellite system and the ground segment must meet the relevant requirements of service reliability in addition to meeting the conventional functional and performance requirements.

Service availability is the focus of users' attention. At present, there is no unified definition of service availability. Galileo system defines service availability as the average percentage of the time that the service meets the specified "accuracy, integrity and continuity" at any point within the service scope during the design life. The International Civil Aviation Organization (ICAO) defines service availability as the percentage of the total time that the system can be used for navigation based on reliable information provided to users within a period. There are different understandings of "reliable information". ICAO requires that as long as it meets the accuracy and integrity requirements, and does not need to meet the continuity requirements, the Federal Aviation Administration (FAA) stipulates that it must meet the requirements of accuracy, integrity, and continuity at the same time to be reliable information.

Continuity and integrity are the special characteristics of satellite navigation systems, which are closely related to life safety applications. Continuity refers to the probability that healthy Signal in Space (SIS) can work continuously and healthily without unscheduled outages within the specified time interval, that is, the description of the ability of "continuous available" within this period. Integrity is a measure of confidence in the correctness of the information provided by the system. It covers the ability of the SIS to send warning information to the receiver in time when the SIS cannot be applied. Integrity is often described as "Integrity Risk (IR)". IR refers to the probability of an error that can cause the calculated position error to exceed the maximum Alert Limit (AL) and fail to notify the user within the specified Time to Alert (TTA).

The relationship between availability, continuity, and integrity of navigation constellation is as follows:

- (1) According to the accuracy and integrity requirements, availability can be divided into accuracy availability and integrity availability. Accuracy availability refers to the availability when the accuracy is used as the judgment threshold, and integrity availability refers to the availability when the integrity is used as the judgment threshold. When the integrity protection margin is adopted, the risk of false alarm is considered in the margin calculation.
- (2) The continuity and availability of SIS are related to the satellite outage. Satellite outage includes scheduled outages and unscheduled outages. All outages will affect availability. Continuity is only related to unscheduled outages, such as hard failures and soft failures. Outages that can be notified in advance within the

specified time, such as satellite orbital maneuvers, on-orbit maintenance, etc., will lead to the satellite being unavailable, but will not cause continuity risk.

- (3) Service continuity mainly refers to the probability that the position service will not have unscheduled interruption over a specified time interval. The higher the integrity requirements of users and the more stringent the AL and IR requirements, the greater the probability of causing an alarm and the greater the continuity risk.
- (4) The integrity and continuity of SIS are related to alarms, which are interrelated and restricted. When the satellite sends an alarm indication within the specified TTA, it indicates that the satellite is unavailable, but it will not cause a loss of integrity and continuity. However, if the satellite does not send an alarm within the specified TTA, it will lead to the loss of integrity and continuity.

2.1.1.2 Service Availability

This book defines the service availability of the navigation constellation as the percentage of time that the Radio Navigation Satellite Service (RNSS) meets the specified performance standards within a period.

The service availability is different for different user locations, and different observation times. The availability of a certain location at a certain time is called instantaneous availability, the statistics of availability of the same location at different times is called single point availability, and the statistics of different single point availability of a service area is called service area availability. Taking the constellation operation cycle as the observation period, single-point availability can be obtained by statistical analysis of instantaneous availability on sampling time. Within the service area, grids are divided according to certain longitude and latitude intervals, and the service area availability can be obtained by statistical calculation of the single-point availability results of all grids. Generally, service availability refers specifically to accuracy availability. The accuracy requirements here refer to the positioning availability accuracy limit.

The positioning availability accuracy limit is related to the User Equivalent Range Errors (UERE) and the Dilution of Precision (DOP). When the UERE is fixed and assuming that the UERE values of all satellites are the same, the accuracy limit is determined by the DOP limit. DOP limit value adopts DOP value under a certain hypothetical limit state.

For example, the Standard Positioning Service (SPS) position availability standards of GPS are listed in Table 2.1.

2.1.1.3 Service Continuity

In this book, the service continuity of navigation constellation is defined as the probability that the system will continue to meet the accuracy and integrity requirements over a specified time interval, under the condition that the system meets the