Guidance
Document
GD28-2023

China Classification Society

Guidelines for Reliability Verification of Ship Equipment and Systems

2023

Effective from July 1, 2023

Contents

Foreword

According to the requirements of China Classification Society's Rules for Intelligent Ships, the equipment and components of scenario awareness system and autonomous navigation system of intelligent navigation system shall have sufficient reliability to minimize the probability of failure. In recent years, with the continuous development of domestic ship equipment and the continuous improvement of ship intelligence level, the application of new energy under the low-carbon zero-carbon strategy has driven the emergence of new equipment and systems one after another, and the industry's attention to the reliability of ship equipment and systems has gradually increased.

Based on the above rule requirements and industry needs, the Society has formulated these Guidelines to specify the basic methods and general requirements for reliability testing and verification of ship equipment and systems, and provide guidance for shipowners, equipment and system manufacturers, computer software and embedded system developers, inspection and test organizations.

According to the environmental characteristics of equipment and systems, these Guidelines specify the classification of environmental parameters and their severity levels, put forward environmental test requirements under different severity levels, and give recommended methods for determining comprehensive environmental conditions for reliability verification of equipment and systems. These Guidelines introduce the test purpose, test environment, test contents and test methods of equipment, computer software and embedded software respectively.

Based on the compliance test results of equipment, computer software and embedded software, the Guidelines also provide requirements for reliability evaluation and calculation of equipment and systems, and gives common reliability models and their calculation methods for reliability indicators.

The Guidelines are prepared and updated by China Classification Society and published through the webpage http://www.ccs.org.cn. The comments of interested parties on the Guidelines can be fed back to rd@ccs.org.cn.

Chapter 1 General

1.1 Scope

Thess Guidelines specify the basic methods and general requirements for reliability testing and verification of equipment and systems, and provides guidance to shipowners, equipment and system manufacturers, software and embedded system developers, inspection and test organizations.

Thess Guidelines are positioned as a “guideline” in the technical document hierarchy, and is a non-mandatory technical document that explains the rules and application on new technologies to ships and offshore facilities.

1.2 General

Reliability verification is to evaluate whether it complys the prespecified reliability indicators through various tests of item operation or simulation. Through statistics and inference of various data obtained from the test, corresponding reliability index parameters are obtained for further judgment if the specified requirements can be met.

1.3 Reliability Verification of Equipment and Systems

According to the characteristics of equipment and systems, three methods for reliability verification of equipment and systems accepted in these Guidelines include: field test, laboratory test and simulation test.

The environmental suitability and compliance test profile of equipment and systems shall comply the requirements of Chapter 4 of the Guidelines.

The equipment compliance test shall comply the requirements of Chapter 5 of the Guidelines.

The compliance test of computer software shall comply the requirements of Chapter 6 of the Guidelines.

The compliance test of embedded software shall comply the requirements of Chapter 7 of the Guidelines.

The system reliability assessment shall comply the requirements of Chapter 8 of the Guidelines.

If the reliability of equipment and systems cannot be verified by applying Chapters 5 to 8 of the Guidelines, one of the methods in Failure Mode and Effects Analysis (FMEA)/Failure Mode, Effects and Criticality Analysis (FMECA) or Fault Tree Analysis (FTA) can be used to analyze the failure modes, consequences and risk results of equipment and systems as the basis for verifying reliability. For detailed application methods of FMEA, FMECA or FTA, refer to the Guidelines for the Application of Formal Safety Assessment to Ships of CCS. and IEC 60812:2018.

The reliability verification of ship equipment and systems shall be carried out by the Society or a third-party test verification organization recognized by the Society, and shall pass the witness and review of the Society. The third-party test and verification organization carrying out equipment and systems reliability verification shall comply the relevant requirements of Chapter 2 of Part 1 of the Guidelines for Accreditation of Ship Product Testing Bodies of the Society. For equipment and systems that have passed the reliability verification according to the Guidelines, the Society shall issue a compliance certificate. See Chapter 9 of the Guidelines for details.

Chapter 2 References

2.1 General

The references below are indispensable for the application of this Guideline. For references with version No. indicated, only the edition cited applies. For references without version No., the latest edition is applicable to these guidelines.

Table 2.1 References

S/N	Version No.	Chinese Name	Corresponding International Standards
1	-	China Classification Society Rules for Classification of Sea-going Steel Ships and its Amendments	-
2	-	China Classification Society Rules for Intelligent Ships	-
3	-	China Classification Society Guide for Survey of Intelligent Equipment	-
4	-	China Classification Society Guideline for Type Approval Test of Electric and Electronic Products	-
5	-	China Classification Society Guideline for the Application of Formal Safety Assessment (FSA) to Ships	-
6	GB/T5080. 1-2012	Reliability Testing - Part 1:Test Conditions and Statistical Test Principles	IEC60300-3-5:2001 Dependability management - Part3-5: Application guide - Reliability test conditions and statistical principles
7	GB/T5080.2-2012	Reliability Test - Part 2: Design of Test Cycles	IEC 605-2:1994 Equipment reliability testing - Part2: Design of test cycles
8	GB/T 2423 series	Environmental Testing for Electric and Electronic Products	IEC 60068-2: Environmental Testing-Part2
9	GB/T 11804-2005	Environmental conditions for electric and electronic products-Terminologies	-
10	GB/T 14597-2010	Environmental Climatic Conditions Appearing in Different Altitudes for Electrical Products	-
11	GB/T 14092.3-2009	Environmental Condition for Machinery Products - High Altitude	-
12	GB/T 4796-2017	Classification of environmental conditions—Environmental parameters and their severities	IEC 60721- 1-2002 Classification of environmental conditions-Part 1: Environmental parameters and their severities
13	GB/T 4797.1-2018	Classification of Environmental Conditions - Environmental Conditions Appearing in Nature - Temperature and Humidity	IEC60721-2- 1-2013 Classification of environmental conditions-Part2- 1: Environmental conditions appearing in nature - Temperature and humidity

S/N	Version No.	Chinese Name	Corresponding International Standards
14	-	Classification of Environmental Conditions - Part 3: Classification of Groups of Environmental Parameters and Their Severities	IEC 60721-3-0-2020 Classification of environmental conditions - Part 3-0: Classification of groups of environmental parameters and their severities - Introduction
15	GB/T 4798.6-2012	Classification of Environmental Conditions - Classification of Groups of Environmental Parameters and Their Serverities: Ship Environment	IEC 60721-3-6- 1987 Classification of environmental conditions. Part 3: Classification of groups of environmental parameters and their severities. Introduction. Ship environment
16	GB/T 20159.6-2008	Classification of Environmental Conditions - Guidance for the Correlation and Transformation of Environmental Condition Classes to the Environmental Tests - Ship Environment	IEC TR 60721-4-6: 2003 Amendment 1 - Classification of environmental conditions - Part 4-6: Guidance for the correlation and transformation of environmental condition classes of IEC 60721-3 to the environmental tests of IEC 60068 - Ship environment
17	GB/T 6994-2006	Electrical Installation in Ships - Definitions and General Requirements	IEC 60092- 101:2018 Electrical installations in ships - Part 101: Definitions and general requirements
18	GB/T 37079-2018	Equipment Reliability - Reliability Assessment Methods	IEC 62308:2006 Equipment reliability - Reliability assessment methods
19	GB/T 34986-2017	Methods for Product Accelerated Testing	IEC 62506:2013 Methods for product accelerated testing
20	GB/T 38634-2020	Systems and Software Engineering-Software Testing	ISO /IEC/IEEE 29119-2015: Software and systems engineering- Software testing
21	GB/T 29832.1-2013	Reliability of System and Software - Part 1: Indicator System	-
22	GB/T 29832.2-2013	Reliability of System and Software - Part 2: Metric Method	-
23	GB/T 29832.3-2013	Reliability of System and Software - Part 3:Testing Method	-
24	GB/T 11457-2006	Information Technology - Software Engineering Terminology	-
25	GB/T 28171-2011	Embedded software reliability testing method	-
26	GB/T 22033-2017	Information technology—Terminology for embedded systems	-
27	GB/T 30093-2013	Reliability Technique Review Procedure for Automation Control System	-

S/N	Version No.	Chinese Name	Corresponding International Standards
28	-	Mathematical Expressions for Reliability, Availability, Maintainability and Maintenance Support Terms	IEC 61703-2016 Mathematical expressions for reliability, availability, maintainability and maintenance support terms
29	GB/T 14093.6-2009	Environmental Technical Requirements of Machinery Products for Ocean Environment	-
30	GB/T 7826-2012	Analysis Techniques for System Reliability - Procedure for Failure Mode Effects Analysis (FMEA)	IEC 60812:2006 Analysis techniques for system reliability - Procedure for failure mode and effects analysis(FMEA)
31	GB/T 37981-2019	Analysis Techniques for Dependability - Reliability Block Diagram and Boolean Methods	IEC61078: 2006 Analysis techniques for dependability - Reliability block diagram and boolean methods

Chapter 3 Terms and Abbreviations

3.1 Terms

3.1.1 item

The item of this Guideline refers to ship equipment and systems, in which the software system includes computer software and embedded software as well as their combinations.

3.1.2 fault

The fault is the loss of ability to perform as required due to an inherent condition.

3.1.3 reliability

Reliability is the ability of an item to complete specified functions under specified conditions and within specified time intervals.

3.1.4 useful life

The useful life is the time interval from the first use of an item until it no longer complys user requirements due to uneconomical operation and maintenance or being discarded.

Note 1: "First use" does not include testing activities in which the previous item was handed over to the end user.

3.1.5 reliability (measure)

Reliability (measure) in this Guideline is referred to as reliability for short, that is, the probability of performing according to requirements within a time interval (t_1, t_2) under given conditions of the item.

Note 1: The given conditions include various factors affecting reliability, such as operation modes, stress levels, environmental conditions and applicable maintenance.

Note 2: It is usually assumed that the item is in a state of performing as required at the beginning of a given time interval.

Note 3: When $t_1=0$ and $t_2=t$, $R(0, t)$ can be reduced to $R(t)$, which is called the reliability function or survival function of the item. See IEC61703: 2016 for details.

3.1.6 environmental adaptation

Environmental adaptation is the ability of an item to achieve all its intended functions and/or performance and/or avoid damage under various environmental effects that it may encounter during its service life. It requires that the item shall function normally without any damage in harsh extreme climate, mechanical, biochemical and other environments during use. Generally, items that can adapt to extreme environment are also deemed to be able to adapt to conventional environment.

3.1.7 environmental parameter

Environmental parameters are one or more physical, chemical and biological properties characterizing an environmental factor, such as temperature, humidity and acceleration. For example, the environmental factor vibration is characterized by the parameters: type of vibration (sinusoidal, random), acceleration and frequency.

3.1.8 group of environmental parameters and their severites

A group of environmental parameters and their severities is a set of characteristic values of environmental conditions used for a specific application or purpose.

3.1.9 severity (of operation or environmental parameter)

The severity indicates the magnitude of each operation or environmental parameter. It determines the level of stress acting on an item.

3.1.10 reliability test

Reliability test is a test to measure (determine), verify or compare the reliability easures or properties of an item.

3.1.11 compliance test

Compliance test is a test used to prove whether the characteristics or performance of an item comply its specified reliability requirements.

3.1.12 repairable item

A repairable item is an item that, after it fails, can be restored under given conditions to the extent that it can perform required functions.

Note 1: "Given conditions" may include technical, economic and other considerations.

Note 2: An item is repairable under some conditions, but non-repairable under other conditions.

3.1.13 non-repairable item

A non-repairable item is an item that, after it fails, cannot be restored under given conditions to the extent that it can perform required functions.

Note 1: "Given conditions" may include technical, economic and other considerations.

Note 2: An item is non-repairable under some conditions, but repairable under other conditions.

3.1.14 maintainability

Maintainability is the probability that a given maintenance activity will be completed within the time interval (t_1, t_2) assuming that it starts at t=0 and using specified procedures and resources under specified conditions.

Note 1: When t_1=0 and t_2= t, $M(0, t)$ is reduced to $M(t)$, which is called the maintainability function.

3.1.15 life test

Life test is a test to verify the useful life or storage life of items under specified conditions.

3.1.16 test plan

The test plan is a guide for the personnel performing the tests. It includes statistical test plans (tested item information, faulty item handling methods and test end criteria), and further specifies test conditions, test facilities and operating procedures, observations, test reports and analysis of test data.

3.1.17 discrimination ratio

Discrimination ratio D ($D > 1$) characterizes a test plan by its ability to distinguish between acceptable and unacceptable dependability measures. The discrimination ratio is a figure of merit of a test plan.

3.1.18 (instantaneous) failure rate

Failure rate is the limit value of the ratio of the conditional probability of failure within the time interval (t, $t+\Delta t$) to the interval length Δt when Δt tends to 0, assuming that the item is available at time t, if any.

3.1.19 (instantaneous) failure intensity

Failure intensity is the limit value of the ratio of the average number of failures for repairable items in a time interval (t, $t+\Delta t$) to the interval length Δt when Δt tends to 0, if any. That is, the failure intensity is the number of failures per unit time.

3.1.20 hardware

Hardware is a physical device used to process, store or transmit computer programs or data.

3.1.21 software

Software is computer programs, procedures and possibly related documentation that are relevant to the operation of a computer system.

3.1.22 software reliability

Software reliability has two meanings: one is the probability that software will not cause system failure within a specified time under specified conditions. This probability is a function of the system input and used by the system, as well as defects in software. If a defect exists, the system input determines whether an existing defect will be encountered. The second is the ability of the program to perform required functions within a specified time period and under specified conditions.

3.1.23 software maturity

Software maturity refers to the ability to avoid software failure caused by faults of the software itself, and can be measured by the indicators below:

The degree of failure is used to measure the extent of occurrence and resolution of software failures, mainly including failure density and failure resolution rate.

Fault degree is used to measure the extent of discovery and troubleshooting of faults of the software itself, mainly including fault density and potential troubleshooting rate.

The test degree is used to measure the extent to which software has been tested, mainly including test coverage rate and test pass rate.

Effectiveness is used to measure the effectiveness of software operation, mainly including mean time between failures, effective service time rate and cumulative effective service time.

3.1.24 software (error) tolerance

Software (error) tolerance refers to the ability of software to maintain a specified performance level in case of failure or violation of specified interfaces, and can be measured by the indicators below:

Proper function is used to measure the degree of effort made by software to maintain normal operation, mainly including avoiding downtime rate and avoiding failure rate.

Misoperation resistance rate is a measure of the degree of software effort made to resist misoperation.

3.1.25 software recovery

Software recovery refers to the ability of software to rebuild a specified performance level and restore directly affected data in case of failure, and can be measured by the indicators below:

The restart success is used to measure the degree of software reuse after downtime, mainly including average downtime, average recovery time and other indicators.

Repair success is used to measure the degree of software repairability after an exception occurs, mainly including repairability and repair effectiveness.

3.1.26 embedded system

An embedded system is a special purpose computing system implanted within an application object for information processing or control.

3.1.27 embedded software

Embedded software is software that complys the special requirements of embedded system application environment.

3.1.28 internally mounted

Internal mounted means that the item system is installed in a compartment that can prevent environmental impact to completely isolate the item system from the external environment.

3.1.29 externally mounted

External mounted means that the item system is installed outside and cannot prevent any influence from external environment.

3.1.30 reliability validation test

Reliability validation test is a test to confirm whether the current reliability level of embedded software complys user needs under given statistical confidence, that is, to confirm whether the specified reliability objectives are met.

3.1.31 cascaded

Behavior that directly results from the initial behavior, e.g., cascaded deflection, cascaded failure, cascaded deviation.

3.1.32 simulation test

Virtual testing and test carried out for algorithm functions such as collision avoidance and perception based on the application scenarios of ship equipment and systems.

3.1.33 lab test

It refers to the specified type of inspection/testing conducted by a laboratory with certain qualifications and capabilities.

3.1.34 field test

Field test refers to the test field test or on-board application environment test.

3.1.35 profile

The timing sequence description of incidents and environments experienced by the item, for example, the task profile is the timing sequence description of incidents and environments experienced by the item during the period when it completes the specified task.

3.1.36 durability

The durability of equipment refers to the capacity of equipment to complete specified functions before reaching the limit state under the specified conditions of use, storage and maintenance, and is generally measured by life parameters. Life paramters include the time to first overhaul, useful life, time between overhauls, total life, storage life and reliable life.

3.2 Abbreviations

The following abbreviations apply to the Guideline:

MTBF: Mean Time Between Failures.

MTTF: Mean Time to Failure.

MTTR: Mean Time to Repair.

FI/FIO: Ratio of Provable Failure Intensity to Failure Intensity.

Chapter 4 Classification of Ship Environmental Parameters and Their Severities and Comprehensive Environmental Conditions for Reliability Verification

4.1 General

Environmental adaptation mainly represents the survivability of a product in various environments, including extreme environments, that may be encountered during the item's useful life. Reliability represents the capacity of an item to function properly in typical environments during its useful life. It is stipulated in the Guidelines that item reliability verification shall be carried out in combination with the corresponding environmental conditions of the ship, and the applicable environment severities of the item shall be indicated. The Guidelines take the passing of environmental adaption tests as a pre-requirement for reliability verification.

4.2 Requirements for Classification of Ship Environmental Parameters and Their Severities

The severities given in the Guidelines have a very low probability of being exceeded. Only severe conditions that may affect the structural integrity or functional performance of a product are included. In a certain period of time, the occurrence rate may vary at different locations. For example, as the vibration environment differs between the central control console and the ship control console at the machine location, their occurrence rates will be different at the same time. Such frequencies of occurrence shall be considered for any environmental parameter. They should additionally be specified if applicalbe. See IEC60721-3-0 2021 for details.

4.2.1 Requirements for General Reference

The Guidelines give the classes of climatic environmental conditions (K), bioenvironmental conditions (B), chemically active substances (C), mechanically active substances (S) and mechanical environmental conditions (M). For a given product, reference should be made to the total set of classes, e.g. 6K2/6B2/6C2/6S1/6M4.

The combination of minimum classes 6K1/6B1/6C1/6S1/6M1 is applicable to products and systems installed in weather-protected (such as watertight) locations, which withstand the corresponding environmental conditions during normal use. The combination of the highest classes 6K5/6B2/6C3/6S3/6M4 covers a wide number of installations aboard most types of ships including locations with very severe conditions. See 4.2.2 to 4.2.6 for the description of class notation of each environmental condition, and see Appendix 1 for the comparison table of environmental conditions.

The most extreme climatic types, such as extreme cold and extreme dry heat, are generally found only in the polar and inland regions and are therefore not included in the Guidelines. However, it is possible that ships may withstand such extreme climatic conditions when sailing in inland waters (rivers and lakes). If extreme climate types are to be withstood, the climatic environmental conditions shall be determined on a case-by-case basis.

For the service area of Qinghai Lake and inland waters of Tibet Autonomous Region (including the river system of the Yarlung Zangbo River and inland river and lake system) as well as other high-altitude service areas, the requirements for high-altitude environmental conditions shall also be considered. See GB/T 14597-2010 for the relevant requirements of electrical products and GB/T 14092.3-2009 for the relevant requirements of mechanical products.

4.2.2 Requirements for Classification of Environmental Climatic Conditions

Environmental climatic conditions are classified into the following seven class notations.

6K1: 6K1 includes conditions of various products installed in totally weatherprotected, heated and ventilated locations after warm-up, excluding machinery spaces and locations containing equipment dissipating considerable heat. The product is not exposed to solar radiation through glass or other transparent materials

6K1 includes both the warm damp and the steady-state warm damp climate types, as well as submerged products in all areas except those with particularly high water temperature, for example, the Arabian Gulf.

6K2, in addition to the conditions covered by 6K1, it covers the conditions of various locations with heating and ventilation conditions in all climate types except for cold before and during temperature rise. For ventilated locations, 6K2 also covers both the warm damp and the steady-state warm damp climate types. These products may be subjected to wetness, to heat radiation from heating elements and to solar radiation through glass or other transparent materials. 6K2 also includes submerged products in areas with particularly high water temperature.

6K3, in addition to the conditions covered by 6K2, it also covers various products installed in machinery spaces as well as in close proximity to equipment dissipating considerable heat, 6K3 also covers products placed close to gates, ramps, etc., which are opened temporarily for loading and unloading.

6K4, in addition to the conditions covered by 6K3, 6K4 covers conditions in non-ventilated locations, which are subjected to solar radiation, rain and water jets except in the Type of Climate Cold. It also covers non-weatherprotected products in all Types of Climate except Cold, but not in areas with abnormal rain intensities and hurricanes.

6K4 also includes products installed on hot parts of the machine, and withstand the influence of direct solar radiation and water flow except for scouring by large waves.

6K5, in addition to the conditionscovered by 6K4, it includes products installed in unheated weatherprotected locations and in non-weatherprotected locations in the Type of Climate Cold. It also covers products in refrigerated cargo spaces as well as in non-weatherprotected locations in ships operating in areas with abnormal rain intensities and hurricanes and products subjected to heavy seas.

6K6 represents the conditions covered by the Warm Damp and Warm Damp Equable types of Open-Air Climate (tropical damp type of climate, in areas with tropical rainforests).

6K7 represents the conditions covered by the Warm Dry, Mild Warm Dry and Extremely Warm Dry types of Open-Air Climate (tropical dry type of climate, in areas near the tropics such as deserts).

4.2.3 Requirements for Classification of Bioenvironmental Conditions

Bioenvironmental conditions are classified into the following two class notations:

6B1: it covers installations in ships operating in areas without particular risks of attacks from flora or fauna. It also covers other ships where the installations are located in compartments of such construction that mould growth and attacks by animals are not likely.

6B2, in addition to the conditions covered by 6B1, it includes non-protected installations in ships operating in areas where mould growth and attacks by animals may occur.

4.2.4 Requirements for Classification of Chemically Active Substances

Chemically active substances are classified into the following three class notations:

6C1: it includes installations that are not exposed to salt mist, engine exhaust gas and emissions from adjacent industrial pollution sources and are fully protected against climate, and also includes various installations on the deck of ships sailing in inland freshwater areas and with protective measures against engine exhaust, and not operating close to industries with considerable air polluting emissions.

6C2, in addition to the conditions covered by 6C1, 6C2 covers totally weatherprotected installations which are subjected to salt mist and to engine exhausts.

6C3,in addition to the conditions covered by 6C2, 6C3 covers non-weatherprotected installations. It also covers conditions in ships operating close to industries with considerable air polluting emissions.

4.2.5 Requirements for Classification of Mechanically Active Substances

Mechanically active substances are classified into the following three class notations:

6S1: it covers installations protected from sand,dust and ingress of soot .

6S2, in addition to the conditions covered by 6S1, 6S2 covers installations, both weatherprotected and non-weatherprotected where sweeping of dusty decks may take place. It also covers locations subject to emissions from boiler exhausts (soot).

6S3, in addition to the conditions covered by 6S2, it includes various non-weatherprotected installations, including those in ships operating close to sand deserts.

4.2.6 Requirements for Classification of Mechanical Environmental Conditions

Mechanical environmental conditions are classified into the following four class notions:

6M1 only includes installations in ships which are not powered by engines.

6M2, in addition to the conditions covered by 6M1, 6M2 includes installations in engine-powered ships larger than 1,000 metric tons dead weight, installations except for stern locations in ships smaller than 20,000 metric tons dead weight. It excludes product installations directly connected to loading or reciprocating machinery.

6M3, which, in addition to the conditions covered by 6M2, also includes installations in ships smaller than 1 000 metric tons dead weight and in stern locations of ships smaller than 20 000 metric tons dead weight. Products connected directly to loading systems, container Guideliness, cranes and installations in dredgers are also included.

6M4, in addition to the conditions covered by 6M3, 6M4 covers products connected directly to reciprocating types of machinery.

4.3 Requirements for Environmental Test with Different Severities

During the environmental test of products, it is necessary to clearly specify the environment in which the product is placed, the performance parameters that shall be measured before, during and after the test, and the failure criteria. See IEC TR 60721-4-6: 2003 and the Guidelines for Type Approval Test of Electric and Electronic Products (2015) issued by the Society for the test requirements under environmental conditions with different severities. For the environmental test that have passed the third-party inspection and test agency accepted by the Society or carried out as agreed upon based on special circumstances, no repeated environmental tests are required. The environmental severities corresponding to the environmental tests of items shall be indicated in accordance with the requirements of Section 4.2.1. See IEC TR 60721-4-6: 2003 for specific environmental conditions and conversion relations between tests.

4.4 Requirements for Profile of Reliability Verification

4.4.1 Requirements for Life Profile

The life profile is a timing sequence description of various incidents and states (including environmental conditions, working modes and their continuation) that the ship equipment and systems are to experience from the time of receipt to the end of life or disabling. The life profile addresses each significant incident during the useful life, such as storage and transportation, test and inspection, standby and on-call state, operational use or task, and other possible incidents. The life profile is the basis for determining the environmental conditions that a product will encounter.

4.4.2 Requirements for Task Profile

The task profile is a timing sequence description of all important incidents and states that the ship equipment and systems will experience during the period when they complete the specified tasks, and it is part of the life profile. A product or system may be used to perform a single function or multiple functions. Therefore, there may be one or more task profiles. The task profile is the basis for determining the main environmental conditions that a product or system will encounter in use, depending on the requirements for use of the product or system.

4.4.3 Requirements for Environmental Profile

The environmental profile is a diagram for the relationship between various main environmental parameters and time that the item will be encountered during storage, transportation and use, which shall be drawn according to the task profile. Each task profile corresponds to one environmental profile, so the environmental profile may be one or more.

4.4.4 Requirements for Test Profile

The test profile is a diagram for the relationship between environmental parameters and time directly used for tests, which is obtained by processing the environmental profile as per certain rules. For the test profile, environmental conditions outside the task profile shall also be considered , such as temperature environments of autonomous navigation and berthing in open waters. For items designed to perform a function, there is a one-to-one correspondence between the test profile, the environmental profile and task profile. For items designed to perform multiple functions, multiple test profiles shall be combined into a comprehensive test profile according to certain rules. An example of a comprehensive test profile is provided in Appendix 2 to the Guidelines.

4.5 Requirements for Comprehensive Environmental Conditions of Reliability Compliance Test

If there are provisions for conditions of tests on the shipowner or target ship equipment and systems, the conditions of tests shall be determined according to the existing provisions. If there are no other provisions for the shipowner or target ship equipment and systems, the compliance test shall be conducted under the combined action of voltage input, temperature, vibration, humidity and other relevant test conditions. The magnitude of the test conditions shall be determined according to the target task profile and working environment profile of the item.

In order to simulate as realistically as possible the actual environment in which the item will be used, the measured stress (especially temperature and vibration) shall be preferred, and the estimated stress may also be used. The stresses may also be obtained through simulation test or by calculation. In case of failure to obtain effectively the stresses listed above, the stresses provided in 4.5.1, 4.5.2 and 4.5.3 of the Guidelines may be used by reference to the mounting position and environment for use of the item.

(1) Measured Stress

The measured stress refers to the stress determined after analysis and processing based on the data measured near the mounting position of the item under test when the item is used to perform a typical task profile in actual use.

(2) Estimated Stress

The estimated stress refers to the stress determined after analysis and processing based on the data measured at similar locations of the item with similar purposes when the item is used to perform a similar task profile. The estimated stress may be used only in the event that measured stress cannot be obtained.

(3) Reference Stress

When measured and estimated stresses cannot be determined, the requirements for reference stress given in the Guidelines may be adopted.

When specifying the comprehensive environmental conditions for compliance tests of ship equipment and systems, consideration shall be given to the installed location of items on board and the type of the ship. For example, unsheltered items installed in decks, superstructures and mast areas often endure more severe environmental stresses. in order to include the worst storage and transportation environments, cold soak and thermal soak environments should be added during comprehensive environmental test. for products with a working task profile under rainy environmental conditions, the influence of rainfall shall also be considered when designing their compliance test profiles. for products installed in engine rooms, fuel tanks and cargo holds containing volatile oils, the influence of oil mist shall also be considered.

Ship equipment and systems are divided into the following three categories according to their mounting position and environment on the ships:

(1) Externally installed items.

(2) Internally installed items in compartments without temperature control.

(3) Internally installed items in compartments with temperature control.

4.5.1 Externally Installed Items

4.5.1.1 Requirements for Electrical Stress and Working Cycle

The electrical stress includes the power-on/off cycle, the specified working mode and cycle of the item, the specified nominal input voltage and its maximum allowable deviation. During the working cycle, the input voltage shall vary between the several grades as shown in Fig. 4.5.1.1 (1). Unless specified by the shipowner or client, the input voltage range shall be 6%~10% of the nominal voltage or comply with the relevant standard. After the performance measurement of the item under test is completed at nominal voltage and room temperature, the minimum and maximum voltages shall be applied respectively according to Fig. 4.5.1.1 (1) and Fig. 4.5.1.1 (2), and the working cycle shall be carried out. The item shall not be powered on during cold soak and thermal soak, and shall be powered off 10% of the random time at other times.

4.5.1.2 Requirements for Vibration Stress

The vibration stress value and profile shall be determined according to the field service category, installed location and expected usage of the product. When determining the actual vibration stress, the following factors shall be considered at least: vibration type, frequency range, vibration quantity, direction and mode of applying vibration.

Vibration stresses shall be applied over a randomly selected 25% of the working cycle as shown in Figures 4.5.1.1 (1) and 4.5.1.1 (2). The vibration spectrum shall comply with Fig. 4.5.1.2. The test shall be conducted in a certain axial direction as specified by the requirements for use or in the user contract. The vibration procedures are as follows:

(1) Vibration stress shall be applied for 6h randomly selected every 24h, and the vibration cycle shall be 3h.

(2) Random vibration shall be carried out according to the following regulations when applying voyage and transportation random spectrum:

① Frequency range: 10Hz~200Hz.

② Magnitude (total r.m.s value): 10 m/s^2.

③ Duration: 22min.

Note1: The temperature control referred to in the Guidelines includes temperature control installations and thermostats. Temperature control installations refer to installations that control the temperature within a limited range, while thermostats refer to installations or combinations of installations that combines sensing temperature and controlling heater power.

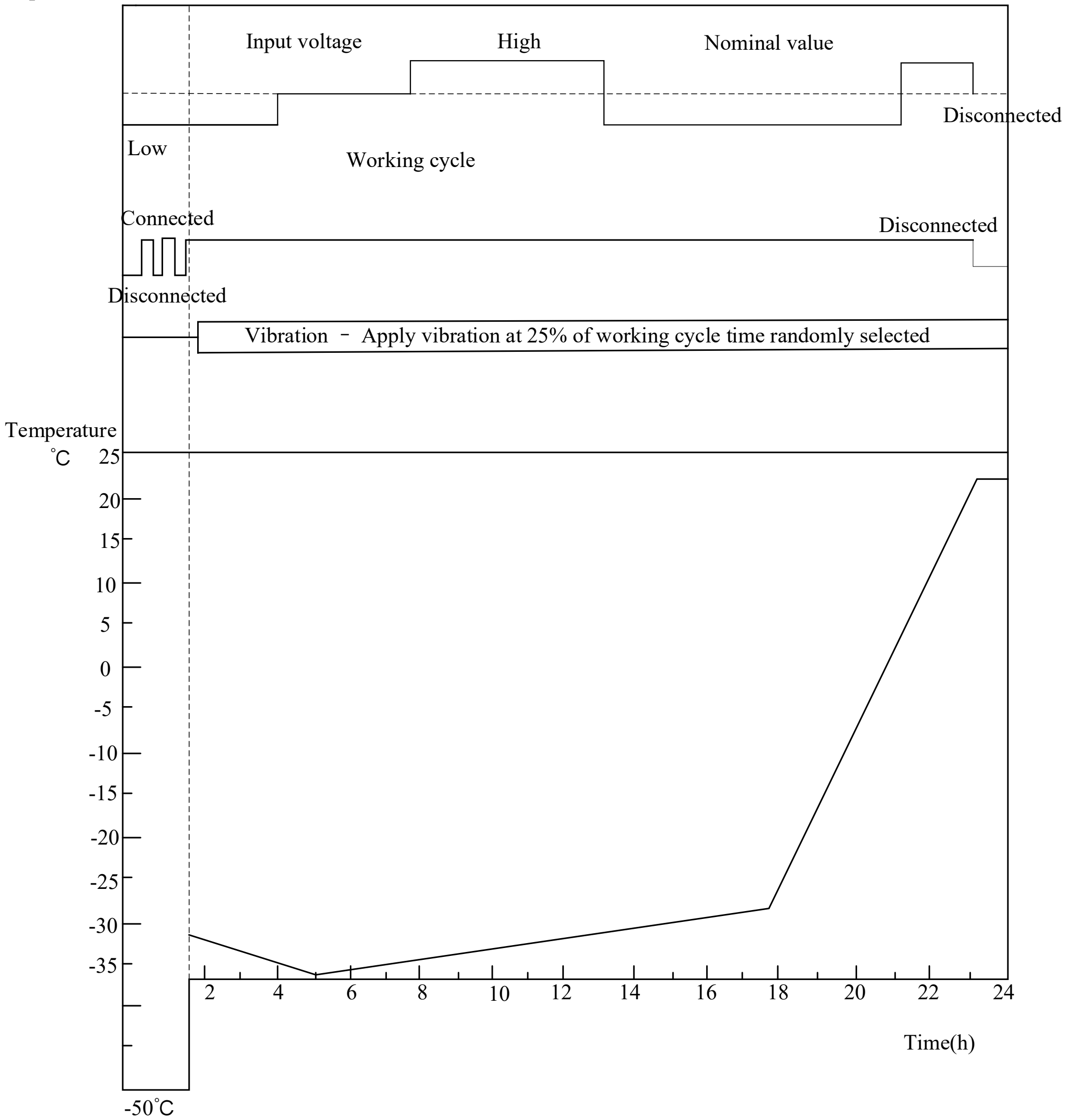


Fig. 4.5.1.1 (1) Synthetic Test Profile (Cold Cycle) for Externally Installed Items

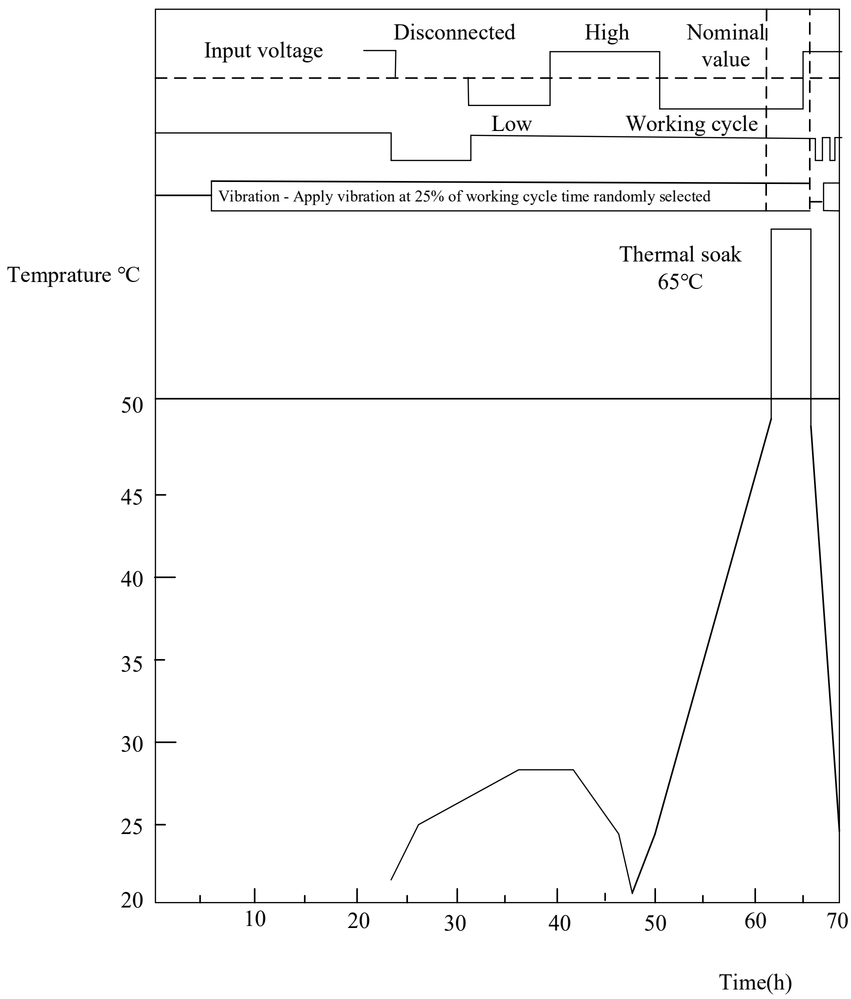


Fig. 4.5.1.1 (2) Test Profile (Thermal Cycle) of Externally Installed Products

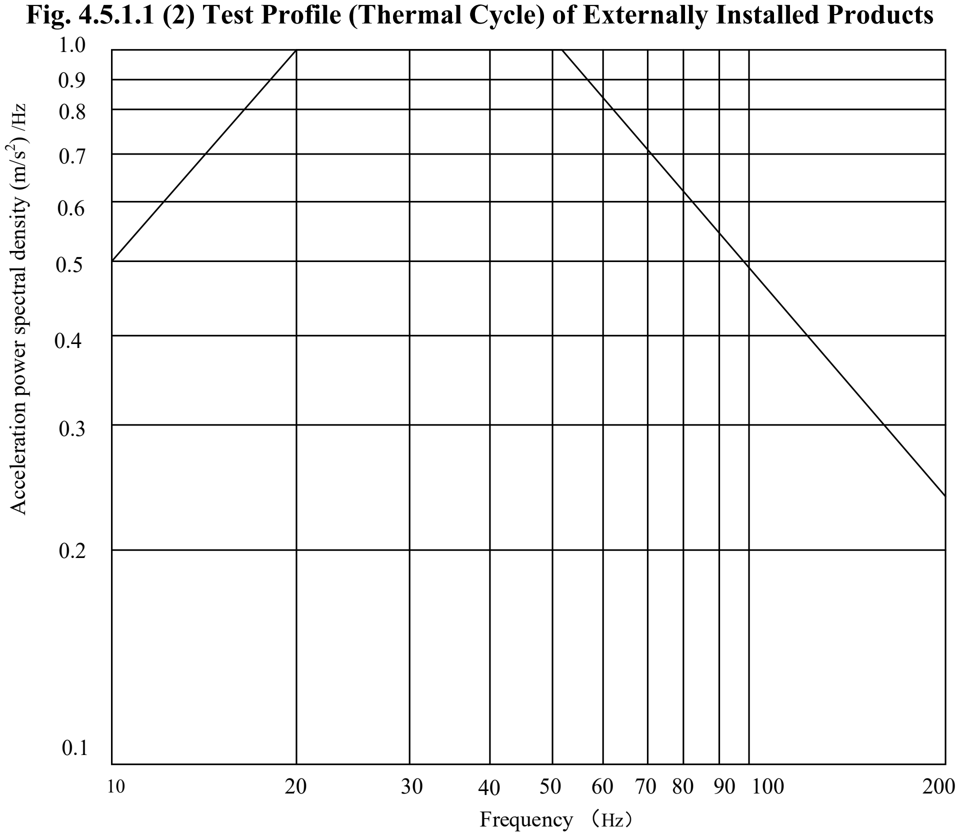


Fig. 4.5.1.2 Random Spectrum during Navigation and Transportatio

4.5.1.3 Requirements for Temperature and Humidity Stress

During the test cycle, water vapor is sprayed in at appropriate stages as needed for adjusting humidity stress to simulate environmental conditions experienced in use. The temperature stress shall realistically simulate the actual environment experienced by the item under test in use. When determining the temperature stress, the following factors shall be considered at least: initial temperature (thermal soak, cold soak), working temperature (range, temperature change rate and duration), temperature changes in each task profile, cooling airflow (equipment power consumption, congestion and cooling air flow). In addition, the actual application environment of the item under test shall be considered to avoid damage to the test piece caused by overload.

For externally installed products, the temperature and humidity profile shall be as follows, with a tolerance of ±5% for all relative humidity:

(1) Reduce the temperature to -50°C as soon as possible from 22°C and 25%~75% relative humidity, and then raise the temperature to -32°C after being kept at -50°C (cold soak) for 1.75h (without power on), with the cold soak being carried out only during the first 3 cycles.

(2) Reduce the temperature slowly to -34.5°C within 3.5h.

(3) Raise the temperature slowly to -28°C within 13h.

(4) Raise the temperature to 22°C within 5h.

(5) Keep the temperature at 22°C and adjust the relative humidity to 25%~75% within 1h.

(6) Raise the temperature to 25°C and relative humidity to 95% within 2h.

(7) Raise the temperature slowly to 29°C within 10h, and keep the relative humidity at 95% for 5h.

(8) Reduce the temperature slowly to 25°C and keep the relative humidity at 95% within 5h.

(9) Reduce the temperature to 22°C and relative humidity to 25%~75% within 2h.

(10) Rise the temperature to 25°C and adjust the relative humidity to 65% within 2h.

(11) Raise the temperature slowly to 48°C and reduce the relative humidity to 25% within 12h.

(12) Raise the temperature to 65°C (thermal soak) as soon as possible, raise the relative humidity to 95%, keep it for 2h (without power on), and then reduce the temperature to 48°C, with the thermal soak being carried out only during the first 3 cycles.

(13) Reduce the temperature slowly to 22°C and relative humidity to 25%~75% within 6h.

(14) Repeat procedures (6) to (13) five more times.

(15) Return to procedure (1) and repeat the above cycle until the required test duration is reached.

4.5.2 Internally Installed Products in Compartments without Temperature Control

For internally installed products of compartments without temperature control, the complete test profile is shown in Fig. 4.5.2 (1) and Fig. 4.5.2 (2).

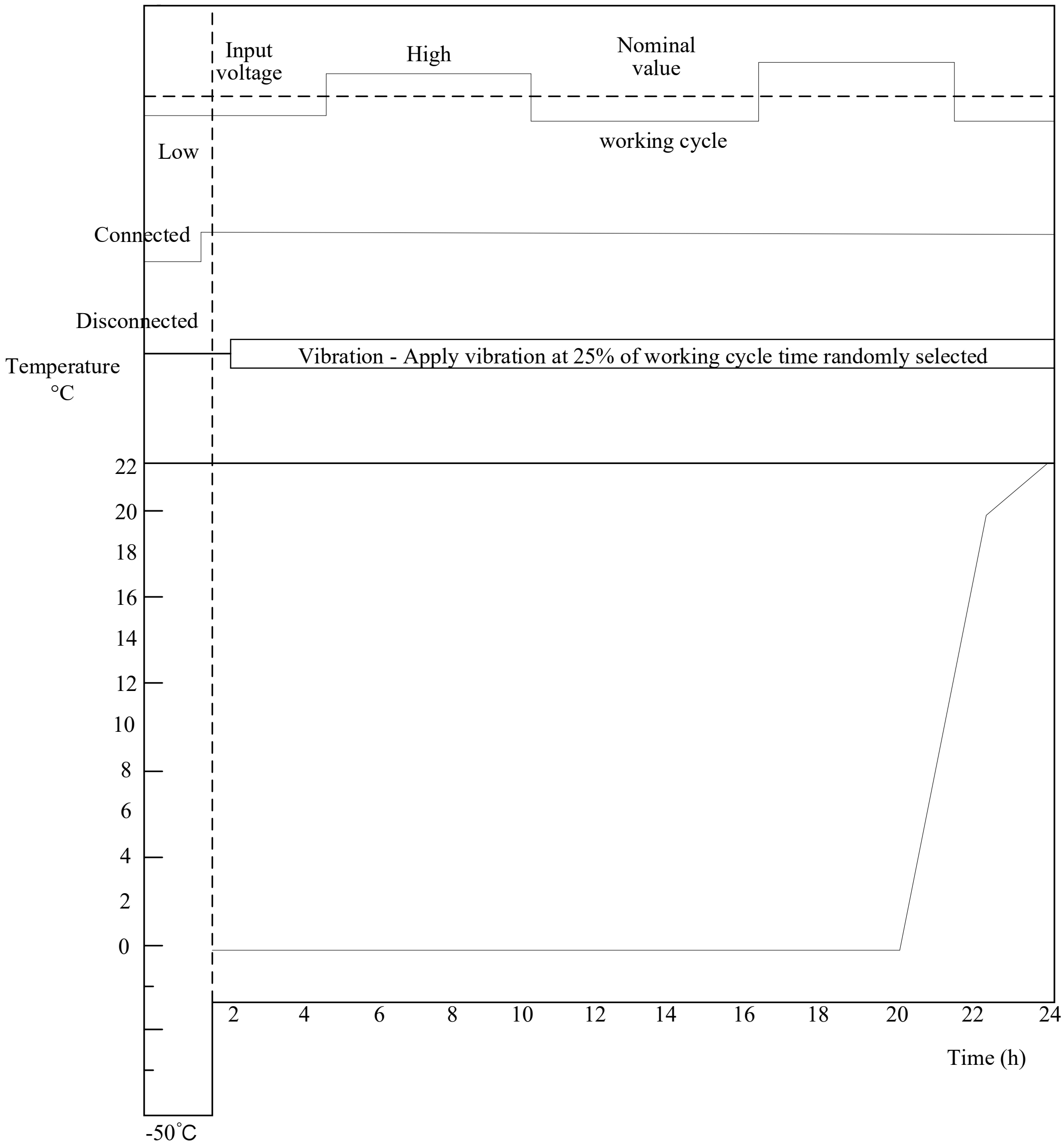


Fig. 4.5.2 (1) Test Profile (Cold Cycle) of Internally Installed Items without Temperature Control

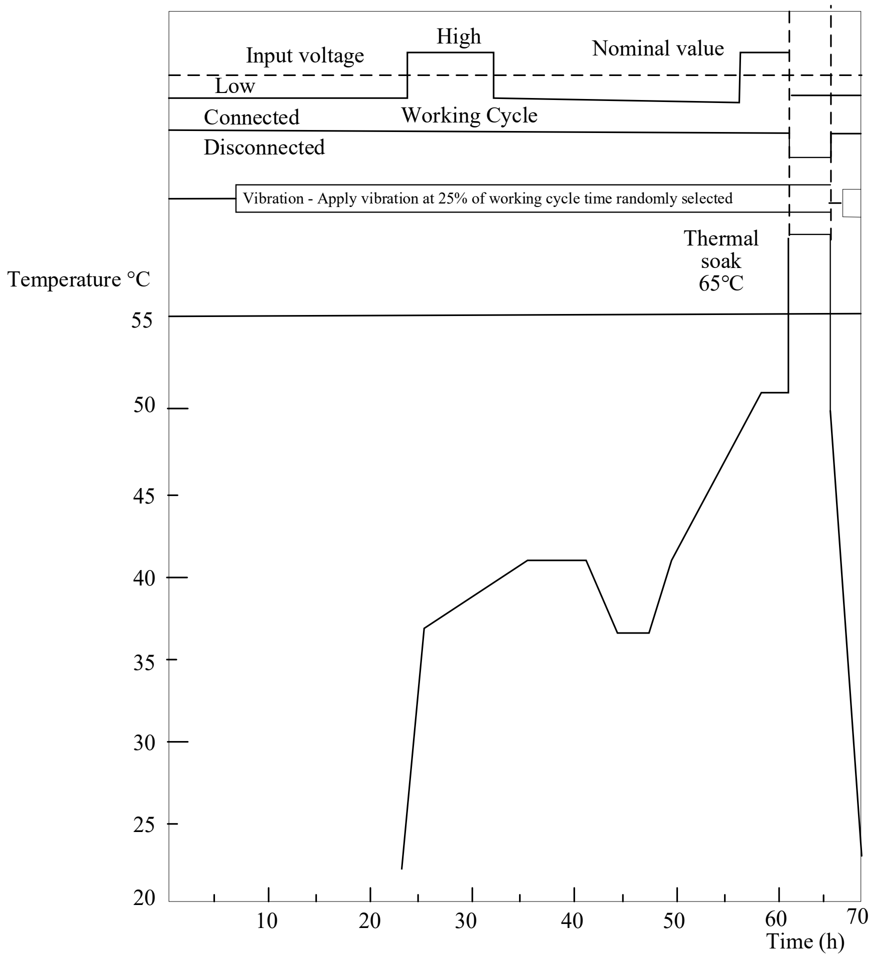


Fig. 4.5.2 (2) Test Profile (Thermal Cycle) of Internally Installed Items without Temperature Control

4.5.2.1 Requirements for Electrical Stress and Working Cycle

See the requirements in 4.5.1.1.

4.5.2.2 Requirements for Vibration Stress

See the requirements in 4.5.1.2.

4.5.2.3 Requirements for Temperature and Humidity Stresses

For internally mounted items of compartments without temperature control, the temperature and humidity profile shall be as specified below with a tolerance of ±5% on all relative humidity.

(1) Reduce the temperature to -50°C as soon as possible from the relative humidity of 22°C and 25%~75%, and then raise the temperature to 0°C as soon as possible after being kept at -50°C (cold soak) for 1.75h (without power on), with cold soak carried out only during the first 3 cycles.

(2) Raise the temperature to 19°C within 2h after being kept at 0°C for 19.5h.

(3) Adjust the temperature and relative humidity to 22°C and 25%~75% respectively within 1h.

(4) Adjust the temperature and relative humidity to 37°C and 50% respectively within 2h.

(5) Slowly adjust the temperature and relative humidity to 41°C and 48% respectively within 10h, and keep it for 5h.

(6) Adjust the temperature and relative humidity back to 37°C and 50% respectively within 5h.

(7) Keep the temperature at 37°C and reduce the relative humidity to 43% within 2h.

(8) Adjust the temperature and relative humidity to 41°C and 33% respectively within 2h.

(9) Slowly adjust the temperature and relative humidity to 50°C and 21% respectively within 9h, and keep it for 4h.

(10) Raise the temperature to 65°C (thermal soak) as soon as possible, raise the relative humidity to 95%, keep it for 2h (without power on), and then reduce the temperature to 50°C as soon as possible, with thermal soak carried out only during the first 3 cycles.

(11) Slowly adjust the temperature and relative humidity back to 22°C and 25%~75% respectively within 5h.

(12) Repeat steps (4) to (11) five more times.

(13) Return to step (1) and repeat the above cycle until the required test duration is reached.

4.5.3 Internally Installed Products of Compartments with Temperature Control

For internally installed products of compartments with temperature control, the complete test profile is shown in Fig. 4.5.3 (1) and Fig. 4.5.3 (2).

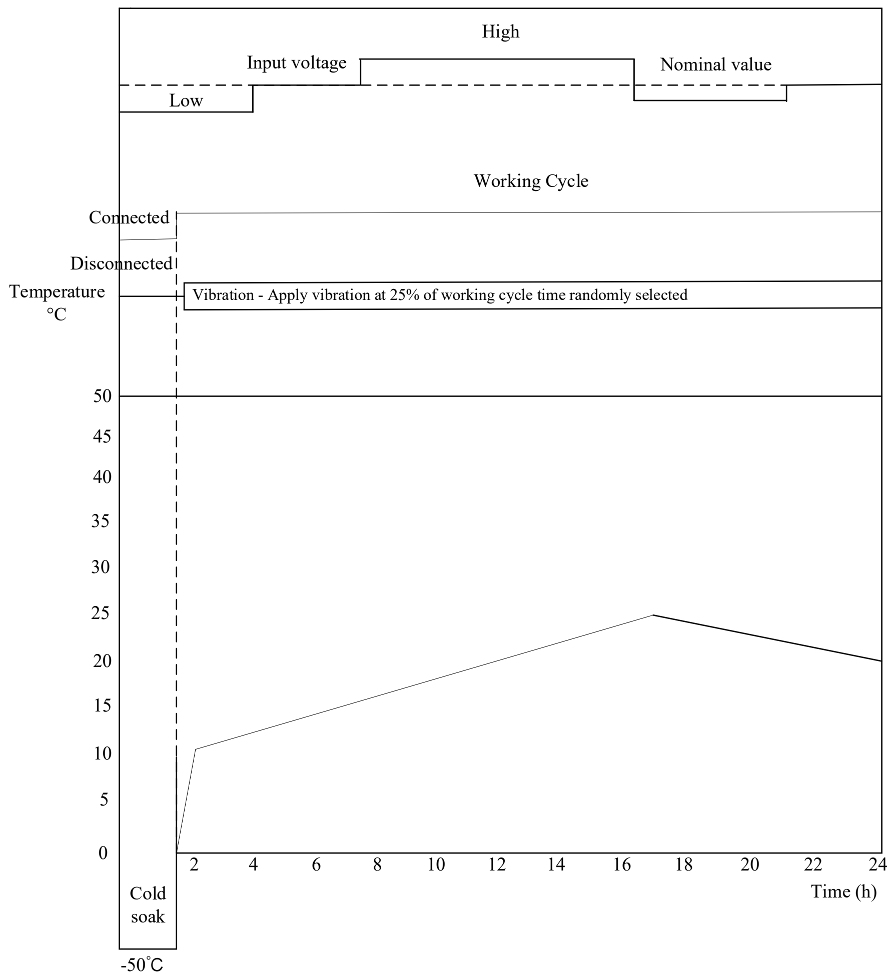


Fig. 4.5.3 (1) Test profile (front part) of Internally Installed Products of Compartments (with temperature control)

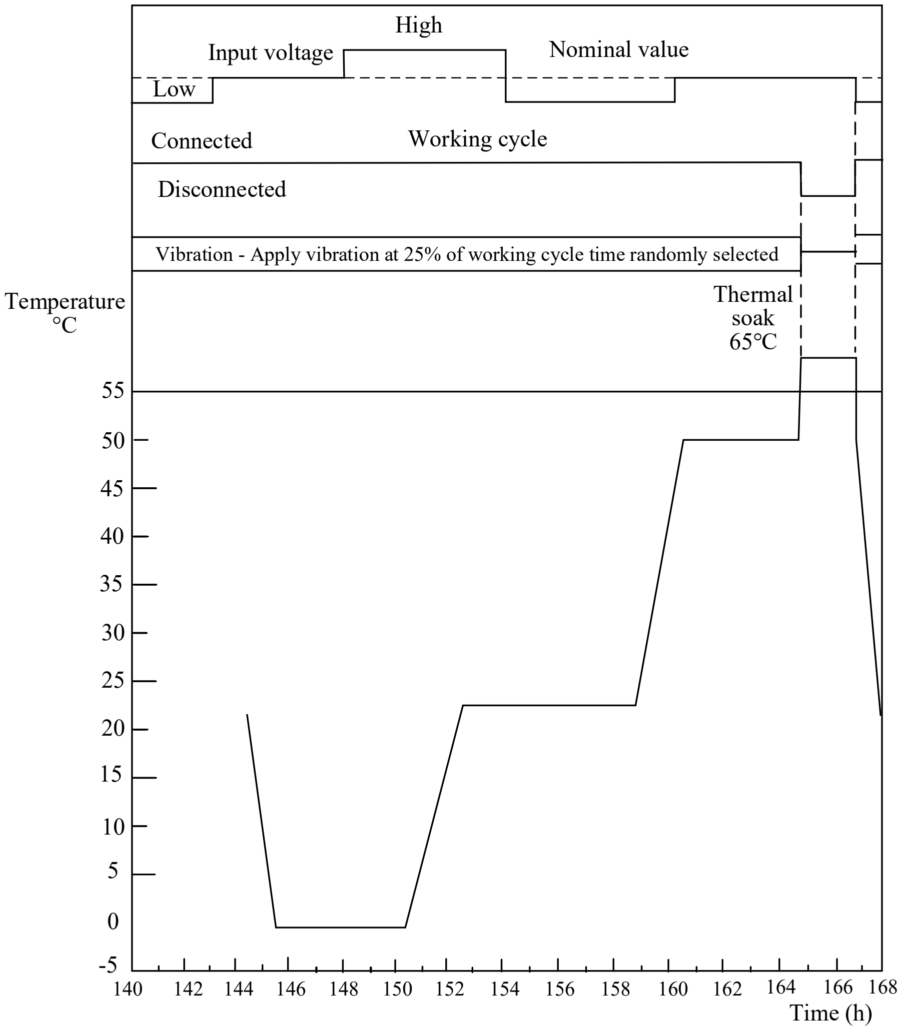


Fig. 4.5.3 (2) Test profile (rear part) of internally mounted items of compartments (with temperature control)

4.5.3.1 Requirements for Electrical Stress and Working Cycle

See 4.5.1.1.

4.5.3.2 Requirements for Vibration Stress

See 4.5.1.2.

4.5.3.3 Requirements for Temperature and Humidity Stress

For internally installed products in compartments with temperature control, the temperature and humidity profile shall be as specified below with a tolerance of ±5% on all relative humidity.

(1) Reduce the temperature to -50°C (cold soak) as soon as possible from the relative humidity of 22°C and 25%~75%, and then raise the temperature to 10°C and adjust the relative humidity to 75% within 0.25h after being kept at -50°C (cold soak) for 1.75h (with power on), with cold soak carried out only during the first 3 cycles.

(2) Slowly adjust the temperature and relative humidity to 25°C and 30% respectively within 15h.

(3) Slowly adjust the temperature and relative humidity to 22°C and 30% respectively within 7h.

(4) Repeat steps (1) to (3) five more times.

(5) Reduce the temperature to 0°C within 1h and keep it for 5h.

(6) Adjust the temperature and relative humidity to 22°C and 46% respectively within 2h, and keep it for 7h.

(7) Adjust the temperature and relative humidity to 50°C and 21% respectively within 2h, raise the temperature to 65°C (thermal soak) as soon as possible after being kept at 50°C for 4h, and then quickly reduce the temperature to 5°C after being kept at 65°C for 2h (without power on), with thermal soak carried out only during the first 3 cycles.

(8) Adjust the temperature and relative humidity to 22°C and 25%~75% respectively within 1h.

(9) Return to step (1) and repeat this cycle until the required test duration is achieved.

Chapter 5 Reliability Verification of Ship Equipment

5.1 General

This chapter applies to electrical, electronic, mechanical, pneumatic, hydraulic and material equipment, with computer systems excluded.

5.2 Test Purpose

In general, compliance test shall be carried out for newly developed or improved equipment with reliability index requirements, especially for key or high-tech equipment. The verification of equipment characteristics or performance with the specified reliability requirements shall be verified based on the test data.

The result of the compliance test is “accepted” (conforming) or “rejected” (non-conforming). The verification test is based on the theory of statistical hypothesis testing, which assumes parameters for the set probability model. The test plan plan and judgment standard shall be determined according to one of the following two characteristics, and then further determined by decision risks and discrimination ratio. One is the number of acceptable relevant failures (which can be zero) for a specified number of tests or within a specified test duration. the other is the ratio of acceptable test times to acceptable test duration for the specified number of relevant failures (which can be zero).

Corresponding decision-making risks include the manufacturer’s risk and the user’s risk. The manufacturer’s risk is the probability of rejection when the equipment has a specified acceptable reliability value (Category I risk), while the user’s risk is the probability of acceptance when the equipment has a specified unacceptable reliability value (Category II risk). To minimize Category I and II risks of the equipment, the manufacturer shall make sure that the reliability of the equipment is better than the specified acceptable value, and the same is true for the user. The discrimination ratio corresponds to the reliability metrics. success/failure rate, failure rate and failure intensity are optional. See GB/T 5080.1-2012 for the types and comparison of statistical plans, and see GB/T5080.5-1985 and GB/T5080.7-1985 for test plans.

5.3 Test Environment

Generally, the compliance test is carried out with representative equipment that can represent the technical state of the mature equipment and reflect the design and manufacturing level. Laboratory test or field test can be used as the test method.

The compliance test shall be carried out in such a way as to simulate the actual conditions of use, including environmental, operating and maintenance conditions. See Chapter 4 of the Guildeline for environment-related requirements.

The test shall be carried out in the presence of surveyors or by a recognized independent third-party inspection and testing agency accepted by the Society or as specifically agreed.

5.4 Test Content

The test content mainly include statistical test plan design, test profile design and test implementation.

Statistical test protocols, test conditions, test facilities, operating procedures, observations, test reports, and test data analysis shall be included in the test plan. Among them, the applicable reliability indicators and acceptable values, the validity of test distribution hypothesis, the product matrix and specific sampling methods for test sampling, the test equipment for monitoring the test operation of products, maintenance equipment and test procedures, and measures to be taken when the tested products and test facilities fail shall be specified.

Any requirements for product compliance test shall be included or specified in the product contract or product technical specification.

5.5 Test Method

5.5.1 Statistical Test Plan

The test plan shall describe the number of products to be tested, the way to deal with the faulty equipment (maintenance, replacement, removed), and the criteria for ending the test.There are two basic test plans. The products in the test can be replaced or unreplaced/repaired or unrepaired.

(1) Truncated sequential test

During a truncated sequential test, the products shall be monitored continuously or at short intervals according to the pre-determined time for acceptance, rejection and truncation, and the accumulated related test duration and the number of relevant failures shall be compared with the criteria for determining whether to accept, reject or continue the test.

(2) Fixed-time/-number truncated test

During a fixed-time/-number truncated test, the truncated time/number of failures shall be specified in advance, and the tested products shall be monitored continuously or at short intervals until the cumulative related test duration exceeds the pre-determined related test duration (accepted) or the pre-determined number of relevant failures (rejected) occurs.

The test plan shall be selected based on statistical considerations. Exponential distribution applies to electronic products, some electromechanical products and complex functional systems whose reliability index is measured by time, while binomial distribution applies to success-failure products whose reliability index is success rate. If none of the above applies, other modes of distribution may be considered, such as Weibull distribution.

5.5.2 Test Profile Design

See Sections 4.4 and 4.5 of Chapter 4 of the Guideline for test profile design.

5.5.3 Test Process

See Fig. 5.5 for the process of compliance test. See [5.1.2] in GB/T 5080.1-2012 for specific requirements for product compliance test. See [7] and [8] in GB/T 5080.1-2012 for the requirements for test data collection and analysis.

5.6 Life Test

According to the time required and test conditions for obtaining expected information, life tests can be divided as normal and accelerated. Usually, a normal life test on the high reliability equipment requires longer time. Accelerated tests are usually used to shorten the market cycle of the equipment, reduce equipment costs and satisfy demands for economic and efficient test methods.

Regarding the way of stress increase, accelerated life tests can be divided as constant-stress, step-stress and progress-stress. For equipment with accelerating life index, accelerated life tests can be carried out in accordance with Appendix E of GB/T 34986-2017, and the test output is the reliability parameter or life index. Normal life tests shall be carried out over some equipment whose life indexes (e.g. cycle life of switches, the opening and closing times of folding plates) are not accelerating. See Section 5.5 of this chapter for test methods.

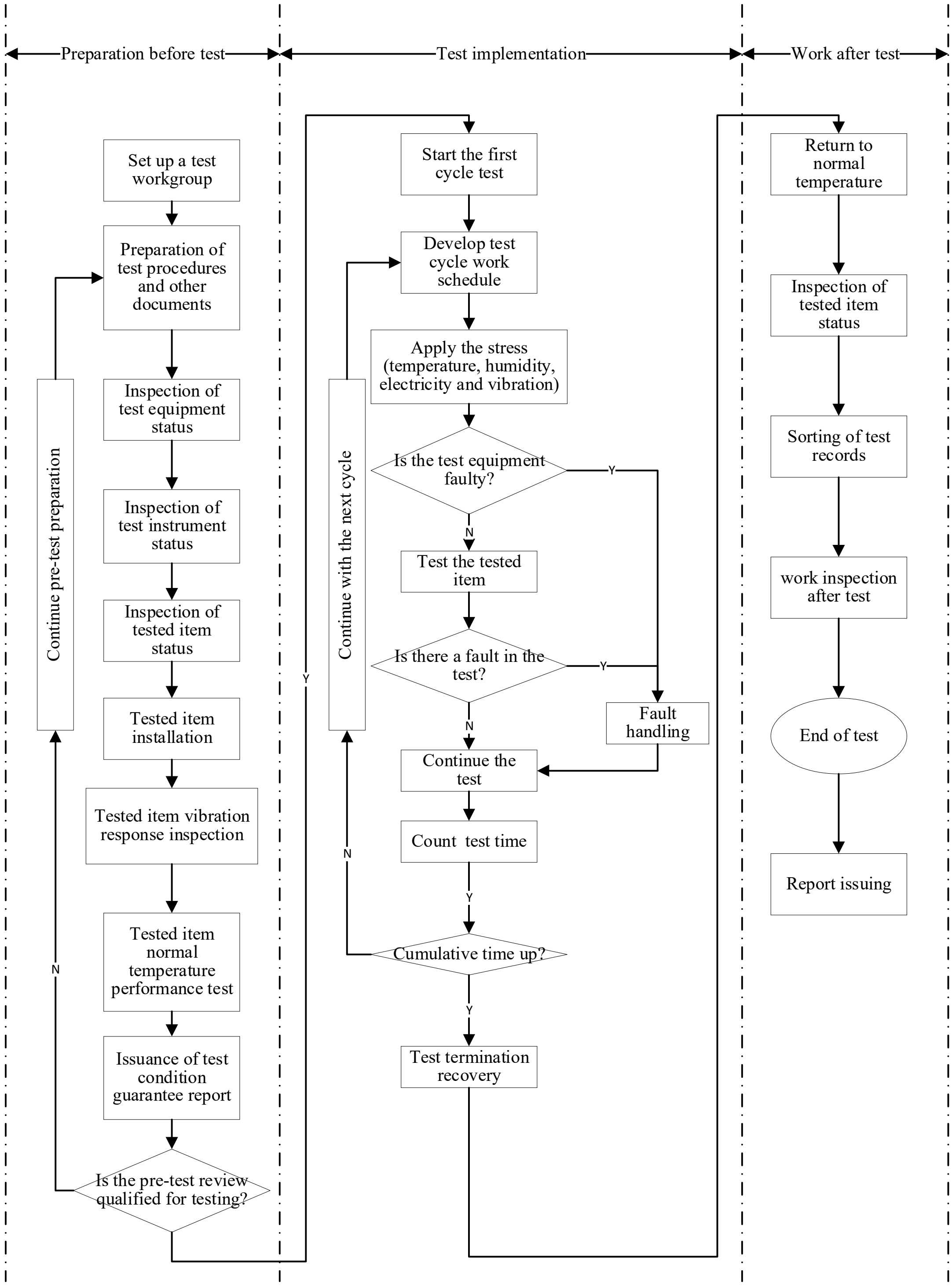


Fig. 5.5 Flow Diagram of Compliance Test

Chapter 6 Reliability Verification of Ship Computer Software

6.1 General

The reliability of computer software is a software quality index, and software failure may endanger the entire system.

Software reliability verification is based on software testing, which is the main means to ensure software quality and improve software reliability. A lack of adequate test work makes it impossible to effectively analyze and predict software reliability. Before software reliability verification, make sure that the metrics comply the predetermined requirements, that is, the precondition of software reliability verification is that the software has been running for a period of time and has passed the functional test. See ISO/IEC/IEEE 29119 for requirements related to software testing.

Software requires hardware installations for program execution, storage and transmission, for which relevant software/hardware environment and network environment shall also be comprehensively considered in the software reliability test.

This chapter provides the reliability verification requirements applicable to ship computer software in combination with the requirements of Guidelines for Safety and Reliability Assessment for Shipboard Software, Guidelines on Maritime Cyber Risk Assessment and Cyber Safety Management System and Guidelines for Survey of Intelligent Equipment of the Society.

6.2 Test Purpose

The reliability indexes of computer software can be mainly divided as maturity, tolerance and recovery. Setting suitable reliability metrics of computer software can provide software demanders, evaluators and suppliers with a unified method for measuring, testing and evaluation. This chapter aims to verify whether the software meets reliability metrics.

6.3 Test Environment

The test environment includes the software/hardware and network environment corresponding to the tested software system, the selected test tools, and the set test scenario. See Section 4.5 of Chapter 4 of the Guideline for the comprehensive environmental stress requirements of the test scenario.

6.4 Test Content

For reliability metrics, failure data and software reliability models are used to evaluate the reliability of software operation and confirm whether it complys user requirements.

6.5 Test Method

6.5.1 Software Reliability Index

When testing software reliability verification, testers shall analyze and determine the reliability indexes in accordance with the reliability requirements provided by the user. See Table 6.5.1 for the relationship between software reliability indexes and test values.

Table 6.5.1 Comparison of Software Reliability Indexes and Test Values

Reliability indexes			Test value	Calculation method	Description
Maturity	Degree of failure	Failure density	A, number of failures actually detected B, total number of actual test cases	X=A/B	X⩾0 The smaller the X value, the better, and the X value shall get smaller with the test process.
		Failure resolution rate	A, number of non-recurring failures under the same conditions B, number of failures actually detected	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better
	Degree of fault	Fault density	A, number of faults actually detected B, item size (e.g. source lines of code or function points)	X=A/B	X⩾0 The smaller the X value, the better, and the X value shall get smaller with the test process.
		Potential fault rate	A_1, the total number of potential faults predicted, with selecting a reliability growth estimation model A_2, number of faults actually measured B, item size (e.g. source lines of code or function points)	$X=ABS(A_1-A_2)/B$	X⩾0 The smaller the X value, the better, and the X value shall get smaller with the test process.
		Troubleshooting rate	A_1, number of faults excluded A_2, Number of faults actually measured A_3, the total number of potential faults predicted , with selecting a reliability growth estimation model	$X=A_1/A_2$ $Y=A_1/A_3$	0.0 against X⩽1.0, 0.0 against Y⩽1.0, The closer X and Y are to 1.0, the better
	Degree of test	Test coverage	A, number of test cases actually executed in the test period B, number of test cases planned to be executed according to coverage requirements	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better
		Test pass rate	A, number of test cases passed during the test or operation B, number of test cases planned to be executed according to coverage requirements	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better
	Validity	Mean time between failure intervals	T_1, run time cycle T_2, Time interval between cumulative successive failures A, total number of failures actually detected	$X=T_1/A$ $Y=T_2/A$	X>0, Y>0. the greater X and Y values, the better
		Effective service time rate	A, effective service time B, cumulative total service time	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better

Reliability indexes			Test value	Calculation method	Description
		Cumulative effective service time	T, cumulative recorded service time without failure	X=T	X⩾0 The greater the X value, the better
Fault tolerance	Normal operation	Downtime avoidance[1] rate	A, number of failures resulting in downtime, determined through analysis B, number of failures actually detected in the failure density test	X=1-A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better
		Downtime avoidance rate	A, number of test cases without critical and serious failures B, number of test cases performed in failure mode	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better
	Misoperation resistance rate	-	A, number of test cases without critical and serious failures B, number of test cases performed in misoperation mode	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better
Recovery	Degree of restart success	Average downtime	T, cumulative time from downtime to normal use of software in a specific test cycle N, number of downtimes observed (or recorded) during a specific test cycle	X=T/N	X > 0 The smaller the X value, the better
		Mean time to restoration	T_1 ,T_2 ,... , T_n, time from each failure to full recovery N, total number of software recovery attempts during a specified test cycle	X= $(T_1+T_2+\ldots\ldots+T_n)$ /N	X > 0 The smaller the X value, the better
	Degree of repair success	Repairability	A, number of test cases successfully recovered, determined through analysis B, number of recovery test cases executed	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better
		Repair effectiveness	A, number of test cases successfully recovered within the target recovery time, determined through analysis B, total number of recovery test cases executed	X=A/B	0.0⩽X⩽1.0 The closer X is to 1.0, the better

Note 1: Downtime means that the user's all tasks have been stopped or the user has lost control of the system before system restart, resulting in forced halt of the computer.

6.5.2 Software Reliability Test Methods

Computer software reliability test methods include expert review, technical testing, mathematical calculation, and user survey. See Table 6.5.2 for comparison of the four test methods.

Table 6.5.2 Commonly Used Software Reliability Testing Methods

Method name	Judgment criteria	Object	Means	Result
Expert review method	Subjective	List of review items	Score	Qualitative
Technical testing method	Objective	Software test data	Automatic testing tools/manual testing	Quantitative
Mathematical calculation method	Objective	Software test data	Mathematical model calculation	Quantitative
User survey method	Subjective	Specific questionnaire	Complete the questionnaire	Qualitative

To obtain objective and quantitative measuring results, technical testing method or mathematical calculation method is usually applied in newly developed software with high new technology content and high reliability requirements.

6.5.3 Test Procedure

The process of a software reliability test is shown in Fig. 6.5.3 (1). The key steps are described as follows, and other steps are specified in Appendix A of GB/T 29832.3-2013.

(1) Reliability Model

During the software reliability test, the reliability model shall be determined as early as possible with consideration of its assumption that shall conform to the actual situation of the software. Analysis of each assumption is necessary, and a relatively mature and widely used model shall be selected for analysis when other conditions are met. Regarding the total number of failures within a certain time, exponential failure time model, Weibull or Gamma failure model are the key considerations. See GJB/Z161-2021 for details of the above models. For the failure distribution of time, Poisson distribution and binomial distribution are the key considerations. Exponential failure time model is a finite failure model with exponential failure strength function. Weibull distribution and Gamma distribution, which are widely used in equipment reliability modeling, also apply to the software field for the purpose of expressing the relationship between the expected number of failures and the function of failure intensity.

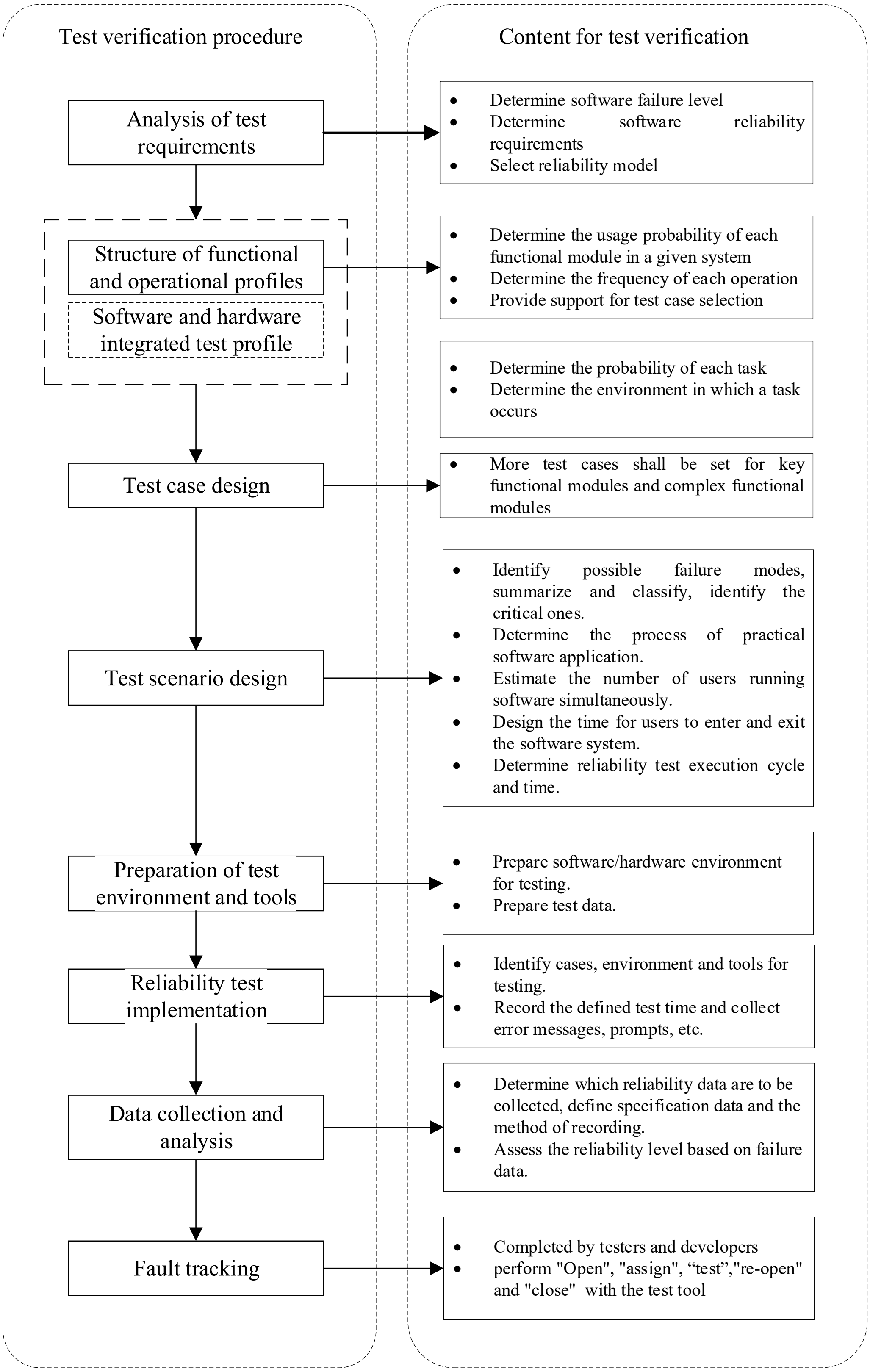


Fig. 6.5.3 (1) Software Reliability Test Procedure

(2) Functional and Operational Profiles of Software

The structure of functional profile critically impacts the selection of test cases for software reliability. For software in use, the usage probability of each function varies. Meanwhile, there is a certain relationship between functions and operations. One function corresponds to one or more operations, and a group of functions can be merged into a different group of operations, making the use probability of each operation different. The functional and operational profiles describe the actual use of the software in detail. In actual tests, the functional and operational profiles shall be combined and tailored according to the actual situation for construction of the test profile.

The testing work shall be reasonably distributed according to the frequency of different functions, so that the actual use of the software can be reflected truly in the software reliability testing and every function can be fully tested.

(3) Integrate Test Profile of Software/Hardware

During a verification test, the actual use conditions (including environmental and working conditions) shall be simulated as much as possible, and all possible task ranges shall be covered as much as possible. The use of equipment can be divided into three interrelated levels: task, function and operation. Tasks are the goals that the equipment is expected to achieve, and each task cannot happen simultaneously. One or more functions are implemented through one or more operations, ultimately completing a task. The probability of task occurrence can be determined through equipment maintenance data and usage logs. At the same time, for the use of equipment, the task determines the main environmental conditions.

To sum up, according to the actual situation of the equipment, a software and hardware integrated test profile can be designed. The design process is shown in Fig. 6.5.3 (2). For the combined environmental stress of the equipment, please refer to Chapter 4, Section 4.5 of the Guidelines. for the structure of the software test profile, please refer to Section 6.5.2 (2) of the Guidelines. The combined environmental stress of any equipment shall be assigned to the software test profile.

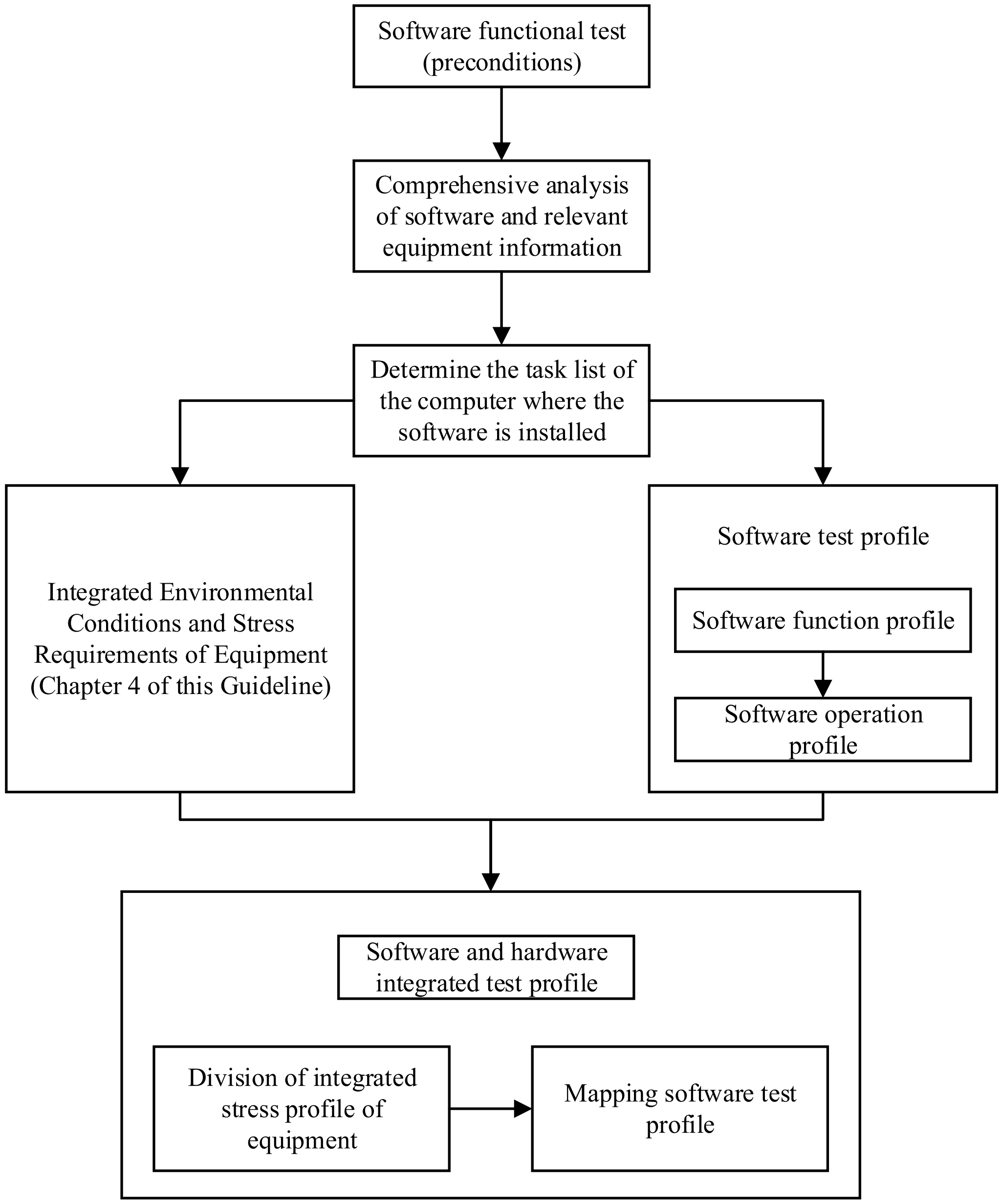


Fig. 6.5.3 (2) Design Process for Integrated Software and Hardware Test Profile

Chapter 7 Reliability Verification of Embedded Software for Ship Equipment

7.1 General

Ship equipment includes software systems with embedded characteristics that involve data interaction between software and hardware components. Therefore, it is necessary to conduct reliability testing and verification for embedded software.

7.2 Test Purpose

To verify whether the embedded software for ship equipment complys the requirements stated in the embedded system development contract or project development plan.

To verify the software reliability requirements and quantitative reliability requirements specified in the system and subsystem design documents, software requirement specifications and software design descriptions.

To assess the reliability level of current embedded software for ship equipment.

7.3 Test environment

It should replicate the target environment for ship equipment operation, or provide a highly consistent simulation laboratory environment.

It should be equipped with necessary test instruments for the application verification of ship equipment, such as frequency source, waveform generator, standard voltage and current source, protocol analyzer, etc.

It should provide the necessary test environments such as temperature, humidity and vibration for the operation of ship equipment. Please refer to Chapter 4 of the Guidelines for details. It should support the complete external input-output environment required for the operational profile of the ship equipment.

7.4 Test Contents

Before the release or delivery of ship equipment/embedded software products, reliability confirmation tests shall be carried out to confirm that reliability indicators specified in the contract are met.

7.5 Test Method

7.5.1 General

When conducting reliability testing for ship equipment's embedded software, it is essential to establish clear reliability objectives. If the applicant has not provided specified reliability objectives, the methods described in section 7.5.2 can be used to determine the reliability objectives.

Once the reliability objectives are established, the following steps should be followed: Develop a testing plan, create an operational profile, carry out test preparation, execute the reliability test, analyze and evaluate test results and finally generate a reliability test report.

7.5.2 Determination of Reliability Objectives

7.5.2.1 Determining Failure Degree

For embedded software for ship equipment, the failure degree shall be determined according to the scope and target users of the products. Typically, the failure degree is classified based on their impact on human life, cost, and system capabilities. By categorizing the level of failure degree, the failure data can be analyzed to determine whether defects need to be identified and resolved during the testing process. The table below provides suggested levels of failure degree.

Table 7.5.2.1 Levels of Failure degree of Embedded Software

Failure degree level	Description of failure
1	Inability to perform one or more critical operations
2	Inability to perform one or more important operations
3	Inability to perform one or more operations, but with available remedies
4	Minor defects in one or more operations

7.5.2.2 Establishing Failure Intensity Objective

Based on the target users of ship equipment, failure intensity objective is established for embedded software. The table below provides a recommended comparison between failure intensity objective, failure interval, and failure effect.

Table 7.5.2.2 Failure Intensity Objective, Failure Interval and Failure Effect

Failure Effect	Typical Failure Intensity Objective	Failure Interval
Causing casualties or economic losses of more than RMB 10 million	10^{-6}	114a
Causing no casualties but economic losses of RMB 100,000 or more	10^{-4}	10000h
Causing no casualties but economic losses of RMB 10,000 or more	10^{-3}	1000h
Causing no casualties but economic loss of more than RMB 1,000	10^{-2}	100h
Causing no casualties but little economic loss	10^{-1}	10h
Causing no casualties but minor or no economic losses	1	1h

Note1: In the table, “a” represents days, and “h” represents hours.

7.5.2.3 Selection of Common Metrics

Since embedded software in ship equipment generally operates continuously, the calendar time metric for embedded software is aligned with the execution time metric. Calendar time, represented by hours (h), is selected as the universal metric (used for incidents that commonly occur) in this testing method. Table 7.5.2.3 provides a comparison between the reliability of a 1-hour task and the equivalent failure intensity for specific time intervals.

Table 7.5.2.3 Reliability of a 1-hour Task and Equivalent Failure Intensity for Specific Time Intervals

Reliability of a 1-hour Task	Specific Period Failure Intensity
0.368	1 failure/1h
0.9	105 failures/1000h
0.959	1 failure/day

Reliability of a 1-hour Task	Specific Period Failure Intensity
0.99	10 failures/1000h
0.994	1 failure/week
0.9986	1 failure/month
0.999	1 failure/1000h
0.99989	1 failure/year

The conversion of failure intensity and reliability is carried out according to the following formula:

$$\lambda = -\frac{\ln R}{t}$$

$$R = \exp(-\lambda t)$$

Where:

λ :Failure intensity.

R :Reliability.

t :Number of time units.

7.5.3 Development of Operational Profiles

7.5.3.1 General

The operating profile of the embedded software for ship equipment can be constructed using tables or graphical representations. When developing operational profiles, the following steps should be followed: Determine the inputs and related data fields. analyze the reliability requirements of the system. classify and list all possible operating modes. analyze the external conditions that impact the software's operational modes and assess their degree of influence. analyze and combine the interrelationships among different functional requirements. merge closely related functional modules and provide input variable combinations for partially related functional modules.

7.5.3.2 Determining the Operation Mode

Different embedded software may have significantly different operating modes. The Guidelines recommend using the method provided in Table 7.5.3.2 to determine the operating modes.

Table 7.5.3.2 Methods for Determining Operating Modes

Determining the Operation Mode	Determination method
Major and Minor Time Differences	Significant differences in the timing or frequency of transactions within a day or during specific time periods.
Different user types	Administrators, regular users, beginners, etc.
Significant difference in input	Large and multilateral inputs
Power supply limit	Power supply requirements
Temperature limit	Temperature requirements
Electromagnetic limit	Requirements for Electromagnetic Compatibility

Determining the Operation Mode	Determination method
Significant changes in other environments	Requirements for humidity, vibration, salt spray and noise
Patterns required by industry standards	Requirements specific to industries such as telecommunications, power, banking, etc.

7.5.3.3 Determining Initiators of Operations

The operation initiator includes the user, external conditions and embedded system itself, which shall be identified according to the determination method provided in Table 7.5.3.3.

Table 7.5.3.3 Methods for Determining operation initiator

Operation initiator	Determination method
User	User operation, remote login, etc.
External conditions	External inputs, e.g. input of a quantity, receipt of input signals.
Embedded system	Conditions identified by software and hardware of embedded system, such as memory anomalies, interrupt signals and internal variables.

7.5.3.4 Selection of Expression Method

There are two common expression methods for operational profiles: table-based and graphical representation. The Guidelines recommend using the table-based method to list all the operation modes, operation initiator, operations themselves, and their occurrence rates in a tabular format.

7.5.3.5 Creation of operation table

The creation of the operation table requires reference to user requirements, software instructions, industry regulations, relevant standard requirements, etc. Typically, the table is divided based on the initiators of operations. The comprehensiveness of the coverage shall be taken into account when defining input spaces and operating overlay input spaces. Table 7.5.3.5 provides an example of creating an operation table.

Table 7.5.3.5 Example of Creating an Operation

Identify the initiator	Operation
A (External input of a signal)	Output a signal to external 1
	Output a signal to external 2
B (User input of a command)	Displays a line of information
C (Internal data storage full)	Prompt “data full”
	System signal light on

7.5.3.6 Determination of Occurrence Rate

The occurrence rate of each operation is determined based on user requirements, software specifications, instructions for use, experience and other information. Table 7.5.3.6 gives an example of how to determine the occurrence rate.

Table 7.5.3.6 Example of Occurrence Rate

Operation	Occurrence Rate (Occurrences per Hour)

Output a signal to external 1	10
Output a signal to external 2	10
Displays a line of information	1000
Prompt “data full”	0.001
System signal light on	0.001
Total	1020.002

7.5.3.7 Determination of Occurrence Probability

The occurrence probability of each operation is determined by dividing the occurrence rate of each operation by the total occurrence rate. Table 7.5.3.7 illustrates how to calculate the occurrence probability.

Table 7.5.3.7 Occurrence Probability Example

Operation	Occurrence Probability
Output a signal to external 1	0.0098
Output a signal to external 2	0.0098
Displays a line of information	0.9804
Prompt “data full”	0.00000098
System signal light on	0.00000098
Total	1

7.5.4 Test preparation

7.5.4.1 General

Test preparation involves generating test case input files based on probability distribution information and the test plan, calculating or specifying the expected output for each test case, setting up the testing environment, selecting or developing testing tools, and designing test cases. When preparing test cases, it is essential to ensure comprehensive test coverage.

7.5.4.2 Preparation of test cases

Test case preparation activities mainly include:

(1) Estimating the number of new test cases required for the current version.

(2) Allocating new test cases among the systems to be tested.

(3) Allocating new test cases among new operations within each system.

(4) Specifying new test cases.

(5) Developing new test cases and integrating them with existing ones.

(6) Designing initial reliability test cases for newly developed software based on previous phase test cases.

7.5.4.2.1 Estimating the number of test cases required

Estimate the number of test cases required, taking into account time and cost factors. Take the minimum value of these two numbers as the number of test cases planned to be prepared:

① Time is calculated by multiplying the available time by the number of available personnel and dividing by the average time to prepare a test case.

② Costs are calculated by dividing the budget allocated for test case preparation by the average cost of preparing each test case. For retesting, such as regression testing, only the number of newly added test cases is considered.

7.5.4.2.2 Allocation of Test Cases

Allocate specific number of test cases for each operation. For regression testing, only test cases for newly modified operations are considered. Based on the occurrence probabilities of operations, perform the following tasks:

① Identify key operations that occur infrequently (low probability but important to test) and allocate the number of test cases for each of these operations. Key operations refer to those that can cause personal injury or significant loss, and an adequate number of test cases should be assigned to these operations.

② Identify occasional operations (rare operations) and allocate one test case for each. Occasional operations refer to operations with very low occurrence probabilities. The purpose of allocating one test case is to ensure that at least one test case is assigned to such operations.

③ Distribute the remaining test cases among the remaining operations based on their occurrence probabilities.

7.5.4.2.3 Specifying test cases

Specify test cases for each operation. The steps for specifying test cases include:

① From the value ranges of the direct input variables for an operation, identify value range combinations that exhibit similar failure behaviors.

② After selecting the value range combinations for the input variables, randomly choose input variables from the set of value range components to create a test case.

③ Once the test cases are selected, create test case scripts.

7.5.4.3 Preparation of Test Process

Prepare a test process for each operation mode by establishing or adjusting the test operation profile and operation occurrence rates. The adjustments mainly occur during regression testing or testing processes influenced by requirement changes.

7.5.5 Execute the test.

7.5.5.1 General Requirements

The test environment for the software under test (including hardware configuration and software support environment) shall be consistent with the expected actual use environment.

Conduct testing for each test case according to the test plan and sequence, and assess whether the software output matches the expected results. During testing, record the test results, execution time, and assessment outcomes. If a software failure occurs, record the failure symptoms and timing for failure analysis purposes.

7.5.5.2 Allocation of test time

Testing time is allocated using the following methods:

(1) Allocate test time among the systems to be tested.

(2) Prioritize functional testing to ensure comprehensive execution of test cases and perform regression testing on the previous version. Allocate the remaining time to load testing.

(3) Allocate testing time among the operation modes during load testing.

(4) Test time is allocated in hours.

The estimated testing time can be calculated using the following formula:

$$t = \frac{T_N}{\lambda_F}$$

Where:

t : Test time measured by natural or clock time unit.

λ_F : Failure intensity objective.

T_N : Normalized failure time (MTTF number), as follows:

$$T_N = \frac{\ln \frac{\beta}{1-\alpha}}{1-\gamma}$$

Where:

γ : Discrimination ratio.

α : Developer risk, which is the probability of erroneously concluding that the failure intensity objective has not been reached when it has actually been reached.

β : Customer risk, which is the probability of erroneously concluding that the failure intensity objective has been reached when it has not been reached.

7.5.5.3 Test Invocation

The functional test calls the test cases in the assigned order to perform testing.

A regression test is performed after each major software modification. Regression testing should comprehensively examine areas affected by requirement changes. It is important to distinguish between random testing and regression testing as they have different requirements. Test cases should be invoked based on the impact domain.

7.5.5.4 Identifying Occurred Failures

During testing, the test outputs should be analyzed to identify the occurrences of failures, including their time of occurrence and intensity.

7.5.5.4.1 Analyzing Deviations in Test Outputs

Deviation analysis of test outputs is conducted using automated tools or through manual review of test results to determine the deviations between the actual execution results and the expected behavior. During the deviation analysis process, cascaded are not taken into account.

7.5.5.4.2 Determining Which Deviations Are Failures

For the observed deviations, it is necessary to determine whether they qualify as failures.

Failures caused by hardware errors are not included in the statistical analysis of embedded software failures. However, failures that require software fault tolerance and prevention of critical errors should be considered and included in the analysis.

7.5.5.4.3 Estimating the Time of Failure Occurrence

The failure occurrence time is estimated using a unified time metric, namely calendar time, measured in hours, and accumulated in chronological order. The estimation of failure occurrence time includes all functional tests, regression tests, and load tests performed during the specified time period.

In cases where multiple failures occur simultaneously, resulting in zero failure intervals, random times should be estimated within the recorded time interval to replace these zero intervals.

7.5.5.4.4 Assigning Failure Severity

The level of each failure should be determined based on the established criteria outlined in Table 7.5.2.1.

7.5.5.4.5 Forming Test Records

Test records should be created according to the executed test cases, documenting the test process, test results, runtime, failure occurrence time, and failure symptoms. Table 7.5.5.4.5 provides an example of a test record

Table 7.5.5.4.5 Example of Test Record

Incident	Time	Time interval between failures/min
Start	08:00, January 1, 2021	0
Failure 1	08:35, January 1, 2021	35
Failure 2	09:10, January 1, 2021	35
Failure 3	13:20, January 1, 2021	250
Failure 4	15:30, January 1, 2021	130
End	16:00, January 1, 2021	30/NA[1]

Note 1: NA indicates that no failure at the end of the test and it passes the test. 30 indicates that failure at the end of the test, with a failure time interval of 30 minutes (min).

7.5.6 Reliability Confirmation Test

7.5.6.1 General

Reliability confirmation testing is performed to confirm whether the current reliability level of embedded software complys the user’s requirements, with a given statistical reliability, i.e., to confirm whether the current reliability level of embedded software meets the specified reliability targets. The Guideline use failure execution time and reliability diagrams for confirmation testing.

7.5.6.2 Failure Execution Time Confirmation Testing

The reliability test time (T) for embedded software can be calculated using the following formula, given the Customer risk (β) and the lower limit of Mean Time Between Failures (MTBF) denoted as θ:

$$T = -\theta \ln \beta$$

Where:

θ : Lower limit of the MTBF.

β : Customer risk.

This confirmation test is applicable to the reliability verification test of embedded software with MTBF within 1000h. For embedded software with an MTBF greater than 1000h, a reliability demonstration test shall be used.

7.5.6.3 Reliability Demonstration Test

A reliability demonstration chart is constructed based on the levels of Customer risk and developer risk. Failures are plotted on the diagram, and based onthe region in which the failures fall, the tested embedded software is determined to be accepted, rejected, or further tested.

First, consult with the supplier and customer to determine the levels of developer risk (α) and customer risk (β). The method for constructing the reliability demonstration chart can be referenced from Appendix 5 of the Guidelines.

Generally, the developer risk (α) and customer risk (β) should be selected below 20%, with a maximum not exceeding 30%. For embedded software with high reliability requirements, the developer risk (α) and customer risk (β) should be within 10%.

When plotting the reliability demonstration chart, it is necessary to calculate the boundaries for continuation and acceptance, as well as for continuation and rejection, and draw the boundary lines. These boundary lines can be determined using the following two equations:

$$T_{N,A}(n) = \frac{A - n \ln \gamma}{1 - \gamma}$$

where:

$T_{N,A}$: Normalized failure time of the continuation and acceptance boundary for the number of failures already occurred.

n : Failure number.

A : $A = \ln \dfrac{\beta}{1 - \alpha}$

γ : Discrimination ratio, i.e. the ratio of maximum acceptable failure intensity to failure intensity objective, taken from 1.1 to 2.0. The higher the reliability requirement, the smaller the value should be.

$$T_{N,\mathrm{B}}(n) = \frac{B - n \ln \gamma}{1 - \gamma}$$

where:

$T_{N,B}$: Normalized failure time of the continuation and rejection boundary for the number of failures already occurred

n : Failure number.

B : $B = \ln \dfrac{1-\beta}{\alpha}$

γ : Discrimination ratio, i.e. the ratio of maximum acceptable failure intensity to failure intensity objective, taken from 1.1 to 2.0. The stricter the reliability requirement, the smaller the value should be.

In the reliability demonstration chart below, the manufacturer risk α=0. 1, the user risk β=0. 1 and the resolution γ=2.

A specification-quantified metric (MTTF) is calculated from the number of failures and the time unit in which they occur. Fig. 7.5.6.3 Vertical axis: failure number (n). Horizontal axis: normalized failure data (T_n) in the reliability demonstration chart. Based on the following criteria:

If it falls in the "continue" region, the result is uncertain. testing should continue.

If it falls in the "reject" region, there is little possibility of meeting the objective. it is not worth testing further.

If it falls in the "accept" region, testing ends and accept the software.

Continue testing as long as the point remains within the continue region until the end of testing. Calculate the FI/FIO ratio, and if the ratio is greater than 5 and failures occur, reject the software. If the ratio is less than 5, accept the software.

The FI/FIO ratio is characterized by λ_D:

$$\lambda_D = \frac{T_{N,A}(n)}{t_t \lambda_F}$$

Where:

t_t : Number of time units at the end of test.

λ_F : Failure intensity objective.

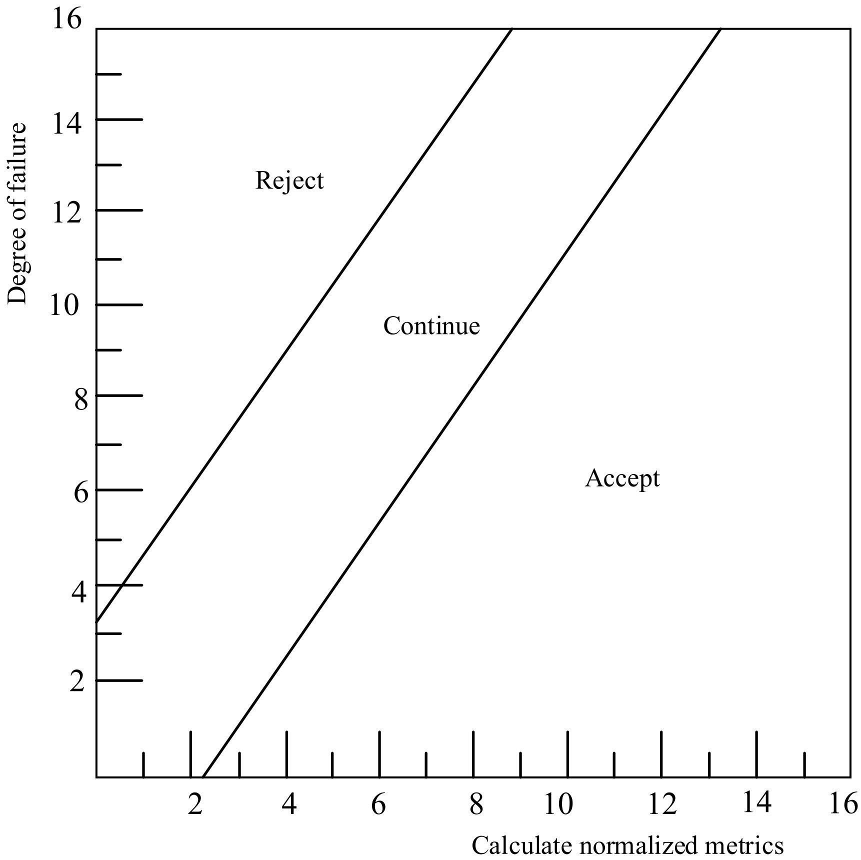


Fig. 7.5.6.3 Normalized Metrics (MTTF)

Chapter 8 Evaluation and Verification of Ship System Reliability

8.1 General

The reliability assessment of ship systems is conducted in a hierarchical manner, considering different stages of the system's lifecycle. Sufficient exposure of defects and effective corrective measures should be taken at lower assembly levels. Common reliability characteristics are listed in Table 8.1.

Table 8.1 Common Reliability Characteristics

System level	Service condition	
	Continuous or intermittent operating time (Repairable)	Continuous or intermittent operating time(Non-repairable)
System-level	*R*(*t*)[a] or MTBF[b]	MTTF
Sub-system device or equipment	*R*(*t*)[a] or MTBF[b]	MTTF
Components	λ^c	λ^c
[a] Reliability [b] Mean time between failures [c] Failure rate		

The reliability function represents the probability that a system will operate without failure to time *t*. For non-repairable objects and systems, the commonly used reliability function *R* (*t*) =*R* (*0*, *t*), where *R* (0) =1. *R* (*t*) can be calculated from the formula below:

$$R(t) = \exp\left(-\int_0^t \lambda(u)du\right)$$

where *λ* (*u*) is the instantaneous failure rate of the item . For a constant failure *λ* (i.e., the time to failure of an exponential distribution), the above formula simplifies to:

$$R(t) = e^{-\lambda t}$$

For non-repairable items or systems, MTTF can be calculated by the formula:

$$\text{MTTF} = \int_0^\infty R(t)dt$$

Where, in the case that the failure time follows an exponential distribution, MTTF reduces to

$$\text{MTTF} = \frac{1}{\lambda}$$

Although the value of MTTF can be calculated for almost any failure time distribution with corresponding constant or non-constant failure rate, it should be ensured that the failure rate is indeedconstant for calculating the constant failure rate in reverse by MTTF. For redundant systems consisting of non-repairable components, the above calculation formulas are not applicable. For repairable items, if a component unit fails, the system can be restored to its normal working state after repair, and is often measured by MTBF and MTTR.

For systems without consideration of maintenance and failure sequence, these Guidelines recommend the reliability block diagram (RBD) method for reliability analysis and evaluation, and give several common system types (see 8.2). For systems requiring consideration of failure sequence or maintainability, other modeling techniques (e.g. MARKOV model, see Appendix 6) may be considered. For the reliability analysis and evaluation methods of other complex systems, refer to GB/T 37981-2019 or IEC61078:2006.

8.2 Common System Types

8.2.1 Series System

If each element of the system is required to realize the overall function of the system, only when all units of the system work normally can the system work normally. As long as any unit fails, the system will fail. Such a system is called a reliability series system, and its reliability block diagram is as shown in the figure below:

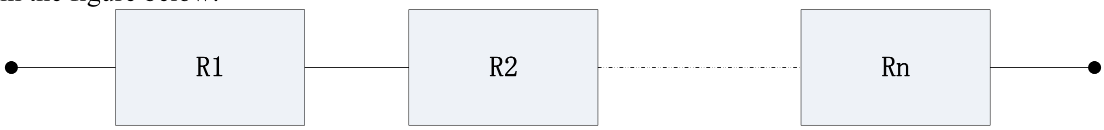


Fig. 8.2.1 Series Reliability Block Diagram

For a series system, the reliability function of the system is calculated by the formula below:

$$R_S(t) = \prod_{i=1}^{n} R_i(t)$$

If the individual elements have exponentially distributed failure times, then

$$R_i(t) = e^{-\lambda_i t}$$

And,

$$R_S(t) = e^{-\lambda_S t}$$

$$\lambda_S = \lambda_1 + \lambda_2 + \cdots + \lambda_n$$

Where:

$R_S(t)$:Reliability function of the system.

$R_i(t)$:Reliability function of different parts.

λ_S :Constant failure rate of the system.

λ_i :Constant failure rate of different parts.

i :R1, R2, ⋯, Rn.

It can be seen that the more parts in series, the lower the reliability of the system.

8.2.2 Parallel System

If several elements or sub-systems of a system realize the overall function of the system in redundant manner, these units are considered to be connected in parallel, as shown in Fig. 8.2.2:

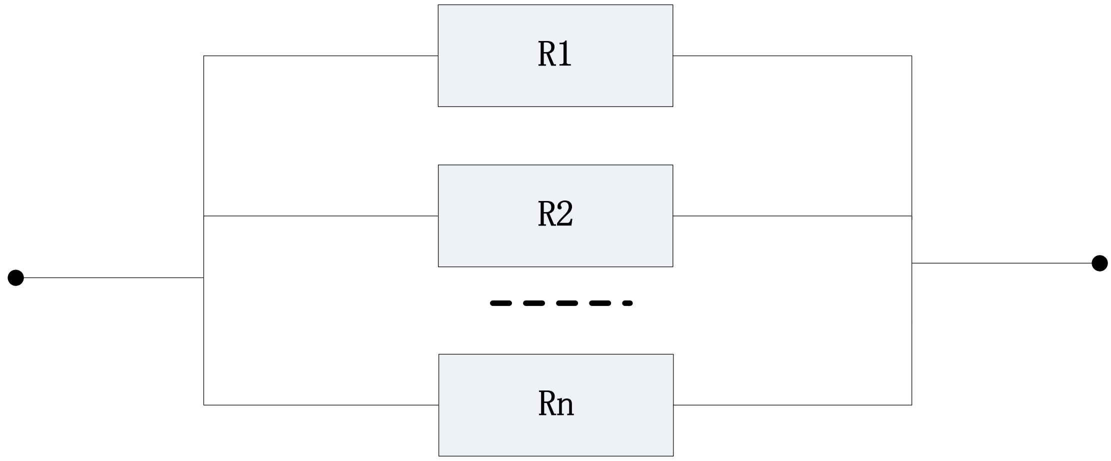


Fig. 8.2.2 Parallel Reliability Block Diagram

For systems with non-repairable elements, use the formula below:

$$R_S(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right]$$

If the individual elements have exponentially distributed failure times, then

$$R_i(t) = e^{-\lambda_i t}$$

$$\mathrm{MTTF_{sys}} = \int_0^{\infty} \left[1 - \prod_{i=1}^{n} R_i(t)(1 - e^{-\lambda_i t})\right] dt$$

Where:

$R_s(t)$:Reliability function of the system.

$R_i(t)$:Reliability function of different parts.

$\mathrm{MTTF_{sys}}$:MTTF of the system.

λ_i :Failure rate of different parts.

I :R1, R2, …, Rn.

8.2.3 Mixed Structure

In general, a ship system is not only composed of simple series or parallel systems, but also usually may be a mixed structure. The series-parallel system can be simplified into several typical series or parallel subsystems, and then the “equivalent model method” is used to calculate its reliability. The series-parallel model has a “series-parallel” structure and a “parallel-series” hybrid structure, as shown in Fig. 8.2.3.

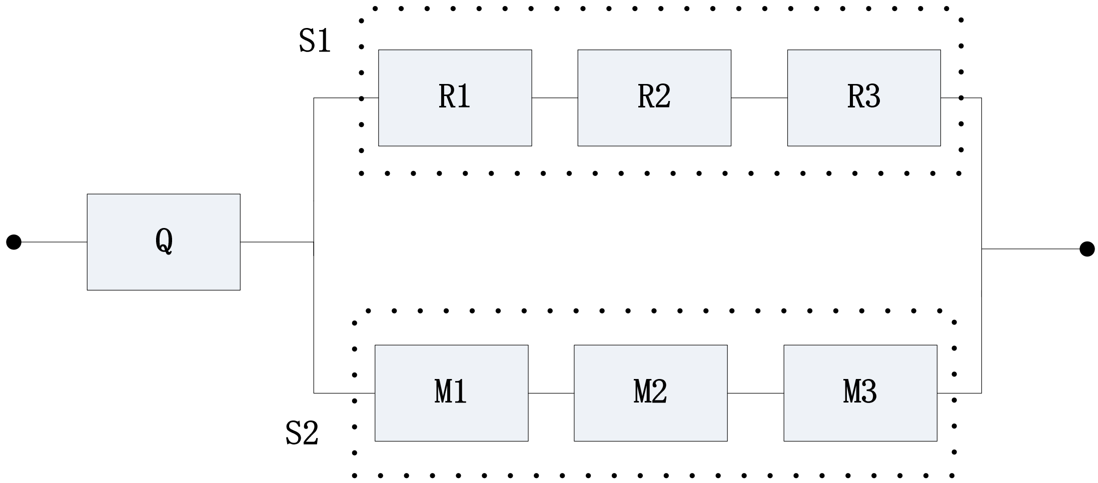


Fig. 8.2.3 Reliability Block Diagram of Mixed Structure

Then the failure rate of sub-system S1 in the whole system is,

$$\lambda_{S1} = \lambda_{R1} + \lambda_{R2} + \lambda_{R3}$$

Then the failure rate of sub-system S2 in the whole system is,

$$\lambda_{S2} = \lambda_{M1} + \lambda_{M2} + \lambda_{M3}$$

If each unit conforms to exponential distribution, then the MTTF of the whole system is:

$$\mathrm{MTTF}_{\mathrm{sys}} = \int_0^\infty R_S(t)dt = \int_0^\infty e^{-\lambda_Q t}\left[1-\left(1-e^{-\lambda_{S1}t}\right)\left(1-e^{-\lambda_{S2}t}\right)\right]dt$$

Where:

λ_{S1} :Failure rate of system S1, with S1 including R1, R2 and R3.

λ_{S2} :Failure rate of system S2, with S2 including M1, M2 and M3.

λ_Q :Failure rate of equipment D.

$R_S(t)$:Reliability function of the system.

$\mathrm{MTTF}_{\mathrm{sys}}$:MTTF of the system.

8.2.4 K/N Model

In addition to the three models listed in 8.2.1, 8.2.2 and 8.2.3, if a voting system design is used to improve the assembly reliability of the ship system, the voting model shall be used to calculate and evaluate the system reliability. The characteristic of such a system is that in the *n* units constituting the system, if the number of units without failure is no less than *k* (*k* between 1 and *n*), the system will not fail, which is also called as *k*/*n* system. Generally, the reliability of *n* units is the same and all are R, so the reliability calculation of the system is:

In a *k*/*n* voting system, if *k*=1, the system is a parallel system of *n* elements. if *k*=*n*, the system is a series system of *n* elements.

8.3 Evaluation and Verification Requirements for Complex System

For some large-scale ship systems with high complexity and many types of constituent elements, due to its small number of moldings and few theoretical increments for sampling, it is impossible to carry out tests or testing by evaluating the reliability of a single unit product. The decomposition method is usually used for such complex large-scale systems: any large-scale system is composed of several subsystems, each of which consists of equipment and softwares, between which pyramid-like model structure can be established, and a correct and complete model structure shall be established to make relatively accurate assessment of system reliability. See IEC 62308: 2006 IDT for other relevant requirements.

Typically, these system evaluation requirements are as below.

(1) Carry out tests and testing of each unit of the system in laboratory or virtual testing environment.

(2) Carry out test field testings and sea trials for the system under typical working conditions.

(3) Carry out a small number of real-ship use tests on the system, conduct FMEA/FMECA analysis before the use test, and review relevant reports.

(4) Evaluate the system reliability by combining the test and testing results of the above three methods.

Through the above methods and based on the principle of minimum use risk, the reliability assessment and verification of complex systems are realized with fewer system-wide use tests, with the main process as below:

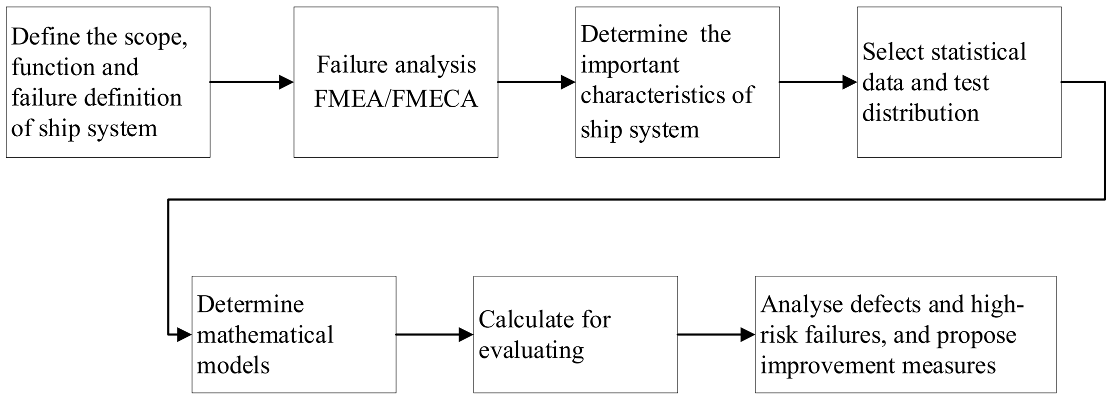


Fig. 8.3.1 Reliability Assessment of Complex System

Chapter 9 Verification and Review

9.1 Data Requirements

For ships applying for reliability verification of ship equipment and systems, computer software and embedded software, the shipowner, equipment manufacturer and software developer shall submit the documents below to China Classification Society for review.

(1) Product model and version information.

(2) Product specification.

(3) Product function specification.

(4) Product environmental condition and severity level.

(5) Product reliability compliance test profile requirements.

(6) Product environmental test report.

(7) Product reliability compliance test report.

(8) Product reliability test summary report.

(9) Product reliability test completion review.

(10) Product reliability block diagram (for reference).

(11) Type approval test report (if any).

(12) Other necessary supporting materials.

The reliability test report generally includes the contents below:

(1) Test content, purpose and conclusion.

(2) Test basis.

(3) Test time, place and participants.

(4) Description of tested products.

(5) Test statistical plan.

(6) Description of comprehensive environmental conditions and stress application methods.

(7) Test facilities and instruments.

(8) Preparation before test.

(9) Description of test process.

(10) Description of number, categoty and handling of faults in test.

(11) Reliability assessment conclusion.

(12) Existing problems and suggestions.

(13) Other relevant matters to be explained.

9.2 Reliability Verification and Compliance Certificate

China Classification Society carries out reliability verification of ship equipment and systems according to the Guidelines and the documents provided by the applicant, with specific verification methods and processes detailed in Chapters 4 to 8 of these Guidelines. For ship equipment and systems, computer software and embedded software that have passed the reliability verification, China Classification Society shall issue a compliance certificate (see Appendix 7).

For sister ships or series ships, if their equipments and systems are identical and have passed the reliability verification, an application can be made to issue a Compliance Certificate for Reliability Verification after confirmation by the Society and exempt from repeated verification. In case of any technical state change (e.g. change in applicable standards, equipment model replacement, equipment performance index change, software update and upgrade, etc.) between the equipment or system of sister ships or series ships and those that have passed reliability verification, it is necessary to submit the changes to the Society for review and reverify their reliability according to the Guidelines. After the verification is passed, a new compliance certificate will be granted by the Society according to the changed technical state.

9.3 Operational Data Feedback

After being put into operation, the users of ship equipment, computer software and embedded software that have obtained the compliance certificate according to the Guidelines shall provide China Classification Society with use information every year, including fault and maintenance record data, etc., for reliability evaluation by China Classification Society, so that the users can master the reliability performance of the equipment, computer software and embedded software in the whole life cycle, make timely decisions on maintenance or replacement and ensure that the reliability level of equipment and systems is basically equivalent to that when the certificate of conformity is obtained, with the details as below:

(1) Operation monitoring data and alarm, fault and maintenance records of equipment and systems, generally including the basic description of date and time of faults, fault phenomenon, fault cause (if any), serial number or version number of failed product, involved equipment, software or system, working conditions and environmental conditions at the time of fault, as well as maintenance or recovery time, occurrence time of each subsequent fault and its maintenance or recovery time.

(2) Fault symptoms of equipment and systems, including original symptoms of partial or total overall failure, parameter values beyond the specified range, software error description, etc..

(3) For repairable items, the maintenance or recovery time after fault shall be provided. for non-repairable items with service life parts and replacement products, MTBF, MTTF, MTTR and other parameter information shall be provided.

Appendix 1 Comparison Table of Environmental Conditions

Schedule 1-1 Classification of Climatic Conditions

Environmental Parameters	Units	Class						
		6K1	6K2	6K3	6K4	6K5	6K6[f]	6K7[f]
(1) Low temperature, air	℃	+5	-25	-25a	-25	-40b	+5	-20
(2) Low temperature, water	℃	Freezing point of water [c]					+15	+15
(3) High temperature, air	℃	+40	+40	+55	+70	+70	+55	+70
(4) High temperature, surface [d]	℃	—	—	—	+70	+70	+70	+70
(5) High temperature, water	℃	+30	+35	+35	+35	+35	+35	+35
(6) Gradient change of temperature, air/air	℃ ℃/min	— —	-25/+20 1	-25/+40 3[a]	-25/+40 3	-25/+40 3	+5/+40 3	-20/+40 3
(7) Temperature change, air/water	℃	—	—	—	+40/+5	+40/+5	+40/+15	+40/+15
(8) Humidity (not combined with rapid temperature changes)	% ℃	95 +30	95 +35	95 +35	95 +45	95 +45	95 +35	95 +45
(9) Humidity (combined with rapid temperature change at high relative humidity) air/air	% ℃	— —	— —	95 -25/+35	95 -25/+35	95 -25/+35	95 +5/+30	95 -20/+30
(10) Humidity (combined with rapid temperature change at high water content [e]) Air/air	g/m^3 ℃	— —	— —	— —	60 +70/+15	60 +70/+15	60 +55/+15	60 +70/+15
(11) Low relative humidity	% ℃	10 +30	10 +30	10 +30	10 +30	10 +30	10 +30	10 +30
(12) Movement of surrounding medium, air	m/s	Negli-gible	Negligible	Negligible	30	50	50	50
(13) Precipitation, rain	mm/min	—	—	—	6	15	15	15
(14) Radiation solar	w/m^3	Negli-gible	700	700	1120	1120	1120	1120
(15) Radiation heat	w/m^3	Negli-gible	600	1200	1200	1200	1200	1200
(16) Water from sources other than rain	m/s	—	0.3	0.3	3	10	10	10
(17) Wetness	—	—	Wet surfaces					

[a] A number of products located in machinery spaces are only required to operate after a period of warm-up of the machinery spaces. For these products the low temperature for operation is + 5°C, and the gradual change of temperature condition only applies to the non-operational state. [b] Ships will normally not navigate when air temperatures are below – 40°C. Products may, however, be left unprotected on ships which are temporarily laid up in harbour for the coldest period of the year. In such cases, products in the non-operational state, may have to withstand temperatures down to – 55°C. In exceptional cases in inland waters, ships may also navigate when temperatures are below – 40°C. [c] Freezing point may be lower than 0 °C due to presence of salt or pollution, etc. [d] Surface temperatures refer to hot parts to which the products may be attached. More extreme surface temperatures can exist, for instance on machines, and may have to be considered. [e] The product is assumed to be subjected to a rapid decrease of temperature only (no rapid increase). The figures of water content apply to temperatures down to the dew point. at lower temperatures the relative humidity is assumed to be approximately 100 %. [f] Tropical climatic conditions are classified according to 6K6 (humid heat) and 6K7 (dry heat).

Schedule 1-2 Classification of Biological Conditions

Environmental Parameters	Units	Class	
		6B1	6B2
(1) Flora, in air	—	Negligible	Presence of mould, fungus, etc.
(2) Fauna, in air	—	Negligible	Presence of rodents and other animals harmful to products

Note1: Externally installed products on submerged parts of the hull will be subjected to flora and fauna of the water (algae,crustations, corals).

Schedule 1-3 Classification of Chemically Active Substances

Environmental Parameters		Units	Class		
			6C1	6C2	6C3
Substances in the air [a,b]	(1) Salt mist	mg/m^3 cm^3/m^3	—	Presence [c]	Presence [c]
	(2) Sulfur dioxide (SO_2)	mg/m^3 cm^3/m^3	0.1 0.037	1.0 0.37	1.0 0.37
	(3) Hydrogen sulfide, H_2S	mg/m^3 cm^3/m^3	0.01 0.0071	0.5 0.36	0.5 0.36
	(4) Nitrogen oxide (expressed in the equivalent values of nitrogen dioxide)	mg/m^3 cm^3/m^3	0.1 0.052	1.0 0.52	1.0 0.52
	(5) Ozone (O_3)	mg/m^3 cm^3/m^3	0.01 0.005	0.01 0.005	0.1 0.05
	(6) Hydrogen chloride (HCl)	mg/m^3 cm^3/m^3	0.1 0.066	0.1 0.066	0.5 0.33
	(7) Hydrogen fluoride (HF)	mg/m^3 cm3/m3	0.003 0.0036	0.003 0.0036	0.03 0.036
	(8) Ammonia (NH_3)	mg/m^3 cm^3/m^3	0.3 0.42	0.3 0.42	3.0 4.2
Substances in the water [d]	(9) Sea salt	kg/m^3	Negligible	Negligible	30

[a] As other substances and varying degrees of severity may be present due to a specific cargo carried. For oil tankers should refer to IEC 60092-505.
[b] Explosive gases are not considered in this part, and therefore not included.
[c] No specific data index is available at present.
[d] Substances in water other than sea salts are not included, as they are considered to have a negligible effect on electrotechnical products already protected from the effect of sea salts.

Schedule 1-4 Classification of Mechanically Active Substances

Environmental Parameters	Units	Class		
		6S1	6S2	6S3
(1) Sand in the air	g/m^3	—	0.1	10
(2) Dust sedimentation	$mg/(m^2 \cdot h)$	Negligible	3.0	3.0
(3) Soot deposition	—	—	Soot is present	

Note1: Other severities of dust and sand may occur due to specific cargoes, eg. dusty material and sand (including abrasive substances). The distribution of particle size and chemical composition is important as well as the quantity of the particles.(No values at present.)

Note 2: In machinery spaces, droplets of oil may be present in the air. A concentration of 3 mg/m^3 air may occur. Higher concentrations up to 20 mg/m^3 air may be present close to diesel engines, or in oil separator rooms.

Schedule 1-5 Classification of Mechanical Conditions

Environmental Parameters	Units	Class			
		6M1	6M2	6M3	6M4
(1) Steady vibration (sinusoidal) [a] Displacement Acceleration Frequency range	 mm m/s^2 Hz	 — — —	 1.5 10 2~13 13~100	 1.5 20 2~18 18~100	 1.5 50 2~28 28~100
(2) Unsteady vibration (including shock) [b] Type I Shock response spectrum peak acceleration a Type II Shock response spectrum peak peak acceleration a Type III Shock response spectrum peak peak acceleration a	 m/s^2 m/s^2 m/s^2	 50 100 —	 100 300 —	 100 300 500	 100 300 500
(3) Angular motion tilt [c] Rotation around X axis (heeling) Angle Rotation around Y axis (trim) Angle	 ° °	 15 10	 15 10	 15 10	 15 10
(4) Angular swing [c] Rotation around X axis (rolling) Angle Frequency Rotation around Y axis (pitching) Angle Frequency Rotation around Z axis (yawing) Angle Frequency	 ° Hz ° Hz ° Hz	 22.5 0.14 10 0.2 4 0.05	 22.5 0.14 10 0.2 4 0.05	 22.5 0.14 10 0.2 4 0.05	 22.5 0.14 10 0.2 4 0.05
(5) Steady-state acceleration [c] X axis (longitudinal dropping) Acceleration	 m/s^2	 5	 5	 5	 5

Environmental Parameters	Units	Class			
		6M1	6M2	6M3	6M4
Y axis (horizontal dropping) Acceleration Z axis (vertical dropping) Acceleration	 m/s^2 m/s^2	 6 10	 6 10	 6 10	 6 10

[a] Vibration generated by conventional ship engines is mainly of a sinusoidal nature with a pronounced low frequency content. High frequency vibration up to 2000 Hz and of intensities up to 50 m/s^2 will, however, be present in icebreakers. Random vibration is also present in ships due to forces produced in the contact between the hull or propeller and the water. The levels are normally low, and therefore random vibration has not been included.

[b] The shock is expressed in terms of peak acceleration a.

[c] The three mutually perpendicular coordinate axes relative to the ship are:

X = fore and aft direction

Y = transverse direction

Z = vertical direction

Appendix 2 Example of Reliability Test Verification Profile

The reliability task profile can be decomposed into several different types of working states, such as:

Opening/closing working state of products in different environments.

Continuous working state of products in different environments.

Storage/dormancy state of products in different environments, etc.

According to different seaworthy areas, the environmental conditions and requirements of the products are also different. The actual synthetic profile should comprehensively consider the characteristics of the products themselves and the requirements of use scenarios. The following table is an example of the task profile of ship electronic components considering temperature rise change:

Schedule 2 Example of Task Profile of Ship Electronic Components Considering Temperature Rise Change

Task profile stage	Duty ratio (pening time/closing time)		Daily start of navigation		Anchorage berthing		Berthing in the port		Docking maintenance (Twice every 5 years legally, 0.4 unit/year)	
Navigation area	On	Off	Thermal cycle (Times/year)	Temperature change amplitude (℃/time)	Thermal cycle (Times/year)	Temperature change amplitude (℃/time)	Thermal cycle (Times/year)	Temperature change amplitude (℃/time)	Thermal cycle (times/year)	Temperature change amplitude (℃/time)
Oceangoing	0.73	0.27								
Offshore	0.68	0.32								
Coastal	0.70	0.30								
Shielded Navigation area	0.63	0.47								
Inland river	0.58	0.42								
Inland lake	0.56	0.44								

Note1: The profile parameters in the table shall be taken according to the actual situation. Generally, there are several methods to obtain the parameters as follows.

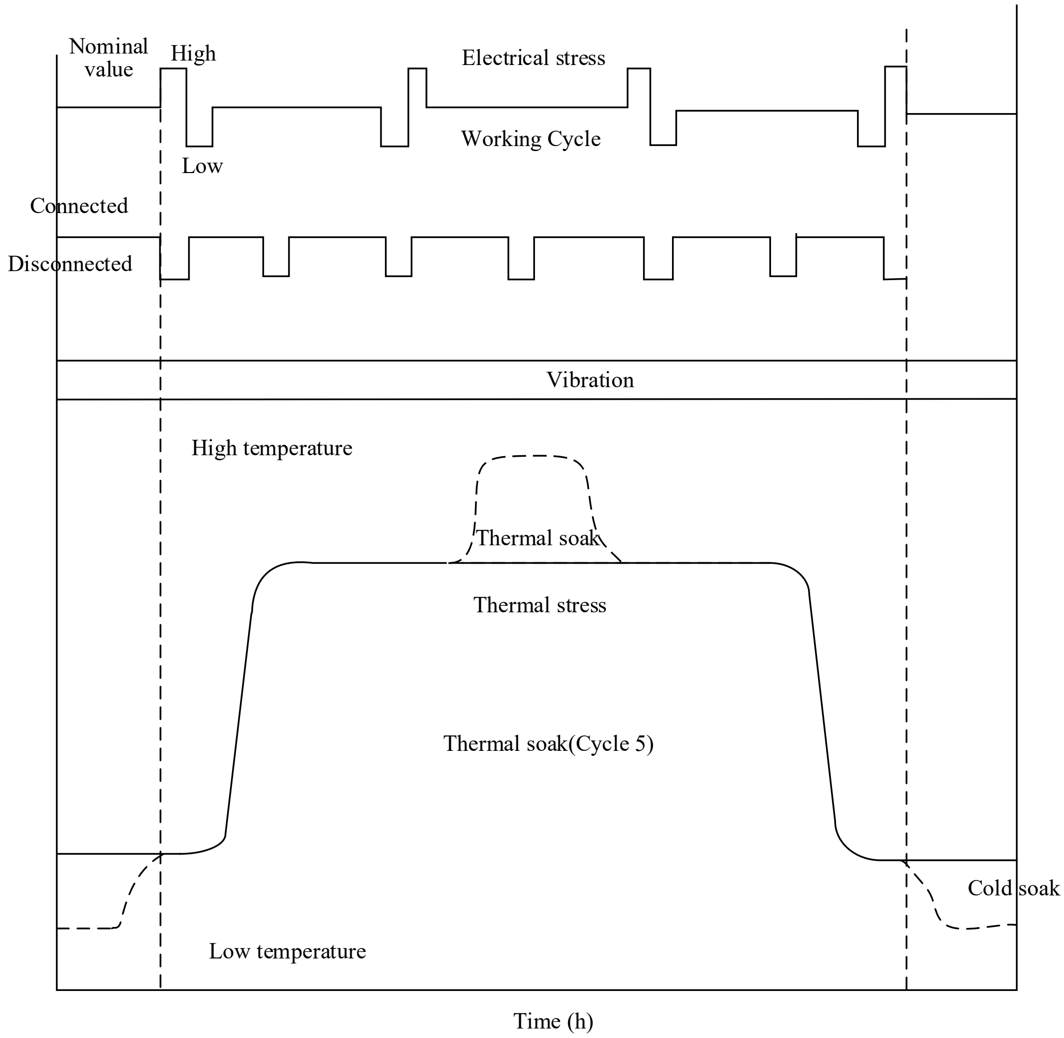
(1) Data measured near the installation position of the tested product when the product performs a typical task profile in actual use.

(2) Same or similar product data used in the same or similar working, physical and support environments.

(3) Physical and engineering analysis data of the product under expected use environmental conditions.

(4) Test data of product suppliers or general data sources in the industry. The confidence level of parameters shall be considered when such general data sources are used, and better replacement data shall be obtained through continuous iteration during the use of products.

For the product comprehensive environmental test profile of ship equipment and systems, unless otherwise specified by the shipowner or user, the temperature change rate of the test chamber shall be at least 5°C/min. Depending on the installation, deployment and use environment of equipment and systems, thermal soak and cold soak can be selected. At this time, vibration, electrical stress and working cycle are not applied. During cold soak, the humidity shall reach a level sufficient to cause obvious condensation, frost and icing.



Attached Fig. 2 Example of Reliability Test Verification Profile for Ship Equipment and Systems

Appendix 3 Requirements for Implementation of Reliability ComplianceTest

1 Overview

1.1 Test purpose and classification

The reliability verification test is to verify whether the product reliability complys the specified requirements.

The reliability verification test is divided into the reliability qualification test and the reliability acceptance test according to the nature of products.

The reliability qualification test is to verify whether the design of newly developed products meets the specified minimum acceptable quantitative requirements for reliability.

The reliability acceptance test is a test to determine whether the products formally transferred into batch production meet the quantitative requirements for reliability.

1.2 Statistical concept

The reliability index, a time characterization of product performance, is a random variable and cannot be tested by instruments. It can only be tested through sampling test or life cycle statistics.

The reliability use index of the products is also a reliability target value, which is also referred to as the specified value in the contract. In the test plan, it can be sample value θ_0.

The reliability use index that the products must achieve is called the reliability threshold, which is referred to as the minimum acceptable value in the contract and θ_1 in the test plan.

The verification test plan is based on statistical mathematics and related to statistical concepts such as “individual”, “total”, “batch”, “sample”, “sample size”, “random sampling” and “distribution”.

1.3 General

The test program must be jointly discussed and approved by the representatives from the product manufacturer, test site and China Classification Society.

The statistical test plan is specified by the product user in the contract and selected from relevant standards. GJB899a-2009, GB/T 5080.1-2012/IEC 60300-3-5:2001 are recommended.

The technical state of the test samples shall be approved.

The test profile shall be representative of the actual use environmental conditions.

The test shall be carried out at the test site determined in the test program, and if necessary, witnessed by the Society on site.

2 Requirements of Verification Test Program

2.1 Content requirements of test program

Reliability verification shall include but not be limited to the following.

Test object and quantity.

Test purpose and progress.

Test plan.

Test conditions: stress and tolerance provided by the test equipment, testing equipment and accuracy requirements.

Test site: a recognized independent third-party inspection and test agency accepted by the Society or a site determined through negotiation according to special circumstances.

Set up review points, and carry out Failure Report Analysis and Corrective Action System (FRACAS) requirements.

2.2 Requirements of test plan

2.2.1 Formulating a test plan according to the requirements of the program

The contents of the test plan include:

Test items:

Select the statistical test plan: number, discrimination ratio D, risk α and β, test duration T, sample quantity, replaceability.

Test profile.

Failure criteria and classification.

Division of responsibilities of relevant testing parties.

Guarantee conditions of planned progress, funds, personnel and resources such as maintenance equipment.

Other reliability activity information.

2.2.2 Selected factors of test plan

For the fixed-time truncated test, the cumulative test duration is determined to facilitate the arrangement and management of the test plan, but it may not be the most economical.

For the fixed-number truncated test, the cumulative number of relevant failures is determined. When non-replaceable tests are taken, the number of samples is also determined and it may not be the most economical.

Equal-probability ratio sequential testing: It requires fewer failures and cumulative test time to reach the decision criteria compared to timed truncation and fixed-sample truncation testing. However, it is difficult to determine the sample quantity and test duration in advance, making it less convenient for test planning and management. The maximum cumulative test time and cumulative failure count may exceed those of timed truncation or fixed-sample truncation testing.

To sum up, the selection of the test plan should be determined through consultation between the two parties involved (developer or customer).

2.3 Test Conditions

The compliance test profile shall represent the typical service conditions of the product:

Functional mode: When the product has more than one usage mode, the percentage of time occupied by each shall be analyzed to determine the mode conversion method and put forward typical working modes for test.

Input requirements: During the test, the testing equipment inputs a series of signals to the sample to ensure normal operation. Load conditions: the output terminal of the sample shall be loaded to simulate the usage state, testing the sample's output performance.

Sample operation: During the test, product operators shall simulate the use state and perform operations accordingly.

Assurance conditions: The parameters of power supply, water supply and gas supply, and other utilities provided by the laboratory shall comply the requirements.

Test profile: Whenever possible, comprehensive stress test equipment should be used to simulate the product's usage conditions. and combined stresses such as temperature, humidity, vibration, and air pressure should be applied to the sample.

Sample maintenance and repair: The test program may specify periodic maintenance procedures for the sample which should be maintained regularly according to the product's user manual, without altering its technical state. In the event of a sample failure, repairs should be permitted, and the product developer should ensure the necessary conditions and implementation without changing the sample's technical state.

2.4 Test Procedure

The test procedure shall be formulated according to the test plan, and approved by the customer before being implemented as documented test plans. . The content includes: test process.

Samples and their technical conditions.

Characteristic parameters to be tested, failure criteria and their tolerances, testing time period and methods.

Comprehensive environmental conditions and their tolerances.

Test log and the required data recording contents, as well as the recording time interval.

Failure record forms and their registration contents, analysis report requirements.

Provisions for interrupting the test, including scheduled maintenance time, situations after a failure occurs, situations where the test conditions exceed the tolerances and cannot be corrected, and other management needs.

Disposal procedures for sample failures, including timely recording of failure phenomena applied stress conditions, and operational actions, confirming the failure, reporting to the test manager, interrupting the test when the temperature reaches the ambient temperature point, removing the faulty sample, repairing the sample or continuing the test (in non-substitutable test plans, after the repaired sample passes the inspection. in substitutable test plans, after installing a backup sample), analyzing whether the failure is related, conducting FRACAS, and documenting the fault handling process.

2.5 Test Review

Test review includes: test program review, test plan review, test procedure review, test preparation review, in-test review and comprehensive review upon test completion. The first four reviews can be carried out together, with the presence of representatives from the customer and China Classification Society if necessary. The in-test reviews shall be carried out as appropriate such as reviewing fault handling, test progress, and the termination of sequential testing, organized by the on-site test manager. The comprehensive review upon test completion should be conducted after the preparation of the test report and should evaluate the test results, the level of product reliability, conclusions regarding acceptance or rejection, FRACAS reports, and the implementation of problem handling and corrective measures.

2.6 Joint Test Team

The joint test team consists of representatives from the testing party, product suppliers, users (shipowners), and representatives from China Classification Society who are professionals from various fields such as testing, general design, production, and quality reliability. Generally, the testing party serves as the team leader, with representatives from the product manufacturer and user serving as deputy team leaders, responsible for the coordination of the implementation of the test program. The team's specific responsibilities include: conducting test reviews and test procedures, reviewing test data, approving the classification of sample failures and corrective measures for FRACAS, and approving test interruption procedures.

2.7 Requirements for Test Report

The test report is an official record of the product's reliability level. It includes various original records generated during the test, as well as reports on the processing of test results and conclusions. The test report should be compiled and maintained as a complete archive and submitted to China Classification Society.

Appendix 4 Reliability Test Cases

Appendix 4 provides examples of reliability test cases that can be used as references for test case design. For other test cases, please refer to Appendix C of GB/T 28171-2011.

1. Fault Injection Testing

The steps for fault injection testing are as follows:

(1) Fault injection. Introduce defects, faults, and failures into the code. Determine the appropriate locations for insertion and add necessary code if required.

(2) Execute the test. Activate the injected faults by providing necessary input data, generating internal or external incident, sending specific messages, etc..

(3) Collect test results. Collect data, observations, etc., at the predefined observation points. Also, collect various abnormal phenomena observed in the system under test, such as system crashes, resets, etc..

(4) Evaluate test results. Based on the collected test data, in conjunction with actual usage and design requirements, assess whether the observed phenomena are considered normal. Generally, the following two criteria are used to determine whether the modification process should be initiated:

① Occurrence of severe faults after fault injection that are unacceptable to the user.

② Inability of the system to recover and still remain in a faulty state after stopping the fault injection.

2. Task Delay Testing

The purpose of the task delay test is to understand whether the impact on the system after task delay complys the requirements. The specific test steps are as follows:

(1) Insert empty loops in the tasks for delay processing and recompile the program.

(2) Construct test data and activate the task under test.

(3) Observe whether there is a significant performance degradation in the system, whether other faults occur, and whether there are any changes in the inter-task interaction timing and the impact of these changes.

3.Frequent Interrupt Testing

The test steps for frequent interrupt testing are as follows:

(1) Measure the execution time (t_1) of a single normal interrupt for the interrupt under test.

(2) Locate the corresponding pin of the interrupt source and insert the input signal from the interrupt signal generator. Adjust the interrupt interval (t_2).

(3) Continue to decrease the time interval of the interrupt signal so that $0.5\ t_1 > t_2 > 0.25\ t_1$, which means that two interrupt requests occur while processing the interrupt service routine. Observe the system's operation.

(4) Add an interrupt count variable to the interrupt service program, recompile and run the program. After normal operation, use the interrupt signal generator to quickly send 1000 interrupts within a very short time and observe the system operation.

4. Repeat Interrupt Testing

The test steps for repeating interrupt testing are as follows:

(1) Modify the code to call the interrupt service routine multiple times when responding to an interrupt. Recompile the program.

(2) Trigger the interrupt according to actual conditions and observe the operation of the program.

5. Interrupt Loss Testing

The test procedure for interrupt loss testing is as follows:

(1) Modify the interrupt service routine to selectively or randomly return at the entry point. Recompile the program.

(2) Trigger the interrupt according to actual conditions and observe the operation of the system.

6.Interrupt Suspension Testing

The test procedure for interrupt suspension testing is as follows:

(1) Run the program to make the tested program run normally, then clear the enable bit of the tested interrupt and disable the interrupt.

(2) Trigger the interrupt according to actual conditions and observe the operation of the system.

7.Interrupt Service Routine Delay Testing

The test steps for interrupt service routine delay testing are as follows:

(1) Insert empty loops in the interrupt service routine and recompile the program.

(2) Trigger the interrupt according to actual conditions to ensure that the interrupt service routine under test can be executed.

(3) Observe the operation of the system.

8. All Interrupts Trigger Testing During The Single-board Startup Process

The test steps for triggering all interrupts during the single-board startup process are as follows:

(1) Select the location to add the test code.

(2) Add a infinite loop statement at the chosen position in (1).Inside the infinite loop, add a counter or perform a blinking LED operation. Recompile the program.

(3) Once the program enters the infinite loop, trigger each interrupt source one by one. Check for any abnormalities and verify if the counter is incrementing or the LED is still blinking.

(4) Repeat steps (2) and (3) for each location where other interrupt statements are present until all interrupt statements have been tested.

9. Unused Interrupt Trigger Testing

The test steps for triggering unused interrupts are as follows:

(1) Mask all unused interrupt sources.

(2) Run the program to simulate actual conditions and trigger all unused interrupts.

(3) Observe the operational state of the program and check for any abnormalities.

(4) Check if the interrupt flag is set.

10. Interface Data Length Error Test

The test steps for interface data length error are as follows:

(1) Modify the code to allow direct sending of messages in hexadecimal format from the backend. Recompile the program and run it.

(2) Send a zero-length message, where the value of the length field is set to 0. Observe how the program handles this scenario.

(3) Send an excessively long message, where the length value exceeds the maximum allowed length, and observe the operation of the program.

(4) Send a message with a length field value that falls outside the allowed range, and observe the operation of the program.

11. Interface Data Type Error Test

The test steps for interface data type error testing are as follows:

(1) Modify the code to allow direct sending of messages in hexadecimal format from the backend. Recompile the program and run it.

(2) Send a message with a message type that falls outside the allowed range. Observe how the program handles this scenario.

12. Data Error Testing

The steps for testing data errors are as follows:

(1) Modify the code to allow direct sending of messages in hexadecimal format from the backend. Recompile the program and run it.

(2) Send a message with a message type that falls outside the allowed range. Observe how the program handles this scenario.

13. Consistency Error Testing for Message Data

The steps for testing consistency errors in message data are as follows:

(1) Modify the code to allow direct sending of messages in hexadecimal format from the backend. Recompile the program and run it.

(2) Send a message with a message type that falls outside the allowed range. Observe how the program handles this scenario.

14.Message Packet Loss Testing

The steps for message packet loss testing are as follows:

(1) Add appropriate code to the program to intercept all passing messages from the original message flow, and then forcibly discard them at a certain rate. The ratio can be dynamically adjusted and recompile the program.

(2) Run the program and create suitable inputs to ensure there is message flow within the program. Gradually adjust the packet loss rate from low to high and then from high to low and observe the operation of the system.

(3) Disable the packet loss functionality to eliminate the packet loss fault, observe the operation of the system, and check if the states of various modules are consistent and if the system can recover to normal operational state.

15. Soft Error Test

The process of transmitting data being modified due to software errors is referred to as soft errors. The steps for soft error testing are as follows:

(1) Add test code to intercept message packets from the message flow, forcibly modify message data at a certain ratio, and recompile the program.

(2) Create suitable input to ensure that messages pass through the message flow modified in step (1).

(3) Observe the operation of the system, check for any alarms, heap corruption, and crashes in the system, and check whether the status of the relevant internal modules is consistent.

(4) Disable the error code program, observe the operation of the system and check whether the system can resume normal operation.

16. Message Delay Testing

The steps for message delay testing are as follows:

(1) Modify the code, add an appropriate logic to intercept messages from the message pathway, and send these intercepted messages to a delay queue, where they are held for a specified period of time. After the delay period, the messages from the delay queue are sent out at their original intervals, effectively extending the time for each message by the same duration. The delay time can be adjusted.

(2) Recompile the program and create test input data to ensure that messages pass through the tested message flow.

(3) Adjust the delay time for the messages and observe system operation.

17. Message Replication Test

The steps for message replication testing are as follows:

(1) Select an appropriate location in the message pathway and add testing code to duplicate the passed messages according to a specific rule. This duplication can be based on a certain rate or a particular characteristic.

(2) Recompile the program and create test input data to ensure that messages pass through the tested message flow.

(3) Observe the operation of the program.

18.Message Disorder Testing

The steps for message disorder testing are as follows:

(1) Select an appropriate location in the message pathway and add testing code to introduce disorder into the message sequence.

(2) Recompile the program and create test input data to ensure that messages pass through the tested message flow.

(3) Observe the operation of the program.

(4) Stop introducing disorder into the message sequence and observe the operation of the system.

19.Burst Traffic Testing

The steps for burst traffic testing are as follows:

(1) Set up the necessary tools or add appropriate testing code to send arbitrary high-volume messages or data to the system under test.

(2) Run the program and configure the tested network connection. To achieve the maximum processing capacity, open all available ports that can input data into the system and provide corresponding input.

(3) Adjust the traffic to the maximum level and run the system for a period of time. Then, reduce the traffic to a lower level and run it for a while. Repeat this process several times, gradually increasing the traffic back to the maximum level. Repeat this several times to observe the operation of the system.

20. Long-Term High Traffic Testing

The steps for long-term high traffic testing are as follows:

(1) Set up the necessary tools or add appropriate testing code to send arbitrary high-volume messages or data to the system under test.

(2) Run the program and configure the tested network connection. To achieve the maximum processing capacity, open all available ports that can input data into the system and provide corresponding inputs.

(3) Adjust the traffic to the maximum level and run the system for an extended period of time and observe the operation of the system. After a predefined duration, reduce the traffic to 0 and observe the operation of the system during the low traffic phase.

Appendix 5 Reliability Demonstration Chart Preparation

When performing the reliability confirmation test to draw the reliability demonstration chart, it is required to determine the boundaries of continue region and accept region, as well as the boundaries of continue region and reject region, and draw the boundary lines. The Guidelines recommend drawing the reliability demonstration chart according to the following methods.

The intersection point of T_N (when n=0) with the horizontal axis:

$$T_{N,A}(n) = \frac{A}{1-\gamma}$$

$$T_{N,B}(n) = \frac{B}{1-\gamma}$$

The intersection point of T_N (when n=16) with the horizontal axis:

$$T_{N,A}(16) = \frac{A-16\ln\gamma}{1-\gamma}$$

$$T_{N,B}(16) = \frac{B-16\ln\gamma}{1-\gamma}$$

The intersection point of n (when T_N = 0) with the vertical axis:

$$n_A(0) = \frac{A}{\ln\gamma}$$

$$n_B(0) = \frac{B}{\ln\gamma}$$

The intersection point of T_N (when T_N = 16) with the vertical axis:

$$n_A(16) = \frac{A-16(1-\gamma)}{\ln\gamma}$$

$$n_B(16) = \frac{B-16(1-\gamma)}{\ln\gamma}$$

To facilitate ease of use, typical parameters are provided in the following table:

Schedule 5(1) The values of the intersection points of various horizontal and vertical axes for regions and boundaries

Intersection point location	Discrimination ratio γ		
	2	1.5	1.1
The horizontal axis at n=0	-A,-B	-2A,-2B	- 10A,- 10B
The horizontal axis at n=16	-A+11. 1,-B+11. 1	-2A+13.0,-2B+13.0	- 10A+15.2,- 10B+15.2
The vertical axis at T_N=0	1.44A,1.44B	2.47A,2.47B	10.5A,10.5B
The vertical axis at T_N=16	(A+16) /0.693 (B+16) /0.693	(A+8) /0.405 (B+8) /0.405	(A+1.6) /0.0953 (B+1.6) /0.0953

Schedule 5 (2) The values of A and B under various levels of developer risk and customer risk conditions.

Developer risk	Parameter	Customer risk			
		0.1	0.05	0.01	0.001
0.1	A	-2.20	-2.89	-4.50	-6.80
	B	2.20	2.25	2.29	2.30
0.05	A	-2.25	-2.94	-4.55	-6.86
	B	2.89	2.94	2.99	2.99
0.01	A	-2.29	-2.99	-4.60	-6.90
	B	4.50	4.55	4.60	4.60
0.001	A	-2.30	-2.99	-4.60	-6.91
	B	6.80	6.86	6.90	6.91

As shown in Schedule 5(2), a rapidly changes with customer risk but has minimal variations with developer risk. It determines the intersection point of the acceptance boundary with the horizontal axis at n=0. Therefore, the acceptance boundary will undergo significant changes with customer risk but only minor changes with developer risk. B rapidly changes with developer risk but has minimal variations with customer risk. It determines the intersection point of the rejection boundary with the vertical axis at TN=0. Consequently, the rejection boundary will experience significant changes with developer risk but only minor changes with customer risk.

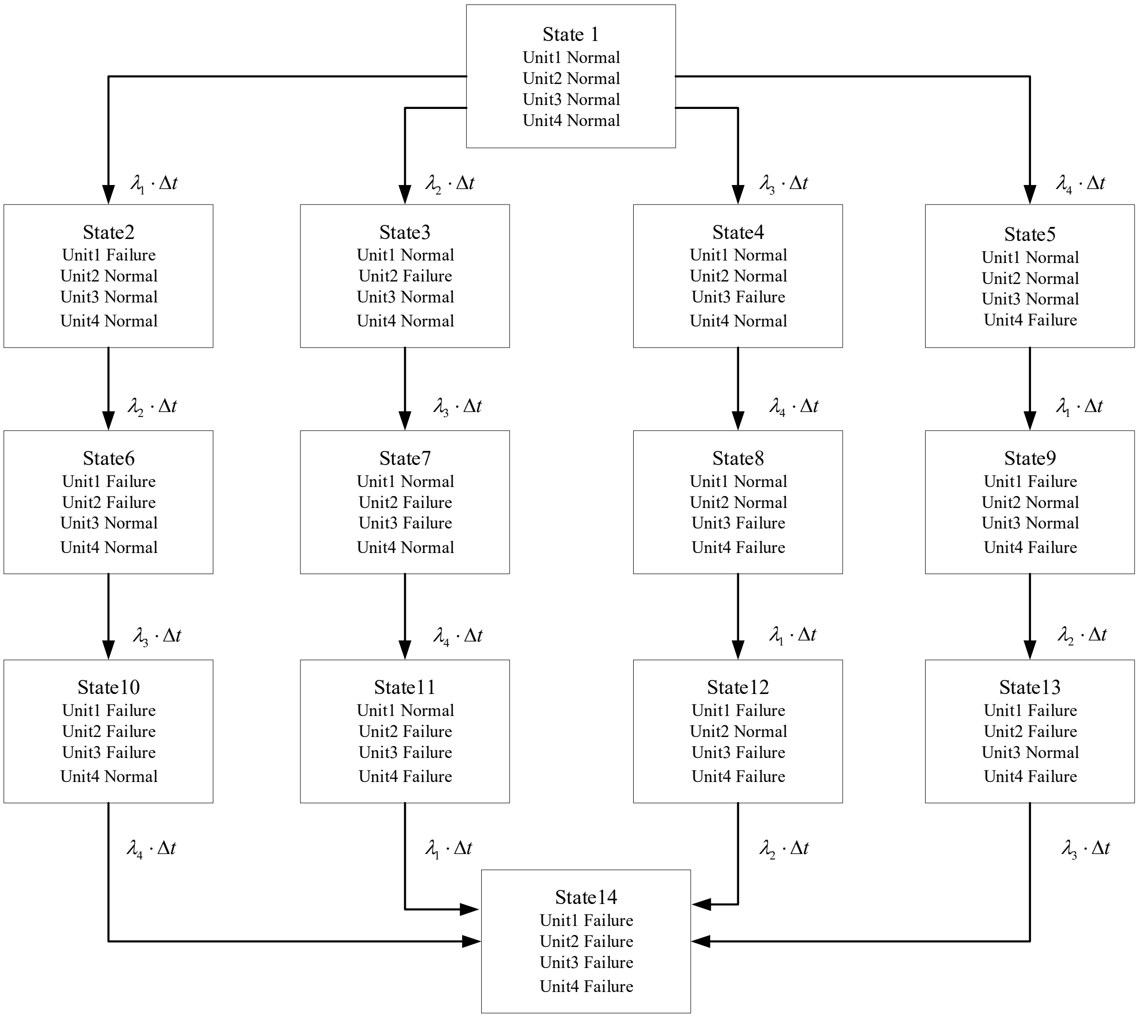
During confirmation testing, reliability demonstration chart can be plotted for all combinations of customer risk and developer risk as needed. Alternatively, reliability demonstration chart can be plotted only for customer risk and developer risk that are symmetric. When the risks are not symmetric, an approximation can be used that is sufficiently close.

As the discrimination rate, customer risk level, or developer risk level decreases, the continue region widens. Therefore, if there is a need to reduce the tolerable errors in estimating failure intensity or mitigate the risk of incorrect decision-making to reach the reject region or accept region, additional tests are required.

Appendix 6 MARKOV Model and Its Reliability Evaluation Calculation

This appendix provides an example of a 4-unit Markov model. In this model, it is assumed that each unit has two states: normal state and failure state. The overall state of the model is determined by the combination of these two states for each unit. It is assumed that each unit has a constant failure rate λ, and the probability of transitioning to a failed state is approximately $\lambda\Delta t$. The model ignores failure modes where two or more units fail simultaneously at time t.

The state transition of the MARKOV model process is as follows:



Attached Fig. 6 (1) 4 Unit MARKOV Model State Transition Diagram

The Markov differential equation is derived by describing the probability P for each state. The behavior of the system is characterized as memoryless, meaning that the future state of the system only depends on the most recent preceding state and is independent of all past states. Therefore, the future stochastic properties of the system depend solely on the present and are not influenced by the past or how the current state was reached. The probability of transitioning from one given state to another state must remain the same (stationary) throughout all past and future times. Based on the above Markov process, the equations for the four-state Markov model are as follows:

$$
\begin{cases}
P_1(t+\Delta t) = P_1(t)\left[1-\left(\lambda_1+\lambda_2+\lambda_3+\lambda_4\right)\Delta t\right] \\
P_2(t+\Delta t) = P_1(t)\lambda_1\Delta t + \left[1-\left(\lambda_2+\lambda_3+\lambda_4\right)\Delta t\right]P_2(t) \\
P_3(t+\Delta t) = P_1(t)\lambda_2\Delta t + \left[1-\left(\lambda_1+\lambda_3+\lambda_4\right)\Delta t\right]P_3(t) \\
P_4(t+\Delta t) = P_1(t)\lambda_3\Delta t + \left[1-\left(\lambda_1+\lambda_2+\lambda_4\right)\Delta t\right]P_4(t) \\
P_5(t+\Delta t) = P_1(t)\lambda_4\Delta t + \left[1-\left(\lambda_1+\lambda_2+\lambda_3\right)\Delta t\right]P_5(t) \\
P_6(t+\Delta t) = P_2(t)\lambda_2\Delta t + \left[1-\left(\lambda_3+\lambda_4\right)\Delta t\right]P_6(t) \\
P_7(t+\Delta t) = P_3(t)\lambda_3\Delta t + \left[1-\left(\lambda_1+\lambda_4\right)\Delta t\right]P_7(t) \\
P_8(t+\Delta t) = P_4(t)\lambda_4\Delta t + \left[1-\left(\lambda_1+\lambda_2\right)\Delta t\right]P_8(t) \\
P_9(t+\Delta t) = P_5(t)\lambda_5\Delta t + \left[1-\left(\lambda_2+\lambda_3\right)\Delta t\right]P_9(t) \\
P_{10}(t+\Delta t) = P_6(t)\lambda_3\Delta t + \left[1-\lambda_4\Delta t\right]P_{10}(t) \\
P_{11}(t+\Delta t) = P_7(t)\lambda_4\Delta t + \left[1-\lambda_1\Delta t\right]P_{11}(t) \\
P_{12}(t+\Delta t) = P_8(t)\lambda_1\Delta t + \left[1-\lambda_2\Delta t\right]P_{12}(t) \\
P_{13}(t+\Delta t) = P_9(t)\lambda_2\Delta t + \left[1-\lambda_3\Delta t\right]P_{13}(t) \\
P_{14}(t+\Delta t) = P_{10}(t)\lambda_4\Delta t + P_{11}(t)\lambda_1\Delta t + P_{12}(t)\lambda_2\Delta t + P_{13}(t)\lambda_3\Delta t + 1.P_{14}(t)
\end{cases}
$$

Substituting the initial state conditions, we have:

$P_1(0)=1$, $P_2(0)=0$, $\cdots$, $P_{14}(0)=0$

The following equation is obtained:

$$
\begin{cases}
P_1(t) = e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} \\
P_2(t) = -e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + e^{-(\lambda_2+\lambda_3+\lambda_4)t} \\
P_3(t) = -e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + e^{-(\lambda_1+\lambda_3+\lambda_4)t} \\
P_4(t) = -e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + e^{-(\lambda_1+\lambda_2+\lambda_4)t} \\
P_5(t) = -e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + e^{-(\lambda_1+\lambda_2+\lambda_3)t} \\
P_6(t) = \frac{\lambda_2}{\lambda_1+\lambda_2} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} - e^{-(\lambda_2+\lambda_3+\lambda_4)t} + \frac{\lambda_2}{\lambda_1+\lambda_2} e^{-(\lambda_3+\lambda_4)t} \\
P_7(t) = \frac{\lambda_3}{\lambda_2+\lambda_3} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} - e^{-(\lambda_1+\lambda_3+\lambda_4)t} + \frac{\lambda_2}{\lambda_2+\lambda_3} e^{-(\lambda_1+\lambda_4)t} \\
P_8(t) = \frac{\lambda_4}{\lambda_3+\lambda_4} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} - e^{-(\lambda_1+\lambda_2+\lambda_4)t} + \frac{\lambda_1\lambda_4}{\lambda_4\lambda_3+\lambda_4} e^{-(\lambda_1+\lambda_2)t} \\
P_9(t) = \frac{\lambda_1}{\lambda_1+\lambda_4} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} - e^{-(\lambda_1+\lambda_2+\lambda_3)t} + \frac{\lambda_3}{\lambda_1+\lambda_4} e^{-(\lambda_2+\lambda_3)t} \\
P_{10}(t) = -\frac{\lambda_2\lambda_3}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + \frac{\lambda_3}{\lambda_2+\lambda_3} e^{-(\lambda_2+\lambda_3+\lambda_4)t} - \frac{\lambda_1\lambda_4}{\lambda_4(\lambda_2+\lambda_3)} e^{-(\lambda_1+\lambda_4)t} \\
\qquad + \left[\frac{\lambda_2\lambda_3}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)} - \frac{\lambda_3}{\lambda_2+\lambda_3} + \frac{\lambda_1\lambda_4}{\lambda_4(\lambda_2+\lambda_3)} \right] e^{-\lambda_4 t} \\
P_{11}(t) = -\frac{\lambda_3\lambda_4}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + \frac{\lambda_4}{\lambda_3+\lambda_4} e^{-(\lambda_1+\lambda_3+\lambda_4)t} - \frac{\lambda_2\lambda_3}{\lambda_3(\lambda_1+\lambda_2)} e^{-(\lambda_1+\lambda_3)t} \\
\qquad + \left[\frac{\lambda_3\lambda_4}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)} - \frac{\lambda_4}{\lambda_3+\lambda_4} + \frac{\lambda_2\lambda_4}{\lambda_4(\lambda_2+\lambda_3)} \right] e^{-\lambda_1 t} \\
P_{12}(t) = -\frac{\lambda_1\lambda_4}{(\lambda_3+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + \frac{\lambda_1}{\lambda_1+\lambda_4} e^{-(\lambda_1+\lambda_3+\lambda_4)t} - \frac{\lambda_1\lambda_3}{\lambda_1(\lambda_3+\lambda_4)} e^{-(\lambda_1+\lambda_2)t} \\
\qquad + \left[\frac{\lambda_1\lambda_4}{(\lambda_3+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)} - \frac{\lambda_1}{\lambda_1+\lambda_4} + \frac{\lambda_1\lambda_3}{\lambda_1(\lambda_3+\lambda_4)} \right] e^{-\lambda_2 t} \\
P_{13}(t) = -\frac{\lambda_1\lambda_2}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_2+\lambda_4)} e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + \frac{\lambda_2}{\lambda_1+\lambda_2} e^{-(\lambda_1+\lambda_2+\lambda_3)t} - \frac{\lambda_2\lambda_4}{\lambda_2(\lambda_1+\lambda_4)} e^{-(\lambda_2+\lambda_3)t} \\
\qquad + \left[\frac{\lambda_1\lambda_2}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_2+\lambda_4)} - \frac{\lambda_2}{\lambda_1+\lambda_2} + \frac{\lambda_2\lambda_4}{\lambda_2(\lambda_1+\lambda_4)} \right] e^{-\lambda_3 t} \\
P_{14}(t) = 1 - P_1(t) - P_2(t) - \cdots - P_{13}(t)
\end{cases}
$$

The reliability of the system at time t is,

$R(t) = \sum_{i=1}^{n-1} P_i(t)$, n=14

The following can be calculated based on the above:

$$R(t) = -3e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t} + e^{-(\lambda_1+\lambda_2+\lambda_3+\lambda_4)t}\left[\frac{\lambda_2}{\lambda_1+\lambda_2+\lambda_3}+\frac{\lambda_3}{\lambda_2+\lambda_3+\lambda_4}+\frac{\lambda_4}{\lambda_1+\lambda_3+\lambda_4}+\frac{\lambda_1}{\lambda_1+\lambda_2+\lambda_4}\right]$$
$$+e^{-(\lambda_2+\lambda_3+\lambda_4)t}\left(\frac{\lambda_3}{\lambda_2+\lambda_3}\right)+e^{-(\lambda_1+\lambda_2+\lambda_4)t}\left(\frac{\lambda_1}{\lambda_1+\lambda_4}\right)+e^{-(\lambda_1+\lambda_2+\lambda_3)t}\left(\frac{\lambda_2}{\lambda_1+\lambda_2}\right)$$
$$+e^{-(\lambda_1+\lambda_3+\lambda_4)t}\left(\frac{\lambda_4}{\lambda_3+\lambda_4}\right)+\left[\frac{\lambda_1\lambda_2}{(\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3)}\right]e^{-\lambda_4 t}+\left[\frac{\lambda_2\lambda_3}{(\lambda_3+\lambda_4)(\lambda_2+\lambda_3+\lambda_4)}\right]e^{-\lambda_1 t}$$
$$+\left[\frac{\lambda_3\lambda_4}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}\right]e^{-\lambda_2 t}+\left[\frac{\lambda_1\lambda_4}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_4)}\right]e^{-\lambda_3 t}$$

The failure rate of the system is

$$F(t) = 1 - R(t)$$

The mean time to failure of the system is

$$\text{MTTF} = \int_0^\infty R(t)dt$$
$$\text{MTTF} = -\frac{3}{\lambda_1+\lambda_2+\lambda_3+\lambda_4}+\frac{1}{\lambda_1+\lambda_2+\lambda_3+\lambda_4}\left[\frac{\lambda_2}{\lambda_1+\lambda_2+\lambda_3}+\frac{\lambda_3}{\lambda_2+\lambda_3+\lambda_4}+\frac{\lambda_4}{\lambda_1+\lambda_3+\lambda_4}+\frac{\lambda_1}{\lambda_1+\lambda_2+\lambda_4}\right]$$
$$+\frac{\lambda_3}{(\lambda_2+\lambda_3)(\lambda_2+\lambda_3+\lambda_4)}+\frac{\lambda_1}{(\lambda_1+\lambda_4)(\lambda_1+\lambda_2+\lambda_4)}+\frac{\lambda_2}{(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_3)}+\frac{\lambda_4}{(\lambda_3+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}$$
$$+\frac{\lambda_1\lambda_2}{\lambda_4(\lambda_2+\lambda_3)(\lambda_1+\lambda_2+\lambda_3)}+\frac{\lambda_2\lambda_3}{\lambda_1(\lambda_3+\lambda_4)(\lambda_2+\lambda_3+\lambda_4)}+\frac{\lambda_3\lambda_4}{\lambda_2(\lambda_1+\lambda_4)(\lambda_1+\lambda_3+\lambda_4)}$$
$$+\frac{\lambda_1\lambda_4}{\lambda_3(\lambda_1+\lambda_2)(\lambda_1+\lambda_2+\lambda_4)}$$

Appendix 7 Example of Compliance Certificate

CHINA CLASSIFICATION SOCIETY Job No.______

COMPLIANCE CERTIFICATE FOR RELIABILITY VERIFICATION

Applicant ____

Item ____

Model/Version ____

THIS IS TO CERTIFY that the above mentioned equipment and systems have been evaluated and tested by the Society and hereunder confirmed that:

1. The system is in compliance with Guidelines for Reliability Verification of Ship Equipment and Systems on________(equipment/computer software/embedded software/system) . and

2. The system in compliance with the Severity of environmental parameter_________ (Such as 6K2/6B2/6C3/6S1/6M4) .

Issued at__________________

Issued on_________________

____

CHINA CLASSIFICATION SOCIETY