

IEEE Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal Power Stations: Operation Service and Management

IEEE Standards Association

Developed by the
Corporate Advisory Group

IEEE Std 1865.2™-2019

STANDARDS

IEEE Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal Power Stations: Operation Service and Management

Developed by the

Corporate Advisory Group
of the
IEEE Standards Association

Approved 7 November 2019

IEEE SA Standards Board

Abstract: The basic principles, items, methods, performance indicators, and acceptance requirements for the maintenance and testing of the distributed control systems (DCSs) of thermal power plants are specified. This standard is mainly applicable to the maintenance and testing of DCSs of conventional thermal power plants in commercial operation.

Keywords: DCS, distributed control system, fault handling, I&C, IEEE 1865.2™, instrument and control, maintenance, operation service repair, scheduled maintenance, test, technical management, thermal power plant

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 10 April 2020. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-6323-2 STD23987
Print: ISBN 978-1-5044-6324-9 STDPD23987

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/ipr/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore at <http://ieeexplore.ieee.org/> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at <http://standards.ieee.org>.

Errata

Errata, if any, for IEEE standards can be accessed via <https://standards.ieee.org/standard/index.html>. Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore: <https://ieeexplore.ieee.org/browse/standards/collection/ieee/>. Users are encouraged to periodically check for errata.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this IEEE standard was completed, the P1865.2 Working Group had the following membership:

ABB (China), Ltd.	Guangdong Datang International	State Grid Zhejiang Electric Power
China Datang Corporation	Chaozhou Power Generation	Research Institute
China Energy Engineering Group	Co., Ltd.	Zhejiang Datang Wushashan Power
Co., Ltd.	Rundian Energy Science and	Generation Co., Ltd.
Emerson Automation Solutions	Technology Co., Ltd.	Zhejiang Energy Technology
		Research Institute Co., Ltd.

The Working Group gratefully acknowledges the contributions of the following participants. Without their assistance and dedication, this standard would not have been completed.

Yiying Tong, *Chair*
Changsheng Sun, *Vice Chair*
Li Zhou, *Secretary*

Bo Chen	Shuyun Hu	Yan Xi
Chengwei Dai	Guosheng Li	Wei Xue
Bo Feng	Linhu Liu	Feng Yin
Lingyun Guo	Yucheng Liu	Jinbin Zhang
Weimin Guo	Lu Pei	Changzhi Zhao
Boyong Hu	Yongcheng Qiao	Feng Zhu
	Yucong Tian	

The following members of the entity Standards Association balloting group voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

ABB (China), Ltd.	China Southern Power Grid Co.,	North China Electric Power
Beijing GreenValley Technology	Ltd.	University
Co., Ltd.	ChongQing University	Schneider Electric
Beijing Sifang Automation Co.,	Emerson Electric Co.	Southwest Jiaotong University
Ltd.	Harbin Institute of Technology,	State Grid Corporation of China
BII Group Holdings, Ltd.	China	(SGCC)
Chaincomp Technologies Co., Ltd.	Hongguang Electric Group Co.,	Tianjin University
China Datang Corporation	Ltd.	Zhejiang Provincial Energy Group
China Energy Engineering Group	Huawei Technologies Co., Ltd.	Company, Ltd.
Co., Ltd.	Huazhong University of Science	
	and Technology	

When the IEEE SA Standards Board approved this standard on 7 November 2019, it had the following membership:

Gary Hoffman, *Chair*
Ted Burse, *Vice Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Masayuki Ariyoshi	Joseph L. Koepfinger*	Xiaohui Liu
Stephen D. Dukes	Thomas Koshy	Kevin Lu
J. Travis Griffith	John D. Kulick	Daleep Mohla
Guido Hiertz	David J. Law	Andrew Myles
Christel Hunter	Joseph Levy	Annette D. Reilly
Thomas Koshy	Howard Li	Dorothy Stanley

Sha Wei
Phil Wennblom

Philip Winston
Howard Wolfman

Feng Wu
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1865.2™-2019, IEEE Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal Power Stations: Operation Service and Management.

Distributed control systems (DCSs) are in wide use today for monitoring and control of power generating units and their auxiliary systems. However, there are several factors—for example, quality of DCSs, the technical and managerial problems or potential risks involving design and configuration, factory acceptance test, installation and commissioning, operation, maintenance, and test process of DCSs—that may directly or indirectly affect the safe, reliable, and economical operation of power generating units.

The safe, reliable, and economical operation of the DCS is based on proper design and configuration, quality of installation and commissioning, and supported by effective maintenance and technical management. To assure long-term safe, stable, and reliable operation of DCS, it is necessary to exercise effective management and control throughout design and configuration, maintenance, test, and routine service and to exercise comprehensive management of safety related external equipment, and their storage and operating environment and conditions.

Therefore, this standard is developed based on the summarization of experiences and expertise and lessons learned from the operational maintenance, repair, test, troubleshooting, and technical management to serve as an international technical and management standard.

This standard specifies the basic principles of repair and test, test performance indicators, and technical requirements for repair acceptance of DCSs. It mainly covers:

- Environment of DCS
- Operation and test of DCS
- Maintenance of DCS
- Technical management of DCS
- Technical requirements and technical assessment of DCS

This standard specifies the basic items, methods, and technical requirements of scheduled maintenance.

[Clause 6](#), about scheduled maintenance, describes the basic items, methods, and technical requirements of periodic maintenance. [Subclause 5.3](#), covering emergency handling and management of faults, describes the development procedure and structure of emergency plans, general requirements and basic principles to be followed for emergency handling of faults, and handling procedures in case of faults. [Clause 7](#) and [Clause 8](#), about management requirements, cover the technical requirements for repair and operation management, software/hardware and upgrade management, storage, management of spare parts, and software/hardware reliability management of control systems.

Contents

1. Overview	11
1.1 Scope	11
1.2 Purpose	11
1.3 Word usage	11
2. Normative references	12
3. Definitions, acronyms, and abbreviations	12
3.1 Definitions	12
4. General requirements	14
4.1 Operation service	14
4.2 Management rules and procedures	14
4.3 Data and records	15
4.4 Process safety control	15
5. Routine maintenance	16
5.1 Basic requirements	16
5.2 Routine inspection	16
5.3 Defects and troubleshooting	23
5.4 Modification of settings and configuration	35
6. Scheduled maintenance	37
6.1 Basic requirements	37
6.2 Scheduled maintenance of hardware and software systems	37
6.3 System safety maintenance	43
6.4 Shutdown of DCS	45
6.5 Upgrade and modification of DCS	46
7. Technical management of DCS	47
7.1 Introduction	47
7.2 Basic requirements	47
7.3 Management of parameter settings	47
7.4 Performance management	48
7.5 Security management	49
7.6 Management of emergency response to faults	50
7.7 Risk management	51
7.8 Development and management of materials plan	51
7.9 Spare parts management	52
7.10 Management of technical data	52
7.11 Outsourcing management	55
8. Technical assessment of reliability	55
8.1 Introduction	55
8.2 Basic requirements	55
8.3 Assessment contents	57
8.4 Settlement of assessment	65
Annex A (informative) Dynamic and steady-state performance specification for modulation control system (MCS)	67
Annex B (informative) Distributed control system (DCS) inspection form examples	68
Annex C (informative) Modification and setting form examples	80

Annex D (informative) Modulation control system assessment methods.....	82
Annex E (informative) Bibliography.....	100

IEEE Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal Power Stations: Operation Service and Management

1. Overview

1.1 Scope

This standard specifies mechanisms and procedures for the operation service and management of distributed control systems (DCSs) in thermal power stations in commercial operation, enabling stable and reliable operation of DCSs.

Reference may be made to this standard for the operation and maintenance of DCSs in other types of power plants.

1.2 Purpose

This standard provides the items, methods, and technical requirements of operation service, fault handling, and technical management of DCS during the operation of power plants based on the engineering philosophy, methods, procedures, and field experiences of DCSs of varying brands in a number of power plants which have been already verified, aiming at offering guidance for developing operation, maintenance, and technical management manuals for DCS in power plants.

1.3 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (shall equals is required to).^{1,2}

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (should equals is recommended that).

¹The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

²The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

The word *may* is used to indicate a course of action permissible within the limits of the standard (may equals is permitted to).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (can equals is able to).

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 1865TM-2019, IEEE Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal Power Stations: General Requirements and Definitions.

IEEE Std 1865.1TM-2019, IEEE Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal Power Stations: Maintenance and Testing.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* should be consulted for terms not defined in this clause.³

analytic assessment: A qualitative analysis of the condition and documents of the system and equipment, supplemented by a quantitative analysis of their basic performance, in order to confirm whether the reliability of the system or equipment satisfy the requirements.

automatic fault identification and alarming: Automatic identification and judgment of the type and possible source of faults based on available information and giving alarms.

availability of input/output points: A ratio of the number of qualified input/output points to the total number of input/output points inspected by sampling, usually in percentage.

classification of importance: A process of classifying all unit-related instrument and control (I&C) system or equipment according to the degree of impact of faults on the safety, economy, environmental protection, and continuous operation of the unit, within the specified conditions and time period.

correct action rate of protection and interlock systems: A ratio of correct operation times to total operation times of protection and interlock systems during the evaluation period.

correlative signals: Associated signals transmitting between different control components, including hardwired signal, system communication signal, etc.

defect classification: Classify the defects according to their impact on the safe operation of the unit:

a) Critical defects: defects that endanger human health, safety of units, environmental protection, and may lead to Class A fault of equipment.

³*IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

b) Major defects: defects that affect economic operation of units and may lead to Class B fault of equipment.

c) Common defects: defects that do not affect the safe and economic operation of units but may develop to Class B fault or Class A fault.

emergency initiation: A process used to start the emergency response procedure to inform the personnel for the emergency response to be in place according to the emergency level.

emergency response plan: Pre-defined emergency measures which are rapidly and orderly deployed in case of potential or possible emergency.

emergency response: A process whereby working personnel judge faults and determine emergency response level according to working procedure after control system fails.

installation rate of input/output points: A ratio of the number of installed input/output points to the total number of designed input/output points, usually expressed in percentage.

main protection: A general term for boiler master fuel trip (MFT) protection and turbine emergency trip system (ETS).

nominal values: Performance indicators of equipment provided by manufacturers of control system and equipment through instruction manuals, contracts, and other technical data.

physical isolation: The control system network is physically isolated from other network equipment and public network in a way to protect the communication links and the hardware, such as the router, workstation, distributed control system (DCS) hardware, network server, etc., from natural disaster, unauthorized access damage, wiretapping, and other attacks.

process related threats: Attacks encountered by the control system during operation. The attackers obtain unauthorized access to control system to send commands causing failure in the control process.

reliability assessment: A process whereby the inherent ability, performance, and post-improvement effectiveness of the components, units, subsystems, devices, and systems are analyzed, evaluated, and confirmed against the reliability criterion.

reliability management: A management of the activities and functions to verify that all the systems and equipment meet the established reliability requirements.

reliability rating: A process whereby all unit-involved instrument and control (I&C) systems or equipment are analyzed and rated for reliability based on the reliability definition and their achievable reliability level.

routine inspection: Daily inspection performed on equipment at a regular time and with defined route and task.

routine maintenance: A general term of daily maintenance, defect elimination, and emergency handling for system and equipment to help ensure their normal operation.

scheduled maintenance: Preventative maintenance performed on equipment during operation based on a time table and in view of the manufacturer's maintenance requirements and operational field experience.

signal forcing/unforcing: A temporary manual intervention to disable or restore the original functions of signals that fail to meet test or operational requirements during test, startup, shutdown, or operation of units.

system-related threats: Threats caused by bugs in protocol and/or operating system.

technical data: A general term of quality management system documents and process control documents.

testing assessment: Assessment performed based on test data to determine if the reliability of system or equipment can achieve the required level.

4. General requirements

4.1 Operation service

Operation service is important daily work to keep the control system working well. It should follow the general requirements as follows:

- a) Operation service of the control system may include preventive maintenance, perfective maintenance, adaptive maintenance, and corrective maintenance. Through normative routine inspection and maintenance, record the working status of every part of the system and, in case any abnormality is identified, investigate the cause and correct the problem in time. Through scheduled maintenance of the system and test, plus inspection of the technical indicators and the quality requirements, maintain the operating environment and hardware of the control system as well as the required monitoring and control function. As a result, the risks of the control system equipment faults and/or control function abnormality can be avoided or reduced.
- b) Different component faults in the distributed control system (DCS) shall be classified and managed according to the severity of their impact on the control system and the operation process. Possible fault risks and their impact on the system shall be identified. Emergency response plans for the control system under various fault conditions shall be prepared, and emergency response drills shall be regularly conducted according to the emergency plan. If necessary, the emergency plan shall be modified and improved to help ensure that once a fault occurs, a response can be in place on time. According to the class of the fault, the involved plan shall be initiated, and efficient measures shall be taken to avoid the fault propagation.
- c) The reliability of the control system shall be specially evaluated to determine to what degree the performance, functions, and reliability of the control system can satisfy the safe operation requirements of the unit and the requirements of the latest standard. Then, determine the required optimization and improvement.

4.2 Management rules and procedures

The effective management system and personnel training are necessary to ensure that maintenance is carried out as expected. They should follow the general requirements as follows:

- a) Develop routine and scheduled maintenance rules and items in accordance with 7.1 of IEEE Std 1865-2019. Carry out routine inspection, maintenance, defect elimination, and scheduled maintenance and test normatively. Check the quality of operational maintenance and the implementation and applicability of management rules to promptly identify and correct non-conforming items.
- b) By following the requirements of 5.3 of IEEE Std 1865TM-2019, carry out the management and training of the maintenance personnel and verify that the maintenance personnel are technically qualified for the maintenance work. By following the requirements of 5.4 of IEEE Std 1865-2019, verify the required tools/instruments and test equipment for the maintenance work, develop the management methods and control measures, satisfy the environmental conditions for the field work and storage, and satisfy the technical requirements for the maintenance, repair, and tests. Ensure that the verification, maintenance, labeling, recording, usage, and storage environment of the equipment are well controlled.

- c) Develop the management rules for technical data and improve the technical information database in accordance with 5.2 of IEEE Std 1865-2019 while taking into account the importance classification of control system and equipment (see Annex C in IEEE Std 1865-2019), online operational quality requirements, and practical operability.
- d) Establish the management system to help ensure the implementation quality of the maintenance work. Develop management policies, standards, and procedural documents for each maintenance work and file the on-going maintenance work.

4.3 Data and records

Data and records are necessary for traceability management and quality evaluation of the operation service. Data and records management should follow the requirements as follows:

- a) By following the requirements of 5.5 of IEEE Std 1865-2019, establish document and data management rules, complete and valid technical documents for daily management, scheduled maintenance, fault handling, and repair of the DCS. The data may include the control system software and hardware equipment records. In the case of equipment modification or software upgrading, update the records for the software and hardware of the control system promptly. Establish the records of loading rate of the various control stations, operator stations, and data communication bus. Establish the fault records for the software and hardware of the control system and the records for equipment abnormalities caused by faults.
- b) Carry out statistic analysis according to the equipment classification, equipment defect classification, and fault classification. Evaluate the change trend of the module's reliability and provide basic data for determining the replacement period of the module based on the importance classification.
- c) Make technical inspection and technical records in detail for the system and equipment during the entire maintenance process of control system. All records shall be complete and concise, with legible words, authentic data, accurate measurement, and analysis.

4.4 Process safety control

It is the most important requirement to ensure the safety of personnel and equipment during maintenance. To achieve this, the maintenance process safety control should follow the general requirements as follows:

- a) The safety measures for the maintenance and management of the DCS shall be put in place and the safety procedures, work permit policies, supervising policies, and contractor work safety agreement be implemented strictly. Safety responsibilities shall be clearly established. Safety management and inspection shall be strengthened. Safety analysis meetings shall be held regularly and safety measures shall be implemented to help ensure the safety of personnel and equipment.
- b) Effective health, safety, and environment (HSE) measures shall be taken for the entire operational maintenance process to help ensure that working and labor conditions are improved, working personnel and equipment are safe and reliable, the workplace is clean and tidy, and all wastes are disposed properly.
- c) The maintenance personnel shall be familiar with the requirements of item d) in 5.4.3 of IEEE Std 1865-2019, when they get access to the site for maintenance, such as for disassembling equipment. In addition, the tools and the safety equipment to be used shall have a test certificate, and the measurement instruments shall have a quality and calibration certificate. For the operations that may cause fluctuation of process parameters, confirmation from the technical staff shall be sought in advance and safety measures shall be put in place.

5. Routine maintenance

5.1 Basic requirements

In order to effectively implement routine maintenance and to ensure the safety of personnel and control systems during maintenance, it is necessary to follow the basic requirements as follows:

- a) The control system is composed of a variety of interconnected components and parts. Therefore, any latent faults not corrected on time may cause malfunction or fault in part or whole, and affect the reliable operation of the unit. To help ensure stable and efficient operation of the control system, the routine maintenance of the control system shall be standardized as below according to the requirements of IEEE Std 1865-2019:
 - 1) Establish routine inspection rules for the DCS and equipment.
 - 2) Refer to [Annex B](#) for developing a routine inspection checklist for the DCS and equipment.
 - 3) Refer to [Annex C](#) for specifying the settings and the management and execution procedures for software maintenance and modification.
 - 4) Establish the defect and fault records for the DCS and equipment.
- b) Professional personnel shall carry out scheduled inspection and make records according to the routine inspection rules and the routine inspection checklist for the DCS operation. After the routine inspection of each day is completed, record the process, file the routine inspection tables, and record the defects and faults. Moreover, handle the common defects identified in the inspection and report the serious defects to the technical chief.
- c) Care shall be excised not to pull or damage the lines and connectors for power supply, grounding, communication, and input/output (I/O) signal. Before handling any defect or fault which may impair safe operation, the personnel shall evaluate possible impact of the handling process on the system and the effectiveness of the solution (the solution shall be reviewed by DCS manufacturer when necessary) and shall take proper safety measures.
- d) The defect handling shall be immediately suspended in case the system operates abnormally, and then decision needs to be made whether to continue the handling after the causes are identified. Any defect/fault that cannot be eliminated in time shall be recorded, and effective measures shall be taken to avoid the development of such defect/fault.
- e) The operation logs of the control system shall be established to record the information of the control system routine maintenance work, including the processing of the major problems during inspection, modification of parameters, protection switching in/out, software maintenance, hardware replacement, etc. The operation logs record all problems during the system operation, including operating record, screen displays, printed abnormal change of the unit parameters, wrong information and texts, and the counter-measures for the problems, etc.
- f) Complete inspection record and defects handling record shall be established to facilitate the technical department to effectively establish and modify equipment maintenance and repair plan through analyzing the operation status based on the records and data, and to provide the basic data for predictive maintenance and repair by tracing the data source.

5.2 Routine inspection

5.2.1 Methods of inspection

The purpose of routine inspection is to timely learn the operation status of system equipment. Inspect the equipment appearance, status indication, data change, operating noise of components, surface temperature of modules, operating voltage of the system, the temperature at important connections, and operation status

and status indication on displays of equipment in the electronics room, control room, engineer room, and field cabinets. Communicate with the unit operator to know about the operation conditions of equipment and its status before and after the defect emerging. Fill out the DCS equipment checklist and record any problems reported by operators.

Fill out the defect sheet in time for any defects identified during the inspection and report them to the technical team according to the relevant procedure (e.g., the professional personnel are required to analyze the cause of the defects and predict the potential faults and develop a solution plan for the maintenance staff to implement).

5.2.2 Routine inspection of control equipment (hardware system)

5.2.2.1 Inspection of operating environment

The operational stability of the DCS is closely related to the ambient environment. Therefore, the task of routine environment inspection is to check and record the internal and external environment of the unit central control room, engineer station, electronic equipment room, and the sites for DCS equipment based on the inspection checklist, and to detect any defects not in compliance with the following requirements and include them in the maintenance list for elimination:

- a) Indoor temperature shall be kept at $(24\text{ }^{\circ}\text{C} \pm 2\text{ }^{\circ}\text{C})$ and the temperature variation shall be less than or equal to $5\text{ }^{\circ}\text{C}/\text{hour}$; the relative humidity shall be kept at 35% to 65%, and condensation is not allowed under any circumstance; the temperature and humidity of the working environment for the onsite remote equipment shall not exceed the limits specified by the manufacturer (normally temperature between $0\text{ }^{\circ}\text{C}$ and $45\text{ }^{\circ}\text{C}$, humidity between 45% and 70%).
- b) The room shall have continuous fresh air supply and have a slight positive pressure (25.4 Pa to 50.8 Pa) to reduce airborne dust and to keep the room ventilated. Dust, vibration, noise, and electromagnetic radiation shall be lower than the permissible nominal values provided by the manufacturer. Unless otherwise demonstrated through strict tests, it is not allowed to use intercom and mobile within the equipment room. Effective protective measures (installation of shield, warning sign, etc.) shall be made in place for equipment that may cause interference.
- c) Check that the isolation measures for prevention against fire, water, moisture, dust, corrosion, unintentional operation, and entry of pests, such as small rodents and insects, are reliable and meet the requirements of the manufacturer, relevant standards, and equipment operation requirements, including:
 - 1) The installed fire facilities and monitoring equipment shall conform to the legislation requirements, operate properly, be intact, and within the valid period.
 - 2) The anti-leakage measures of condensate from any heating and ventilation system passing over the cabinets and to anti-rain (and typhoon, etc.) for the outdoor doors and windows of the electronics room and the outdoor cabinets shall be effective and reliable.
 - 3) The cable holes at the bottom of the cabinet and at the cable mezzanine are blocked well with fireproof mud, and the sealing between cables is reliable. The strainer at the cabinet door shall be free of damage or obvious accumulated dust, and shall be well ventilated.
 - 4) Measures for prevention against mal-operation of buttons intended for emergency shutdown of unit, shutdown of boiler, shutdown of controls of important pumps and fans shall be intact. The important labels on the cabinet shall be conspicuous, and the labels of power switch and grounding shall be in place and clear.
 - 5) The holes around the room shall all be blocked properly. In the areas where rodents, reptiles, insects, and other living beings are likely to appear, check for trails of mice and harmful insects. Verify doorsills are high enough to avoid entry of harmful living beings.

- 6) All sites where the DCS is located, such as electronic equipment room, engineer stations, etc., shall have door-locking systems with ID card reader and CCTV system. These systems shall be intact and operate properly, and their clocks shall be synchronized with the system clock.
- d) Check that the cooling fans on the control cabinet operate properly (no abnormal sound and no obvious accumulated dust) and that the air flow is normal (one can put a hand behind the ventilation port in the back panel of the cabinet to test the ventilation condition), and that the temperature inside the cabinet is always lower than the settings. Otherwise, measures shall be promptly taken or the problematic parts shall be replaced.
- e) The surface of cabinets and insulating rubber of cabinet door shall be intact. Doorknobs, locks, and lighting in the cabinet shall be in good condition, and door lock and cabinet door can be operated and opened smoothly. Components in the cabinet shall be intact, no terminal wiring be exposed to air, wiring tags be complete and legible, and the grounding of cable shielding wires be free of looseness. The doors of control cabinets/stations (operator station, engineer station, and server station) in normal operation shall be closed.
- f) The DCS shall be clean, tidy, and intact. The associated equipment shall be in good operation status. The sign and nameplates shall be accurate, clear, and complete. During normal operation, the control station and the cabinet door shall be closed.

5.2.2.2 Inspection of power supply system

The power supply system is essential for long-term stable operation of the control system. Once the control system loses power, the normal operation of the unit will be interrupted, which may cause fluctuation of the power grid or damage to the main or auxiliary equipment. Therefore, the operation status and developing trend shall be monitored all the time. In the meantime, during routine maintenance, the following items and requirements for the operational reliability of the power system shall be included in the inspection items:

- a) The display value of the voltmeter for the control system dual-feed power shall be inspected and recorded, and shall be close to the nominal value with a deviation of less than 5%. If the dual-feed power is powered by the uninterruptible power supply (UPS) and the auxiliary power supply system respectively, then the working power source shall be the UPS.
- b) Each working voltage level of the control system shall be measured and recorded in order to verify that it is close to the nominal value. The voltage deviation between the two buses at each working voltage level shall be less than 3% of the nominal value.
- c) The indicators of various power modules and the rotation of cooling fans shall be checked and recorded to confirm that they are in normal operating condition. The self-diagnose function of the power supply for the control system shall be checked and recorded, and the status and records shall be consistent with the results recorded during inspection.
- d) The surface temperature of each power module shall be lower than 60 °C. The surface temperature of power supply bus shall be close to the ambient temperature.
- e) If the power system has a new load connected, check if there are authorizing documents and ensure the abundant capacity is not less than 20%.
- f) The cooling fan of the control cabinet shall not share the same loop of power supply with the DCS; otherwise, independent power supply shall be used.

5.2.2.3 Inspection of communication network

Communication network fault is easily caused by defects such as poor contact at nodes of communication bus, incorrect address (new unit, or new connection point), or abnormality of switch and communication network jam. Timely discover and clearing these defects can avoid or reduce the impact on the safety and stability of units. Therefore, inspection shall be carried out on these defect-favored locations during operation:

- a) Check and record the status of the indicators (power supply, working, and communication) of the communication module, main control module, and I/O module of the control system to confirm that they work well.
- b) Check the indicators of communication equipment, such as the switch, hub, coupler, repeater, optical transceiver, etc., to confirm that they work well and the sound of the fans is normal. Check the log of main equipment, and record any identified problems.
- c) Check that the redundant buses displayed on the monitor status diagram and communication network status diagram are in normal redundancy status, and that the equipment faults, switch faults, and errors of the communication network shall not occur and be displayed in the fault diagnosis display. If feasible, use the automatic fault identification and alarming function of the system to check that the communication network works well. Check the error log of the DCS or log of the switch, and verify that there are no records of warning or faults of network ports/switch.
- d) Use the system diagnosis tool/function or other methods provided by the manufacturer to check that the communication load rate of the data bus is less than the nominal value, and that each control subsystem and all I/O channels and their communication indicators are normal.

5.2.2.4 Inspection of control module

As the core component of the DCS, the controller usually adopts redundant controller and redundancy to achieve bumpless switching. However, during operation, controller offline and abnormal switchover may still occur. To reduce operation faults arising from such abnormalities, the following checks shall be carried out on the control modules and their connections through routine inspection:

- a) Check and record the indicators of various modules (including power supply indicator, communication indicator, and fault and alarm indicator) to verify that they work well, and that the redundant controller has no offline or switching records.
- b) Check that the system self-diagnosis function display and alarm display are consistent with the actual status, redundant equipment is in hot standby mode, and module channels are free of damage.
- c) Check the forced/unforced status of module channels and verify that they are consistent with involved records.
- d) Through the monitoring method provided by the system, check the free space of the memory and the loading ratio to verify that they satisfy the requirements of the relevant standards (normally free space of RAM shall be no less than 40% and the loading ratio shall be no more than 60%).
- e) If feasible, use the automatic fault identification and alarming function of the system to check that the modules work well.
- f) Check that the buckles for installation of modules and those for sockets of prefabricated cables between components in the cabinet are not loose.
- g) Check that the surface temperature of the module is normal.

5.2.2.5 Inspection of HMI stations and peripherals

In the control system, human machine interface (HMI) stations (operator stations, engineer stations, and service stations) and peripherals (printer, keyboard, mouse, etc.) are interface for the operators and the maintenance personnel. To reduce impairment of the reliability of information format conversion, storage, and output caused by mechanical wear and aging of components, etc., the HMI stations and peripherals shall be checked as follow during routine inspection:

- a) Check and record the software and hardware environment of HMI stations and peripherals, and verify that they comply with the system operational requirements.

- b) Check and record the indicators of hardware systems (power supply, hard disk, working, etc.) of HMI stations and servers, and verify that they function normally. Verify that the anti-bump measures for the power button and the reset button are reliable, the fan for the casing is working properly with no abnormal sound, and the keyboard and mouse can be used smoothly.
- c) Check and record the storage for historical data to verify it is in active or default status, and the partitions of hard disk have at least 10% free space. Otherwise, free up the hard disk immediately. Check the document system of the partitions and delete junk documents or export some documents to satisfy the space requirements.
- d) Check and record the screen displays of all HMI stations and servers and the function of historical trend inquiry to verify that they can respond quickly and work properly.
- e) Check the printer to verify that it is in standby or online status. The paper for the printer shall be supplemented in a timely manner. The cartridges shall be replaced once the printing is not clear. If the printer is jammed, the jammed paper shall be promptly cleared.
- f) Check the logs of all HMI stations and record the problems for all levels of the control system.

5.2.2.6 Inspection of satellite time synchronization and clock synchronization

Time synchronization is often based on a highly accurate clock to help ensure normal functioning of commands file access and log analysis of the DCS. Factors that influence satellite time and time synchronization shall be listed in the routine inspection items which are described in detail below:

- a) Check satellite timing device to verify that antenna is installed stably and not shielded, the locking catch of the antenna plug is not loose, the antenna feeder is intact, the outside of the antenna has no dust and no stain, and the antenna is receiving satellite signals properly.
- b) Check that access to the GPS is normal, the clock synchronization server can automatically synchronize its time with GPS (satellite time synchronizer), and the GPS provides time signals automatically.
- c) Check the control stations, HMI stations, and server on the data communication bus of the DCS and verify that time synchronization services are correctly set and work normally. All stations and servers shall share a uniform time scale and be synchronous with that of the clock synchronization server.
- d) Check the clocks of the control systems of different networks and verify that clocks of stations on the data communication bus are synchronous with the master clock.

5.2.3 Inspection of monitoring and control functions

5.2.3.1 Inspection of HMI

The HMI stations have operators in place to monitor the operation of the unit, the process system, and the equipment, and to monitor and process the unexpected situations and faults. The engineer stations have maintenance personnel in place to debug, modify, and backup the application software and to maintain the database. During the operation, unexpected situations, such as interface crashing, response delay, etc., may happen, and they shall be identified and confirmed through HMI inspection as follows:

- a) Check the screens of display, function operation, self-diagnostic function, etc., to verify that they can be switched over smoothly and there is no obvious delay on data refreshing. Alarm signal classification and settings shall be the same as the provided list so that the system can be fully operated according to the design requirements.
- b) Check the display and record screens for the audible and visible alarms, alarm display, sequence of events (SOE), operations and events, etc., to verify that they are working properly. The time sequence shall be appropriate to the actual occurrence sequence. The record of the alarm signals and the abnormal operation events shall be copied and saved.

- c) Check SOE and other printers to verify that they are ready, and the function for printing all reports and tables is normal (the content and time order of the printed reports and tables shall be consistent with reality).
- d) Check the storage and retrieval functions to verify that they are correct. Configure the trend curve display online to help ensure that the display is consistent with the requirements and the time scale and measuring range can be adjusted readily, and the time marker can be moved smoothly.
- e) Check the operation logs, record the problems arising with the control system, and ask the operators for system operation status and requirements.

5.2.3.2 Inspection of data acquisition signals

Based on the requirements for design of process systems of a power plant, the designed I/O signals are continuously acquired and processed, and then stored in real-time and historical databases, so as to achieve the information sharing of the DCS. The reliability and accuracy of data acquisition helps ensure the safe operation of control and protection system; therefore, inspection shall be performed to identify and record abnormal indications in time:

- a) Check the screen displays of the DCS to verify that all signals are used in response to the operational requirements of the unit. Record the signals that could not be used in the operation and verify that the record for the cause analysis and the solution plan are in place.
- b) Check the display values of the parameters to verify that they are consistent with the actual situation of the power production process without significant deviations. Check the actual value and the historical trend of the parameters to verify that the requirements for the process control are satisfied and the display is normal. Record and print the displays and curves of the abnormal parameters, such as wrong parameter values, curve upside-down, sudden change, fluctuation, discontinuousness, signal rate protection action, over range, etc.
- c) The operation mode of the redundancy signal shall follow the requirements for the reliability of operation monitoring.
- d) The deviation of the same measured parameter transmitted from different sensors shall be less than the permissible comprehensive error of the measurement system. The deviation of redundancy signals with the same measurement accuracy shall not be greater than twice the allowable comprehensive error of the measuring system.
- e) During normal operation, frequent alarm signals and flickering of too many parameters shall not occur on display.

5.2.3.3 Inspection of modulation control system (MCS)

With the change of unit load, unit characteristics, and fuel characteristics, the control performance of the MCS may change appropriately. To help ensure that the change of performance of the control system can be timely identified, the following items shall be checked and recorded during inspection:

- a) Check the operation mode for the redundancy signal to verify that it satisfies the reliability requirements for the control functions.
- b) Check the operation mode of the control loop to verify that there is no record for unexpected switching. When a single signal in the redundancy signals becomes abnormal, or when the signal-changing rate is out of the limits, the system shall give alarm. The signal output blocking function shall be disabled when the signal is back to normal (or the action and recovery mode shall satisfy the reliability requirements for the control functions).

- c) Check all control subsystems to verify that they are working reliably and stably. The operation control performance shall satisfy the requirements for control specifications (refer to [Annex A](#)). For the subsystems not in use, explain the causes and make records.
- d) Check the historical trend curve display of the control parameters to verify that there is no abnormal change.
- e) Check that defect and processing records, logic and parameter modification records, and appropriate procedure documents are complete and consistent with the actual conditions.

During inspection, the reliability of the control system shall be analyzed by combining the above-mentioned situations, the control performance, the occurrence number of defects, the trend of control parameters, etc. If the control performance is out of the allowance, the historical curves of involved parameters (command signal, control signal, feedback signal, etc.) shall be plotted for comparative analysis, suggestions on analysis and treatment shall be given, and records are made.

5.2.3.4 Inspection of on-off control

Mal-operation of the protection interlock system may bring economic loss to power plants. To help ensure the reliability of the protection interlock system, in addition to the design of rigorous interlock logics and selection of appropriate control equipment, trip signal sources, correlative signals, and installation positions for signal measurement, effective inspection and maintenance shall be performed during operation.

- a) Check the screen displays of all protection and interlocking systems to verify that there is no abnormality, all systems are online and working properly without signal forced, and appropriate parameters are displayed correctly. The sequence control logic and step sequence shall comply with equipment operational requirements. If there is any nonconforming item, the record and precautionary measures shall be available.
- b) Check that the protective measures for important protection interlock equipment are valid.
- c) For slow variation parameters involved in protection, off-limit alarm for signal change rate and blocking of protection function output shall be set. The protection function shall be automatically reset after restoration of signals, and the alarm signals shall be reset manually.
- d) In case the protection interlock signals adopt redundancy logic, if a single abnormal signal occurs, the system shall give an alarm, and conditions of the signal in redundancy logic shall restore automatically after the abnormal signal disappears. In case of two abnormal signals, the protection actuation signals shall be sent when the system gives an alarm, and the protection actuation signals shall restore automatically after the abnormal signals disappear.
- e) Check the historical curves of the important protection and interlocking signals to verify that there is no abnormal display (such as signal rate protection action, signal climbing, signal fluctuation, operation of redundancy signal, etc.).
- f) Check that the procedure documents are complete and comply with specified procedures when protection interlock signals switching on/off operation, and appropriate signal forcing/unforcing records are consistent with the reality.
- g) Check the records for defects and processing, the records for logic and parameter modification, and the appropriate procedure documents to verify that they are complete, consistent with reality, comply with the specific procedure, and the actual modified content is consistent with the record.
- h) When any events of protection occur, check the record for the occurrence time, main operation parameters, first-out fault signal, the process, and the action cause, and take measures to verify that they are complete and consistent with reality.

5.3 Defects and troubleshooting

5.3.1 Basic requirements

5.3.1.1 Defects classification

During routine maintenance, in order to effectively control defects and faults (for classification of equipment defects and faults, refer to Annex D of IEEE Std 1865-2019), they shall be classified as follows based on their impact so that specific measures can be taken for troubleshooting to control the propagation of the fault:

- a) Critical defects include: DCS power faults, interruption of communication network, controller function loss, two or more operator stations losing monitoring function, and faults of the controllers intended for interlock protection.
- b) Major defects include: DCS power redundancy loss, DCS grounding performance loss, software faults of engineer stations, time synchronization problems, network redundancy loss, controller losing redundancy, important I/O signal problems that impair unit safety, main control system problem, main protection and interlock system problems. For these defects, processing plans shall be in place. Refer to the processing of Class A defects.
- c) Common defects include: Ethernet fault, loss of functions of the history station, slow response during operation of the operator station, fault of mouse at the operator station, fault of the controllers intended for data acquisition, fault of auxiliary equipment of cabinet, printer faults, and partial fault of operator station display. Such defects shall be eliminated after the two classes of defects mentioned above are eliminated.

5.3.1.2 Safety management of troubleshooting

Standardize DCS defect management to help ensure that the equipment defects or system defects occurred during the DCS operation are timely processed. Before the defects are eliminated, verify that safety measures are in place, and the processing will follow the requirements strictly:

- a) The typical critical and major defects occurred during operation shall be eliminated according to the procedures and methods in the authorized emergency response plans.
- b) For rare critical and major defects occurring during operation, before the processing, the feasibility of online processing shall be analyzed, the potential impact of the defect and fault handling and recovery procedures on the system shall be evaluated, and a detailed processing plan (including safety protective measures, processing procedures, and methods) shall be in place. The processing procedures shall be technically proved (if necessary, confirmation from the specialist of the equipment manufacturer is required), and appraised by the technical director to confirm that the procedure is reliable. The processing shall only start after all safety measures are in place.

5.3.1.3 Process management of troubleshooting

In order to eliminate the propagation of fault during the defect processing due to human-involved mishandling (especially the handling after the crashing of redundancy controller), it is necessary to strictly follow the processing and management procedure for the DCS defects and the following principles:

- a) During the processing of critical and major defects, in order to avoid unit tripping due to the propagation of defects, all preventive measures shall be in place by following the plan for emergency unit shutdown.
- b) Before processing, the personnel shall make available the instruments, tools, and spare parts required, familiarize with the processing plan, establish the safety measures, and handle relevant formalities according to the specified procedure. Brief the operators on the defect processing details. For the

procedures that may cause fluctuation of process parameters, authorization from the process personnel is required.

- c) Supervision shall be in place during the processing. Keep detailed records of the fault and defect processing process, and verify that the following requirements are met:
 - 1) When faulty equipment is removed out of service, the control, interlock, and protection devices that are related to safe operation of the involved unit shall be switched to manual mode, isolation measures (including wrapping insulation protection on the signal wires) shall be in place for all points and equipment with forced signals, labels placed properly onsite, and relevant record made. Anti-static wristlet shall be worn when disassembling and installing the modules to avoid electrostatic damage to the modules.
 - 2) Before the modules are replaced, the settings and configurations of the new module shall be checked. Confirm that the configurations inside the module satisfy the requirement of the original module, including all communication ports, the switches or jumpers for address, power supply and redundancy, I/O function, and control algorithm function. Predict the potential events during the module replacement and put the protective measures in place. In the meantime, switch the control mode of involved control loops, control procedures, and interlock to manual. During the switchover, the new module can be inserted into the right module location only by the maintenance staff after the supervisor confirms the module location and settings for other switches. During handling, when it is necessary to restart an abnormal control module, measures shall be taken to avoid mistaken sending of output signal during initialization of control module, and involved preventive measures shall be taken according to the emergency shutdown plan.
 - 3) Abnormality found in the handling process shall be treated in accordance with item d) of 5.1
 - 4) Before the end of the handling process, according to the record made in item 1), remove the isolation measures, reset the points and equipment with forced signals to working status (installation accuracy reconfirmation and tightness check shall be carried out after the cables are connected to the original positions). In the meantime, the working site shall be cleaned up and the protective measures shall be improved.
 - 5) After the processing, timely report to the operators, and disclose the operation precaution details to the operation department. The operators shall then carry out tests to verify that the defects have been eliminated.
- d) For the defect processing that requires the equipment to be taken out of the operation, it shall be restored to operation in the scheduled time. After the processing, the supervisor shall do acceptance check to confirm that the fault has been cleared without any potential hazard and sign the acceptance document. Then the equipment can be put back into operation.

5.3.1.4 Records and reports

All the records on the handling process of equipment defects shall be correct and complete; such records shall include:

- a) The operation status of unit, details of faults or defects, abnormal phenomena, the alarm on the display, and the reporter of the event when the unit is abnormal.
- b) Details of the defect checking, analysis, and tests.
- c) Defect processing details (including methods and procedures used, the detail of the replacement, and the problems occurred during the processing).
- d) Records made by the supervisor regarding the procedures and results of the abnormality processing, as well as the analysis and summary of the abnormality processing.

DCS defects elimination shall be recorded in time, and reports shall be provided after the critical and major defects are processed. These records and reports shall be classified and filed for the convenience of inquiry and comparison with historical data and to provide basic data for predictive maintenance.

5.3.2 Treatment of hardware defects

5.3.2.1 Environmental problem processing

Environmental problems identified during inspection of the sites where the DCS is located, such as unit central control room, engineer stations, service stations, electronic equipment room, etc., shall be inspected and processed according to the relevant requirements:

- a) When the environment temperature does not meet the requirements, timely inform the operator to check the working status of central air-conditioning system. If necessary, switch on the spare air conditioner in the electronic equipment room or add a new air conditioner to maintain the temperature within the standard value. When the air conditioner fails, the room temperature shall be strictly monitored to help ensure that it will not exceed the manufacturer's permissible range (15 °C to 30 °C). In winter, when the room humidity cannot be controlled within the specific range, an air moisturizer shall be introduced to reduce electrostatic discharge caused by overly dry air. If the temperature and humidity of the working site of remoted controlled equipment cannot be controlled within the range, it shall be included in the maintenance and repair plan, and it may be solved by adding a ventilation device or relocating the equipment.
- b) Any defect of protection of the electronic equipment room identified during inspection shall be timely filled into the defect sheet and the department in charge shall be informed to handle it. After processing, recheck the situation to verify that the defect has been eliminated.
- c) DCS equipment sites, such as electronic equipment room, engineer stations, etc., shall have door locking system with ID card reader and CCTV system. If there is an abnormality or the clock is not synchronized with the control system clock, it shall be timely filled into the defect sheet and the department in charge shall be informed to handle it. The former defect shall be eliminated timely and the latter defect shall be eliminated by adjusting the clocks when the unit is shut down for maintenance.
- d) When there is obvious accumulated dust on the cabinet cooling fan, or there is some abnormal sound from the fan, or the fan cannot keep a normal air flow, or the temperature inside the cabinet is higher than the setting, dust shall be timely cleaned and the fan shall be replaced. Before replacement, it is necessary to confirm that the new fan has the same voltage, power, and rotation speed as the old one. After replacement, check that the power cable is secured and the air flow direction of the fan is correct. The replacement time shall be recorded such that the replacement cycle of the fan can be made available.
- e) If there is any damage to the appearance of cabinet, insulating rubber of cabinet door, doorknobs, locks, components in the cabinet and lighting, or the cabinet door cannot be opened smoothly, such defects shall be handled in time. In case exposed wires are found in the cabinet, the person in charge shall identify the cause and then restore the wiring (any wires that have been identified as idle shall be wrapped and then put into the wiring duct). If the grounding connection of cable shielding wires gets loose, fasten it immediately.
- f) If the labels or nameplates of the equipment and cables are missing or not clear, supplement or fix them.

5.3.2.2 Treatment of power system defects

The defect sheet shall be filled out and defects eliminated in time if during inspection any of the following are found:

- The power supply displays of the power system and the control system fail to meet the requirements.
- The temperature of connection points in the power supply circuit fails to meet the requirements.
- The working status of the indicators and surface temperature of all modules in the power system fail to meet the requirements.
- There are protection alarms for overcurrent, overvoltage, or input surge protection of the UPS, or abnormal switching of standby power supplies, etc.

The common faults that occur in the power system and the troubleshooting processes are as follows:

- a) When the display values of voltmeters of the two power supplies of the control system do not comply with requirements, the power supply device shall be inspected, adjusted, or handled by professional electricians. If the UPS is not the working power supply during normal operation, the power supply identification circuit shall be added during scheduled maintenance.
- b) If the indicators of power modules show abnormal operating status, the problem shall be processed in view of the status codes. If the self-diagnosis is not consistent with the inspection result, the integrity of the self-diagnose function of the power system and the reliability of the connections between the communication cables shall be checked and tested and processed accordingly.
- c) When all levels of working voltages drift from the nominal values of the power supply, or when the deviation between dual-feed voltage at the same voltage level exceeds the nominal value, if these defects cannot be eliminated through adjustment and are not caused by improper connection of power supply circuit or external causes, the power module shall be replaced.
- d) When the surface temperature of the power module is over 60 °C, or when the surface temperature at connections of output circuit of the power module and the surface temperature of power supply bus are higher than the environment temperature, the cause may be investigated from the problems described below, and the defects can be processed once the safety measures are in place:
 - 1) Problems caused by other factors outside power supply system: Power increase caused by the faults of control system parts, local short-circuiting of power supply circuit of the control system, new power load added in violation of requirements, etc.
 - 2) Problems caused by circuits of power supply system: If the problem is caused by the poor quality or aging of the power module, the module shall be replaced. If the problem is caused by the increased contact resistance of the power module output loop or the connection point of the busbar, a power shutdown shall be arranged after the safety measures are in place.
- e) When the standby power supply cannot be switched automatically, the contact reliability (whether poor contact is caused by the formation of overheating oxide layer) of terminals, the effectiveness of connection and switching of standby power supply, the rationality of switching time of switching device, and the correctness of connection of redundant power supply (shall not be led from the same section) shall be checked to identify the cause, and then take appropriate measures.
- f) In case of faults such as mal-operation of protection caused by fluctuation of operating voltage, the power supply stability on power supply side, the interference caused by startup of high-current equipment, the reliability of power module, the tightness of connection of voltage circuit, and the rationality of settings for mal-operation protection shall be checked until the cause is identified, and then take appropriate measures.
- g) For new loads without authorization documents, contact the person in charge to remove them. If the power system is capable of these extra loads, the authorization documents shall be obtained according to the specific procedures.

5.3.2.3 Treatment of communication network defects

Before processing, the cause for the defects or faults shall be further confirmed through system status diagram and network status diagram, the alarm and fault information of network ports, or switch recorded in the DCS error log and the switch's log. The following appropriate measures shall be taken during the processing:

- a) When the indicators of the power, working status, and communication status for the network self-diagnose functions and equipment of the control system (including switch, hub, coupler, and transponder) are abnormal, investigate the defect cause in view of the status codes and handle it. If feasible, use the automatic fault identification and alarming function of the system to identify the defect.
- b) When the redundancy bus is not in redundancy working status or there are frequent switching and network error records, or when the communication loading rate of the communication bus exceeds the nominal values, or the control subsystems, I/O channels, and communication indications become abnormal, the defects shall be filled in and handled by the DCS specialists or the technical staff from the DCS manufacturer.
- c) When there is accumulated dust on the fan and the operating sound is abnormal or cannot provide sufficient air flow, clean the dust or replace the fan. If the communication fibers and cables are not properly connected, it shall be dealt with when the unit is shut down for maintenance.
- d) If the communication abnormality is caused by poor connection of the communication terminals, clean and tighten the terminals. If the abnormality still exists, then the terminals shall be re-secured with the special tool.
- e) During communication maintenance, the address of the network card, master control card, and data relay card shall be confirmed to be accurate. When reconnecting the network parts after maintenance, the diagram for the network identification and connection shall be strictly followed to avoid the network part connection errors.
- f) When network loses its redundancy, before handling such defect, check the status of communication points connected to the controller, set the appropriate adjustment equipment to manual, and set the parameters manually. Verify that the safety measures for the redundancy network are in place before the network faults are cleared. During the processing, the operator shall switch the unit control to local control, reduce the operations, and keep the load stable. The maintenance staff shall take care not to make the wire terminals touch the conductive cabinet, other conductors, or contact the redundant terminals. Do not change the ports of the communication cables at will.

5.3.2.4 Treatment of control station (modules) defects

When the defects of the control station (modules) are processed during the operation of the unit, switching between master/slave controllers shall be avoided as practically as possible; otherwise, measures shall be taken to switch the related control systems to manual to avoid impact on unit operation. Other defects shall be dealt with as follows:

- a) When there are abnormal situations, such as abnormal indicators of the module operation status, offline, redundancy switching, channel damage, etc., the fault cause shall be confirmed through the hardware or software fault indications and the fault code. If feasible, use the automatic fault identification and alarming function of the system to identify the defect. Process the fault and keep records according to the procedure and operation card.
- b) When the self-diagnosis display and alarm display of the system are inconsistent with the actual conditions, redundant equipment is not in hot standby, and it is confirmed that the settings of communication unit address and communication connection are correct, the redundant equipment not in hot standby shall be restarted.

- c) When the storage of the controller has less than 40% free space or the loading rate is more than 60%, clean and delete the accumulation. The cause shall be identified and appropriate measures shall be in place.
- d) If the buckles for installation of modules and those for sockets of prefabricated cables get loose, DCS operators shall carry out reliability analysis and take safety measures to verify that signal is not sent accidentally because of the vibration.
- e) If the surface temperature of the modules is too high, after ruling out the external causes, the DCS operators shall carry out the reliability analysis, and according to the importance of the module, take measures to reduce temperature or replace the modules.
- f) If the actual forcing of module channels is inconsistent with that in the record, the personnel involved shall find out and solve the problems; the department shall put the protective measures in place to prevent the defect from happening again.

5.3.2.5 Treatment of HMI defects

Problems of the HMI of the control system are mostly caused by mechanical wear, component aging, hard disk or card faults, etc. The HMI consists of multiple working stations with the same function. Faults in one station shall not affect the monitoring of the system, and shall be dealt with in a timely manner to avoid the propagation of the faults.

- a) If the HMI and the peripheral's software and hardware environment do not satisfy the system operational requirements, the problem shall be processed according to 5.3.2.1.
- b) For abnormal operation status light of the HMI station and the hardware system (power, hard disk, module, etc.) of the server, as well as the display color error of the engineer station (the status for bus and its branches, all workstations and redundancy controller, etc.), confirm the cause of the abnormality or fault through the fault information in the self-diagnose system and the appropriate code analysis, and carry out appropriate process. If the operation response is getting slower, the communication load rate of CPU, communication load rate, connection reliability of communication connectors, and probability of virus invasion shall be checked. If control operation fails, check if it is caused by software defect or fault of hardware, such as trackball mouse, and if it is found that process channel functions normally, corresponding operating units may be re-started or reset. If the problem still exists, then replace the doubtful components; or if the operator station breaks down, restart it.

NOTE—The startup time is different from one manufacturer to another, ranging from tens of seconds to several minutes.⁴

- c) If fans operate with noise, dust shall be removed and lubrication oil shall be applied; risks of unintentional operation of the power button and reset button shall be cleared. If the keyboard or mouse fails to response correctly and cannot be solved by removing contamination from internal mechanical contacts and ensuring that cable joints are reliably connected, replace the keyboard or mouse.
- d) When the free space in the hard disk partitions is less than 20%, clean up the hard disk, check the document system of the partitions, and delete junk documents or export some documents out of the hard disk to satisfy the requirements.
- e) If the printer cannot print properly or cannot be in standby status, check and clear the faults from the settings and hardware. When the paper is low, supplement paper; when the print shows that the ink is insufficient, the cartridges shall be timely replaced; if the printer is jammed, the jammed paper shall be timely cleared.
- f) If there is an abnormality of the external tape recorder, disk recorder, disk storage devices, or other hardware, they should be timely replaced.

⁴Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

- g) If there are problems with extracting an operation log of the HMI station, appropriate measures should be in place to reduce potential problems.

5.3.2.6 Treatment of satellite time synchronization and clock synchronization defects

The installation and maintenance problems of the satellite timing devices as well as the satellite timing and synchronization problems during operation shall be eliminated in a timely manner. After putting the protective measures in place, process the problems as follows:

- a) If the satellite signals are not received, or the time of the clock synchronization server is asynchronous with that of the satellite time synchronizer, check the reliability of communication circuit between antenna, clock synchronizer, and DCS.
- b) When the synchronization setting of the control stations, HMI stations, and the server on the DCS data communication bus is incorrect, or the time of the stations is not synchronized with the time synchronization server, the DCS time shall be changed and refreshed in the time-refreshing window on the engineer station during the shutdown of the unit.
- c) When the clocks of control systems of different networks are asynchronous, or the clocks of the control system are asynchronous with each other, the time shall be adjusted and synchronized.

5.3.3 Treatment of function defects

5.3.3.1 Treatment of HMI monitoring defects

Defects of the HMI monitoring function will influence the operators and cause the following system operation to drift from the original targets or cause incidents due to response delay. Therefore, the defects in the HMI need to be handled as follows:

- a) When no response is received from the HMI, check if the connections are loose, whether there is a conflict between the series ports or between the interrupt request numbers. If the problem is caused by the conflict, adjust the resource to avoid the conflict.
- b) When the screen toggle is not smooth, check and handle the following problems one by one: hardware fault, network connections, signal jam, data overflow, configurations of screen picture, virus infection, etc., until the screen toggle is back to normal.
- c) When there are Class A alarm signals (normally in red) in an operator station or engineer station, investigate the cause and handle it immediately.

CAUTION

The alarm signal shall not be confirmed in the alarm window of the engineer station; rather, it shall be processed by the operator in the operator station.

- d) For problems on other alarm signals, screen display, and record, they shall be handled on time.
- e) When the content of the printed reports or the recorded time of the SOE are different from the actual conditions, or when the historical curves cannot be retrieved after SOE print, or when the order of the SOE time is different and has large deviation, the configurations of the SOE and the communication settings shall be checked.
- f) Analyze the alarm signals and abnormalities during unit operation and handle the problems reported by the operators in a timely manner.

5.3.3.2 Treatment of data acquisition defects

The defects of data acquisition shall be prioritized for processing according to their importance. During the processing, the following principles shall be followed:

- a) The Class A and Class B signal defects shall be eliminated in a timely manner. Before the elimination, evaluate the possible impact on the abnormal status of the signal continuity and the recovery process, and put the safety measures in place to help ensure a safe process procedure.
- b) For signals that cannot be switched in time according to operational requirements of units and cannot be processed during operation, cause analysis records shall be available and handling plans shall be provided.
- c) For the abnormal parameter display and curves, the cause shall be analyzed and judged and the appropriate measures shall be in place:
 - 1) For abnormal signals, such as obvious parameter inconsistency, the following methods can be used one by one to check and correct the defect: tighten connections, check and calibrate components and channels, check the reliability of field temperature measurement components, check the accuracy of the installation location and level correction of pressure sensors, etc.
 - 2) For abnormal signals—such as a sudden parameter change, fluctuation, or signal rate protection action, etc.—the following items can be checked and corrected one by one to address the defect: the grounding reliability and continuity of the shielding layer, the effectiveness of the anti-interference measures, the possibility of the start/stop interference from field large current equipment, etc.
 - 3) For abnormal signals, such as parameter discontinuity and over-range, etc., make comprehensive analysis of the operation of the main equipment, loop connections, and field instruments to confirm whether it is the real situation of the process procedures or if there is something wrong with the signal system.
- d) When the signal measurement deviation is out of tolerance, calibrate the measurement components, DCS channels, and compensation cable (thermocouple signal) and check the accuracy of the physical location correction for components that do not satisfy the requirements; they need to be replaced. Eliminate the deviation impact from the onsite measurement-point location, the environment of instruments, and loop temperature compensation. Tighten the loop connections to eliminate the deviation attributable to contact heating and contact resistance.
- e) For frequent alarm signals and flicker of parameter values, after checking and confirming that the equipment and instruments are working properly, arrange for professional personnel to demonstrate the reasonability of the default alarm settings and the necessity of modification. If necessary, adjust the alarm value settings through the specific procedure.

5.3.3.3 Treatment of modulation control defects

If an important control system is involved, fault-prevention measures of the modulation control system (MCS) shall be in place before the handling process. Evaluate the possible impact of the handling and recovery procedure on the system, take appropriate safety measures, and generate a safe process procedure before the process. During the processing, the following principles shall be followed:

- a) When there is abnormal switching in the operation mode of the control loop, analyze and confirm the cause of the abnormal switching. If necessary, optimize the logic of the control loop.
- b) When there is a jump in the historical trend curve of the control parameters, check whether it is the real situation of the main equipment, caused by interference, or caused by a defect of the control system itself, and take corrective measures accordingly.