

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Nuclear power plants – Electrical power system – General requirements

**Centrales nucléaires de puissance – Système d'alimentation électrique –
Exigences générales**

IECNORM.COM : Click to view the full PDF of IEC 63046:2020



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2020 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform

The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC -

webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary

67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



Nuclear power plants – Electrical power system – General requirements

**Centrales nucléaires de puissance – Système d'alimentation électrique –
Exigences générales**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 27.120.20

ISBN 978-2-8322-8817-7

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	5
INTRODUCTION.....	7
1 Scope.....	9
1.1 General.....	9
1.2 Application: new and pre-existing plants	11
1.3 Framework.....	11
1.4 Interaction with level 2 standards	11
2 Normative references	13
3 Terms and definitions	14
4 Abbreviated terms	23
5 Overall Electrical Power System life cycle	24
6 Architecture of Electrical Power System: identification of requirements.....	25
6.1 Objectives.....	25
6.2 Safety requirements applicable to the electrical architecture design.....	26
6.2.1 Defence in Depth.....	26
6.2.2 Application of Single Failure Criterion.....	26
6.2.3 Management of the Common Cause Failure.....	26
6.2.4 Loss Of Off-site Power conditions.....	26
6.2.5 Station Black Out conditions.....	27
6.2.6 Loss of Electrical Power conditions.....	27
6.2.7 Application of internal and external Hazards.....	27
6.2.8 Nuclear security requirements.....	28
6.2.9 Classification requirements.....	28
6.2.10 Probabilistic requirements	28
6.3 Electrical requirements.....	28
6.3.1 Requirements coordinated with the electric grid operator.....	28
6.3.2 Electrical disturbances.....	29
6.4 Functional performance requirements	29
6.5 Maintenance requirements.....	30
7 Design of the electrical architecture.....	30
7.1 Objectives.....	30
7.2 Safety design provision.....	30
7.2.1 Defence in Depth in the Electrical Power System.....	30
7.2.2 Single Failure in the Electrical Power System	31
7.2.3 Common Cause Failure in the Electrical Power System	31
7.2.4 Provisions for coping with Loss Of Off-site Power	37
7.2.5 Provisions for coping with Station Black Out	38
7.2.6 Provisions to avoid or reduce Loss of Electrical Power	38
7.2.7 Classification consideration	38
7.2.8 Provisions to achieve the reliability target for the Electrical Power System	39
7.3 Electrical design provision	40
7.3.1 General	40
7.3.2 Coordination with the grid.....	40
7.3.3 Design to achieve electrical requirements.....	40
7.4 Functional and performance design provisions.....	46
7.4.1 General	46

7.4.2	Electrical Power System studies	46
7.4.3	Design of the Interruptible Power Supply System.....	49
7.4.4	Design of the Uninterruptible Power Supply System	49
7.5	Maintenance	50
7.5.1	Consideration of the maintenance in the electrical design.....	50
7.6	Multi-unit shared electrical power systems	51
7.7	Electrical system layout	51
7.8	Supporting and associated systems for the Electrical Power System	51
7.9	Overall quality assurance programs	52
7.10	Requirements for output documentation	53
7.10.1	General	53
7.10.2	Architecture principles	54
7.10.3	Single line diagrams	55
8	Sub-system requirements	55
8.1	Electrical Power System basis requirements	55
8.1.1	General	55
8.1.2	System Design	56
8.1.3	Single line diagram	56
8.2	Equipment design specification	56
8.3	Equipment requirements	56
8.4	AC Interruptible Electrical Power Supply System	56
8.5	AC/DC Uninterruptible Power Supply System.....	57
8.6	Coordination and interaction with power grid.....	57
8.7	Earthing	57
9	Verification of the architecture of the Electrical Power System.....	57
9.1	General.....	57
9.2	Computerised tools and models verification	57
9.2.1	Electrical Power System verification	57
9.2.2	Layout of electrical power systems and equipment verification	57
9.3	Test requirements.....	58
10	Overall integration and commissioning	59
10.1	General.....	59
10.2	Requirements	59
10.3	Output documentation.....	60
11	Overall operation and maintenance	60
11.1	General.....	60
11.2	Requirements	60
11.3	Output documentation.....	60
12	System quality assurance plan	61
12.1	General.....	61
12.2	System verification plan	61
12.3	System configuration management plan.....	62
12.4	Fault resolution procedures.....	62
Annex A (informative)	Basic safety issues in NPPs	63
A.1	General.....	63
A.2	Plant safety objectives	63
A.3	Plant safety analysis	63
A.3.1	General	63

A.3.2	Analysis of event sequences	64
A.3.3	Assessment of design basis: deterministic/probabilistic methods	64
A.4	Defence in Depth	64
Annex B (informative)	AC Interruptible Electrical Power System	67
B.1	General.....	67
B.2	Electrical design provisions.....	67
B.2.1	Steady state conditions for Electrical Power System	67
B.2.2	Electrical disturbances.....	68
B.3	Design of the Interruptible power system	71
B.3.1	Design of the preferred power supply	71
B.3.2	Design of the off-site power supply	71
B.3.3	Design of on-site preferred power supply	72
B.3.4	Design of the AC interruptible power systems important to safety	72
B.3.5	Design of internal standby sources	72
B.4	Preferred power supply system (from IAEA SSG 34:2016, chapter 6, clauses 6.1 to 6.44)	73
B.4.1	General	73
B.4.2	Operation	73
B.4.3	Grid interface and agreement with grid operator	73
B.4.4	Reliability of the preferred power supply	73
B.4.5	Off-site power supplies	74
B.4.6	Availability	75
B.4.7	Independence of off-site circuits	75
B.4.8	Switchyard.....	76
B.5	Safety power supply system supporting DBC	76
B.5.1	General	76
B.5.2	Design (from IAEA SSG 34:2016, chapter 7, clauses 7.36 to 7.63)	77
B.5.3	Testing (from IAEA SSG 34:2016, chapter 7, clauses 7.64 to 7.67).....	79
B.5.4	Performance criteria (transient and dynamic) (from IAEA SSG 34:2016, chapter 7, clauses 7.68 to 7.70).....	79
B.5.5	Relay protection of standby power sources (from IAEA SSG 34:2016, chapter 7, clauses 7.71 to 7.75).....	79
B.5.6	Support systems for standby AC power sources	80
B.5.7	Fuel for standby AC power sources	80
B.6	Power supply system important to safety supporting DEC	80
B.6.1	General	80
B.6.2	Design (from IAEA SSG 34:2016, chapter 8, clauses 8.1 to 8.18)	81
B.7	Mobile sources connections network.....	82
B.8	Monitoring and switching of buses	82
Annex C (informative)	Earthing	84
Annex D (informative)	Logic diagram followed for the design of the EPS.....	85
Bibliography		86
Figure 1 – Scope of work of this document.....		10
Figure 2 – Architecture of Electrical Power System		12
Figure 3 – Connections between the overall Electrical Power System life cycle and the life cycles of the electrical power sub- systems.....		25
Figure 4 – Typical voltage design bases (IEC 62855).....		43
Table A.1 – Support of the electrical power supply for the defence in depth of the plant		66

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**NUCLEAR POWER PLANTS –
ELECTRICAL POWER SYSTEM –
GENERAL REQUIREMENTS**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 63046 has been prepared by subcommittee 45A: Instrumentation, control and electrical power systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
45A/1348/FDIS	45A/1355/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "<http://webstore.iec.ch>" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

IECNORM.COM : Click to view the full PDF of IEC 63046:2020

INTRODUCTION

a) Technical background, main issues, and organisation of the Standard

The purpose of this standard is to provide the high level specification and requirement to implement a suitable Electrical Power System in a Nuclear Power Plant (NPP).

The electric power system in NPPs supports reactor systems important to safety. It also allows electric energy production providing the transmission grid with active and reactive power and electro-mechanical inertia.

The designers, operators of NPPs (utilities), equipment suppliers, systems evaluators and licensors, may use this document.

b) Situation of the current Standard in the structure of the IEC SC 45A standard series

The entry point of the IEC SC 45A standard series should be summary report introducing the two first level standards for I&C (IEC 61513) and the Electrical Power System (IEC 63046).

This document is the first level IEC SC 45A document tackling the issue of general requirements for Electrical Power System and sub-systems.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of this Standard

It is important to note that this Standard establishes no additional functional requirements for safety systems.

To ensure that the Standard will continue to be relevant in future years, the emphasis has been placed on issues of principle, rather than specific technologies.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level documents of the IEC SC 45A standard series are IEC 61513 and IEC 63046. IEC 61513 provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 63046 provides general requirements for electrical power systems of NPPs; it covers power supply systems including the supply systems of the I&C systems. IEC 61513 and IEC 63046 are to be considered in conjunction and at the same level. IEC 61513 and IEC 63046 structure the IEC SC 45A standard series and shape a complete framework establishing general requirements for instrumentation, control and electrical systems for nuclear power plants.

IEC 61513 and IEC 63046 refer directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation, defence against common cause failure, control room design, electromagnetic compatibility, cybersecurity, software and hardware aspects for programmable digital systems, coordination of safety and security requirements and management of ageing. The standards referenced directly at this second level should be considered together with IEC 61513 and IEC 63046 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 or by IEC 63046 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45 standard series, corresponds to the Technical Reports which are not normative.

The IEC SC 45A standards series consistently implements and details the safety and security principles and basic aspects provided in the relevant IAEA safety standards and in the relevant documents of the IAEA nuclear security series (NSS). In particular this includes the IAEA requirements SSR-2/1, establishing safety requirements related to the design of nuclear power plants (NPPs), the IAEA safety guide SSG-30 dealing with the safety classification of structures, systems and components in NPPs, the IAEA safety guide SSG-39 dealing with the design of instrumentation and control systems for NPPs, the IAEA safety guide SSG-34 dealing with the design of electrical power systems for NPPs and the implementing guide NSS17 for computer security at nuclear facilities. The safety and security terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

IEC 61513 and IEC 63046 have adopted a presentation format similar to the basic safety publication IEC 61508 with an overall life-cycle framework and a system life-cycle framework. Regarding nuclear safety, IEC 61513 and IEC 63046 provide the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector. In this framework IEC 60880, IEC 62138 and IEC 62566 correspond to IEC 61508-3 for the nuclear application sector.

IEC 61513 and IEC 63046 refer to ISO as well as to IAEA GS-R part 2 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

At level 2, regarding nuclear security, IEC 62645 is the entry document for the IEC/SC 45A security standards. It builds upon the valid high level principles and main concepts of the generic security standards, in particular ISO/IEC 27001 and ISO/IEC 27002; it adapts them and completes them to fit the nuclear context and coordinates with the IEC 62443 series. At level 2, IEC 60964 is the entry document for the IEC/SC 45A control rooms standards and IEC 62342 is the entry document for the ageing management standards.

NOTE 1 It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied.

NOTE 2 IEC/SC 45A domain was extended in 2013 to cover electrical systems. In 2014 and 2015 discussions were held in IEC/SC 45A to decide how and where general requirements for the design of electrical systems were to be considered. IEC/SC 45A experts recommended that an independent standard be developed at the same level as IEC 61513 to establish general requirements for electrical systems. Project IEC 63046 was launched to cover this objective. As IEC 63046 is published, from now on this Note 2 of the introduction of IEC/SC 45A standards will not be included in the newly published standards.

NUCLEAR POWER PLANTS – ELECTRICAL POWER SYSTEM – GENERAL REQUIREMENTS

1 Scope

1.1 General

This document:

- provides requirements and recommendations for the overall Electrical Power System. In particular, it covers interruptible and uninterruptible Electrical Power Systems including the systems supplying the I&C systems;
- is consistent and coherent with IEC 61513. Like IEC 61513, this document also highlights the need for complete and precise requirements, derived from the plant safety goals. Those requirements are prerequisites for generating the comprehensive requirements for the overall Electrical Power System architecture, and for the electrical power supply sub-systems;
- has to be considered in conjunction with and at the same level as IEC 61513. These two standards provide a complete framework establishing general requirements for instrumentation, control, and Electrical Power System for Nuclear Power Plants.

This document establishes:

- the high level specification and requirement to implement a suitable Electrical Power System in a NPP that supports reactor systems important to safety. It also enables electrical energy production providing the transmission grid with active and reactive power and electro-mechanical inertia;
- the relationships between:
 - the plant safety requirements and the architecture of the overall Electrical Power System and its sub-systems (see Figure 1) including:
 - a) the contribution to the plant Defence in Depth;
 - b) the independency and redundancy provisions;
 - the electrical requirements and the architecture of the Electrical Power System and its sub-systems;
 - the functional requirements and the architecture of the Electrical Power System and its sub-systems;
 - the requirements associated with the maintenance strategy and the architecture of the Electrical Power System and its sub-systems;
- the design of Electrical power sub-systems (e.g. interruptible and uninterruptible);
- the requirements for supporting systems of Electrical Power System (HVAC, I&C, etc.);
- the Electrical Power System life-cycle framework.

This document does not cover the specification of:

- I&C systems;
- the transmission lines connecting to substations outside the NPP;
- electrical equipment requirements already defined in the industrial IEC standards;
- electrical power for security systems (e.g., fences, surveillance systems, entrance control);

- This document does not consider power production requirements.



Figure 1 – Scope of work of this document

NOTE Figure 1 is based on IAEA SSG34:2016, Figure 3, with adaptation regarding the scope.

This figure provides only an example. Various possible arrangements of buses, loads, generators and interconnections would meet the requirements of SSR-2/1. Furthermore, many elements of the plant system, such as buses that are not important to safety and direct current power systems, are not shown. This figure is intended only to represent the relationship between the elements of the plant power systems that are within the safety classification and the preferred power supply. The elements of the preferred power supply that are not within the bounds of the important to safety power supply are outside the scope of the plant safety classification. The system elements included in the important to safety power supplies will differ according to plant design and the classification methods applied in different States. The classification methods are held by IEC 61226. Some plant designs may not require safety standby power sources. All nuclear power plants are expected to have safety direct current power supplies.

1.2 Application: new and pre-existing plants

This document is applicable to the Electrical Power System of new nuclear power plants and upgrading or back fitting of existing plants.

For existing plants, only a subset of requirements may be applicable and this subset should be identified at the beginning of any project.

1.3 Framework

This document consists of six normative clauses (an overview is provided in Figure 2):

- Clause 6 addresses the identification of requirements;
- Clause 7 addresses the design of the electrical architecture;
- Clause 8 addresses the sub-system requirements;
- Clause 9 addresses the verification;
- Clause 10 addresses the overall integration and commissioning;
- Clause 11 addresses the overall operation and maintenance.

1.4 Interaction with level 2 standards

This document shall permit an electrical designer to establish the list of requirements applicable for the design.

It also provides the different provisions applicable for the different requirements.

These provisions will be applied to the different type of power networks (sub-system):

- interruptible AC power network;
- uninterruptible power network.

Moreover, other transverse level 2 standards will define requirements applicable to electrical architecture definition.

The nuclear standards linked with the safety provisions (such as safety classification, separation, qualification or surveillance testing, etc.) are considered as input data for this document.

6	Architecture of Electrical Power System: Identification of requirements			
6.2 Safety requirements 6.2.1 Defence in Depth 6.2.2 Application of Single Failure Criterion 6.2.3 Management of the Common Cause Failure 6.2.4 Loss Of Off-site Power conditions 6.2.5 Station Black Out conditions 6.2.6 Loss of Electrical power conditions 6.2.7 Application of internal and external Hazards 6.2.8 Nuclear security requirements 6.2.9 Classification requirements 6.2.10 Probabilistic requirements			6.3 Electrical requirements 6.3.1 Requirements coordinated with the electric grid operator 6.3.2 Electrical disturbances	
			6.4 Functional, performance requirements	
			6.5 Maintenance requirements	
7	Overall Architecture of Electrical Power System and structured approach: Design of the electrical architecture			
7.2 Safety design provision 7.2.1 Defence in Depth in the Electrical Power System 7.2.2 SF in the Electrical Power System 7.2.3 CCF in the Electrical Power System 7.2.4 Provisions for coping with LOOP 7.2.5 Provisions for coping with SBO 7.2.6 Provisions to avoid or reduce Loss of Electrical Power 7.2.7 Classification consideration 7.2.7.2 Qualification 7.2.7.3 Surveillance Testing 7.2.8 Provisions to achieve the reliability target for the Electrical Power System			7.3 Electrical design provision 7.3.2 Coordination with the grid 7.3.3 Design to achieve electrical requirements 7.4 Functional and performance design provisions 7.4.2 Electrical Power System studies 7.4.3 Design of the Interruptible Power Supply System 7.4.4 Design of the Uninterruptible Power Supply System 7.5 Maintenance 7.5.1 Consideration of the maintenance in the electrical design	7.6 Multi-unit shared electrical power systems 7.7 Electrical system layout 7.8 Supporting and associated systems for the EPS 7.9 Overall quality assurance programs 7.10 Requirements for output documentation
8	Sub-System requirements			
8.1 Electrical Power System basis requirements			8.4 AC Interruptible Electrical Power Supply System	8.6 Coordination and interaction with the grid
8.2 Equipment design specification			8.5 AC/DC Uninterruptible Power Supply System	8.7 Earthing
8.3 Equipment requirements				
9	Verification of the architecture of the Electrical Power System			
9.2 Computerised tools and models verification			9.3 Test requirements	
10	Overall integration and commissioning			
10.2 Requirements			10.3 Output documentation	
11	Overall operation and maintenance			
11.2 Requirements			11.3 Output documentation	
12	System quality assurance plan			
12.2 System verification plan			12.3 System configuration management plan	12.4 Fault resolution procedures

Figure 2 – Architecture of Electrical Power System

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 60038:2009, *IEC standard voltages*

IEC 60671, *Nuclear power plants – Instrumentation and control systems important to safety – Surveillance testing*

IEC 60709:2018, *Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Separation*

IEC/IEEE 60780-323, *Nuclear facilities – Electrical equipment important safety – Qualification*

IEC 60964:2018, *Nuclear power plants – Control rooms – Design*

IEC/IEEE 60980-344, *Nuclear facilities – Equipment important to safety – Seismic qualification*

IEC 61225, *Nuclear power plants – Instrumentation, control and electrical power systems – Requirements for static uninterruptible DC and AC power supply systems*

IEC 61226:2020, *Nuclear power plants – Instrumentation, control and electrical power systems important to safety – Categorization of functions and classification of systems*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems*

IEC 62671, *Nuclear power plants – Instrumentation and control important to safety – Selection and use of industrial digital devices of limited functionality*

IEC 62808, *Nuclear power plants – Instrumentation and control systems important to safety – Design and qualification of isolation devices*

IEC 62855:2016, *Nuclear power plants – Electrical power systems – Electrical power systems analysis*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

IEC 63272, *Nuclear facilities – Electrical power systems – AC interruptible power supply systems*

ISO 9001:2015, *Quality management systems – Requirements*

IAEA Safety Guide GS-G-3.1:2006, *Application of the management System for facilities and activities*

IAEA GS-R, Part 2:2016, *Leadership and Management for Safety*

IAEA Safety Guide SSG-34:2016, *Design of electrical power systems in Nuclear Power Plants*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <http://www.electropedia.org/>
- ISO Online browsing platform: available at <http://www.iso.org/obp>

NOTE The current terms have been defined based on IAEA and IEC definitions. Some have been slightly modified or adapted to the electrical scope.

3.1

alternate power supply

power source reserved for the use for the power supply to the plant during total loss of all non-battery power in the safety power systems (station blackout) and other design extension conditions

[SOURCE: IAEA SSG-34:2016]

3.2 anticipated operational occurrences

deviation of an operational process from normal operation that is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions

Note 1 to entry: Examples of anticipated operational occurrences are loss of normal electrical power and faults such as a turbine trip, malfunction of individual items of a normally running plant, failure to function of individual items of control equipment, and loss of power to the main coolant pump.

Note 2 to entry: Some States and organizations use the term abnormal operation (for contrast with normal operation) for this concept.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.3

cable route

physical pathway through the plant along which multiple cables can be laid, such as through a room or duct in the plant building, or a metal duct, tray, or tube, or a duct below or gantry over roads

[SOURCE: IEC 60709:2018, 3.3]

3.4

common cause failure

CCF

failure of two or more structures, systems or components due to a single specific event or cause

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.5

component

one of the parts that make up a system

Note 1 to entry: A component may be a hardware component (e.g. transistors, integrated circuits, motors, relays, solenoids, pipes, fittings, pumps, tanks and valves) or a software component (e.g. modules, routines, programmes, software functions).

Note 2 to entry: A component may be made up of other components.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.6

defence-in-depth

hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions

Note 1 to entry: Five levels of defence in depth are discussed in IAEA SSR-2/1:2016:

- a) The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety.
- b) The purpose of the second level of defence is to detect and control deviations from normal operation in order to prevent anticipated operational occurrences from escalating to accident conditions.
- c) The purpose of the third level of defence is to prevent damage to the reactor core and releases of radioactive material requiring off-site protective actions and to return the plant to a safe state by means of inherent and/or engineered safety features, safety systems and procedures.
- d) The purpose of the fourth level of defence is to prevent the progress of, and to mitigate the consequences of, accidents that result from failure of the third level of defence by preventing accident sequences that lead to large radioactive releases or early radioactive releases from occurring.
- e) The purpose of the fifth and final level of defence is to mitigate radiological consequences of a large release or an early release of radioactive material that could potentially result from an accident.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.7

design basis accident

postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits

Note 1 to entry: Design basis condition refer to design basis accident

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.8

design extension conditions

postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions include conditions in events without significant fuel degradation and conditions with core melting

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.9

diversity

presence of two or more independent (redundant) systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure

Note 1 to entry: Examples of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity), and different sizes of equipment, different manufacturers, and types of equipment (which provide diversity of equipment) that use different physical methods (which provide physical diversity).

Note 2 to entry: Functional diversity. Application of diversity at the level of functions in applications in methods (which provide physical diversity). process engineering (e.g. for the actuation of a trip on both a pressure limit and a temperature limit).

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.10

division

collection of items, including their interconnections, that form one redundancy of a redundant system or safety group. Divisions may include multiple channels

Note 1 to entry: In the context of this document, “division” includes a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

[SOURCE: IAEA SSG-39, 2016]

3.11

electrical isolation

electrical isolation is used to prevent electrical failures in one system from affecting connected systems. Electrical isolation controls or prevents adverse interactions between equipment and components caused by factors such as electromagnetic interference, electrostatic pickup, short circuits, open circuits, earthing, or application of the maximum credible voltage (AC or DC)

[SOURCE: IAEA SSG-34:2016 and SSG-39: 2016]

3.12

Electrical Power System

EPS

system performing electrical power generation, transmission and distribution; performing supply functions to operate plant equipment (pumps, valves, heaters, etc.) and to I&C systems

Note 1 to entry: The Electrical Power System is composed by several electrical power sub-systems.

Note 2 to entry: An electrical system can integrate E/E/PE items to perform its internal electrical control and protection.

3.13

electrical power sub-system

two main sub-systems are defined (each of them covering the different level of Defence in Depth):

- interruptible power supply system;
- uninterruptible power supply system.

each sub-system covers the following levels:

- power supply system not important to safety;
- power supply system important to safety:
 - safety power supply system supporting DBC;
 - power supply system supporting DEC.

3.14

Electrical Power System life cycle

necessary activities involved in the implementation of an Electrical Power System occurring during a period of time that starts at a concept phase with the system requirements specification and finishes when the Electrical Power System is no longer available for use

3.15

electrical source transfer

transfer from an initial electrical power source to an alternative supply source (automatically or manually) when the initial electrical power source does not provide the performance required by the Electrical Power System

Note 1 to entry: A bus transfer or the transfer to standby AC power source are electrical source transfers.

3.16

equipment

assembly of components designed and manufactured to perform specific functions

Note 1 to entry: Sensors, cables, electrically operated valves, I&C cabinet or racks are examples of equipment.

[SOURCE: IEEE Standards Dictionary Online]

3.17

frontline system

system composed of mechanical equipment (pumps, valves, heaters, etc.) that directly acts on the plant process to perform a function

3.18

house load operation

operation of a nuclear power plant to supply power only to its own electrical loads

[SOURCE: IEC 62855:2016, 3.2]

3.19

human factors engineering

engineering in which factors that could influence human performance and that could affect safety are understood and are taken into account, especially in the design and operation of facilities

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.20

I&C system

system, based on electrical and/or electronic and/or programmable electronic technology, performing I&C functions as well as service and monitoring functions related to the operation of the system itself

Note 1 to entry: The term is used as a general term that encompasses all elements of the system such as internal power supplies, sensors, and other input devices, data highways and other communication paths, interfaces to actuators and other output devices (see Note 2). The different functions within a system may use dedicated or shared resources.

Note 2 to entry: The elements included in a specific I&C system are defined in the specification of the boundaries of the system.

Note 3 to entry: According to their typical functionality, IAEA distinguishes between automation / control systems, HMI systems, interlock systems and protection systems (see Clause B.4).

[SOURCE: IEC 61513:2011, 3.29]

3.21

independence

condition that exists when successful completion of a system's required functions is not dependent upon any behaviour including failures and normal operation of another system, or upon any signals, data, or information derived from the other system

Note 1 to entry: The following definition is to be found in the IAEA Safety Glossary edition 2016 for "independent equipment": "Equipment that possesses both the following characteristics: a) The ability to perform its required function is unaffected by the operation or failure of other equipment; b) The ability to perform its required function is unaffected by the occurrence of the effects resulting from the initiating event for which it is required to function..". This IAEA definition is limited to equipment but is consistent with the definition given in this document.

Note 2 to entry: For the Electrical Power System, independence can be required between divisions or between different level of Defence in Depth (LoDiD).

[SOURCE: IEC 60709:2018, 3.13]

3.22

interruptible power supply system

power supply of loads for which a defined power supply interruption time does not impair the mission of the safety objective

3.23

item important to safety

item that is part of a safety group and/or whose malfunction or failure could lead to radiation exposure of the site personnel or members of the public

Note 1 to entry: Items important to safety include:

- a) those structures, systems and components whose malfunction or failure could lead to undue radiation exposure of the site personnel or members of the public.
- b) those structures, systems and components that prevent anticipated operational occurrences from leading to accident conditions.
- c) Safety features (for design extension conditions).
- d) those features which are provided to mitigate the consequences of malfunction or failure of structures, systems or components.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.24

loss of electrical power

plant condition corresponding to a Station Black-Out Condition and also the loss of alternate AC power supplies

Note 1 to entry: DC power supplies and uninterruptible AC power supplies may be available as long as batteries can supply the loads.

3.25

loss of off-site power

simultaneous loss of electrical power to all unit safety buses, requiring the standby AC power sources to start and supply power to the safety buses

Note 1 to entry: DC systems and uninterruptible AC systems safety buses are not included.

[SOURCE: IEC 62855:2016, 3.4]

3.26

mission time

operational period required for electrical loads or sources after the initiation of accidental conditions during which equipment shall be capable of operating within the limits of its acceptability criteria for the specified operating conditions

3.27

nuclear security

the prevention and detection of, and response to, criminal or intentional unauthorized acts involving nuclear material, other radioactive material, associated facilities or associated activities or the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive material or their associated facilities

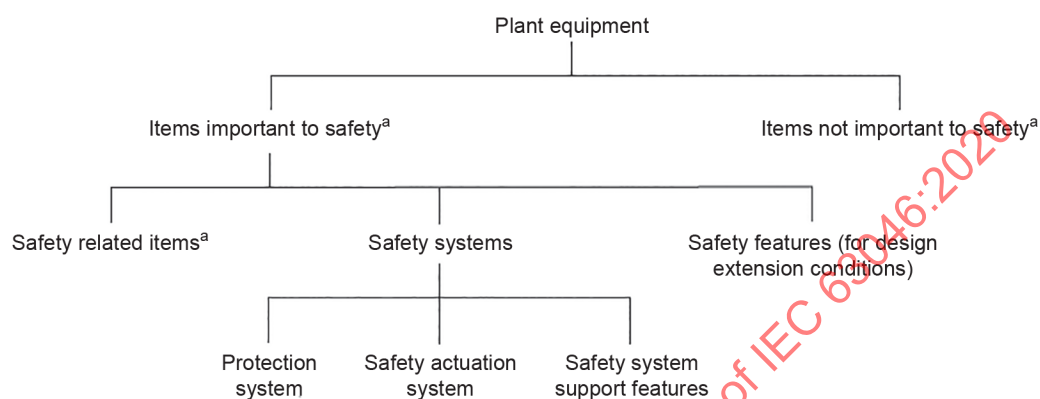
[SOURCE: IAEA Safety Glossary, 2018 edition]

3.28 performance

effectiveness with which an intended function is carried out (e.g; time response, accuracy, sensitivity to parameter changes)

[SOURCE: IEC 61226:2020, 3.16]

3.29 plant equipment

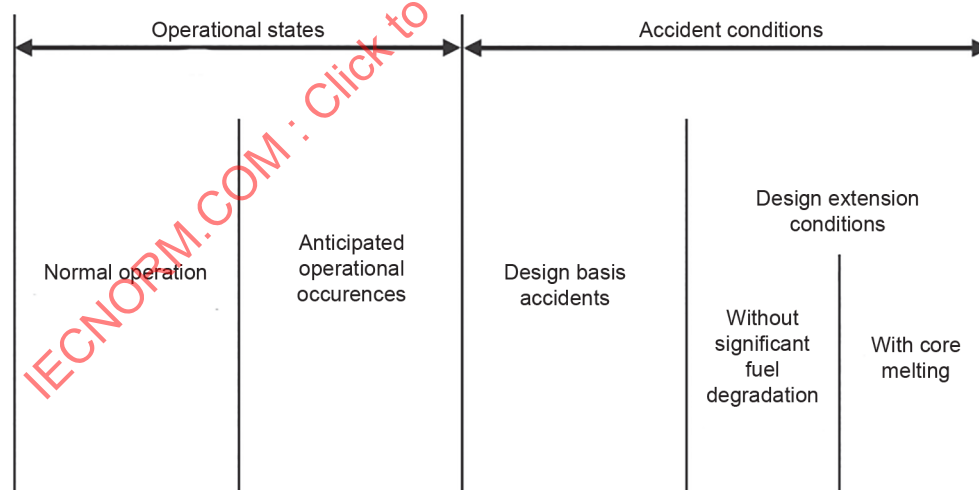


^a In this context, an 'item' is a structure, system or component.

IEC

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.30 plant states



IEC

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.31 power balance

steady state active and reactive power required by the Electrical Power System

3.32 preferred power supply.

power supply from the transmission system to the safety classified electrical power system

Note 1 to entry: Some portions of the preferred power supply are not part of the safety classification.

Note 2 to entry: In the standard context, the transmission system is out of scope. The limits of PPS are the switchyard that connects the NPP to the grid.

[SOURCE: IAEA SSG 34, 2016]

3.33 probabilistic safety assessment

PSA

comprehensive, structured approach to identifying failure scenarios, constituting a conceptual and mathematical tool for deriving numerical estimates of risk

Note 1 to entry: Three levels of probabilistic safety assessment are generally recognized.

Level 1 comprises the assessment of failures leading to determination of the frequency of core damage.

Level 2 includes the assessment of containment response, leading, together with Level 1 results, to the determination of frequencies of failure of the containment and release to the environment of a given percentage of the reactor core's inventory of radionuclides.

Level 3 includes the assessment of off-site consequences, leading, together with the results of Level 2 analysis, to estimates of public risks.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.34 quality

degree to which a set of inherent characteristics of an object fulfils requirements

[SOURCE: ISO 9000:2015, 3.6.2]

3.35 quality assurance

part of quality management focused on providing confidence that quality requirements will be fulfilled

[SOURCE: ISO 9000:2015, 3.3.6]

3.36 quality management

management with regard to quality

[SOURCE: ISO 9000:2015, 3.3.4]

3.37 redundancy

provision of alternative (identical or diverse) structures, systems and components, so that any single structure, system or component can perform the required function regardless of the state of operation or failure of any other

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.38 restoration time

maximum time required by an electrical equipment belonging to a system to be re-supplied by an electrical power source

3.39 robustness of the Electrical Power System

ability of the Electrical Power System to perform its safety missions withstanding failures and /or electrical disturbances

3.40**safety assessment**

assessment of all aspects of facilities and activities that are relevant to protection and safety; for an authorized facility, this includes siting, design and operation of the facility

analysis to predict the performance of an overall system and its impact, where the performance measure is the radiological impact or some other global measure of the impact on safety

the systematic process that is carried out throughout the design process (and throughout the lifetime of the facility or the activity) to ensure that all the relevant safety requirements are met by the proposed (or actual) design

Note 1 to entry: In the context of the design of the Electrical Power System, it is an analysis which provide for all type of conditions, the loads required.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.41**safety case**

collection of arguments and evidence in support of the safety of a facility or activity

Note 1 to entry: This will normally include the findings of a safety assessment and a statement of confidence in these findings.

Note 2 to entry: For a disposal facility, the safety case may relate to a given stage of development. In such cases, the safety case should acknowledge the existence of any unresolved issues and should provide guidance for work to resolve these issues in future development stages.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.42**safety classification**

for nuclear power plants, the assignment to a limited number of safety classes of systems and components and other items of equipment on the basis of their functions and their safety significance

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.43**safety group**

assembly of equipment designated to perform all actions required for a particular initiating event to ensure that the limits specified in the design basis for anticipated operational occurrences and design basis accidents are not exceeded

Note 1 to entry: The IEEE 308-2001 note clarifies: A safety group may include one or more divisions. In a design where each division can accomplish a safety function, each division is a safety group. However, a design consisting of three 50 % capacity systems separated into three divisions would have three safety groups; any two out of three divisions are required to be operating to accomplish the safety function.

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.44**safety related system**

system important to safety that is not part of a safety system

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.45

safety system

system important to safety, provided to ensure the safe shutdown of the reactor or residual heat removal from the reactor core, or to limit the consequences of anticipated operational occurrences and design basis accidents

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.46

single failure

failure which results in the loss of capability of a single system or component to perform its intended safety function(s), and any consequential failure(s) which result from it

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.47

single failure criterion

criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure

[SOURCE: IAEA Safety Glossary, 2018 edition]

3.48

standby AC power source

power source, capable of supplying the necessary power in anticipated operational occurrences and accident conditions, in the event of the loss of off-site power and main generator

3.49

station blackout

plant condition with complete loss of all AC power from off-site sources, from the main generator and from safety classified standby AC power sources to the essential and nonessential switchgear buses

[SOURCE: IAEA SSG-34:2016]

3.50

system disturbance

electrical disturbance

unplanned sudden change in electric power system operating condition that causes widespread power quality problems or interruptions

Note 1 to entry: In this document the term “electrical disturbance” is used.

Note 2 to entry: A system disturbance can be initiated by a fault in the transmission system, a trip of a generation unit, loss of load, or any combination thereof. System disturbance can lead to abnormal ranges of frequency or voltage, loss of power system stability or cascading outages of power transmission circuits and as well widespread interruption of customer load.

Note 3 to entry: The electrical disturbances can also generate electromagnetic disturbances that may affect the Electrical power systems.

[SOURCE: IEC 60050-692:2017,692-1-10]

3.51

transmission system operator

party responsible for providing and operating networks for long distance transmission of electricity as well as regional distribution and responsible to ensure the system security with a high level of reliability and quality

3.52**uninterruptible power supply system**

power supply for loads required to ensure functional availability during the unavailability of the interruptible power supply

Note 1 to entry: Specific loads requiring high voltage stability can also be supplied power by the uninterruptible power supply system.

Note 2 to entry: Typical loads of the uninterruptible power supply systems are: isolation valves, dampers, I&C and monitoring systems.

4 Abbreviated terms

NOTE Elaborated based on IAEA and IEC and electrical power systems symbols and abbreviations and adapted to the electrical scope.

AC	alternating current
BIL	basic insulation level
CCF	common cause failure
CDF	core damage frequency
CM	configuration management
DBA	design basis accident
DBC	design basis conditions
DBE	design basis event
DC	direct current
DEC	design extension conditions
DiD	defense in depth
DSO	distribution system operator
E/E/PES	electrical/electronic/programmable electronic system
EMI	electromagnetic interference
EMIT	examination maintenance in-service inspection and surveillance testing
EPS	Electrical Power System
EQ	environmental qualification
ETS	equipment technical specification
HMI	human machine interface
HV	high voltage
HVAC	heating ventilation and air conditioning system
I&C	instrumentation and control
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Group
I/O	input/output
LEP	loss of electrical power
LoDiD	level of defence in depth
LOOP	loss of offsite power
LV	low voltage
NPP	nuclear power plant
PIE	postulated initiating events
PPS	preferred power supply
PSA	probabilistic safety assessment

QA	quality assurance
SBO	station black out
SF	single failure
SFC	single failure criterion
SSC	structure, system and component
SLD	single line diagram
SSG	specific safety guide
SSR	specific safety requirement
TSO	transmission system operator
UPS	uninterruptible power supply

5 Overall Electrical Power System life cycle

The phases of a typical overall Electrical Power System life cycle include:

- a) review of the requirement applicable to the Electrical Power System (see Clause 6):
 - safety requirements applicable (see 6.2);
 - electrical requirements (see 6.3);
 - functional, performance requirements (see 6.4);
 - maintenance requirements (see 6.5);
- b) design of the electrical architecture (see Clause 7):
 - safety design provisions (see 7.2);
 - electrical design provisions (see 7.3);
 - functional and performance design provisions (see 7.4);
 - maintenance provisions (see 7.5);
- c) electrical sub-systems requirements (see Clause 8);
- d) verification of the architecture of the Electrical Power System (see Clause 9);
- e) overall integration and commissioning of the systems (see Clause 10);
- f) overall operation and maintenance (see Clause 11).

The connections between this life cycle and the life cycles of the electrical sub-systems are shown in simplified form in Figure 3.

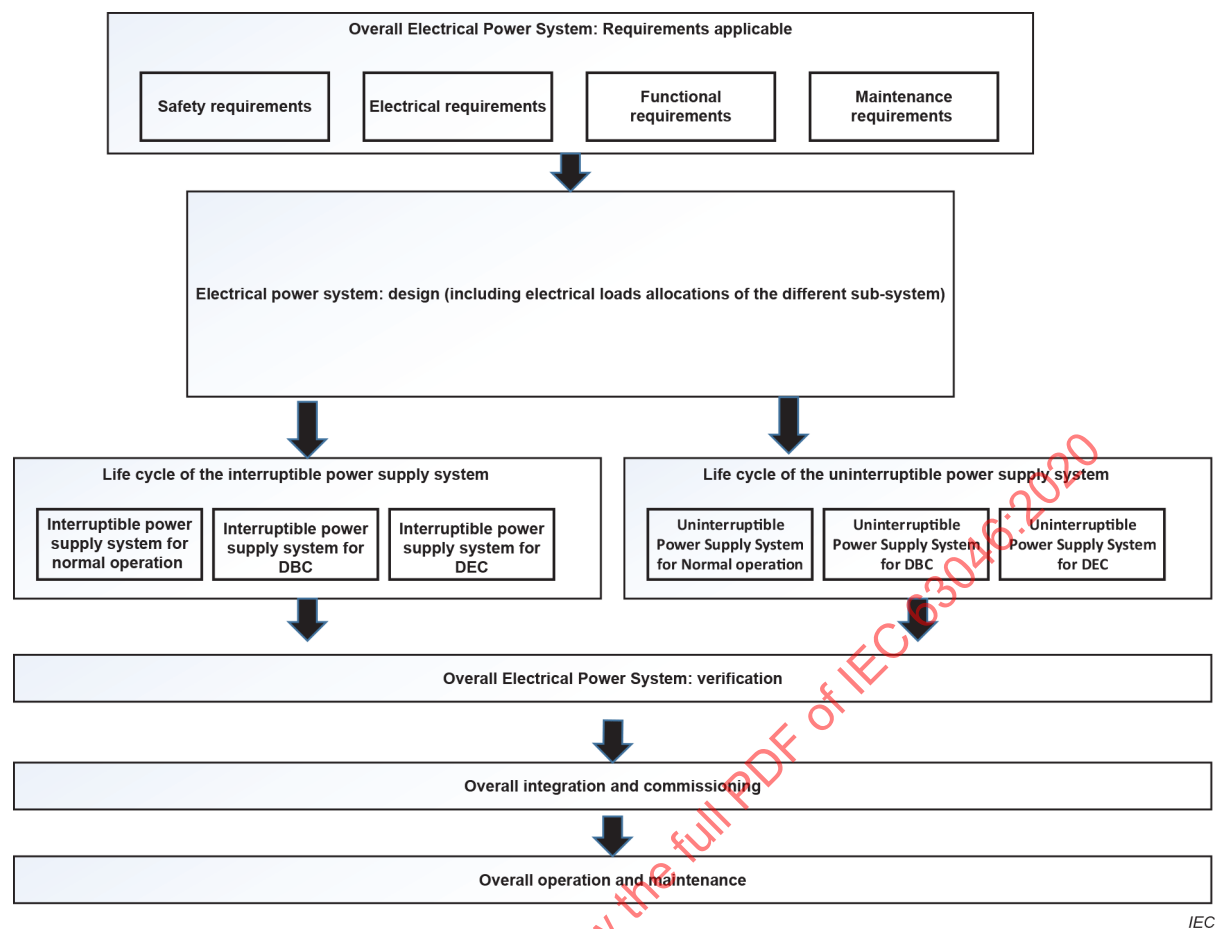


Figure 3 – Connections between the overall Electrical Power System life cycle and the life cycles of the electrical power sub- systems

6 Architecture of Electrical Power System: identification of requirements

6.1 Objectives

The objective of this clause is to define the requirements applicable to the design of the Electrical Power System.

The Electrical Power System architecture shall:

- comply with the safety requirements applicable to the NPP such as:
 - provision of a Defence in Depth approach consistent with that of supported systems and their importance to safety in accordance with the plant design basis;
 - application of Single Failure Criterion;
 - management of Common Cause Failure;
 - Loss Of Off-site Power conditions;
 - Station Black Out conditions;
 - Loss of Electrical Power conditions;
 - robustness against Internal and External Hazards;
 - categorisation and classification requirements;
 - reliability requirements for probabilistic safety assessment.

- comply with the electrical requirements applicable to the NPP such as:
 - requirements coordinated with the electric grid operator;
 - robustness of the Electrical Power System against electrical disturbances.
- comply with the functional requirements applicable to the Electrical Power System (as a support system);
- comply with the requirements associated with maintenance strategy;
- support the full lifecycle of the nuclear power plant (commissioning, operation, and decommissioning).

The safety requirements and their application to the supporting Electrical Power System shall be broken down and derived within the electrical power architecture, electrical power sub-systems and equipment requirements.

NOTE It is assumed that for the design of the Electrical Power System in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standard for conventional electrical equipment would be applied.

The combination of applicable requirements for safety and maintenance strategy should be established as an input data.

6.2 Safety requirements applicable to the electrical architecture design

6.2.1 Defence in Depth

The electrical design process should develop the Defence in Depth concept in accordance with the plant safety design basis.

The strategy regarding implementation of the different LoDiD in the project should be specified as an input data to clarify the following:

- levels of Defence in Depth for each operating condition;
- boundaries between the levels of Defence in Depth;
- requirements for independence between these levels.

6.2.2 Application of Single Failure Criterion

The single failure criterion shall be applied to a system such that it shall be capable of performing its defined task in the presence of any single failure.

Applicability of the single failure criterion shall be specified for each LoDiD as an input data from the safety assessment for the electrical design.

NOTE Usually SF criteria is applicable at DBC level.

6.2.3 Management of the Common Cause Failure

In the design of the Electrical Power System the robustness against common cause failures shall be assessed to meet the safety requirements of the supported functions.

The robustness requirements for the system should be established and substantiated based on relevant reliability data derived either from plant, or a set of plant, national and international databases.

6.2.4 Loss Of Off-site Power conditions

The Electrical Power System shall be designed so as to reduce the risk of loss of off-site power during design basis conditions in all specified plant operating states and conditions.

Adequate provisions shall be included in the design to prevent any fuel damage during a Loss Of Off-site Power condition in order to maintain the electrical power supply system's ability to support plant safety functions.

6.2.5 Station Black Out conditions

The Electrical Power System shall be designed so as to reduce the risk of station black out conditions during design extension conditions in all specified plant operating states and conditions.

Adequate provisions shall be included in the design to prevent any fuel damage during station blackout conditions in order to maintain the plant's ability to support safety functions and remove decay heat during design extension conditions.

6.2.6 Loss of Electrical Power conditions

The Electrical Power System shall be designed to reduce the risk of loss of electrical power during design basis conditions and design extension conditions in all specified plant operating states.

A LEP condition is a plant condition corresponding to a Station Black-Out Condition and the loss of alternate AC power supplies.

Robustness against a LEP condition shall be specified as an input data for the electrical design.

6.2.7 Application of internal and external Hazards

6.2.7.1 General

The Electrical Power System important to safety shall be robust against hazards applicable to the NPP.

The following minimum list of hazards should be considered:

6.2.7.2 External hazards

- earthquake;
- external flooding;
- climatic conditions;
- lightning;
- EMI (external sources);
- missiles;
- airplane crash;
- industrial environment (such as industrial plant near the NPP site generating an hazard risk for the NPP).

The assessment for each hazard shall consider:

- design basis conditions,
- design extension conditions,
- site specific requirements.

NOTE Example of climatic conditions: low and high temperature (air temperature and heat sink), snow, high wind, ice storm.

6.2.7.3 Internal hazards:

- water hazards from direct and indirect sources, such as spray and seepage through roofs, walls, raceways and conduits;
- fire;
- missiles;
- steam jets;
- pipe whip;
- chemical explosions;
- flooding;
- failure of adjacent equipment;
- EMI (internal sources).

Hazards and combination rules between hazards to be considered shall be identified as input data for the electrical design.

6.2.8 Nuclear security requirements

The design of Electrical Power System shall consider the applicable nuclear security (physical plant protection) requirements.

These requirements shall be identified as input data for the electrical design.

6.2.9 Classification requirements

IEC 61226 defines a method of assignment of the plant specified functions into categories according to their importance to safety.

Subsequent classification of the I&C and electrical power systems performing or supporting these functions, based on the assigned category, then determines relevant design criteria.

The safety class of the electrical power sub-system part following the LoDiD shall not be lower than the safety class of the systems supplied by the Electrical Power System.

6.2.10 Probabilistic requirements

PSA targets shall be identified as input data for electrical design.

6.3 Electrical requirements

6.3.1 Requirements coordinated with the electric grid operator

The electric grid operator can be the TSO (Transmission System Operator) or the DSO (Distribution System Operator) dependent upon the voltage of the connection to the grid.

The following input data should be considered for the grid connections as defined by the electric grid operator:

- grid voltage and frequency span;
- the minimum and maximum short circuit capacity of the Grid at the connection point;
- the reliability of the grid;
- fault ride through requirements;
- frequency response requirements;
- requirements for trip to house load (if applicable).

- the design of the EPS should also consider the specific requirement of the electric grid operator (associated with the energy production).

6.3.2 Electrical disturbances

Electrical disturbances can generate variations from the rated operating values defined for the three main electrical quantities:

- voltage (U);
- current (I);
- frequency (f).

The electrical disturbances can originate from:

- the electrical installation itself;
- human actions;
- natural events.

Symmetrical and asymmetrical disturbances can affect the plant. These events can be initiated:

- in the transmission system or as a consequence of the plant separating from the grid owing to anticipated faults or voltage and frequency variations beyond the defined acceptable levels;
- by the tripping of the main generator, leaving the on-site power systems only connected to either the off-site power systems or the on-site standby power systems;
- in the on-site power systems, as a result of an electrical event such as a motor starting, a short circuit fault or switching surges.

NOTE Examples of electrical disturbances can be found in IEC 62855.

An electrical disturbance can initiate a common cause failure of the entire Electrical Power System due to the electrical common point: the grid connection on one side and the main generator on the other side.

The robustness of the Electrical Power System against CCF inducing SBO and LEP conditions should be supported by effective protection against electrical disturbances.

The effects of electrical disturbances and potential protection measures should be analysed in accordance with IEC 62855 and appropriate protection measures implemented.

6.4 Functional performance requirements

As a support system, the Electrical Power System supplies front line systems or other support systems of the plant (such as HVAC or I&C) depending on the requirements of the supported systems.

The electrical design process requires the following inputs from the supported systems designers:

- the load list and associated electrical data required to perform the functions not important to safety and important to safety, during operation, DBC and DEC;
- the type of power supplies required per load (interruptible or non-interruptible);
- functional and performance requirements of functions important to the safety required to meet the general plant safety requirements;
- the mission time and maximum restoration time for loads in case of supply from on-site power supply (AC or DC);

- the design basis environmental conditions.

6.5 Maintenance requirements

Plant maintenance has two main objectives:

- maintaining equipment important to safety to support plant safety and functional requirements;
- meeting power production targets (out of the scope of this document).

The impact of plant maintenance should be considered in the design of the electrical architecture.

The maintenance strategy shall be used to specify the maintenance requirements. These should be derived from the Plant Design Bases, operational and safety requirements.

7 Design of the electrical architecture

7.1 Objectives

The designer should consider the following plant requirements in the design of the Electrical Power System architecture:

- provisions to achieve nuclear safety requirements;
- provisions to achieve the electrical performance requirements;
- provisions to achieve the functional requirements;
- provisions to achieve the maintenance requirements.

7.2 Safety design provision

7.2.1 Defence in Depth in the Electrical Power System

The Electrical Power System shall follow a Defence in Depth approach consistent with that of the supported systems.

To provide robustness against identified electrical events (such as LOOP or SBO conditions), the Electrical Power System shall include:

- a comprehensive electrical design of the Electrical Power System and its sub-systems following the LoDiD approach, taking account of:
 - inherent characteristics;
 - use of measure(s) with one or several levels of defence in case of electrical faults (electrical protection system).
- power sources associated to the different LoDiD for supplying the frontline equipment and support systems.
- Following SSG34, generally 3 electrical supplies are identified:
 - preferred power supply (covering LoDiD 1&2);
 - safety power supply (covering LoDiD 3);
 - alternate power supply (covering LoDiD 4);
- The requirement to integrate each power source in the EPS design shall be justified through the performance design provisions (refer to 7.2.5).

The safety power system supporting DBC functions shall be supplied by the preferred power supplies backed up by the standby power sources.

The power system supporting DEC functions should be supplied by the safety power system supporting the DBC or by an alternate power supply in design extension conditions.

The preferred power supplies shall be the normal power supplies for all plant systems important to safety. They shall always be the first choice of power supply to the electrical safety power systems.

In order to meet plant safety claims regarding resilience to extended unavailability of power sources, the provision of mobile power sources or additional power supplies should be considered.

An example of design bases considerations for electrical power systems is provided in informative Annex A.

NOTE Specific backed-up systems only designed for protection of equipment not important to safety are not part of this description.

7.2.2 Single Failure in the Electrical Power System

The provision of redundancy in the Electrical Power System design is the principal factor in meeting the single failure criterion.

The provision of redundancy in the Electrical Power System design should support robustness in relation to the single failure criterion and improve the system reliability.

The design concept of the safety systems and the supporting Electrical Power System shall be consistent so that the redundancy provisions of the electrical power generation and distribution systems correspond to those of the supplied systems.

All exceptions to the SFC shall be justified in the safety analysis.

7.2.3 Common Cause Failure in the Electrical Power System

7.2.3.1 Types of CCF

7.2.3.1.1 General

The possibility of common cause failures, which could render the safety power systems unavailable to perform their safety functions on demand, shall be considered in the design, maintenance, testing and operation of the safety power systems and their support systems.

Several sources of CCF potentially affect the Electrical Power System:

- CCF arising from internal or external hazards;
- CCF arising from internal or external electrical disturbances;
- CCF of electrical equipment and components;
- CCF caused by software errors in programmable digital items;
- CCF caused by human factors (including operation and maintenance activities).

7.2.3.1.2 CCF resulting from internal or external hazards

The following provisions shall be considered to protect against internal and external hazards:

- inherent design characteristics of the equipment (e.g. Basic Insulation Level for equipment relating to design basis lightning hazard);
- Electrical isolations (e.g. surge arresters);
- Physical separation (e.g. fire hazard).

7.2.3.1.3 CCF induced from electrical disturbances

Electrical disturbances can initiate a common cause failure on the entire Electrical Power System due to their electrical common point, the grid on one side and the main generator on the other side.

The provisions to protect against this type of CCF should include:

- inherent design characteristics of the equipment (e.g. the short circuit capacity for electrical equipment);
- a well-designed protection system
- physical separation and electrical isolations.

7.2.3.1.4 CCF on electrical equipment and components

The provisions to protect against this type of CCF should include:

- diversity (at functional or equipment level).

The electrical CCF analysis should evaluate the potential common cause failures of the equipment composing the EPS.

Particular attention should be paid on the following equipment:

- on-site AC sources (e.g. diesel generator sets, combustion gas turbine sets);
- uninterruptible power systems including:
- batteries;
- rectifiers, inverters, converters.

The protection provisions against CCF should be justified through reliability data and CCF analyses.

7.2.3.1.5 CCF caused by software errors in programmable digital items or cyber-attacks in programmable digital items in the Electrical Power System

With the use of programmable digital items embedded in components of the Electrical Power System, the vulnerability to common cause failures and cyber attacks associated shall be evaluated to protect against a CCF condition on the Electrical Power System.

The provisions applicable are the use of dedicated standards such as IEC 62671 for programmable digital items to minimise the risk of this kind of CCF.

The sensitivity to cyber-attacks of systems containing programmable digital items should be considered (following IEC 62859).

7.2.3.1.6 CCF caused by human factors

The provisions to protect against this type of CCF should include:

- choices in the design of HMI interfaces;
- physical separation.

NOTE Different personnel could also bring robustness against this kind of CCF (administration procedure).

Concurrent activities (such as tests or maintenance) on redundant equipment which can generate a CCF condition shall not be performed in the same time frame.

Assessment of the operability of equipment can lessen the risk of CCF due to human factors.

A human factors analysis of the Electrical Power System should be performed in order to identify activities or operations which can initiate a CCF.

7.2.3.2 Provisions against Common Cause Failure

7.2.3.2.1 General

Independence provides defence against a single event, internal hazards, external hazards or electrical disturbances from affecting redundant safety systems.

It also provides defence against a single event or hazard or disturbance from affecting systems that provide different levels of Defence in Depth.

Consideration of failure processes should include:

- failures resulting from design basis events;
- common internal or external hazards or electrical disturbances;
- failure of support systems;
- common errors in design, manufacture, operations or maintenance;
- CCF induced by:
 - electrical connections between systems in different divisions or LoDiD;
 - data exchange between systems in different divisions or LoDiD;

Redundant portions of safety groups shall be independent of one another to ensure that the safety group can perform its safety functions during and following any event.

Independence requirements between redundant or diverse part of circuits contributing to the same safety function shall be derived from the frontline supported safety feature.

The provision of physical separation, diversity and/or electrical isolation should support meeting independence requirements.

The benefit of using several diversified support systems (steam, compressed air, etc.) instead of a common electrical support system should be considered.

7.2.3.2.2 Physical separation

The requirements for physical separation of circuits and equipment shall be met by the use of distance, barriers, or any combination.

The level 2 standard IEC 60709 defines methods and provisions to achieve separation.

In the framework of the application of single failure criterion, segregation shall be applied to reduce the risk of common cause failure of redundant parts of a system and its essential support systems against hazards like fire, flooding, explosion, such that a single failure and its consequences do not lead to the failure of more than one redundant provision.

7.2.3.2.3 Diversity within electrical power systems and equipment

The application of diversity to the design reduces the possibilities of common cause failures of redundant systems due to common cause failure at system or equipment level.

If required following a CCF analysis, the electrical power systems shall be diversified in accordance with the requirements of the supported safety feature.

Diversity should be implemented during the design, manufacturing, operation configuration, and maintenance phase or combinations of them.

Human diversity (different personnel) should also be taken into account in the design and operation of the Electrical Power System.

The following approaches to diversity should be considered:

a) Functional diversity:

- diversity based on the physical principles of the implementation of the design, technology or functions.

b) Material (or physical) diversity:

- diversity between the systems that fulfil the same function (use of a diversified, dedicated and independent system or of an existing system), e.g.: the preferred power supply should be diverse from the stand-by on site power supply.
- diversity between the redundant equipment or components within the same system (diversity integrated into the system), for example: use of different battery technologies.
- diversity between equipment manufacturers or batches.

The adequacy of the diversity provisions should be established and substantiated based on relevant reliability data derived from either the plant database, or a series of plant, national or international databases.

The implementation of diversity can add to the complexity of the Electrical Power System and can increase the risk for errors in operation and maintenance. Diversity provision should be based on the requirements identified by comprehensive analysis.

Where the design basis requires diversity for programmable digital items of an Electrical Power System, the implementation should be based on the requirements of 7.2.3.3.3.

In order to use diversity between equipment manufacturers, the diverse equipment should not have common components which can initiate a CCF.

7.2.3.2.4 Electrical isolation

Electrical isolation facilities shall be provided to reduce the risk of electrical failures in one system from affecting connected systems. Electrical isolation controls should reduce adverse interactions between equipment and components caused by factors such as electromagnetic interference, electrostatic pickup, short circuits, open circuits, earthing or overvoltage conditions.

Electrical isolation shall be achieved by the use of isolation devices, shielding and wiring techniques, or combinations of these.

Electrical isolation implemented between systems important to safety shall follow the requirements of IEC 60709.

When interfaces exist between electrical components of higher and lower class, the component at the interface shall be designed to prevent a failure or the consequences of degraded conditions from propagating from a lower safety classified component to higher safety classified components. This component shall be classified in accordance with the highest safety class of the interconnected equipment.

Isolation devices for very low voltage systems shall be designed according to IEC 62808. Typical isolation devices are: amplifiers, control switches, current transformers, fibre or photo optic couplers, relays, transducers, circuit breakers, fuses.

Isolation devices for electrical power loads shall be designed according to IEC industry standards. Typical isolation devices are circuit breakers and fuses associated with or without contactors or switches.

7.2.3.3 Management of the Common Cause Failure requirements for the Electrical Power System

7.2.3.3.1 General

The design process for the Electrical Power System shall include a CCF analysis.

7.2.3.3.2 Independence implementation for the Electrical Power System

7.2.3.3.2.1 General

The adequacy of design features to provide independence should be substantiated.

7.2.3.3.2.2 Independence between LoDiD

The interruptible power supply system important to safety shall have provisions to be supplied from different electrical power sources following the LoDiD approach.

If non-electrical systems provide diverse mean for accomplishing a given function important to safety, their associated power supplies and instrumentation and control systems shall be independent of the power supplies and instrumentation and control systems from which they are designed to be diverse.

The alternate standby source of the power system important to safety supporting DEC shall be independent from the standby source of the safety power system supporting DBC.

The Electrical Power Supply important to safety supporting DEC should be independent from the safety Power Supply supporting DBC.

Additionally, if the alternate power supply comprises several sources each with a dedicated function (e.g. avoid core melt and manage severe accident), each power supply supporting the dedicated DEC function shall be functionally independent from the safety power system supporting DBC and from other power supplies supporting DEC.

The potential for misalignment, human errors or configuration error (local or remote) between the different LoDiD especially between sources should be avoided except for some specific maintenance or surveillance testing configurations. All exceptions from this requirement shall be substantiated.

Electrical power sources of different LoDiD shall not be operated in parallel at the same switchboard level except for periodic test supported by safety analysis.

7.2.3.3.2.3 Independence between divisions

Failure of one redundant electrical power division shall not render other redundant electrical power divisions inoperable.

The safety on-site power supply of a given division shall supply that division only. All special case exceptions shall be substantiated.

Electrical systems belonging to one division should be supplied with power from that division. All exceptions from this requirement shall be substantiated by analysis.

Sub-systems of the process equipment (as pump, motorised valve and controller for the same process system) should be fed from the same electrical power division.

A single failure in the monitoring of the power supply shall not result in the monitoring of an entire division being inoperable.

Safety-classified equipment in different divisions shall be electrically isolated.

Independent protection devices shall be provided between divisions.

Redundant divisions of the safety Electrical Power System shall not be interconnected except for temporary maintenance operation.

It shall not be possible for an electrical fault to be transmitted between divisions.

7.2.3.3.2.4 Independence between classification levels

The interface between the systems important to safety and systems of lower safety classification shall be designed to ensure that there is no adverse impact on equipment important to safety from equipment with a lower safety classification resulting from disturbances in the plant electrical power systems.

Systems important to safety shall be independent from systems of lower safety classification to ensure that the systems important to safety can perform their safety functions during and following any event requiring performance of these functions.

As far as practicable, loads not important to safety should not be supplied from electrical power systems important to safety.

If it is necessary to power loads not important to safety from electrical power systems important to safety, the loads not important to safety shall be provided with safety classified isolation devices with same safety class than the supporting electrical power system.

When it is impractical to provide adequate separation and isolation from electrical faults between a safety classified circuit and a circuit of a lower safety classified function, the lower safety classified circuit (associated circuit) shall be:

- analysed or tested to demonstrate that the associated safety class circuit will not be unacceptably degraded;
- identified as part of the associated safety division;
- electrically isolated from other components in the same manner as the circuits of the associated safety division.

Loads not important to safety which could affect the ability of the Electrical Power System important to safety to operate should be automatically disconnected during an electrical source transfer.

7.2.3.3.3 Independence implementation for the programmable digital items

Programmable digital items are used in many electrical power equipment and their use is increasing in many proprietary items with no alternatives available for some items of equipment.

A study should be carried out to identify and record:

- the location of programmable digital items embedded in equipment and function of these devices;

- failure modes and the potential for common cause failure of programmable digital items.

The consequences of CCF caused by programmable digital items should be assessed.

Consideration shall be given to diversity in the electrical system design to reduce the system vulnerability to CCF from programmable digital items.

Particular attention should be taken where there are proposals to network electrical protection systems through programmable protection relays with two way communication from central control systems.

These systems present a significant risk of common cause failure and should be avoided wherever possible for NPPs.

Where a networked system with two way communication is implemented then comprehensive validation and verification of the programmable devices should be undertaken to demonstrate the mitigations against potential CCF that the risk of CCF due to software error or cyber attack is acceptable in accordance with overall facility safety case.

Where programmable digital items are installed in the electrical system design their implementation shall be validated based on their safety classification.

This validation shall follow the procedures defined in IEC 62671.

System cyber security vulnerabilities and consequence associated with the Electrical Power System should be assessed where programmable digital items are implemented.

Justification of a programmable digital items should be based on the assessment of safety function(s)/failure modes.

Programmable digital items in electrical systems should be considered in the context of the overall electrical design and safety case.

Implementation of programmable digital items in electrical power systems requires a multi-disciplinary involvement.

7.2.4 Provisions for coping with Loss Of Off-site Power

The design should include provisions to detect this condition in order to initiate appropriate automatic or manual actions.

The following design measures to cope with a Loss Of Off-site Power should be considered (following the functional requirements applicable to the EPS and based on the electrical need of the supported loads):

- provision of adequate battery capacity to supply power to safety classified instrumentation and control equipment, and other vital equipment required in design basis conditions;
- installing standby AC power sources which fulfil the independence requirements between divisions (refer to 7.2.3.3.2);
- design the NPP with passive safety features.

The power balance, restoration time and the mission time of the systems supplied during a LOOP condition should be provided as input data to select the adequate solutions.

7.2.5 Provisions for coping with Station Black Out

The design should include provisions to detect this condition in order to initiate appropriate automatic or manual actions.

The following design measures should be considered:

- provision of adequate battery capacity to supply power to safety instrumentation and control equipment, and other vital equipment required in design extension conditions;
- installing an alternate AC power source that is diverse in design and is protected from hazards that could degrade the preferred power supply and standby on-site power sources;
- use of NPP to NPP connections where there are no CCF risks between the two units power source (where connections are made between NPPs it shall not be possible for a fault on one NPP to impact on the other);
- design the NPP with passive safety features.

The power balance, restoration time and the mission time of the systems supplied during a SBO condition should be provided as input data to select the adequate solutions.

7.2.6 Provisions to avoid or reduce Loss of Electrical Power

The design should include provisions to detect this condition in order to initiate appropriate automatic or manual actions.

The provisions to avoid or reduce this condition are:

- robustness of the Electrical Power System against CCF;
- adequate reliability of the equipment of EPS.

The following design measures should be considered to cope with a LEP condition:

- adequate autonomy for the uninterruptible power system source to monitor the severe accident parameters;
- the provision of an additional power source to supply severe accident functions (including the adequate connection points to permit this type of power supply);
- design the NPP with passive safety features.

The power balance, restoration time and the mission time of the systems supplied during a LEP condition should be provided as input data.

7.2.7 Classification consideration

7.2.7.1 General

Each electrical system shall be classified following the classification of the loads supported. All non-compliances shall be substantiated.

The classification of the DBC and DEC levels will be performed following the requirements of IEC 61226.

Once the Electrical Power System has been classified following IEC 61226, two main methods should be applied to verify the adequacy of the performance and reliability requirements on electrical power systems and equipment important to safety:

- qualification;
- surveillance and testing.

7.2.7.2 Qualification

Electrical equipment items shall be qualified in accordance with their functional requirements and service and environmental conditions.

Electrical power systems and components important to safety shall be qualified for their intended function over their service life in their anticipated environmental operating conditions.

The primary objective of qualification is to demonstrate with reasonable assurance that equipment important to safety can perform its safety function(s) without experiencing failures in all postulated conditions.

IEC/IEEE 60780-323 describes the basic requirements for qualifying electrical equipment important to safety and interfaces (electrical and mechanical) that are to be used in NPP.

IEC/IEEE 60980-344 provides recommended practises for seismic qualification of electrical equipment on a NPP.

7.2.7.3 Surveillance testing

For the electrical power systems important to safety, the following parameters should be periodically tested:

- operation of the electrical power sub-system and its components including performance of the associated power sources;
- transfer between electrical power sources;
- activation of protection (and associated fault-clearing devices);
- performance of the energy conversion equipment items, in particular those equipped with power electronics.

The electrical design should permit surveillance and testing activities of the parameters listed above.

IEC 60671 provides technical requirements and recommendations for the implementation of surveillance testing for I&C systems important to safety.

The general requirements for surveillance testing (Clause 6) should be followed for electrical power systems important to safety.

7.2.8 Provisions to achieve the reliability target for the Electrical Power System

The three main measures to increase the reliability of the Electrical Power System are:

- correctly specify components and procure reliable components;
- provide redundancy inside the division and between divisions;
- provide diversity between LoDiD and between divisions.

Electrical power systems important to safety shall be redundant to the degree necessary to meet design basis reliability requirements.

The reliability of the Electrical Power System shall be assessed with regard to the overall safety objective based on the PSA analysis.

On site provisions should be made to back up off site power sources where required to meet the plant safety requirements. These provisions should use measures such as additional on site power sources and the provision of automatic actuation of standby supplies.

In order to achieve PSA targets consideration should be given to modification of the architecture by the provision of redundancy to address component reliability issues and diversity to address CCF issues.

7.3 Electrical design provision

7.3.1 General

The electrical design should consider the following main input data in order to determine the performances of the electrical power subsystem:

- requirements and performances of the grid supply;
- performance requirement for loads supplied (refer to 7.4);
- electrical disturbances.

7.3.2 Coordination with the grid

The voltage and frequency range shall be derived from the applicable Grid Code.

The grid requirement shall be discussed and agreed with the electric grid operator so as not to impact the performance of equipment supporting functions important to safety.

NPP support for grid stability shall not adversely affect the capability of the EPS to support plant safety functions.

7.3.3 Design to achieve electrical requirements

7.3.3.1 General

Variations in voltage, current and frequency of the Electrical Power System of the nuclear power plant in any mode of plant operation shall not degrade the performance of any system equipment important to safety.

The variations and transients in voltage, current and frequency on the safety classified buses that could result from events on the preferred power supply or the on-site electrical power source shall be identified.

The design of the different sub-systems should be based on a balance between robustness by the design with withstand capacity or system or component protected by the electrical protection system.

All modes of operation and both symmetrical and asymmetrical events should be considered in the analyses. An event could challenge different components in the electrical power systems, depending on rise time, fault time, amplitude or asymmetry.

IEC 62855 provides the electro-technical engineering guidelines to perform this specific analysis for AC and DC electrical power systems in the NPP.

The frequency and voltage characteristics of the equipment power supply shall be specified.

The specification of system frequency and voltage characteristics should be based on the worst case configuration.

Each characteristic shall be defined by a nominal value and normal, exceptional and very exceptional variation ranges (also known as operating conditions).

These variations should be derived from the grid or from on-site power sources.

The normal operating condition is not limited in time, but the degraded operating conditions should be specified for a maximum duration and a maximum frequency rate or cumulative minimum and maximum duration.

7.3.3.2 Steady-state conditions for Electrical Power System

The following parameters of each sub-system and each LoDiD should be specified:

- voltage range;
- frequency range;
- current range.

These values should be determined:

- at the equipment terminal of the supported equipment in steady state, not including transient phenomena;
- based on the characteristics of the off-site and on-site power sources.

The tolerances and operating parameters of the equipment and systems should be considered in demonstrating the robustness to electrical disturbances of the electrical systems important to safety.

7.3.3.3 Electrical disturbances

7.3.3.3.1 General

The capability of the Electrical Power System to withstand electrical disturbances should be verified by:

- comprehensive analyses that identify all possible events (initiators) that could occur on the Electrical Power System based on international guides and standards, regulation reports, operating experience, international publications, studies or reports;
- definition of the potential preventive measures to reduce or eliminate the initiating event;
- characterization of the electrical phenomena (frequency range, voltage and/or current amplitude);
- definition of the protective measures associated with the electrical phenomena (by provisions of adequate inherent characteristics of equipment or by electrical protection system).

7.3.3.3.2 Electrical power systems voltage

7.3.3.3.2.1 Undervoltage condition

The undervoltage and time delay set points for degraded voltage protection should be determined by analysis of the voltage requirements of the loads (important or not to safety) at all on-site Electrical Power System levels (electrical normal operation limit).

The minimum voltage of the consumer shall be specified and by analysis, it shall be shown that the voltage remains above the limit.

Assessment of the voltage drop should confirm that the voltage at the terminals remains above the minimum voltage which could result in the loss of functions.

a) Acceptable voltage drop

This corresponds to a transient voltage drop with the following characteristics:

- the voltage is above the minimum voltage required to operate the load for an ongoing time.

or

- the voltage is lower than the minimum voltage required to operate the load; **and** the duration of this under voltage is **lower** than the limit associated to initiate an electrical source transfer.

An acceptable voltage drop shall not initiate an electrical source transfer.

b) Unacceptable voltage drop

This corresponds to a transient voltage drop with the following characteristics:

- the voltage is lower than the minimum voltage required to operate the load;

and

- the duration of this under voltage is **greater** than the limit associated to initiate an electrical source transfer.

The effect of short term transients on the electrical source transfer should be assessed.

The electrical source transfer strategy between the different electrical power sources should enable use of the different sources of the DiD if available.

An electrical source transfer shall be initiated in the event of an unacceptable voltage drop after a suitable time delay to allow clearance of upstream or downstream disturbances.

7.3.3.3.2.2 Overvoltage conditions

Overvoltages should be analysed to confirm that equipment withstand capabilities are not exceeded.

Overvoltages caused by lightning and EMC, switching overvoltages and overvoltages resulting from earthfaults in isolated networks should be considered in the analysis.

An overvoltage protection scheme should be provided to protect against overvoltages causing the withstand capabilities of the equipment to be exceeded (taking into account the priority level of the function performed by the system).

A study should be performed to substantiate the coordination between the overvoltage maximum value and time durations and the coordination with the design of Electrical Power System equipment.

Figure 4 is only provided as an example, the voltage levels and time durations are plant specific.

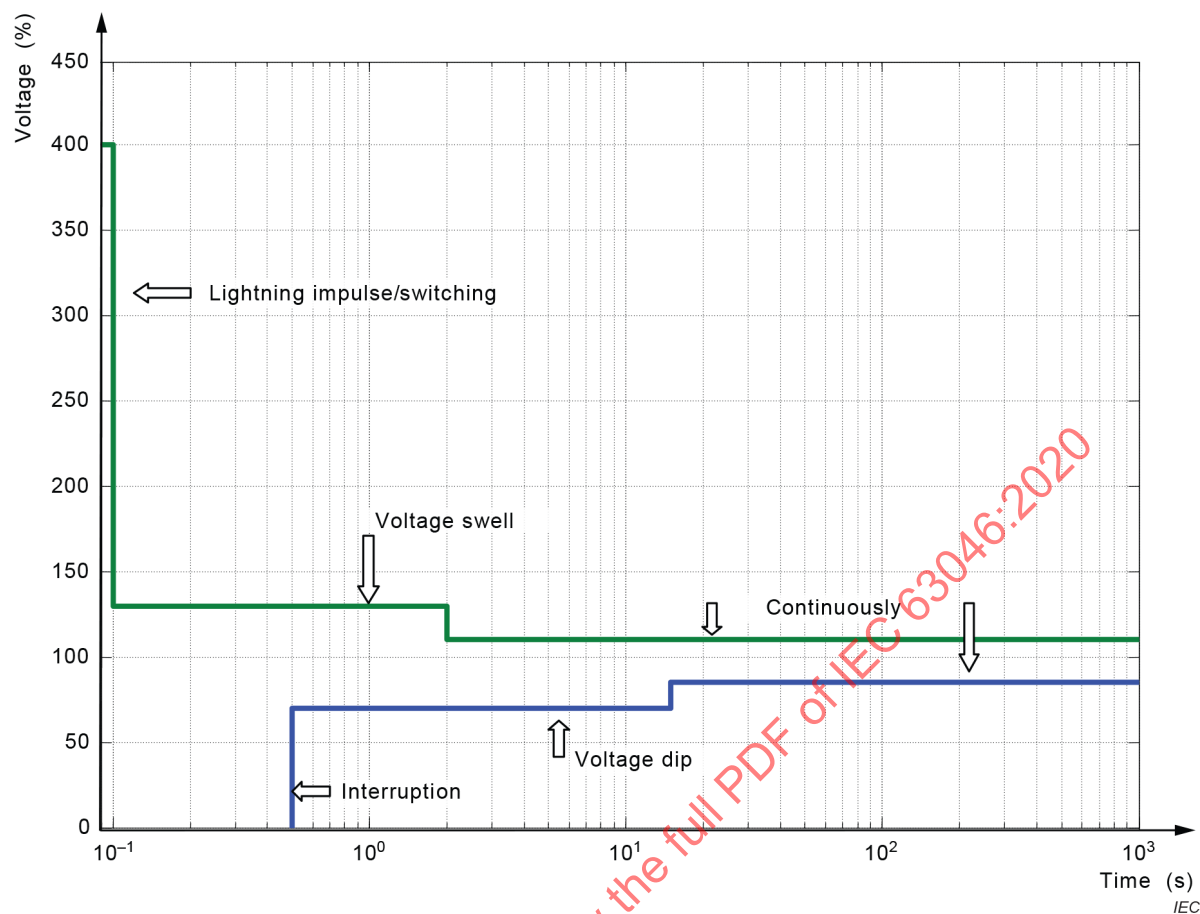


Figure 4 – Typical voltage design bases (IEC 62855)

7.3.3.3.2.3 Unbalanced voltage

Consideration should be given in the electrical disturbances analysis to unbalanced voltages and their potential consequences on electrical operation.

7.3.3.3.3 Current

The studies associated with current disturbances shall take into account:

- electrical faults;
- overloads;
- inrush currents;
- Geomagnetically Induced Currents (if applicable).

7.3.3.3.4 Frequency

The impact of frequency variations shall be assessed.

An analysis should be undertaken by the responsible technical groups of the functional impact of under and over frequency on the process loads such as fluid systems.

The operation of the Electrical Power System shall not be impacted by harmonics (e.g. risk of operation of overload protection).

The total harmonics distortion (current and voltage) should be evaluated.

The effects of harmonics generated by the grid or plant equipment should be evaluated and appropriate measures should then be taken to provide robustness against the harmonics.

Limits for levels of harmonic generation by equipment should be defined and the robustness of equipment against the generated harmonics should be assured.

7.3.3.4 Inherent characteristics of equipment

Electrical power systems shall be designed and constructed in such a manner that they can withstand maximum design voltages and currents in any plant state or operating mode.

7.3.3.5 Electrical protection system

7.3.3.5.1 General

An electrical protection system shall be provided to:

- protect electrical equipment from voltages, frequency and currents outside the defined operating conditions (in addition with the inherent characteristics of equipment);
- support continuity of supply by isolating faults so that they do not impact on the availability of the overall system.

The electrical protection system can be split in two parts:

- electrical source transfer when the source does not have the capability to support the loads;
- protection scheme to protect site personnel and equipment from electrical disturbances on the Electrical Power System.

The electrical protection scheme for the plant and the design of the plant's components shall be such that disturbances in the power supply do not jeopardize the required operation of safety power systems and connected loads.

If under voltage or under/over frequency and limits are exceeded, the load shall be transferred to the back up supply sources after appropriate time delays.

The Electrical Power System shall be robust and capable of fulfilling its task during fast and slow electrical transients and fault conditions.

An evaluation of the impact of electrical disturbances on all the on-site electrical power systems (AC and DC) should be undertaken in accordance with the methodology described in the section 7.3.3.3.1.

The design bases should cover all modes of operation and all possible events that could impact the Electrical Power System of the nuclear power plant.

The design of the different sub-systems should be based on a balance between robustness by designing equipment with appropriate withstand capacity and protection of systems or components by the electrical protection system.

Specific analysis should confirm that the electrical protection system meets requirements for equipment protection and maintaining supplies to electrical power systems important to safety.

7.3.3.5.2 Design of the monitoring and electrical source transfer

The quality, range and performance of the power supply shall be monitored continuously on each busbar which requires an automatic electrical source transfer.

Buses affected by degradation of the power supply from a given power source shall be disconnected from this power source if the degradation exceeds the specified design levels.

Studies should be performed to analyse the performance of Electrical Power System during electrical source transfers following the standard IEC 62855.

7.3.3.5.3 Design of the electrical protection scheme

7.3.3.5.3.1 General

The electrical protection system shall protect against the rated withstand capability of the equipment being exceeded.

7.3.3.5.3.2 Factors to consider

Protection coordination studies shall be performed taking into account all operating and transient conditions.

The studies should include all possible types of series and shunt faults, including events such as loss of one or two phase(s) and earth faults in systems operating with an isolated neutral.

The design of the electrical protection scheme should include consideration of both symmetrical and asymmetrical faults.

The protection scheme should include consideration of reacceleration currents following voltage sags and bus transfers.

7.3.3.5.3.3 Implementation

The following requirements should be taken into account in order to ensure the electrical coordination of the system:

- the protection system operating time should be compatible with the equipment withstand capability and the system performance requirements,
- a failure or maintenance of part of the protection system.

The protection scheme shall be capable of the following:

- fast action to protect personnel and property:
 - operating the required devices upon detection of unacceptable conditions to reduce the severity and extent of disturbances to the Electrical Power System, equipment damage, and potential hazards to personnel and property,
 - protective devices should be designed to initiate the circuit breaker to clear fault currents rapidly to avoid hazards and to prevent disturbances causing other protection devices to operate.
- selectivity:
 - ensuring that only faulted equipment is disconnected from the power supplies,
 - in case of short circuits and overloads, protective devices should be designed to operate selectively in all planned connection configurations of the Electrical Power System.

The protection scheme should be implemented in a graded approach to avoid the spurious tripping of upstream devices.

Individual protective devices installed to protect components during testing should be designed so that their operation does not endanger a system's capability to operate.

Protection devices that protect the power supply from a standby power source against immediate catastrophic failure should be in service in all modes of operation.

NOTE Examples of such devices include those that protect the standby power source from catastrophic failures, such as overspeed protection and generator differential protection.

Trip devices that protect the standby power source from non-catastrophic failures could be bypassed, following appropriate safety assessment, when the standby power source is supplying safety loads during emergency operation, but should be in service during normal operation and testing of the standby source.

The coordination studies should include assessment of the internal equipment protection.

7.3.3.5.3.4 Protection device requirements

Fault detection and fault clearing devices should be used for the prompt removal from service of any element of a power system when abnormal conditions occur which could cause degradation or failure of operating equipment.

Programmable digital protective devices shall be designed, verified and qualified for use in accordance with the safety function that they are intended to support and should be in accordance with the requirements of 7.2.3.3.3 and IEC 62671.

The design of the protective devices for the Electrical Power System and for components of nuclear power plants shall comply with IEC and National standards that apply to the safety of electrical equipment and electrical installations, as well as with other relevant regulations on electrical equipment and electrical installations.

7.3.3.6 Electrical parameters measurement and events recording

In addition to the electrical protection system (electrical source transfer and protection scheme), the design should provide the requirements for measurement of electrical parameters and event recording.

The designer should identify and implement all measurements required to analyse any type of electrical events.

The electrical plant equipment specification should specify all required output signals.

The events recording system should record the same time stamp for all measurements.

Consideration of cyber security should be given to electrical parameters measurement and event recording.

7.4 Functional and performance design provisions

7.4.1 General

The power system design shall support the functional requirements of the plant systems important to safety.

7.4.2 Electrical Power System studies

7.4.2.1 General

The electrical power systems of the nuclear power plant should meet all functional requirements under steady-state conditions, and degraded conditions as defined in the design basis.

7.4.2.2 Assignment of the loads to the sub-systems

The design should assign and allocate the loads (and especially loads important to safety) to the various electrical sub-systems based on criteria such as sensitivity to the loss of voltage, active and reactive powers, restoration time and mission time.

Two main sub-systems are defined:

- Interruptible power supply;
- Uninterruptible power supply.

7.4.2.3 Margin

A margin strategy should be established and should identify the different margins applicable and the level of margin associated:

- margin to cover modification during the NPP project design phases;
- margin to cover modification during the operation lifetime of the plant;
- margin to cover tolerances (for protection settings for examples);
- safety margin;
- margin to cover transient operation.

The adequacy of the equipment rating margins should be confirmed regularly in conjunction with the replacement of major components, plant modifications and periodic safety reviews.

Electrical equipment should be specified with an adequate design margin to ensure that future plant upgrades and modifications can be implemented without exceeding equipment ratings.

7.4.2.4 Power balance

The power balance study should support the initial design of the main electrical components.

The power balances should be:

- established for steady and transient states and for active and reactive powers;
- reviewed in the event of changes to plant loading.

The power balance should be individually determined for each division.

Power balances of electrical power systems should be established with a deterministic approach taking into account the following:

- functional and operational configuration:
 - all operating modes;
 - the operation from on-site or off-site power sources;
 - different loading steps (time for re-loading);
 - the operating configurations of the Electrical Power System (e.g. maintenance, test, operation) and interlocking facilities;
- safety analysis:
 - the different states and accidents listed in the safety analysis;
 - operating modes following single failures of electrical equipment;
- the power requirement for the maximum and minimum ambient conditions;
- electrical inputs:
 - maximum and minimum power requirements;

- voltage range;
- frequency range;
- efficiency and losses.

Simultaneous load factor should be determined from functional assessment and applied to intermittent loads.

Where cross-connections are provided the power requirements of the cross-connected loads shall be taken into account.

During an electrical source transfer, a non-safety classified load shall be taken into account as a permanent load in the power balance if it is not disconnected by safety equipment.

The power balance should collate:

- load active and reactive power;
- inductive motor loads;
- postulated initiating events;
- operating states and backup equipment;
- start-up time, mission time;
- type of network (interruptible or uninterruptible).

7.4.2.5 Voltage level

The nominal voltage levels to supply all systems, except the main generator system, should be in accordance with IEC 60038:2009, Table 1, Table 3, and Table 6 'preferred' columns.

The voltage level should be appropriate to the power required and the electrical coordination requirements.

The voltage levels should be optimized based on functional requirements.

7.4.2.6 Switching devices studies

A study should substantiate the position within the distribution system and the mission of each switching device.

The type of the switching device shall be based on this study.

7.4.2.7 Distribution strategy

The distribution strategy should optimize electrical equipment layouts.

The distribution strategy shall not decrease the compliance of the AC interruptible power supply system important to safety with the applicable requirements (6.2, 6.3, 6.4 and 6.5).

The distribution strategy shall not impair required operation in case of electrical disturbances.

7.4.2.8 Earthing system

The earthing system shall provide a low impedance path to connect electrical equipment to earth to prevent hazardous voltages from appearing on equipment and to contribute to the management of electromagnetic interference including lightning phenomenon.

For each network of the interruptible and uninterruptible power system, the earthing system connection should be defined according to:

- reliability of the network (in case of short circuit for example);
- ability to detect the first fault.

The electrical protection scheme design should take the earthing system into account.

7.4.2.9 Interlock study

For buses with facilities for the connection of different supply sources, an interlock system shall be provided.

Interlocks between breakers should be provided to prevent connecting circuits in parallel that could result in adverse voltage or current conditions on common buses.

7.4.2.10 Loss of control voltage study

A study should be performed to determine the effects of a loss of control voltage on system operations.

7.4.3 Design of the Interruptible Power Supply System

The AC interruptible power system can be divided into three parts:

- the AC interruptible power supply system supporting plant loads for normal operation and anticipated operational occurrences;
- the AC interruptible power supply systems important to safety comprising:
 - the interruptible safety power supply system supporting DBC;
 - the interruptible power supply system important to safety supporting DEC.

The design of the interruptible power system shall cover:

- the preferred power supply;
 - design of the off-site power supply;
 - design of on-site preferred power supply;
- the AC interruptible power systems important to safety;
- the on-site standby sources.

NOTE A level 2 standard (IEC 63272) covers the design of the Interruptible Power System.

7.4.4 Design of the Uninterruptible Power Supply System

The uninterruptible power system can be divided into three parts:

- the uninterruptible power supply system supporting plant loads for normal operation and anticipated operational occurrences;
- the uninterruptible power supply systems important to safety composed by:
 - the uninterruptible safety power supply system supporting DBC;
 - the uninterruptible power supply system important to safety supporting DEC.

The design of the uninterruptible power system shall cover:

- the uninterruptible power systems important to safety;
- the power sources.

NOTE A level 2 standard (IEC 61225) covers the design of the uninterruptible Power Supply System.

7.5 Maintenance

7.5.1 Consideration of the maintenance in the electrical design

The following provisions should be considered to support continuity of power supplies during maintenance activities:

- redundancy of the function or equipment considered;
- temporary cross-connection between divisions.

During outages to facilitate maintenance operations the number of power sources and operable buses may be decreased in accordance with the plant's operational limits and conditions. The design of the power system shall take into account the requirement to maintain electrical equipment whilst complying with the defined operating limits.

In the case of maintenance during operational demands on a safety system the use of cross-connections should be considered during a defined maintenance time frame.

If adopted, temporary connections between redundant divisions may be made during shutdown if a safety assessment confirms the following:

- that the cross-connections have interlocks that cannot be defeated by simple switch operation;
- that the effects of these connections on the reliability of plant safety functions and on their vulnerability to common cause failure is acceptable.

Cross-connections on safety systems shall meet the following criteria:

- justification on the acceptability of the cross-connection from a safety perspective;
- provision of two electrical isolation devices in series, one at each end;
- evidence that the use of the cross-connection will not result in an electrical failure on the supplied division causing the loss of the supplying division;
- cross-connections shall not increase potential fault level beyond equipment withstand levels;
- cross-connections shall be de-energized during normal operations except where required for maintenance activities.

The design of electrical power systems should include maintenance plans for all systems and components.

Electrical power systems important to safety should be designed to facilitate surveillance and maintenance activities, to permit timely access and, in the case of failure or error, to allow easy diagnosis and repair in order to reduce risks to maintenance personnel.

The maintenance strategy shall establish requirements for electrical equipment to be provided with equipment health monitoring to facilitate surveillance and maintenance.

Design provisions to facilitate maintenance, troubleshooting, and repair should include:

- avoidance of locating equipment in areas with conditions of extreme temperature or humidity;
- avoidance of locating equipment in areas with high radiation levels;
- taking into account human factors (capabilities and limitations) in performing the required maintenance activities;
- provision of sufficient space around the equipment to ensure that maintenance staff can perform their tasks safely in normal working conditions.

Provisions for the maintenance of electrical power systems important to safety should be assessed to confirm that any effects on the safety of the plant are acceptable.

NOTE Periodical testing is covered in 7.2.7.3.

7.6 Multi-unit shared electrical power systems

A hazard or an electrical disturbance in one unit should not affect the other unit.

7.7 Electrical system layout

The layout of the electrical equipment should:

- provide independence between:
 - redundant or diversified portions of a function important to safety;
 - electrical systems important to safety and other systems:
 - a) interconnected equipment;
 - i) classification;
 - ii) isolation;
 - b) adjacent equipment;
 - i) separation;
 - ii) electrical isolation;
 - iii) physical barriers.
- comply with:
 - national regulations in relation to escape route and fire suppression management;
 - the plant's requirements on:
 - c) electrical equipment and cable installation rules e.g.;
 - i) segregation requirement;
 - ii) optimization of the cable routing, lengths and cross sections;
 - iii) cable route design with various components (enclosures, racks, terminals); cable supports, cable types (copper, fibre), electrical and I&C openings and equipment rooms;
 - iv) cable route and cable layout;
 - v) equipment room design;
 - d) hazard mitigation;
 - e) the choice of cables for building infrastructures, I&C and power systems;
 - f) easy access for maintenance and cable installation.

7.8 Supporting and associated systems for the Electrical Power System

The safety classification and the design of supporting and associated systems shall be such as to ensure that the performance of these systems is consistent with the safety significance of the system or component that they serve at the nuclear power plant:

a) Compressed air systems

The specification for any compressed air system that serves an item important to safety at the nuclear power plant shall define the requirements for quality, flow rate and cleanliness of the air.

b) Air conditioning systems and ventilation systems.

Systems for air conditioning, heating, cooling and ventilation should be provided as appropriate in auxiliary rooms or other areas at the nuclear power plant to maintain in all plant states the required environmental conditions for systems and components important to safety.

Particular attention shall be given to the ventilation system for electrical rooms with an explosive atmosphere risk (e.g. battery rooms).

c) I&C

The I&C system which monitors and controls the electrical power system important to safety shall be developed in accordance with IEC 61513.

The interface between electrical signals and the Main Control Room and local indications and alarms (HMI) should be managed during the design.

IEC 60964 establishes requirements for the human-machine interface in the main control rooms of nuclear power plants.

The reliability of the power supply of monitoring and control systems should be assessed.

d) Lighting

The lighting strategy should consider the requirements for electrical rooms in all conditions in order to assign the required loads to supplies with standby sources.

e) Communication system

A communication system strategy should be defined in all conditions.

f) Control voltage system

The reliability of the power supply of control voltage systems should be assessed.

Particular attention should be given to these support systems in order to limit the risk of disturbances on operation of the Electrical Power System or risk of CCF affecting the entire Electrical Power System due to failure(s) on supporting systems. The electrical design should define requirements for supporting systems.

7.9 Overall quality assurance programs

This document assumes that a quality assurance program or preferably an integrated management system exists as an integral part of the NPP project and that it provides control of the constituent activities.

The safety classified part of the Electrical Power System should be consistent with the requirements of IAEA GS-R Part 2 and IAEA GS-G- 3.1.

- a) Quality assurance programmes shall be established and implemented for each activity related to the overall electrical power system life cycle.
- b) The quality assurance programs shall include all activities that are necessary to achieve quality and the activities which verify that the required quality has been achieved.
- c) The verification activities shall be defined in verification plans. The verification plans should include the resources, process and outputs of the phases of the overall EPS life cycle and should define:
 - procedures and tools for verification activities;
 - the records to be kept and verified;
 - the safety relevant aspects to be verified;
 - procedures for the resolution of failures and incompatibilities;
 - the criteria for declaring each phase complete;
 - the final reports to be produced showing the compliance of the outputs of the phase with the inputs requirements and the resolution of anomalies.

- d) The quality assurance programs shall be planned and included within the general quality assurance program of the NPP project, and its activities shall be included within the general schedule of the activities of the NPP project.

7.10 Requirements for output documentation

7.10.1 General

Information, analyses, and computations supporting design of the electrical power systems important to safety should be documented and controlled in accordance with the quality records system established for the plant.

Documentation records should be prepared to support the design of individual system features or functions. Each design documentation record should be verified in accordance with the requirements of ISO 9001 completed by the IAEA requirements issued from GS-R Part 2, and should include sufficient information to allow further independent checking or review.

The information and studies should comply with the items listed in the documentation supporting design of the electrical power systems important to safety.

The documentation of the electrical power systems should include the substantiation of:

- design bases.
- a description of the overall Electrical Power System including:
 - details of how the nuclear power plant is connected to the grid;
 - an explanation of the degree of redundancy of the electrical power systems important to safety;
 - identification of interfaces with the auxiliary systems.
- a description of the separation criteria for installing equipment, cables and raceways, including wiring and components inside panels.
- single-line diagrams, functional control diagrams, schematic diagrams, connection diagrams, panel wiring diagrams and system descriptions.
- layout plans for the on-site Electrical Power System together with the arrangements of equipment and associated support systems.
- layout plans of cable routes, including trays, ducts and conduits, throughout the plant and identification of redundant divisions and cables and their routing.
- raceway schedules showing cables contained in each raceway segment and the fill percentage of each segment.
- circuit schedules identifying for each field cable its connection points, cable type and routing through the raceway system.
- an electrical load analysis showing the inventory of electrical loads. For electrical power systems important to safety this should show a time dependent loading from which the capabilities of the necessary components of the power system are calculated.
- operating procedures and maintenance manuals for electrical power systems and equipment.
- periodic testing and maintenance requirements for electrical power systems and equipment.
- documentation of acceptance tests and commissioning tests for electrical power systems and equipment.
- quality management records.
- analysis of current, voltage and frequency disturbances.

- studies of steady state load and voltage profile studies that show the voltages throughout the power system for various modes of plant operation (and generator load to power factor), including design basis events, normal operation and conditions of degradation in voltage.
- transient load and voltage studies that show the profile of the loads that are sequentially applied to the preferred power supplies and standby power sources in various modes of plant operation.
- an electrical source transfer study that analyses the effects of voltage, phase angle and frequency, and the effects of motor reacceleration on buses and motors before, during and immediately after automatic transfers.
- short circuit studies to determine the maximum and minimum fault currents throughout the power system for various modes of plant operation, including design basis events, for use in analysing the fault clearing and withstand capability of the electrical equipment.
- coordination studies of protective devices and studies of equipment protection that show proper set point selection in all of the protection schemes.
- analysis of fuel storage capacities for standby power sources.
- analysis of the consequences of partial or total loss of power supplies.
- equipment qualification plans, analyses and test reports.
- specifications for electrical power components.

7.10.2 Architecture principles

An Electrical Power System architecture principle document and diagram should be produced to identify the main characteristics of the Electrical Power System including:

- Safety provisions (see 7.2)
 - the relevant safety deterministic rules analysis;
 - the relevant plant events;
 - the plant Defence in Depth approach and its application for the Electrical Power System;
 - the number of electrical divisions based on the combination of safety and maintenance requirements applicable;
 - a CCF risk analysis;
 - the diversification requirements applicable to the Electrical Power System and its equipment;
 - the allocation of main (respectively groups of) safety functions or loads;
 - number and type of on-site power sources (AC, DC);
 - the systems classification;
 - the applicable independence provisions at the sub-system level.
- Electrical design provisions (see 7.3)
 - compliance with the electric grid operator requirements;
 - report of identification of electrical disturbances (with possible measures) and associated impact on electrical quantities (voltage, current and frequency);
 - electrical disturbances studies (covering transient and fault studies);
 - performance requirement of the electrical loads;
 - performance of the Electrical Power System taking into account the different power sources associated with different LoDiD (based on the four previous bullet);
 - load flow studies;
 - electrical source transfer studies;
 - required withstand capacities for electrical equipment of the Electrical Power System;

- protection scheme and electrical protection coordination studies.
- Functional provisions (see 7.4)
 - the distribution arrangement with corresponding switches, power sources and conversion equipment;
 - the grid connection arrangement;
 - the voltage of the electrical power systems;
 - the rating of on-site-sources;
 - the rating of power conversion components;
 - the earthing system connections;
 - load list and assignment of loads in the SLD;
 - the power balances on the different switchboards;
 - a voltage level selection report;
 - the sizing of the main electrical equipment;
 - the sizing of protection devices;
 - a switching device study;
 - an earthing system selection report for each network;
 - an interlocking study;
 - the monitoring provisions;
 - a loss of control voltage study.
- Maintenance provisions (see 7.5)
 - The plant operator should document plant maintenance requirements and the associated provisions.
 - The cross-connections should be identified on the Single Line Diagram (SLD).

7.10.3 Single line diagrams

An overall single line diagram should identify the main characteristics of the Electrical Power System:

- the distribution arrangement with corresponding switches, power sources and conversion equipment;
- the grid connection arrangements;
- the voltage of the electrical power systems;
- the power of standby sources;
- the power of power conversion components;
- the earthing system connections;
- the cross-connection provisions.

8 Sub-system requirements

8.1 Electrical Power System basis requirements

8.1.1 General

The purpose of this clause is to introduce a generic list of topics to be covered when writing a level two standard.

Particularly, the following requirements are applicable to two main sub-system:

- interruptible power supply;
- uninterruptible power supply.

8.1.2 System Design

The two main electrical sub-system level 2 standards follow the same structure as this document, IEC 63046.

The standards define:

- design of the systems with regard to safety requirements;
- design of the systems with regard to electrical requirements;
- design of the systems with regard to functional and performance requirements;
- design of the systems with regards to maintenance requirements;
- system interfaces: to identify and specify requirements related to the interfaces that could compromise, by their functional failure, the auxiliary supporting features of the electrical power systems.

8.1.3 Single line diagram

The AC interruptible power supplies system and/or uninterruptible power supplies single line diagram should define:

- the boundaries of the system and the interfaces with the upstream and downstream systems;
- the safety classified (including associated safety class) and non-safety classified portion of circuits.

8.2 Equipment design specification

The design rules for the different items of electrical equipment should be included in the level 2 standard which will derive the following parameters from this level 1 standard:

- rated voltage and frequency;
- steady-state (voltage range and frequency ranges);
- withstand capacities based on the maximum calculated transients of voltage and current;
- power requirements derived from the load list or power balance;
- autonomy (for power supplies);
- environmental ambient conditions.

8.3 Equipment requirements

A level 3 standard should define equipment requirements commensurate with safety class significance on:

- design;
- fabrication;
- installation and mounting;
- examination, maintenance, inspection and testing.

8.4 AC Interruptible Electrical Power Supply System

A level 2 standard (IEC 63272) will cover this sub-system.

A level 3 standard should cover standby power sources.

In the absence of IEC/SC 45A dedicated standard the clauses of Annex B shall be applied.

8.5 AC/DC Uninterruptible Power Supply System

IEC 61225 shall apply.

8.6 Coordination and interaction with power grid

A level 2 standard should cover this sub-system.

8.7 Earthing

A level 2 standard should cover this sub-system.

In the absence of IEC/SC 45A dedicated standard the clauses of the Annex C shall be applied.

9 Verification of the architecture of the Electrical Power System

9.1 General

Verification shall be carried out and documented at each step of the design:

- verification by studies for the Electrical Power System;
- verification by testing: factory tests at the equipment level;
- verification by testing: on-site at the equipment level;
- verification by testing: on-site sub-system functional tests;
- verification by testing: on-site Electrical Power System functional tests;
- periodic tests during operation or outages.

9.2 Computerised tools and models verification

9.2.1 Electrical Power System verification

Based on IEC 62855, the electrical design of the Electrical Power System shall be verified.

Bounding cases shall be defined for each operating configurations.

9.2.2 Layout of electrical power systems and equipment verification

The layout should be analysed using commercially available software and developed based on technical specifications. The software should have a validated domain and its accuracy and compliance with industry standards should be validated.

This analysis should demonstrate the compliance of the Electrical Power System with the applicable safety requirements.

The layout of electrical equipment should consider the minimum maintenance envelope, space requirements and requirements of the lifting devices for maintenance and replacement of the equipment during the life-cycle management activities.

9.3 Test requirements

The following tests are required dependent on the stage of the NPP design:

- Routine tests;
- Factory tests;
- Site acceptance tests;
- Plant commissioning tests.

The test results shall demonstrate compliance with specifications associated with the different levels (Electrical Power System level, sub-system level and equipment level).

All systems important to safety shall include provisions for testing, including where appropriate, built-in test capabilities.

The equipment testing programme should be coordinated with the operational test programme so that availability requirements of systems and components can be fulfilled. This includes taking into consideration failure rates of components in establishing test frequencies. It is envisaged that certain tests can only be performed during refuelling outages.

Testing arrangements should include test procedures, test equipment interfaces, test equipment requirements and built-in test facilities.

Testing and calibration of system equipment important to safety should be possible in all modes of normal operation, including power operation, while retaining the capability of systems important to safety to fulfil their safety functions.

The capability for testing and calibration during power operation should not adversely affect the safety or the operation of the plant.

If provisions are not made for testing equipment important to safety during power operation, the following should be provided:

- justification that the reliability of the functions is acceptable;
- the capability for testing during shutdown.

A test programme should normally include:

- a description of programme objectives;
- identification of systems and components to be tested;
- test schedule;
- bases and justification for the tests to be conducted and test intervals;
- acceptance criteria;
- a description of the documentation and reports required;
- periodic review of the effectiveness of the programme;
- the individual test procedures to be used to define the tests.

The scope and frequency of testing should be justified as consistent with functional and availability requirements.

Implementation of the test programme should provide:

- objective information on the status of systems and components;
- assessment of the degradation of components;

- data on trends to assist in detecting degradation of components;
- indications of incipient failure within the system;
- requirements for evaluations that should be conducted before repetition of the failed test can be credited as establishing operability.

Evaluation and documentation of the causes of a failed test, and of the remedial actions taken, should be undertaken before the results of a repeated test can be used to demonstrate operability of the systems or components involved. Corrective actions may, for example, include calibration, maintenance or repair of components, or changes to test procedures.

10 Overall integration and commissioning

10.1 General

The objective of this phase is to integrate the Electrical Power System on site and ensure that all functions important to safety and the associated support systems perform as expected during the commissioning tests of the plant.

The commissioning plan of the Electrical Power System should be included in the commissioning programme of the plant systems.

The electrical system is usually used during the construction phase, in the following steps:

- After the electrical system (or part of the system such as a division, a voltage level) has been installed, inspected and verified to comply with electrical and personnel safety demands, it can be energized and put in operation in order to support the construction or tests. The energized parts of the electrical systems can be used for operating electrical loads during the installation of the plant;
- When the plant reaches the commissioning period, the commissioning of the electrical systems are planned together with other commissioning activities;
- After applicable commissioning tests have proved that the electrical system meets all nuclear safety objectives, the electrical system is declared operational from a nuclear safety perspective;
- The impact of the use of a part of the Electrical Power System during the Construction phase shall be considered.

10.2 Requirements

The following requirements are applicable for steps 2 and 3 of 10.1.

- a) The activities should be carried out in a systematic way, with a strategy developed in accordance with the system installation plans, the overall integration and commissioning plans.
- b) The overall integration activity should be carried out with all the related electrical systems installed and individually tested and interfaces with the systems supported.
- c) Programmable digital items with parameters shall be loaded and stored values shall be justified and tested.
- d) Verification and validation of all functions important to safety shall be completed before these functions are placed in service (on a nuclear safety perspective).
- e) Verification and validation of electrical data used for electrical disturbances studies from the tests performed (refer to 7.3.3). In case of variations, the impacts on these studies should be assessed.
- f) Verification and validation of the margin following 7.4.2.3.

10.3 Output documentation

The electrical systems integration documentation with records of chronological evolution of on-site verification and validation activities shall be available before the beginning of operation activity.

The report on the overall commissioning activity shall confirm that the electrical power systems satisfy all expectations for intended use and functions important to safety comply with the overall requirements specifications.

Variations from the design intent that are found are assessed, corrected or referred to the operating organisation so that any effect on plant operation can be taken into account.

11 Overall operation and maintenance

11.1 General

The conditions to be met before entering the operation phase should be agreed before handover from overall commissioning to the operating organisation. The following requirements are independent of this agreement:

- the systems should have completed sufficient testing to confirm that the specified functionality has been provided. Where testing has identified defects, these shall be documented and, if possible, corrected prior to handover;
- adequate user documentation and maintenance plans shall be available.

Operation of the Electrical Power System may start after evaluation of commissioning reports has shown the activity was completed successfully.

NOTE The electrical system can be used during the construction phase (refer to 10.2), the word “operation” in this clause refers to operation on a nuclear safety perspective.

11.2 Requirements

The electrical power systems shall be operated and maintained in order that the requirements for the Electrical Power System supporting functions important to safety are maintained.

- a) The documentation for operation, maintenance defined in 6.5 and 7.5 shall be implemented.
- b) Procedures to be followed by plant operators or maintenance staff in normal operation, anticipated operational occurrences and accident conditions shall be available in the control room or nearby. Their form and content should be in accordance with international or national regulations.

During the lifetime of the nuclear installation, some modifications on loads supported by the Electrical Power System will occur (new load to supply or modification of some electrical characteristics of load in case of replacement), the modification process shall substantiated that the modification will not impact:

- the robustness against CCF,
- the robustness against hazard,
- the robustness against electrical disturbances,
- the margin strategy.

11.3 Output documentation

Chronological documentation of operation, repair and maintenance shall be maintained.

Operational records should be subject to regular review to assess for negative performance trends, and any trends which indicate unacceptable deterioration of electrical equipment should result in appropriate corrective actions.

12 System quality assurance plan

12.1 General

- a) A quality assurance plan shall be established and implemented to cover each of the activities of the system safety life cycle. The requirements for the system quality assurance plan shall be derived from IAEA GS-R Part 2 and ISO 9001.
- b) The system quality assurance plan shall include the activities that are necessary to, achieve the appropriate quality of the system, for verifying that the required quality is achieved, and to provide objective evidence to that effect.
- c) The system quality assurance plan shall include:
 - identification of the governing standards and procedures to be used for the project;
 - identification of the phases of the system life cycle, the elementary tasks and the expected results of each phase;
 - description of relationships and interactions between the different tasks;
 - description of the organisational structure;
 - procurement of components from external suppliers;
 - product identification and traceability;
 - identification of all inspection and testing procedures;
 - identification of QA activities and tasks;
 - identification of personnel/organisations responsible for QA activities and tasks, including requirements for organisational independence between relevant activities in the project lifecycle;
 - procedures for reporting and disposition of non-conformance to requirements, standards and procedures. The procedures shall include consideration of the impact upon NPP safety and shall ensure that all effects of the non-conformance are identified, for example interchangeability, maintenance, spares, operating instructions, etc.
- d) The quality assurance plan shall be established at an early stage of the system life cycle and shall be planned within the general schedule of the other activities of the Electrical Power System life cycle.

12.2 System verification plan

- a) A system verification plan shall be developed describing:
 - the verification process across all the phases of the system safety life cycle,
 - the corresponding organisation and responsibilities.
- b) The outputs generated by each phase of the system safety life cycle shall be verified against its identified inputs.
- c) Every verification step shall produce a report of the analysis performed and the conclusions reached. When a phase is completed, a final report shall be produced, showing the compliance of the outputs of the phase with the inputs requirements and the resolution of anomalies.
- d) Verification shall be carried out by persons competent in the subjects addressed, who have a good understanding of the inputs against which the verification is made; involvement of the representatives of those concerned with the use of the results is recommended.

- e) The thoroughness of the verification plan shall be commensurate with the safety class of the system. The verification plan shall highlight the safety relevant aspects to be verified and should recognise that the probability of fault or omission in complex items is greater than in simpler ones.
- f) The documents subject to a verification review shall be identified in the system quality assurance plan.
- g) The documents involved in a verification review, i.e. inputs and outputs of activities, verification reports, and possibly the tools used to elaborate the outputs, shall be placed under configuration management.

12.3 System configuration management plan

a) Configuration control:

- the configuration control shall provide the facilities guidelines for when to initiate a design freeze (i.e. halt in design process). Procedures and authority required for any further modification following a design freeze shall be defined including the allocation of responsibilities and authorities for CM activities to organizations and individuals within the project structure;
- the status of each controlled item shall be tracked; this includes information on the initial approved version, the status of requested changes and the implementation of approved changes;
- the configuration management plan shall identify the configuration audits and reviews to be held;

NOTE It is good practice to distinguish between internal items (i.e. those developed within the project) and external items (those provided by vendors/subcontractors), and to define activities to control the interface to external items.

- b) The configuration management plan shall be defined at the beginning of the system project and be maintained during the whole system life cycle.

12.4 Fault resolution procedures

Procedures for the reporting and resolution of faults found during system integration verification, during system validation and in later phases shall be established before the corresponding phases begin.

- a) These procedures shall be referenced by the system integration and system validation plan.
- b) These procedures shall apply to all faults found during the system integration phase and system validation phase that require modifications to equipment or system design documents.
- c) They shall ensure that any required re-verification of system design and equipment is performed according to the system configuration management plan.
- d) They shall ensure that any required modification of system design and equipment is carried out according to the modification procedure and to the system configuration management plan.
- e) An evaluation of each fault reported shall be made to determine whether any systematic deficiency exists and also to determine whether the fault was of such a nature that it should have been detected at an earlier phase of the verification.
- f) If this is found to be the case (i.e. it should have been detected at an earlier phase), then an investigation of that phase shall be conducted to determine whether any systematic deficiency of the verification exists.
- g) If the evaluation of faults shows that there is a systematic deficiency of the verification, causing faults in equipment to remain undetected, then the deficiency shall be identified and corrected or justified.

Annex A (informative)

Basic safety issues in NPPs

A.1 General

This informative annex identifies the main safety concepts that are considered in this document for the design of NPP Electrical Power System. The annex provides an overview of the contents of IAEA documents but does not intend to enhance the requirements stated in these documents.

A.2 Plant safety objectives

Any industrial activity that presents risks to workers, members of the public and the environment requires the operator to take all reasonably practicable measures to keep these risks low. One typical risk of nuclear energy is the potential hazard of ionising radiation (see Clause 2 of IAEA SSR-2/1:2016).

The general nuclear safety objective is to protect individuals, society and the environment by establishing and maintaining an effective defence against radiological hazard from NPPs.

A.3 Plant safety analysis

A.3.1 General

A safety analysis of the nuclear plant design should be performed to establish and confirm the design basis for the items important to safety and to ensure that the overall plant design is capable of meeting the limits and reference levels for radiological doses and releases set by the regulatory authority for each plant condition category (see Clause 5 of IAEA SSR2/1:2016).

The scope of the safety analysis should include:

- the demonstration that operational limits and conditions are satisfied for the normal operation of the plant;
- characterisation of the PIEs that are appropriate for the plant design and its location;
- an analysis and evaluation of event sequences which result from PIEs;
- comparison of the results of the analysis with radiological acceptance criteria and design limits;
- establishing and confirming the design basis;
- a demonstration that the management of anticipated operational occurrences and accident conditions is provided by the response of the automatic safety systems in combination with prescribed operator actions.

This plant safety analysis process should be carried out in an iterative manner from the time of initial plant conceptual design to the final plant safety assessment and take into account all details of the plant configuration that may have an influence on safety. The plant safety analysis should take full account of potential human errors in all operational states and under accident conditions.

The objective of this analysis is to demonstrate that the actions which are specified to be carried out by the automatic systems and the operators will result in plant behaviour which maintains radiation doses to site personnel and the public below prescribed limits for normal operating, anticipated operational occurrences and accident conditions.

A.3.2 Analysis of event sequences

The purpose of analysing an event sequence is to identify systematically and in detail all possible consequences of a PIE on the plant, including those arising from auxiliary and support systems and from possible operator error. The results of this event sequence analysis should then be used to determine if the safety requirements set down in the IAEA code of design have been met (see appendix of IAEA SSR-2/1:2016).

Useful analytical tools for identifying possible plant states after a PIE are event tree analysis (qualitative) and fault-tree analysis (quantitative).

It is neither possible nor necessary to include in the safety analysis every event sequence that might occur. However, the safety analysis should identify and consider in detail those PIEs and event sequences that produce bounding cases for safety design. In making the choice of these event sequences, experience with existing plants should be taken into account.

Even with the restriction to bounding case event sequences, as described above, the rigorous application of event tree methodology will, in many practical situations, lead to the identification of many more plant configurations for each PIE than can be realistically analysed in detail. Therefore, it is usually admissible to restrict the detailed analysis to a number of representative event sequences.

A.3.3 Assessment of design basis: deterministic/probabilistic methods

Methods have been developed to assess whether safety objectives have been met (see IAEA 75-INSAG-3).

In the deterministic approach, design basis events should be chosen to bound a range of related possible initiating events which could lead to a challenge to the safety of the plant.

Probabilistic analysis should be used to evaluate the likelihood of any particular sequence and its consequences. This evaluation should take into account the effects of mitigation measures inside and outside the plant.

Deterministic versus probabilistic approach: The lack of sufficient data on component or system behaviour or the inability to specify a suitable mode may prevent a rigorous quantitative probabilistic approach. However, a partial probabilistic approach can often be supplemented by qualitative engineering judgement. A deterministic approach on the other hand requires engineering judgement that implicitly contains some qualitative probabilistic considerations.

In essence, current practice is to use the deterministic approach to design the systems and the probabilistic approach to optimise appropriate parts of the design and to evaluate the overall safety.

A.4 Defence in Depth

A major contribution to the safety philosophy is provided by the defence-in-depth concept. This concept should be applied to all safety activities, whether organisational, behavioural or design-related, to ensure that there are overlapping safety provisions so that if a failure does occur, it would be compensated for or corrected (see IAEA SSR 2/1; IAEA 75-INSAG-3).

A first application of the concept of Defence in Depth to the design process is to provide independent but complementary sets of equipment and procedures in order to prevent accidents or to ensure appropriate protection in the event of prevention failing. Examples of the multiple levels of protection:

- multiple provisions for ensuring each of the basic safety functions, i.e. reactivity control, heat removal and the confinement of radioactivity;
- use of reliable protective devices in addition to the inherent safety features;
- supplementing of the plant control by automatic and operator actions;
- provision of equipment and procedures to mitigate accident consequences.

In general, all the lines of defence should be available at all times as specified for the various operational modes.

- The aim of the first line of defence is to prevent deviation from normal operation. This requires that the plant be soundly and conservatively designed, constructed and operated in accordance with appropriate quality levels and engineering practices.
- The aim of the second line of defence is to detect and intercept deviations from normal operating conditions in order to prevent anticipated operational occurrences from escalating into accident conditions.
- For the third line of defence it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences may not be arrested by a preceding line of defence and so additional equipment and procedures are provided to control the consequences of the resulting accident conditions. A further major objective of this line of defence is to achieve stable and acceptable conditions following the accident.
- The aim of the fourth line of defence is to provide complementary measures and accident management following the non-operation of the third line of defence.
- Beyond the fourth line of defence, there are further contributions to the protection of the public by complementary plant features (not claimed as important to safety) and plans for emergency preparedness, which are largely independent of reactor design.

IAEA SSG-34 provides the following table (see Table A.1):

Table A.1 – Support of the electrical power supply for the defence in depth of the plant

Levels of Defence in Depth	Objective	Essential provisions	Applied to plant Electrical Power System
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Comprehensive design bases, robust and reliable grid, robust and reliable on-site power systems
2	Control of abnormal operation and detection of failures	Control systems, limiting systems and protection systems and other surveillance features	Robust and reliable fault clearing system and coordination of protection, power supply transfer capability, house load operation possibilities
3	Control of accidents within the design basis	Engineered safety features and accident procedures	Robust and reliable safety power systems, robust and reliable on-site standby AC power supplies
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of design extension conditions	Complementary measures and accident management	Robust and reliable alternate AC power supply
5	Mitigation of radiological consequences of significant radioactive releases	Off-site emergency response	Mobile power supply connection point

Annex B (informative)

AC Interruptible Electrical Power System

B.1 General

Note that the requirements of this annex will be covered in IEC 63272. As it is not convenient to repeat the same requirements in different standards (risk of inconsistency when updating one of these standards), this annex should be ignored and removed from IEC 63046 after the publication of IEC 63272.

Where the requirements of this annex are different from those provided in the future issue of IEC 63272, the information of IEC 63272 takes precedence.

B.2 Electrical design provisions

B.2.1 Steady state conditions for Electrical Power System

a) Voltage of Electrical Power System

The static voltage ranges to be taken into account when designing the unit's auxiliaries are derived from:

- the grid voltage for equipment supplied directly from the preferred power supply;
- electrical studies for other types of power supplies (on-site power supplies).

Voltage range limits should be determined at the terminals of the equipment supplied under the following sizing operating conditions:

- the maximum value should be established on the highest specified voltage of the Electrical Power System without voltage drops in the cables and without load.
- the minimum value should be established on the lowest specified voltage of the Electrical Power System including voltage drops in the cables at full load.

The maximum steady-state voltage drop between the power source and the powered equipment relative to the sizing voltage of the electrical distribution should be specified. Consideration of the voltage drop confirms that the voltage at the terminals stays above a minimal voltage which could result in the loss of some functions.

A load flow study should validate the voltage range for electrical equipment of each sub-system (AC interruptible power supply system and DC/AC uninterruptible power supply system).

b) Current

The current values during steady-state operation shall be established at the steady state voltage range limits.

Depending on the type of load (i.e. inductive or resistive), lower or upper voltage limits shall be used.

c) Frequency of power supply

On-site frequency variations (around nominal frequency) originating from the grid should be evaluated and shown to be acceptable for the process (fluid system) and should not impact on equipment such as uninterruptible power supplies.

B.2.2 Electrical disturbances

B.2.2.1 Electrical Power System voltage

a) Undervoltage

Undervoltage can result from the following transient operations or faults:

- grid disturbances;
- electrical fault and relevant clearance;
- starting of motors or group of motors;
- a combination of the above listed causes.

Voltage drop as a result of electrical fault or due to the start of motors:

- shall not cause any permanent disconnection or inadmissible interruption of other loads important to safety in operation;
- shall not result in an electrical source transfer operation (automatic switchover to stand-by off-site power supply or on-site AC power source).

In case of electrical source transfer, a load starting sequence shall be established based on the load characteristics and the capability of the supply source.

b) Overvoltage

Overvoltage can be due to following transient operations or faults:

- low frequency transients such as:
 - load rejection;
 - turbine trip;
 - house-load operation with or without failures of automatic voltage regulation for main generator;
 - transients having their origin at the generator;
 - single-phase to earth fault in an IT earthing scheme;
 - ferroresonance.
- High frequency transient such as:
 - lightning;
 - switching impulse.

1) Lightning

Lightning strikes

- on buildings;
- in the vicinity of the NPP;
- on transmission lines;

can induce disturbances and destruction of electrical and electronic systems.

The analyses should demonstrate that overvoltages caused by lightning do not challenge the equipment important to safety and are below the equipment withstand levels.

2) EMC

Induced voltages/currents should be demonstrated to be within design limits.

Protection should also be provided by the application of good practice in the execution of:

- segregation;
- cable selection and installation;
- cable shielding management;
- effective building/room/panel shielding;
- earthing design;
- etc.

NOTE The electrical protection scheme can use different kinds of voltage protection:

- Protection relays for low frequency transients;
- Surge arrester for high frequency transients.

c) Unbalanced voltage

Unbalanced voltages can result in voltage and current negative phase sequences.

The resulting negative values should be analysed with regard to the withstand capability of the equipment important to safety.

B.2.2.2 Electrical Power System Current

a) Electrical fault

The following faults (short-circuit and insulation fault) should be examined:

- single phase to earth fault;
- phase to phase fault;
- two or three phase to earth fault;
- three phase fault.

Short-circuit calculations according to IEC 60909 (all parts) should be performed to determine maximum and minimum AC currents during fault conditions.

Short-circuit studies are required to determine equipment withstand requirements in the first stage of the design and then to check in the next stage of the project that equipment ratings are adequate.

The maximum calculated short circuit current:

- shall not exceed the maximum fault current withstand capability of all electrical equipment;
- shall not exceed the maximum capability of switching devices.

The electrical protection coordination studies shall demonstrate selective isolation of the faulted circuit.

The selectivity between the different electrical protection levels shall be adequate at minimum calculated short circuit levels.

b) Overload

Overload protection should be taken into account while designing the electrical protection scheme.

c) Inrush current

Inrush current due to motor starting or transformer magnetizing should be taken into account in designing electrical protection schemes.

Inrush currents shall not activate electrical protection.

d) Geomagnetically Induced Currents

A substantiated engineering assessment shall demonstrate that the design measures adequately mitigate the risk of GIC in the NPP.

B.2.2.3 Frequency

a) Under or over frequency

Under- and over-frequency should be assessed to consider the impact on the required power and on the power balance.

The functional impact of the under and over frequency on the process (on fluid system) should be analysed by the responsible technical groups.

b) Harmonics

The operation of the Electrical Power System shall not be disturbed by harmonics (e.g. risk of spurious operation of overload protection without overload situation).

The effects of harmonics generated by the grid or plant equipment and their propagations should be evaluated and appropriate measures should then be taken.

B.2.2.4 Electrical source transfer

The set limit of the parameters and time delay in order to ensure the re-supply by the power source of the next level of defence should be defined.

A time delay prior to disconnection should be considered to allow the system to ride through minor disturbances.

The design of the electrical source transfer should be determined following two possibilities:

- slow transfer;
- fast transfer.

In case of slow transfer, a time delay prior to reconnection should be considered to allow the system to perform the restart the loads. The time delay and reconnection type (manual or automatic connection) should be supported by the results of the accident analyses.

Each division should have an independent scheme for detection and protection to disconnect the safety buses from the preferred power supply, to shed loads from the safety buses and to start the standby power sources in the event of degradation in voltage, degradation in frequency or loss of voltage.

B.3 Design of the Interruptible power system

B.3.1 Design of the preferred power supply

The preferred power supply consists of:

- the off-site part
 - the main off-site power supply consisting of the main transmission system (grid) and its associated switchyard;
 - the standby off-site power supply consisting of the standby grid and its associated switchyard;
- the on-site part:
 - the Unit Transformer and the Auxiliary Transformer(s) connected to the main off-site power supply;
 - the Standby Transformer(s) connected to the standby off-site power supply;
 - the distribution system up to the interruptible power supply system(s) important to safety;
 - the main generator and its associated circuit breaker, if a houseload operation capability is provided.

B.3.2 Design of the off-site power supply

The off-site power system consists of the transmission system (grid) and switchyard connecting the plant with the grid.

The off-site power system should normally provide AC power to the plant in all modes of operation and in all plant states (during power operation, the supply is from the main generator).

It should also provide transmission lines for outgoing power. The boundary between on-site and off-site power systems should be agreed between the electric grid operator and plant operators.

Similarly, large nuclear units with a fast turbine governor and generator excitation systems can enhance robustness to a grid system.

Good functional integration by design and good operational coordination between the grid and nuclear power plant operators during major operating changes either on the grid or at the nuclear power plant are important requirements for the safe and reliable operation of both the grid and the plant.

The physical design of the switchyard should be such as to reduce the possibility that a single equipment failure will cause the failure of off-site circuits.

Electrical power from the transmission network to the on-site electrical distribution system should be supplied by two physically independent circuits (not necessarily on separate rights of way) designed and located so as to reduce the likelihood of their simultaneous failure under operating and postulated accident and environmental conditions.

The standby off-site power supply should be:

- ready for operation;
- capable of being switched on automatically in case of failure of the power supply through the auxiliary transformer(s).

The risk of CCF should be reduced in the grid sub-station by the following:

- where off-site power supplies are shared between multiple units at a multi-unit plant, the ability to disconnect a unit should not affect the availability of the off-site supply to any other units.
- two supplies should not share the same control power supplies.
- the switchyard control power should be unique to the switchyard and should not be fed from the power supplies of the nuclear power plant.

Transient stability studies should be conducted to investigate the transient behaviour of the NPP generator after disturbances on the electrical network in the vicinity of the plant.

The study should determine the capability of the generator to remain connected to the grid and the effects of the transient on the unit electrical power supply system.

The off-site power system design shall satisfy the nuclear safety criteria established in national and international standards, the grid code and electrical design criteria (as stipulated by national electrical codes).

B.3.3 Design of on-site preferred power supply

The physical design of the on-site preferred power supply should be such as to reduce the possibility of a single equipment failure causing the failure of all circuits (main and standby power supplies) supplying loads important to safety.

The standby on-site preferred power supply should be:

- ready for operation;
- capable of being switched on automatically in case of failure of the power supply through the auxiliary transformer(s).

The preferred power supply system and the interruptible power supply system important to safety should be designed such that, on demand from the I&C system, they are automatically disconnected from each other.

B.3.4 Design of the AC interruptible power systems important to safety

The AC on-site power system consists of distribution systems and power supplies within the plant.

Stand-alone power supplies, such as separate power supplies for security systems, are not covered by this standard.

B.3.5 Design of internal standby sources

The design of internal stand-by sources (number of sources, technology) shall be based on:

- the sources' actuation time, operating time and capacity requirements (functional requirements);
- the reliability required for internal stand by sources (safety requirements).

- the operating time and capacity should be based on:
 - regulatory requirements;
 - mission time of the supplied loads;
 - time to re-establish the power supply of the upstream source;
 - required plant fuel capacity for the long term management.

The voltage of the internal sources should enable connection to the AC interruptible networks.

B.4 Preferred power supply system (from IAEA SSG 34:2016, chapter 6, clauses 6.1 to 6.44)

B.4.1 General

The functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances or degraded conditions in the electrical power grid, including anticipated variations in the voltage and frequency of the grid supply.

B.4.2 Operation

The preferred power supply to the safety power systems is the supply from the grid. In power operation, the power supply is normally from the main generator, connected to the grid. The generator will act as a stabilizer against voltage variations on the grid and can power the on-site power systems during house load operation.

B.4.3 Grid interface and agreement with grid operator

The transmission system should be able:

- To supply the nuclear power plant with power during start-up, during shutdown and during emergencies in a stable and continuous way;
- To dispatch the energy from the nuclear power plant in a stable and continuous way.

This applies also after anticipated grid events when the plant remains connected to the grid.

The preferred power supply could also come from a separate connection to the grid. In order to reduce the risk for common cause failure caused by events on the grid, the switchyard or the main generator, it could be investigated whether the different divisions of the electrical power systems of the nuclear power plant could be connected to different preferred power supplies without a significantly increased risk of undue trips and other disturbances.

An agreement shall be established for the restoration of the off-site power supply with a high priority after a grid failure or blackout. A re-supply plan should be established describing how to do this restoration.

B.4.4 Reliability of the preferred power supply

The design of the connection to the grid, the control circuits and the relay protection should be of high quality and should contribute to a reliable preferred power supply.

Events to be considered in the design of the grid connection and the relay protection include:

- Anticipated electrical events including loss of load and out of step scenarios;
- Anticipated electrical events during shutdown;
- Pollution of outdoor equipment;
- Geomagnetic storms;

- Winding to winding faults in transformers and open phase condition.

In areas with a high risk of pollution, an increased length of insulator may be necessary to ensure that insulator contamination does not pose a risk of common cause failure of off-site supplies.

B.4.5 Off-site power supplies

The off-site power supply should have adequate capability to power plant loads in all modes of the nuclear power plant's operation.

It should be noted that voltage levels on the grid could be different when the plant is in shutdown mode.

The transmission system is the source of power to the on-site power system.

The transmission system is also a significant contributor to Defence in Depth for the plant's safety design. The provisions for safe shutdown of a nuclear power plant in transients and accidents, as well as normal shutdown, are more flexible and more reliable if off-site power is available. The power supply should therefore have adequate capability.

Off-site power should be supplied by two or more physically independent off-site supplies that are designed and located to reduce, to the extent practicable, the likelihood of their simultaneous failure.

The total number of transmission line connections to the electrical grid will depend on the capabilities of the entire grid and on the design of the nuclear power plant.

A single transmission line for each off-site power supply may be acceptable if the safety analysis report shows that this arrangement achieves the technical safety objectives

For example, a single off-site power supply might be acceptable for reactors of a design that employs passive engineered safety features.

Nuclear power plants with a single transmission line might have a forced outage rate that is higher owing to line tripping. This should be taken into consideration, in particular in areas where the frequency of lightning strikes on the line is high. In such cases, the nuclear power plant may prematurely reach design thermal stress cycles unless the plant is designed to withstand the effects of the forced outages or unless measures are taken to reduce the number of forced outages, such as by provisions of additional transmission lines and a greater level of protection.

As a minimum, each off-site power supply should have the capability to power all electrical loads required to mitigate the consequences of all design basis accidents and anticipated operational occurrences.

Each off-site power supply required for normal plant operation, start-up and shutdown should have the additional capability to power all the normal electrical loads.

At multi-unit plants, each unit should be connected to two off-site power supplies such that the technical safety objectives are fulfilled simultaneously for all units. The off-site power supplies, provided to meet the recommendation may be shared among two or more plants or units, or they may have separately dedicated circuits.

For multi-unit plants, a single off-site power supply may be acceptable for some reactor designs if it is shown in the safety analyses report that one off-site power connection is sufficient.

Where off-site power supplies are shared between multiple units at a multi-unit plant, the ability to disconnect a unit should not affect the availability of the off-site supply to any other units.

B.4.6 Availability

For NPPs that credit off-site power source in safety analysis, a minimum of one off-site circuit should be designed to be automatically available to provide power to its associated safety divisions within a few seconds in a design basis accident to be able to meet the requirements for accident analysis.

A second off-site circuit should be designed to be available within a short period of time.

The second circuit should preferably also be available within a few seconds in a design basis accident.

The transfer system for the auxiliary loads should be evaluated against the safety requirements for the design.

The transfer to the second circuit, both manually and automatically, should be easy to accomplish.

The transfer capability should only be used when necessary as switching between two live circuits could pose risks.

It is preferred to energize from the secondary circuit after a loss of voltage from the primary circuit. Interlocks between breakers may be used to preclude setting circuits in parallel that could result in adverse voltage or current conditions on common buses.

Variations in voltage and in-rush currents during the transfer should be considered in the design of the transfer sequence.

The more reliable power supply should be selected for use in normal operation of the plant.

Selection of the most reliable power supply for normal operation of the plant reduces the transfer demands on switchgear.

Some nuclear power plants are designed for load rejection on separation from the transmission lines, and for the subsequent reduction of the reactor output and the generator power output to levels sufficient to meet the needs of the disconnected plant for electrical power (the house load) without tripping the steam supply or tripping the turbo generator. This transfer to house load operation will result in frequency excursions and voltage excursions before stable operation is achieved.

In plants designed for house load operation, the on-site power system should be designed to accommodate the variations and transients of voltage and frequency from the generator when transferring from the normal source of supply to house load operation.

A generator circuit breaker may be used as a provision to power the on-site AC power systems immediately from the off-site circuits following the tripping of a main generator. Generator load break switches can be used for this purpose, but the switchover will not be immediate.

B.4.7 Independence of off-site circuits

Two off-site circuits should be designed and located to reduce, to the extent practicable, the likelihood of their simultaneous failure under all plant conditions and in design basis environmental conditions.

Examples of events that could cause simultaneous failure of both off-site circuits include:

- The use of a common take-off structure for both off-site circuits;
- Failure of a single breaker, switchyard bus cable or control power supply that could cause failure of both off-site circuits.

B.4.8 Switchyard

The physical design of the switchyard should be such as to reduce the possibility that a single equipment failure will cause the failure of off-site circuits that are credited with supplying loads important to safety.

At least two supplies should not share the same control power source.

The switchyard control power should be unique to the switchyard and should not be fed from the power supplies of the nuclear power plant.

Control circuits to outdoor switchyards should be equipped with overvoltage protection where they enter the plant and should be isolated from the control circuits inside the plant.

Switchyard equipment should be designed to withstand the stresses of worst case faults.

Electrical Protection Systems should reduce the probability of failure of all off-site circuits that are credited with supplying loads important to safety.

Design features suggested for consideration include:

- Primary and backup relay systems;
- Breaker failure relaying;
- Dual battery systems;
- Dual breaker trip coils.

B.5 Safety power supply system supporting DBC

B.5.1 General

The design of the nuclear power plant shall include a safety power supply capable of supplying the necessary power in anticipated operational occurrences and design basis accidents, in the event of a loss of off-site power.

The on-site power supply considered hereunder is delivered by a standalone generator set with:

- A standalone starting system;
- Mechanical auxiliaries for operation or standby;
- Storage tanks, among them a fuel storage tank and service tank;
- Speed and voltage control;
- Electrical and mechanical protections;
- Control equipment;
- A device allowing full load test is also part of the arrangement.

The mechanical auxiliaries for operation or standby mode for a diesel engine are:

- Cooling system;
- Air intake system;
- Exhaust gas system;
- Lubrication oil system;
- Conditioning system (pre heating, pre-lubrication).

In the absence of IEC/SC 45A dedicated standard the following clauses shall be applied.

B.5.2 Design (from IAEA SSG 34:2016, chapter 7, clauses 7.36 to 7.63)

Standby AC power sources should consist of an electrical power generating unit complete with all auxiliaries and a dedicated separate and independent stored energy supply for both starting and running the prime mover.

The preferred approach is to have only one standby power source per division, avoiding the necessity of parallel operation of generators.

If multiple power sources per division are used, it should be demonstrated that this is a reliable configuration.

The standby power source should have sufficient capacity and capability to start and to continuously supply all loads in its division under the full range of conditions, including allowances for conditions such as:

- Loads that might operate at run-out conditions;
- Loads that might operate in an overload condition;
- Changes in load characteristics due to generator operation at the lower end or upper end of the allowable voltage and frequency ranges;
- Engine derating due to, for example, the higher temperature of the intake air, environmental conditions or the fuel temperature;
- Future load growth.

Diesel generators are specified to operate at a fixed voltage and frequency in the emergency mode of operation. In general, the steady state voltage and frequency are maintained within an allowable tolerance of $\pm 2\%$ relative to the specified value. When electric motors are subjected to voltages below their nominal rating, some of the characteristics will change slightly and the power consumption will increase.

The continuous rating of the standby source prime mover preferably allows 3 000 h to 4 000 h of continuous operation without major overhaul.

A 10 % to 15 % overload capacity for a minimum of 2 h in a 24 h period is typically provided. This provides assurance that the power source can handle the short time loading at the onset of an event when systems of engineered safety features are realigning for injection or cooling system operation and their pumps are operating in run-out conditions or with a higher flow than is assumed in thermohydraulic analyses. The thermohydraulic analyses are normally conservative in such a manner that the expected power consumption of motors could be underestimated.

The capability of motor driven pumps to deliver required flows should be evaluated for generator operation at the lower end of the frequency range.

A variation in frequency affects the torque developed by motors.

It should be demonstrated that the standby power source could operate continuously for the required time period set out in the design bases without any stops for maintenance activities.

The standby AC power source should have an automatic start on loss of preferred power supply to the essential buses.

The standby AC power source may also have an automatic start on actuation of an emergency signal (without loss of power to the safety bus).

The times to start the standby AC power source and to connect loads to this source should be consistent with the assumptions on start-up time made in the safety analysis.

On-site sources of fuel and other consumables (such as lubricating oil) should be sufficient to operate the standby power sources until the off-site power supply can be restored.

Off-site sources of fuel and other consumables may be depended on if sources of replenishment are identified and if on-site sources are sufficient for the time required to replenish supplies. In most States, on-site sources are sized for one to two weeks of operation without replenishment from external sources.

Standby power sources should be independent of electrical power sources and power sources for instrumentation and control systems, other than those sources in their own division.

Instrumentation and control systems used for the starting, coupling, running and protection of a standby power source should be supplied by batteries within their own division.

Loss of the DC power source within the same division as the standby power source could lead to unavailability of the standby AC power source, but it would also cause loss of other functions in the division, thus making the standby AC supply in that division inoperable.

When batteries specifically dedicated to the standby power source are used, they should be subject to adequate surveillance to detect deterioration and failure, to the same extent as for any safety system battery.

Standby power sources should only be used for the period of time necessary to reconnect to reliable and stable preferred or alternative power supplies.

The use of standby power sources for peaking generation should not be allowed.

The Electrical Power System important to safety may supply loads of lower safety classification (including loads not important to safety) provided that the independence requirements of this Safety Guide are met.

Equipment that is not safety classified should be automatically disconnected on an accident signal.

If the load is not disconnected, it has to be taken into account in the balance of the safety system.

The isolation devices between a safety power system and equipment of lower safety classification should be part of the safety system.

The load sequencer should automatically shed all the non-safety loads and should not automatically start non-safety loads.

The load sequencer should only permit the start of non-safety loads after safety loads have been started and it has been determined that there is enough capacity for start and operation of the non-safety loads.

Transfer of a safety power system bus from its standby AC source to a preferred power supply should require manual action.

When multiple safety power divisions are transferred from their standby power source to preferred power supplies, only one division should be transferred at a time.

After a safety division is returned to the preferred power supply, the associated standby AC power source should be made operable in normal standby conditions before transferring another division to the preferred power supply.

B.5.3 Testing (from IAEA SSG 34:2016, chapter 7, clauses 7.64 to 7.67)

Provisions should be provided for the periodic testing of standby power sources during plant operation.

The design of the test provisions should ensure that the standby power source can continue to perform its safety function during testing.

Arrangements for testing should neither compromise the independence of systems important to safety nor introduce the potential for common cause failures.

Examples of testing that either compromises the independence of systems important to safety or introduces the potential for common cause failures are the formation of soot in diesels being tested under no-load conditions, inadequate provision for restoring to normal standby conditions after completion of the test or the introduction of human errors when testing redundant equipment.

B.5.4 Performance criteria (transient and dynamic) (from IAEA SSG 34:2016, chapter 7, clauses 7.68 to 7.70)

The variations in voltage and frequency in power supplied from the standby AC power source should be shown to be within the design basis of the connected loads and the prime mover.

It is expected that voltage and frequency variations will remain within the range for continuous operation. Deviations outside the range during the loading sequence and for short time periods are permitted, provided that the voltage and frequency are restored well before the next load is connected and that the voltage on the motor terminals is sufficient for starting of the loads in each sequential step.

The performance of the standby power source during sequential loading, with continuous loads that would only occur in accident conditions, is usually determined by a mixture of testing and analyses.

B.5.5 Relay protection of standby power sources (from IAEA SSG 34:2016, chapter 7, clauses 7.71 to 7.75)

Trip devices that protect the power supply from a standby power source against immediate catastrophic failure should be in service in all modes of operation of standby power sources.

Examples of such devices include those that:

- Protect the standby power source from catastrophic failures, such as overspeed protection and generator differential protection;
- Protect the power system important to safety from catastrophic failures, such as backup overcurrent protection and low impedance to ground fault protection.

Trip devices that protect the standby power source from non-catastrophic failures should be bypassed when the standby power source is supplying safety loads during emergency operation, but should be in service during normal operation and testing.

The design should provide for individual testing of each trip function and bypass function.

All protection trip actuations for the standby power source should be annunciated in the main control room.

B.5.6 Support systems for standby AC power sources

Support system equipment (e.g. ventilation systems, cooling water pumps and lubrication systems) for redundant division of the standby power sources should be supplied with power from the division it serves in order to preserve the redundancy and independence of the divisions.

The auxiliary systems and support systems of standby AC power sources should be sized for multiple starts.

Starting systems typically have the capacity to support at least five starts.

In order to support this, it is usually necessary to abort any starting attempt after a specified time to preserve resources.

B.5.7 Fuel for standby AC power sources

It should be shown that fuel for standby AC power sources can be stored for long periods.

Fuel oil at a nuclear power plant is stored for extended periods. Some types of fuel are chemically unstable when stored for long periods. Fuel ageing and oxidation can lead to high acid content, high viscosity, and the formation of gums and sediments, which can clog filters. Degradation in fuel quality could cause a common cause failure of the standby AC power sources.

Every fuel delivery should be tested to verify that it meets specifications.

Samples for the testing of fuel will usually be taken on site.

B.6 Power supply system important to safety supporting DEC

B.6.1 General

The design shall include an alternate power source to supply the necessary power in design extension conditions.

In the absence of IEC/SC 45A dedicated standard the following clauses shall be applied.

B.6.2 Design (from IAEA SSG 34:2016, chapter 8, clauses 8.1 to 8.18)

An alternate AC power supply should be provided at or near the nuclear power plant if the plant's design depends on AC power to bring the plant to a controlled state following loss of off-site power and safety standby power sources.

Alternate AC power supplies, including necessary connecting points, are provided to protect electrical power systems against the simultaneous failure of off-site and safety stand-by AC power supplies. This needs AC power sources that are diverse in design and are not susceptible to the events that caused the loss of on-site and off-site power sources.

The alternate AC power supplies with auxiliaries should be qualified for their intended application.

Alternate AC power supplies should have sufficient capacity to operate systems necessary for coping with a station blackout for the time required to bring the plant to a controlled state and to maintain it in a controlled state.

If an alternate AC power source serves more than one unit at a site where safety standby AC power sources are shared between units, the alternate AC power source should have sufficient capacity to operate systems necessary for coping with a station blackout for the time required to bring all units that share the safety AC power sources to a controlled state and to maintain them in a controlled state.

The alternate AC power source for one unit should not normally be connected to the on-site power system of that unit.

Support systems that maintain the alternate AC power source in readiness may be powered from one or more units, provided that this does not affect the operability of the alternate AC power source.

There should be a minimum potential for common cause failure of any safety standby AC power source and the alternate AC power source.

No single point of vulnerability should exist whereby a weather related event, another external event or a single failure could disable any of a unit's safety standby AC power supplies and simultaneously cause the failure of all off-site power supplies and the alternate AC power supplies.

Provision should be made for connecting the alternate AC power supply to one or more safety power system divisions.

The safety power systems should be fed from the alternate AC power supply only after it has been disconnected from other power supplies.

Alternate AC power supplies should be capable of supplying the required loads within the time specified in the plant safety analysis and the plant station blackout coping analysis.

It is preferable that the alternate AC power supplies will be capable of supplying loads as soon as is practicable. Restoring AC power as soon as possible after a station blackout restores a degree of Defence in Depth to the electrical power systems, restores safety systems that depend on AC power and restores support systems (e.g. lighting systems and habitability systems) that significantly enhance the ability of the operators to respond to an event.

The alternate AC power supply may also have the capability to power loads necessary in design extension conditions.

The plant design should include the necessary features to enable the safe use of non-permanent power sources to restore the necessary electrical power supply.

Equipment necessary to mitigate the consequences of a core melt accident should be able to be supplied by any of the power sources.

B.7 Mobile sources connections network

The delay of connection of this mobile power supply source shall be consistent with:

- The maximum autonomy of the severe accident uninterruptible power supply source;
- The maximum delay of operation for severe accident functions supplied by AC interruptible power system.

The mobile power supply sources shall have the following characteristics as regards to the scenario:

- Protected against the consequences of the scenario taken into account;
- Standalone equipment for a predefined mission time;
- Suitable time of connection and transportation;
- Accessible, standardized and robust connection;
- Suitable location for the mobile source;
- Interlocking within the Electrical Power System in order to prevent wrong configuration;
- Suitable setting of the protection as regards to the source design to meet the electrical coordination (voltage, current, frequency).

B.8 Monitoring and switching of buses

Degradation of the preferred power supply of each safety power system bus (i.e. overvoltage, undervoltage, over frequency and under frequency) should be detected on the buses of the safety AC power systems.

Buses affected by degradation of the preferred power supply should be automatically disconnected from their power source if the degradation exceeds the levels specified in the design requirements.

After a bus is disconnected from a preferred power supply that has been degraded, the bus should automatically be connected directly to sources in the following order:

- The alternative off-site power source (part of preferred power supply);
- The standby power source for that division of the safety power system;
- Alternate AC power source.

A time delay may be associated with the disconnection to allow the system to ride through minor disturbances.

The time delay should be supported by the assumptions made in the accident analyses.

It is preferred that two breakers be provided to disconnect each preferred power supply feed to a safety system bus.

If automatic connection to the alternative preferred power supply is not used, it should be shown that this arrangement is in accordance with the design criteria of the plant.

The parameters of the power systems important to safety— including the availabilities claimed in the design analysis — that are relevant to the safe operation of the plant in operational states and under design basis accident conditions should be identified and used in the establishment of operational limits and conditions for the plant.

Each division should have an independent scheme for detection and protection to disconnect the safety buses from the preferred power supply, to shed loads from the safety buses and to start the standby power sources in the event of degradation in voltage, degradation in frequency or loss of voltage.

The following recommendations do not apply to voltage monitoring that is used only for alarms and apply to bus voltage and frequency monitoring and protection schemes for protection against degradation in voltage, degradation in frequency or loss of voltage:

- Bus voltage and frequency should be detected directly from the safety system buses to which the standby power sources are to be connected.
- Degradation in voltage or frequency should be alarmed in the main control room.
- Degradation in voltage or frequency to below acceptable limits should automatically disconnect the affected supply from the safety buses.
 - Two levels of voltage protection with different time delays are necessary: one level to detect loss of off-site power at the safety buses; and a second level to detect degradation in voltage.
- On sensing unacceptably high voltage on a preferred power supply, the affected preferred power supply should be automatically disconnected from the safety system buses:
 - The set point and time delay should be coordinated with the overvoltage capability of connected equipment.
 - The reset value of the monitoring equipment should be lower than the lowest anticipated operating range of voltage of the standby supply.
- Each scheme should monitor all three phases.
- Measuring circuits should be immune to harmonics.
- The protection system design should be redundant.
- Failures in the measuring circuits should not cause incorrect operation or prevent correct operation of the monitoring and protection scheme.
- The design should reduce the risk of unwanted disconnection of the preferred power supply.
 - The use of coincident logic and time delays to override transient conditions is a way to reduce the risk of unwanted disconnection.
- A capability should be provided for testing and calibration during power operation.
 - Indications should be provided in the main control room for any bypasses incorporated into the design.

The undervoltage and time delay set points for degraded voltage protection should be determined on the basis of an analysis of the voltage requirements of the loads important to safety at all on-site distribution system levels.

Improper voltage protection logic can cause adverse effects on the systems important to safety and equipment, such as spurious shedding of loads important to safety from the standby power sources and spurious separation of systems important to safety from off-site power as a result of normal motor starting transients.

Annex C (informative)

Earthing

Earthing system serves to ensure:

- people electrical safety,
- functionality of Electrical power systems and instrumentation and control systems,
- prevention of fire or explosion caused by electrostatic phenomena.

These functions have to be fulfilled in normal configuration, in case of electric default and in case of lightning strikes.

Detailed design guidelines for earthing are available in national and international standards.

In nuclear power generating plant, the design may be more challenged than in other installations because of:

- the powerful electric default current,
- the electric source of EMI,
- the hazard studies guidelines , in particular lightning, EMI, fire, explosion.

Thus the conception of the earthing system need particular studies and some of them may be important for safety.

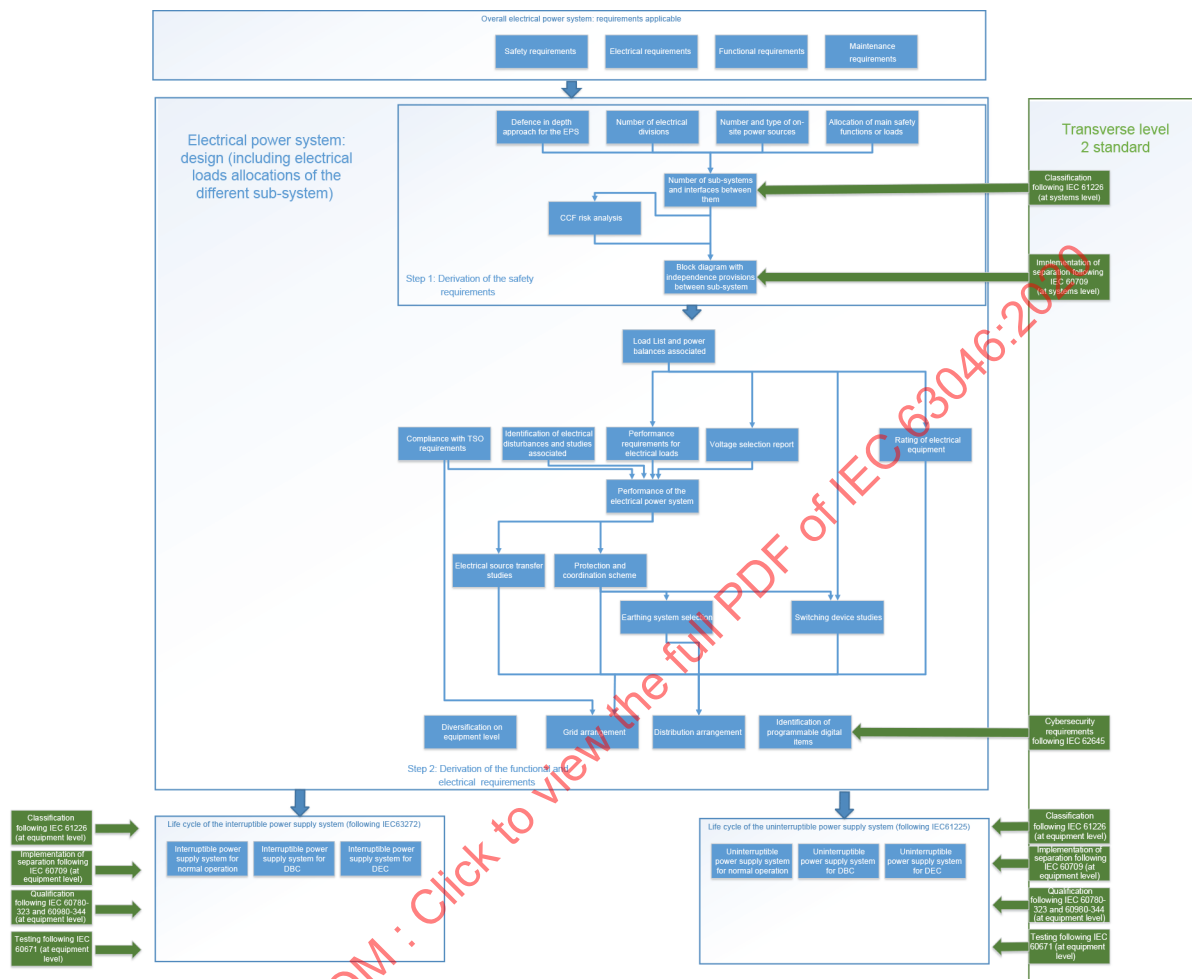
The earthing system may be made of:

- **An earthing network** which contributes to general site equipotentiality and also used to remove interfering currents to earth. It is designed to protect individuals (step and touch voltages) and equipment when removing an HVB (external high voltage system) short circuit or lightning strike current. It is also used to earth the fences. It has to be noted that areas housing the step-down, auxiliary and step-up transformers and the switchyard requires a denser buried earthing grid mesh.
- **A Faraday cage.** Buildings and facilities housing safety classified equipment or whose failure would present an environmental hazard are protected against the effects of lightning strikes (current transmission) by a Faraday cage. It captures the electrical charge, channels it and discharges it to earth via the most direct route. The Faraday cages are connected to the buried earthing grid at the external boundary of the buildings. The Faraday cage also lessens the lightning impulse magnetic field.
- **Equipotential bonding network** which covers additional measures, to cope with the fault current of the internal electrical circuit default and to reduce the electromagnetic coupling inside the buildings and also the electromagnetic effects of lightning currents within the volume to be protected. This network is connected to the equipment exposed conductive parts and the extraneous conductive part.

These measures should be coordinated with requirements in cabling domain (IEC 60709), EMC domain (IEC 62003) to cover additional requirements of electromagnetic compatibility for installations, which reduce the electromagnetic effects caused by lightning and other interference sources.

Annex D (informative)

Logic diagram followed for the design of the EPS



Bibliography

IEC 60034 (all parts), *Rotating electrical machines*

IEC 60050-692:2017, *International Electrotechnical Vocabulary (IEV) – Part 692: Generation, transmission and distribution of electrical energy – Dependability and quality of service of electric power systems*

IEC 60364 (all parts), *Low-voltage electrical installations*

IEC 60364-5-52, *Low-voltage electrical installations – Part 5-52: Selection and erection of electrical equipment – Wiring systems*

IEC 60479 (all parts), *Effects of current on human beings and livestock*

IEC 60880, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions*

IEC 60909 (all parts), *Short-circuit currents in three-phase a.c. systems*

IEC 61000 (all parts), *Electromagnetic compatibility (EMC)*

IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61660 (all parts), *Short-circuit currents in DC Auxiliary installations in power plants and substations*

IEC 61936 (all parts), *Power installations exceeding 1 kV a.c.*

IEC 62003, *Nuclear power plants – Instrumentation, control and electrical power systems – Requirements for electromagnetic compatibility testing*

IEC 62040-3, *Uninterruptible power systems (UPS) – Part 3: Method of specifying the performance and test requirements*

IEC 62138, *Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category B or C functions*

IEC 62271-200, *High-voltage switchgear and controlgear – Part 200: AC metal-enclosed switchgear and controlgear for rated voltages above 1 kV and up to and including 52 kV*

IEC 62305 (all parts), *Protection against lightning*

IEC 62305-1, *Protection against lightning – Part 1: General principles*

IEC 62305-3, *Protection against lightning – Part 3: Physical damage to structures and life hazard*

IEC 62305-4, *Protection against lightning – Part 4: Electrical and electronic systems within structures*

IEC 62340, *Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coping with common cause failure (CCF)*

IEC 62342, *Nuclear power plants – Instrumentation and control systems important to safety – Management of ageing*

IEC 62443 (all parts), *Industrial communication networks – Network and system security*

IEC 62566, *Nuclear power plants – Instrumentation and control important to safety – Development of HDL-programmed integrated circuits for systems performing category A functions*

IEC 62645, *Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements*

IEC 62859, *Nuclear power plants – Instrumentation and control systems – Requirements for coordinating safety and cybersecurity*

ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*

ISO 9000:2015, *Quality management systems – Fundamentals and vocabulary*

IAEA Safety Guide GS-G-3.5:2009, *Management system for nuclear installations*

IAEA Safety Standard Series SSR-2/1:2016, *Safety of Nuclear Power Plant: Design*

IAEA Safety Guide SSG-30, *Safety classification of structures, systems and components in Nuclear Power Plants*

IAEA Safety Guide SSG-39:2016, *Design of instrumentation and control systems in Nuclear Power Plants*

IAEA Nuclear Security Series 17, Reference Manual, *Computer security at nuclear facilities*

IAEA Safety Glossary:2018, *Terminology used in nuclear safety and radiation protection*

IAEA 75-INSAG-3, *Basic Safety Principles for Nuclear Power Plants*

IAEA Nuclear Energy Series NG-T-3.8, *Electric Grid Reliability and Interface with Nuclear Power Plants*

IAEA Safety Report Series 91, *Impact of Open Phase Conditions on Nuclear Power Plants Electrical Power Supply Systems*

IAEA – TECDOC – 1770, *Design Provisions for Withstanding Station Blackout at Nuclear Power Plants*

IEEE 308-2001: *IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations*

SOMMAIRE

AVANT-PROPOS	92
INTRODUCTION.....	94
1 Domaine d'application	96
1.1 Généralités	96
1.2 Application: nouvelles centrales et centrales existantes	99
1.3 Cadre général	99
1.4 Interaction avec les normes de second niveau	99
2 Références normatives	101
3 Termes et définitions	102
4 Termes abrégés	111
5 Cycle de vie de l'ensemble du système d'alimentation électrique	113
6 Architecture du système d'alimentation électrique: identification des exigences	114
6.1 Objectifs	114
6.2 Exigences de sûreté applicables à la conception de l'architecture électrique	115
6.2.1 Défense en profondeur	115
6.2.2 Application du critère de défaillance unique	115
6.2.3 Gestion des défaillances de cause commune	115
6.2.4 Conditions de perte des sources d'alimentation externe	116
6.2.5 Conditions de manque de tension généralisé	116
6.2.6 Conditions de perte totale des alimentations électriques	116
6.2.7 Prise en compte des agressions internes et externes	116
6.2.8 Exigences de sécurité nucléaire	117
6.2.9 Exigences de classement	117
6.2.10 Exigences probabilistes	117
6.3 Exigences électriques	117
6.3.1 Exigences coordonnées avec le gestionnaire de réseau	117
6.3.2 Perturbations électriques	118
6.4 Exigences fonctionnelles et de performances	119
6.5 Exigences de maintenance	119
7 Conception de l'architecture électrique	119
7.1 Objectifs	119
7.2 Disposition relative à la conception de sûreté	119
7.2.1 Défense en profondeur du système d'alimentation électrique	119
7.2.2 Défaillance unique du système d'alimentation électrique	120
7.2.3 Défaillance de cause commune du système d'alimentation électrique	121
7.2.4 Dispositions pour faire face à la perte des alimentations électriques	127
7.2.5 Dispositions pour faire face au manque de tension généralisé	128
7.2.6 Dispositions visant à éviter ou à réduire la perte totale des alimentations électriques	128
7.2.7 Considérations relatives au classement	129
7.2.8 Dispositions visant à atteindre l'objectif de fiabilité du système d'alimentation électrique	130
7.3 Disposition relative à la conception électrique	130
7.3.1 Généralités	130
7.3.2 Coordination avec le réseau	130
7.3.3 Conception conforme aux exigences électriques	131
7.4 Dispositions fonctionnelles et de performances relatives à la conception	138

7.4.1	Généralités	138
7.4.2	Etudes du système d'alimentation électrique	138
7.4.3	Conception du système d'alimentation électrique interruptible	141
7.4.4	Conception du système d'alimentation électrique sans interruption	141
7.5	Maintenance	141
7.5.1	Considérations relatives à la maintenance lors de la conception électrique	141
7.6	Systèmes d'alimentation électrique partagés sur un site à tranches multiples	143
7.7	Installation du système électrique	143
7.8	Systèmes supports et associés au système d'alimentation électrique	143
7.9	Programmes d'assurance qualité d'ensemble	144
7.10	Exigences relatives à la documentation produite	145
7.10.1	Généralités	145
7.10.2	Principes d'architecture	146
7.10.3	Schémas unifilaires	147
8	Exigences relatives aux sous-systèmes	148
8.1	Exigences du système d'alimentation électrique	148
8.1.1	Généralités	148
8.1.2	Conception du système	148
8.1.3	Schéma unifilaire	148
8.2	Spécification de conception des équipements	148
8.3	Exigences relatives aux équipements	149
8.4	Système d'alimentation électrique interruptible en courant alternatif	149
8.5	Système d'alimentation électrique sans interruption CA/CC	149
8.6	Coordination et interaction avec le réseau électrique	149
8.7	Mise à la terre	149
9	Vérification de l'architecture du système d'alimentation électrique	149
9.1	Généralités	149
9.2	Vérification des modèles et outils informatisés	149
9.2.1	Vérification du système d'alimentation électrique	149
9.2.2	Implantation des systèmes d'alimentation électrique et vérification des équipements	150
9.3	Exigences d'essai	150
10	Intégration et mise en service globales	151
10.1	Généralités	151
10.2	Exigences	152
10.3	Documentation produite	152
11	Exploitation et maintenance d'ensemble	152
11.1	Généralités	152
11.2	Exigences	153
11.3	Documentation produite	153
12	Plan d'assurance qualité système	153
12.1	Généralités	153
12.2	Plan de vérification système	154
12.3	Plan de gestion de configuration système	154
12.4	Procédure de résolution des défauts	155
Annexe A (informative)	Questions de sûreté fondamentales dans les centrales nucléaires	156
A.1	Généralités	156

Conditions de régime établi du système d'alimentation électrique	1
Perturbations électriques	2
Conception du système d'alimentation électrique interruptible	3
Conception de l'alimentation préférentielle	4
Conception de l'alimentation externe	5
Conception de l'alimentation interne préférentielle	6
Conception des systèmes électriques importants pour la sûreté interruptibles en courant alternatif	7
Conception des sources internes de secours	8
Alimentation préférentielle (issu du chapitre 6 de l'AIEA SSG 34:2016, 6.1 6.44)	9
Généralités	10
Exploitation	11
Interface réseau et accord avec le gestionnaire du réseau	12
Fiabilité de l'alimentation préférentielle	13
Sources d'alimentation externes	14
Disponibilité	15
Indépendance des circuits externes	16
Poste	17
Système électrique de sûreté prenant en charge les DBC	18
Généralités	19
Conception (issu du chapitre 7 de l'AIEA SSG 34:2016, 7.36 à 7.63)	20
Essais (issu du chapitre 7 de l'AIEA SSG 34:2016, 7.64 à 7.67)	21
Critères de performances (transitoires et dynamiques) (issu du chapitre 7 de l'AIEA SSG 34:2016, 7.68 à 7.70)	22
Protection par relais des sources de secours (issu du chapitre 7 de	23

Figure 1 – Domaine d'application du présent document	98
Figure 2 – Architecture du système d'alimentation électrique	100
Figure 3 – Liens entre le cycle de vie de l'ensemble du système d'alimentation électrique et les cycles de vie des sous-systèmes d'alimentation électrique	114
Figure 4 – Bases de conception de la tension classique (IEC 62855)	134
 Tableau A.1 – Appui du système d'alimentation électrique pour la défense en profondeur	 159

IECNORM.COM : Click to view the full PDF of IEC 63046:2020

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈME D'ALIMENTATION ÉLECTRIQUE – EXIGENCES GÉNÉRALES

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 63046 a été établie par le sous-comité 45A: Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des installations nucléaires, du comité d'études 45 de l'IEC: Instrumentation nucléaire.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
45A/1348/FDIS	45A/1355/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "<http://webstore.iec.ch>" dans les données relatives au document recherché. A cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "*colour inside*" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 63046:2020

INTRODUCTION

a) Contexte technique, questions importantes et structure de la présente norme

L'objectif de la présente norme est de fournir une spécification et des exigences de haut niveau pour la mise en œuvre d'un système d'alimentation électrique approprié dans une centrale nucléaire de puissance (CNP).

Dans une CNP, le système d'alimentation électrique est le support des systèmes importants pour la sûreté des réacteurs. Il permet également la production d'énergie électrique, fournissant la puissance active et réactive et l'inertie électromécanique au réseau de transport.

Le présent document peut être utilisé par les concepteurs, les exploitants de centrales nucléaires, les évaluateurs de systèmes et les régulateurs.

b) Position de la présente norme dans la série de normes du SC 45A de l'IEC

Il convient que le point d'entrée de la série de normes du SC 45A de l'IEC soit un rapport de synthèse introduisant les deux normes de premier niveau : pour l'I&C (IEC 61513) et pour le système d'alimentation électrique (IEC 63046).

La présente norme est le document du SC 45A de l'IEC de premier niveau qui traite des exigences générales pour le système d'alimentation électrique et ses sous-systèmes.

Pour plus d'informations sur la série de normes du SC 45A de l'IEC, se référer au point d) de la présente introduction.

c) Recommandations et limites relatives à l'application de présente norme

Il est important de noter que la présente norme n'établit pas d'exigence fonctionnelle supplémentaire pour les systèmes de sûreté.

Afin d'assurer la pertinence de la présente norme pour les années à venir, l'accent est mis sur les questions de principes plutôt que sur les technologies particulières.

d) Description de la structure de la série de normes du SC 45A de l'IEC et relations avec d'autres documents de l'IEC et d'autres organisations (AIEA, ISO)

Les documents de niveau supérieur de la série de normes du SC 45A de l'IEC sont les normes IEC 61513 et IEC 63046. La norme IEC 61513 traite des exigences générales relatives aux systèmes et équipements d'instrumentation et de contrôle-commande (systèmes d'I&C) utilisés pour accomplir les fonctions importantes pour la sûreté des centrales nucléaires. La norme IEC 63046 traite des exigences générales relatives aux systèmes d'alimentation électrique des centrales nucléaires; elle couvre les systèmes d'alimentation électrique, y compris les alimentations des systèmes d'I&C. Les normes IEC 61513 et IEC 63046 doivent être considérées ensemble et au même niveau. Les normes IEC 61513 et IEC 63046 structurent la série de normes du SC 45A de l'IEC et forment un cadre complet établissant les exigences générales relatives aux systèmes d'I&C et électriques des centrales nucléaires de puissance.

Les normes IEC 61513 et IEC 63046 font directement référence aux autres normes du SC 45A de l'IEC traitant de sujets génériques, tels que la catégorisation des fonctions et le classement des systèmes, la qualification, la séparation des systèmes, la défense contre les défaillances de cause commune, la conception des salles de commande, la compatibilité électromagnétique, la cybersécurité, les aspects logiciels et matériels relatifs aux systèmes numériques programmables, la coordination des exigences de sûreté et de sécurité et la gestion du vieillissement. Il convient de considérer que ces normes de second niveau forment, avec les normes IEC 61513 et IEC 63046, un ensemble documentaire cohérent.

Au troisième niveau, les normes du SC 45A de l'IEC, qui ne sont pas référencées directement par les normes IEC 61513 ou IEC 63046, sont relatives à des matériels particuliers, à des méthodes ou à des activités spécifiques. Généralement, ces documents, qui font référence aux documents de deuxième niveau pour les activités génériques, peuvent être utilisés de façon isolée.

Un quatrième niveau qui est une extension de la série de normes du SC 45A de l'IEC correspond aux rapports techniques qui ne sont pas des documents normatifs.

Les normes de la série produite par le SC 45A de l'IEC sont élaborées de façon à être en accord avec les principes de sûreté et de sécurité de haut niveau établis par les normes de sûreté de l'AIEA pertinentes pour les centrales nucléaires, ainsi qu'avec les documents pertinents de la collection de l'AIEA pour la sécurité nucléaire (NSS), en particulier avec le document d'exigences SSR-2/1 qui établit les exigences de sûreté relatives à la conception des centrales nucléaires, avec le guide de sûreté SSG-30 qui traite du classement de sûreté des structures, systèmes et composants des centrales nucléaires, avec le guide de sûreté SSG-39 qui traite de la conception de l'instrumentation et du contrôle commande des centrales nucléaires, avec le guide de sûreté SSG-34 qui traite de la conception des systèmes d'alimentation électrique des centrales nucléaires, et avec le guide de mise en œuvre NSS17 traitant de la sécurité informatique pour les installations nucléaires. La terminologie et les définitions utilisées pour la sûreté et la sécurité dans les normes produites par le SC 45A sont conformes à celles utilisées par l'AIEA.

Les normes IEC 61513 et IEC 63046 ont adopté une présentation similaire à celle de l'IEC 61508, avec un cycle de vie d'ensemble et un cycle de vie des systèmes. Au niveau sûreté nucléaire, les normes IEC 61513 et IEC 63046 sont l'interprétation des exigences générales de l'IEC 61508-1, de l'IEC 61508-2 et de l'IEC 61508-4 pour le secteur nucléaire. Dans ce domaine, l'IEC 60880, l'IEC 62138 et l'IEC 62566 correspondent à la partie 3 de l'IEC 61508 pour le secteur nucléaire.

Les normes IEC 61513 et IEC 63046 font référence aux normes ISO ainsi qu'aux documents AIEA GS-R partie 2 et AIEA GS-G-3.1 et AIEA GS-G-3.5 pour ce qui concerne l'assurance qualité.

Au second niveau, la norme IEC 62645 est le document chapeau du SC 45A de l'IEC portant sur la sécurité nucléaire. Elle est élaborée à partir des principes pertinents de haut niveau des normes ISO/IEC 27001 et 27002; elle les adapte et les complète pour qu'ils deviennent pertinents pour le secteur nucléaire; elle est coordonnée avec la série de normes IEC 62443. Au second niveau, la norme IEC 60964 est le document chapeau des normes du SC 45A de l'IEC portant sur les salles de commande et la norme IEC 62342 est le document chapeau des normes du SC 45A de l'IEC portant sur la gestion du vieillissement.

NOTE 1 Il est admis par hypothèse que pour la conception des systèmes d'I&C qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) des normes nationales ou internationales s'appliquent.

NOTE 2 Le domaine du SC 45A de l'IEC a été étendu en 2013 pour couvrir les systèmes électriques. En 2014 et en 2015 des discussions ont eu lieu au sein du SC 45A de l'IEC pour décider de la façon et de l'endroit pour établir les exigences générales portant sur la conception des systèmes électriques. Les experts du SC 45A de l'IEC ont recommandé que, pour établir des exigences générales pour les systèmes électriques, une norme indépendante soit développée au même niveau que l'IEC 61513. Le projet IEC 63046 a été lancé pour atteindre cet objectif. Comme la norme IEC 63046 est publiée, à partir de maintenant la présente NOTE 2 de l'introduction sera plus intégrée dans les normes nouvellement publiées.

CENTRALES NUCLÉAIRES DE PUISSANCE – SYSTÈME D'ALIMENTATION ÉLECTRIQUE – EXIGENCES GÉNÉRALES

1 Domaine d'application

1.1 Généralités

Le présent document:

- fournit des exigences et des recommandations pour l'ensemble du système d'alimentation électrique. Il couvre en particulier les systèmes d'alimentation électrique interruptibles et sans interruption, y compris les systèmes alimentant les systèmes d'I&C;
- est en conformité et cohérence avec l'IEC 61513. Tout comme l'IEC 61513, le présent document souligne également la nécessité de disposer d'exigences complètes et précises, issues des objectifs de sûreté de la centrale. Ces exigences constituent les conditions préalables à l'établissement des exigences relatives à l'architecture d'ensemble du système d'alimentation électrique, puis à l'établissement de celles portant sur les sous-systèmes d'alimentation électrique;
- est considéré conjointement avec l'IEC 61513 et au même niveau. Ces deux normes fournissent un cadre complet établissant des exigences générales pour les systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique des centrales nucléaires.

Le présent document établit:

- la spécification et les exigences de haut niveau pour la mise en œuvre d'un système d'alimentation électrique approprié dans une CNP, système qui est le support des systèmes importants pour la sûreté des réacteurs. Il permet également la production d'énergie électrique, fournissant la puissance active et réactive et l'inertie électromécanique du réseau de distribution;
- les relations entre:
 - les exigences de sûreté de la centrale et l'architecture de l'ensemble du système d'alimentation électrique et de ses sous-systèmes (voir Figure 1), y compris:
 - a) la contribution à la défense en profondeur de la centrale;
 - b) les dispositions relatives à l'indépendance et à la redondance;
 - les exigences électriques et l'architecture du système d'alimentation électrique et de ses sous-systèmes;
 - les exigences fonctionnelles et l'architecture du système d'alimentation électrique et de ses sous-systèmes;
 - les exigences liées à la stratégie de maintenance et l'architecture du système d'alimentation électrique et de ses sous-systèmes;
- la conception des sous-systèmes d'alimentation électrique (interruptibles et sans interruption, par exemple);
- les exigences relatives aux systèmes supports du système électrique (CVC, I&C, etc.);
- le cycle de vie du système d'alimentation électrique.

Le présent document ne couvre pas la spécification:

- des systèmes d'I&C;
- des lignes de transport raccordées aux postes extérieurs;
- des exigences relatives aux équipements électriques, déjà définies dans les normes IEC industrielles;
- de l'alimentation des systèmes de sécurité (par exemple clôtures, systèmes de surveillance, contrôle d'entrée);
- des éclairages et des prises de courant.

Le présent document ne tient pas compte des exigences de production électrique.

IECNORM.COM : Click to view the full PDF of IEC 63046:2020

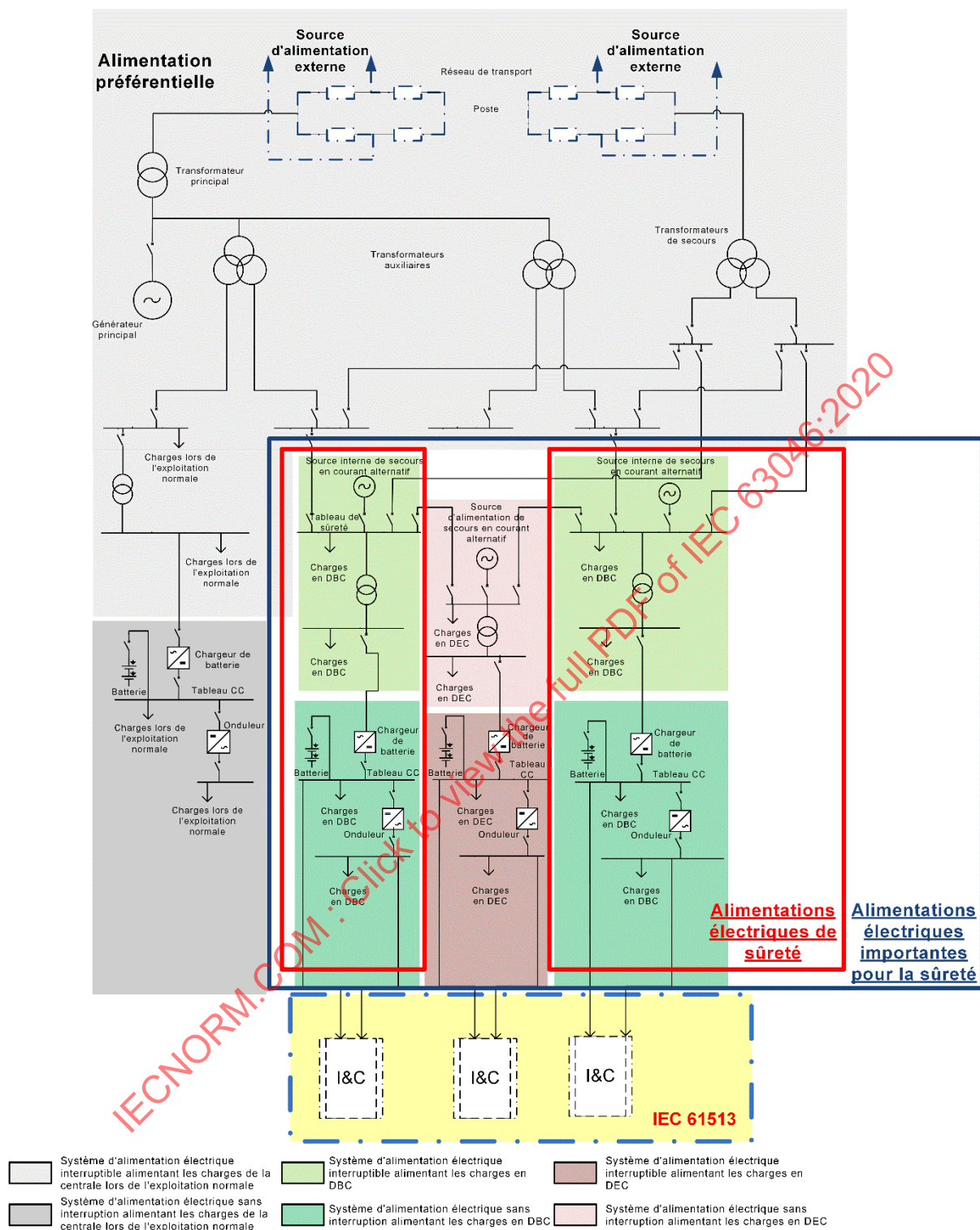


Figure 1 – Domaine d'application du présent document

NOTE La Figure 1 est issue de la figure 3 de l'AIEA SSG-34:2016, adaptée conformément au domaine d'application.

Cette figure fournit seulement un exemple. Différentes dispositions des tableaux, générateurs et branchement peuvent satisfaire aux Prescriptions SSR-2/1 de l'AIEA. De plus, de nombreux éléments du système de la centrale, tels que les tableaux non importants pour la sûreté et les systèmes d'alimentation en courant continu n'apparaissent pas. Le seul objectif de cette figure est de représenter les relations entre les éléments des systèmes de la centrale qui sont du domaine du classement de sûreté et des et du système d'alimentation préférentielle. Les éléments du système d'alimentation préférentielle qui ne sont pas compris dans les limites du système d'alimentation électrique important pour la sûreté sont hors du domaine du classement de sûreté de la centrale. Les éléments système appartenant aux systèmes d'alimentation électrique importants pour la sûreté seront différents suivant la conception de la centrale et les méthodes de classement appliquées par les différents États. Les méthodes de classement sont couvertes par l'IEC 61226. Certaines conceptions de centrale n'exigent pas nécessairement sources de secours internes de sûreté. Toutes les centrales nucléaires de puissance sont supposées avoir des alimentations électriques de sûreté en courant continu.

1.2 Application: nouvelles centrales et centrales existantes

Le présent document s'applique au système d'alimentation électrique des nouvelles centrales nucléaires de puissance ainsi qu'à l'amélioration ou la rénovation des centrales existantes.

Pour les centrales existantes, seul un sous-ensemble des exigences peut être applicable. Il convient de définir ce sous-ensemble au début de chaque projet.

1.3 Cadre général

Le présent document comprend six articles normatifs (dont une vue d'ensemble est fournie par la Figure 2):

- l'Article 6 traite de l'identification des exigences;
- l'Article 7 traite de la conception de l'architecture électrique;
- l'Article 8 traite des exigences relatives aux sous-systèmes;
- l'Article 9 traite de la vérification ;
- l'Article 10 traite de l'intégration et de la mise en service globale ;
- l'Article 11 traite de l'exploitation et de la maintenance d'ensemble.

1.4 Interaction avec les normes de second niveau

Le présent document doit permettre à un concepteur électrique d'établir la liste des exigences applicables à la conception.

Il prévoit également les différentes dispositions applicables aux différentes exigences.

Ces dispositions s'appliqueront aux différents types de réseaux électriques (sous-systèmes):

- alimentation interruptible en courant alternatif;
- alimentation sans interruption.

En outre, d'autres normes transverses de second niveau définiront des exigences applicables à la définition de l'architecture électrique.

Les normes nucléaires liées aux dispositions de sûreté (classement de sûreté, séparation, qualification ou essais de surveillance, etc.) sont vues comme des données d'entrée du présent document.

6 Architecture du système d'alimentation électrique: Identification des exigences		
6.2 Exigences de sûreté	6.3 Exigences électriques	
6.2.1 Défense en profondeur	6.3.1 Exigences coordonnées avec l'opérateur du réseau de transport	
6.2.2 Application de SF	6.3.2 Perturbations électriques	
6.2.3 Gestion des défaillances de cause commune		
6.2.4 Conditions de perte des sources d'alimentations externes	6.4 Exigences fonctionnelles et de performances	
6.2.5 Conditions de perte totale des alimentations électriques		
6.2.6 Conditions de perte d'alimentation électrique	6.5 Exigences de maintenance	
6.2.7 Prise en compte des agressions internes et externes		
6.2.8 Exigences de sécurité nucléaire		
6.2.9 Exigences de classement		
6.2.10 Exigences probabilistes		
7 Architecture globale du système d'alimentation électrique et approche structurée: Conception de l'architecture électrique		
7.2 Disposition relative à la conception de sûreté	7.3 Disposition relative à la conception électrique	7.6 Systèmes d'alimentation électrique partagés à unités multiples
7.2.1 Défense en profondeur du système d'alimentation électrique	7.3.2 Coordination avec le réseau	
7.2.2 SF du système d'alimentation électrique	7.3.3 Conception conforme aux exigences électriques	7.7 Implantation du système électrique
7.2.3 DCC du système d'alimentation électrique		
7.2.4 Dispositions pour faire face à la perte des alimentations externes	7.4 Dispositions fonctionnelles et de performances relatives à la conception	7.8 Systèmes supports et associés au système d'alimentation électrique
7.2.5 Dispositions pour faire face à la perte totale des alimentations électriques	7.4.2 Etudes du système d'alimentation électrique	7.10 Programme d'ensemble d'assurance qualité
7.2.6 Dispositions visant à éviter ou à réduire la perte d'alimentation électrique	7.4.3 Conception du système d'alimentation électrique interruptible	
7.2.7 Considérations relatives au classement	7.4.4 Conception du système d'alimentation électrique sans interruption	7.10 Exigences relatives à la documentation produite
7.2.7.2 Qualification		
7.2.7.3 Essais de surveillance	7.5 Maintenance	
7.2.8 Dispositions visant à atteindre l'objectif de fiabilité du système d'alimentation électrique	7.5.1 Considérations relatives à la maintenance de la conception électrique	
8 Exigences relatives aux sous-systèmes		
8.1 Exigences du système d'alimentation électrique	8.4 Système d'alimentation électrique interruptible en courant alternatif	8.6 Coordination et interaction avec le réseau
8.2 Spécification de conception des équipements	8.5 Système d'alimentation électrique sans interruption CA/CC	8.7 Mise à la terre
8.3 Exigences relatives aux équipements		
9 Vérification de l'architecture du système d'alimentation électrique		
9.2 Vérification des modèles et outils informatisés	9.3 Exigences d'essai	
10 Intégration et mise en service globales		
10.2 Exigences	10.3 Documentation produite	
11 Exploitation et maintenance d'ensemble		
11.2 Exigences	11.3 Documentation produite	
12 Plan d'assurance qualité système		
12.2 Plan de vérification système	12.3 Plan de gestion de configuration système	12.4 Procédure de résolution des défauts

Figure 2 – Architecture du système d'alimentation électrique

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60038:2009, *Tensions nominales de l'IEC*

IEC 60671, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Essais de surveillance*

IEC 60709:2018, *Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique importants pour la sûreté – Séparation*

IEC/IEEE 60780-323, *Installations nucléaires – Equipements électriques importants pour la sûreté – Qualification*

IEC 60964:2018, *Centrales nucléaires de puissance – Salles de commande - Conception*

IEC/IEEE 60980-344, *Installations nucléaires – Equipements importants pour la sûreté – Qualification sismique*

IEC 61225, *Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique – Exigences pour les systèmes d'alimentation en courant alternatif et en courant continu statiques sans interruption*

IEC 61226:2020, *Centrales nucléaires de puissance – Systèmes d'instrumentation, de contrôle-commande et d'alimentation électrique importants pour la sûreté – Catégorisation des fonctions et classement des systèmes*

IEC 61513:2011, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Exigences générales pour les systèmes*

IEC 62671, *Centrales nucléaires de puissance – Instrumentation et contrôle-commande importants pour la sûreté – Sélection et utilisation des appareils numériques à fonctionnalités limitées*

IEC 62808, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Conception et qualification des appareils d'isolement*

IEC 62855:2016, *Centrales nucléaires de puissance – Systèmes d'alimentation électrique – Analyse des systèmes d'alimentation électrique*

IEC 62859, *Centrales nucléaires de puissance – Systèmes d'instrumentation et de contrôle-commande – Exigences pour coordonner sûreté et cybersécurité*

IEC 63272, *Installations nucléaires – Systèmes d'alimentation électriques – Systèmes d'alimentation électrique en courant continu interruptibles*

ISO 9001:2015, *Systèmes de management de la qualité – Exigences*

Guide de sûreté de l'AIEA N° GS-G-3.1:2006, *Application of the management System for facilities and activities* (disponible en anglais seulement)

Normes de sûreté de l'AIEA, Prescriptions N° GS-R partie 2 :2016, *Direction et gestion pour la sûreté*

Guide de sûreté SSG-34 de l'AIEA:2016, *Design of electrical power systems in Nuclear Power Plants* (disponible en anglais seulement)

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse <http://www.electropedia.org/>
- ISO Online browsing platform: disponible à l'adresse <http://www.iso.org/obp>

NOTE Les termes suivants ont été définis sur la base des définitions de l'AIEA et de l'IEC. Certaines définitions ont été légèrement modifiées ou adaptées au domaine électrique.

3.1

alimentation de secours

source d'alimentation électrique réservée à l'alimentation des systèmes électriques classés de sûreté de la centrale en cas de perte totale des sources non secourues par batteries (manque de tension généralisé) et toutes autres conditions hors dimensionnement

[SOURCE: Guide de sûreté SSG-34 de l'AIEA: 2016]

3.2

incident de fonctionnement prévu

AOO

écart de fonctionnement par rapport au fonctionnement normal que l'on s'attend à voir survenir au moins une fois pendant la durée de vie utile de l'installation, mais qui, grâce aux dispositions appropriées prises lors de la conception, ne cause pas de dommage significatif à des constituants importants pour la sûreté ou ne dégénère pas en conditions accidentelles

Note 1 à l'article: Des exemples d'incident de fonctionnement prévu sont la perte d'alimentation électrique normale et des défauts tels le déclenchement turbine, les dysfonctionnements d'éléments individuels normalement en marche sur l'installation, des défaillances de fonctions de dispositifs individuels d'équipement de contrôle-commande et la perte d'alimentation des pompes de refroidissement principales.

Note 2 à l'article: Certains États et organisations utilisent le terme fonctionnement anormal (en contraste avec le fonctionnement normal) pour ce concept.

[SOURCE: Glossaire de sûreté de l'AIEA, 2018]

3.3

chemin de câble

chemin physique sur l'installation, dans lequel de nombreux câbles peuvent être installés, traversant un local ou dans une goulotte dans un bâtiment de l'installation, ou dans une goulotte métallique ou sur une trémie ou dans une gaine ou une conduite en dessous ou un pont au-dessus d'une route

[SOURCE: IEC 60709: 2018, 3.3]

3.4

défaillance de cause commune

DCC

défaillance de plusieurs structures, systèmes ou composants due à un événement ou à une cause spécifique unique

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.5

composant

l'une des pièces constituant un système

Note 1 à l'article: Un composant peut être un composant matériel (par exemple transistors, circuits intégrés, moteurs, relais, solénoïdes, tuyaux, raccords, pompes, réservoirs et vannes) ou un composant logiciel (par exemple modules, routines, programmes, fonctions logicielles).

Note 2 à l'article: Un composant peut être constitué d'autres composants.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.6

défense en profondeur

mise en place hiérarchisée de différents niveaux d'équipements et de procédures variés pour prévenir la multiplication des incidents de fonctionnement prévus et maintenir l'efficacité des barrières physiques placées entre une source de rayonnements ou des matières radioactives et les travailleurs, les personnes du public ou l'environnement, dans différentes conditions de fonctionnement et, pour certaines barrières, dans des conditions accidentelles

Note à l'article: Cinq niveaux de défense en profondeur sont discutés dans la référence [16] (voir la référence [16] pour plus d'information) :

- a) L'objectif du premier niveau de défense est d'empêcher les déviations du fonctionnement normal et les défaillances des dispositifs importants pour la sûreté.
- b) L'objectif du deuxième niveau de défense est de détecter et de contrôler les déviations du fonctionnement normal de façon à empêcher la dégradation d'un incident de fonctionnement prévu en une condition accidentelle.
- c) L'objectif du troisième niveau de défense est d'empêcher la dégradation du cœur et les rejets de matières radioactives nécessitant des actions de protection externes au site et de ramener la centrale dans un état sûr à l'aide de moyens intrinsèques ou de moyens et/ou de dispositifs de sauvegarde, de systèmes et de procédures de sûreté.
- d) L'objectif du quatrième niveau de défense est d'empêcher la progression, et de compenser les conséquences d'accident qui résultent d'une défaillance du troisième niveau de défense en empêchant les séquences accidentelles qui entraîneraient la survenance de rejets radioactifs importants ou de rejets radioactifs précoces.
- e) L'objectif du cinquième niveau de défense est de compenser les conséquences radiologiques de rejets importants ou de rejets précoces de matières qui pourraient résulter d'un accident.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.7

accident de dimensionnement

ensemble de conditions accidentelles à prendre en compte lors de la conception et devant provenir d'événements initiateurs postulés afin d'établir les conditions limites que doit supporter la centrale nucléaire de puissance, sans dépassement des limites acceptables en ce qui concerne la radioprotection

Note 1 à l'article: Les conditions de dimensionnement font référence aux accidents de dimensionnement.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.8

conditions du domaine de conception étendu

DEC

conditions accidentelles postulées qui ne sont pas prises en compte dans les accidents de dimensionnement, mais qui le sont dans le processus de conception de l'installation selon des méthodes de type «hypothèse la plus probable», et dans lesquelles les rejets de matières radioactives sont maintenus dans des limites acceptables.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.9

diversité

présence de plusieurs systèmes ou composants redondants pour l'accomplissement d'une fonction déterminée, lorsque ces différents systèmes ou composants possèdent des attributs différents afin de réduire le risque de défaillance de cause commune, y compris de défaillance de mode commun

Note 1 à l'article: Des conditions d'exploitation différentes, des principes de fonctionnement différents ou des équipes de conception différentes (sources de diversité fonctionnelle) ainsi que des tailles d'équipements différentes, des fabricants différents et des types d'équipements (sources de diversité d'équipements) utilisant des méthodes physiques différentes (sources de diversité physique) sont des exemples de ces attributs.

Note 2 à l'article: Diversité fonctionnelle. Application de la diversité au niveau des fonctions d'application de méthodes (sources de diversité physique) relatives au procédé industriel (par exemple le déclenchement d'une action de protection sur seuil de pression ou sur seuil de température).

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.10

division

ensemble de composants, y compris leurs interconnexions, qui forment une redondance d'un système redondant ou d'un groupe de sûreté. Des divisions peuvent comprendre des canaux multiples

Note 1 à l'article: Dans le contexte du présent document, une "division" inclut un système ou ensemble de composants donné qui permet d'établir et de maintenir l'indépendance physique, électrique et fonctionnelle par rapport à d'autres ensembles de composants redondants.

[SOURCE: Guide de sûreté SSG-39 de l'AIEA, 2016]

3.11

isolement électrique

l'isolement électrique est utilisé pour empêcher les défaillances électriques d'un système d'affecter des systèmes connectés. L'isolement électrique limite ou empêche les interactions dommageables entre équipements et composants conséquences de facteurs tels que les interférences électromagnétiques, les piques électrostatiques, les courts-circuits, les ouvertures de circuits, les mises à la terre ou l'application de la tension maximale crédible (en CC ou en CA)

[SOURCE: Guides de sûreté SSG-34:2016 et SSG-39 de l'AIEA: 2016]

3.12

système d'alimentation électrique

système assurant la production, la transmission et la distribution et qui alimente les fonctions pour faire fonctionner les équipements de l'installation (pompes, vannes, réchauffeurs, etc.) et les systèmes d'I&C

Note 1 à l'article: Un système d'alimentation électrique est composé de plusieurs sous-systèmes d'alimentation électrique.

Note 2 à l'article: Un système d'alimentation électrique peut comprendre des éléments E/E/PE pour réaliser sa régulation et sa protection électriques internes.

3.13

sous-système d'alimentation électrique

deux sous-systèmes principaux sont définis (chacun couvrant les différents niveaux de défense en profondeur):

- alimentation électrique interruptible;
- alimentation électrique sans interruption.

chaque sous-système couvre les niveaux suivants:

- alimentation électrique non importante pour la sûreté;
- alimentation électrique importante pour la sûreté:
 - alimentation électrique de sûreté prenant en charge les DBC;
 - alimentation prenant en charge les DEC.

3.14

cycle de vie du système d'alimentation électrique

activités nécessaires à la mise en œuvre d'un système d'alimentation électrique. Elles ont lieu entre la spécification des exigences du système (lors de la phase de conception) et le retrait du service du système d'alimentation électrique

3.15

basculement de source électrique

basculement d'une source d'alimentation électrique initiale à une source d'alimentation de secours (de manière automatique ou manuelle) lorsque la source d'alimentation électrique initiale ne satisfait pas aux exigences de performances du système d'alimentation électrique

Note 1 à l'article: Un basculement entre les sources externes ou le basculement vers une source interne de secours en courant alternatif sont des basculements de sources électriques.

3.16

équipement

ensemble de composants conçus et fabriqués pour exécuter des fonctions spécifiques

Note 1 à l'article: Les capteurs, les câbles, les électrovannes, les armoires d'I&C ou les châssis sont des exemples d'équipements.

[SOURCE: IEEE Standards Dictionary Online]

3.17

système de première ligne

système composé d'équipements mécaniques (pompes, vannes, réchauffeurs, etc.) qui agissent directement sur le procédé de la centrale afin d'accomplir une fonction

3.18

fonctionnement en régime îloté

régime d'exploitation d'une centrale nucléaire non raccordée au réseau, et dont la puissance produite ne sert qu'à alimenter ses propres auxiliaires électriques

[SOURCE: IEC 62855, 2016, 3.2]

3.19

ergonomie

Ingénierie pour laquelle les facteurs pouvant influencer les performances humaines et avoir des conséquences sur la sûreté sont compris et pris en compte, en particulier au niveau de la conception et du fonctionnement des installations

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.20

système d'I&C

système réalisé sur la base d'éléments E/E/PE, exécutant des fonctions d'I&C ainsi que des fonctions de service et d'affichage liées au fonctionnement du système lui-même

Note 1 à l'article: Le terme est utilisé comme terme général comprenant tous les éléments du système, tels que les alimentations électriques, les capteurs et autres dispositifs d'entrée, les bus de données et autres chemins de

communication, les actionneurs et autres dispositifs de sortie (voir Note 2). Les différentes fonctions d'un système peuvent utiliser des ressources dédiées ou partagées.

Note 2 à l'article: Les éléments contenus dans un système d'I&C donné sont définis dans la spécification des limites de ce système.

Note 3 à l'article: Selon leurs fonctionnalités propres, l'AIEA fait la distinction entre les systèmes de contrôle et de commande, les systèmes d'IHM, les systèmes de verrouillage et les systèmes de protection (voir Article B.4).

[SOURCE: IEC 61513: 2011, 3.29]

3.21 indépendance

condition qui existe lorsque la réalisation avec succès de fonctions nécessaires d'un système ne dépend d'aucun comportement, y compris les défaillances et le fonctionnement normal, d'un autre système, ou d'aucun autre signal, ou donnée ou information provenant d'un autre système

Note 1 à l'article: La définition suivante pour "système indépendant" se trouve dans le glossaire de sûreté de l'AIEA: "Équipement qui possède les deux caractéristiques suivantes: (a) La capacité d'exécuter la fonction demandée n'est pas affectée par le fonctionnement ou la défaillance d'un autre équipement; (b) La capacité d'exécuter la fonction demandée n'est pas affectée par les effets de l'événement initiateur postulé pour lequel il doit fonctionner". Cette définition AIEA est limitée aux équipements, mais est cohérente avec la présente définition fournie dans cette norme.

Note 2 à l'article: Pour le système d'alimentation électrique, l'indépendance peut être exigée entre les divisions ou entre les différents niveaux de défense en profondeur.

[SOURCE: IEC 60709: 2018, 3.13]

3.22 système d'alimentation électrique interruptible

alimentation de charges pour lesquelles un temps de coupure défini de l'alimentation ne compromet pas la mission de l'objectif de sûreté

3.23 constituant important pour la sûreté

constituant faisant partie d'un groupe de sûreté et/ou dont le mauvais fonctionnement ou la défaillance pourrait entraîner une exposition à des rayonnements du personnel du site ou de personnes du public

Note 1 à l'article: Les constituants importants pour la sûreté comprennent:

- a) les structures, systèmes et composants dont le mauvais fonctionnement ou la défaillance pourraient entraîner une exposition induite à des rayonnements du personnel du site ou de personnes du public;
- b) les structures, systèmes et composants qui empêchent les incidents de fonctionnement prévus d'aboutir à des conditions accidentelles;
- c) les dispositifs de sûreté pour les DEC ;
- d) les dispositifs prévus pour atténuer les conséquences d'un mauvais fonctionnement ou d'une défaillance de structures, systèmes ou composants.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.24 perte d'alimentation électrique

situation correspondant à une condition de manque de tension généralisé cumulé à la perte des alimentations de secours en courant alternatif diversifiées.

Note 1 à l'article: Les alimentations en courant continu et les alimentations interruptibles en courant alternatif peuvent être disponibles tant que les batteries peuvent alimenter les charges.

3.25 perte des sources d'alimentation externes

perte simultanée de toutes les sources électriques externes sur tous les tableaux de sûreté de la centrale, exigeant le démarrage des sources internes CA de secours puis la réalimentation des tableaux de sûreté (séquence de reprise diesel)

Note 1 à l'article: Les tableaux de sûreté des systèmes CA sans interruption et des systèmes CC ne sont pas pris en compte.

[SOURCE: IEC 62855 :2016, 3.4]

3.26

durée de mission

période de fonctionnement exigée pour les charges ou les sources électriques après l'initiation de conditions accidentelles, pendant laquelle l'équipement doit être capable de fonctionner dans les limites de ses critères d'acceptabilité pour les conditions d'exploitation spécifiées

3.27

sécurité nucléaire

mesures visant à empêcher et à détecter des actes criminels ou intentionnels non autorisés mettant en jeu des matières nucléaires et autres matières radioactives, les installations associées ou les activités associées, et à intervenir en pareil cas; ou mesures visant à empêcher et à détecter un vol, un sabotage, un accès non autorisé, un transfert illégal ou d'autres actes malveillants mettant en jeu des matières nucléaires et autres matières radioactives ou les installations associées, et à intervenir en pareil cas

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.28

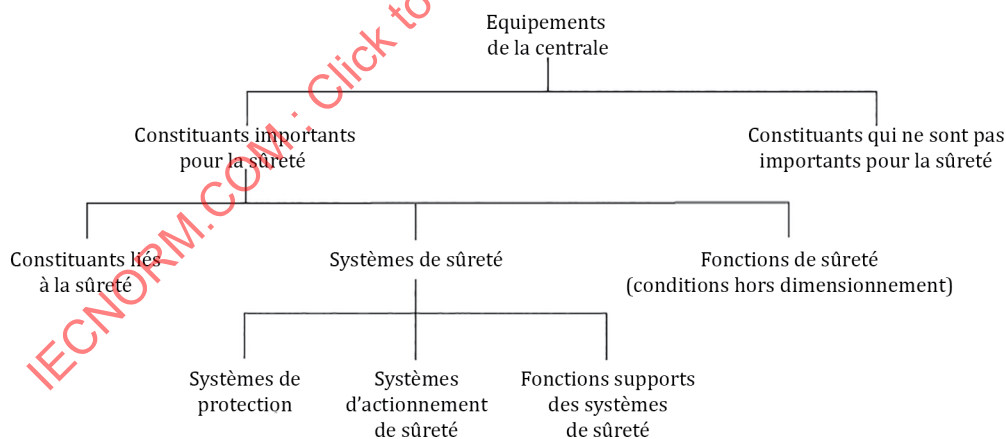
performance

efficacité avec laquelle une fonction prévue est exécutée (par exemple temps de réponse, précision, sensibilité aux variations de paramètres)

[SOURCE: IEC 61226: 2020, 3.16]

3.29

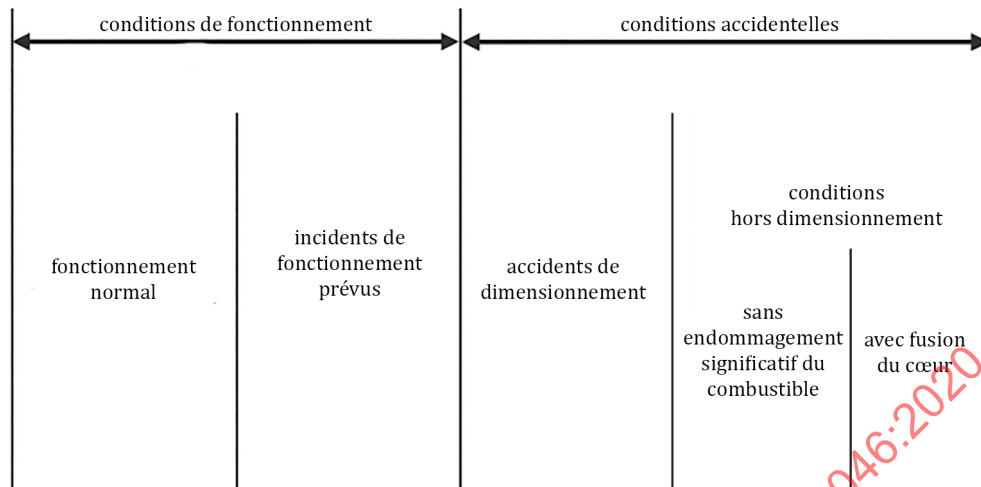
équipements de la centrale



^a Un "constituant" est une structure, un système ou un composant.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.30 états de la centrale



[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.31 bilan de puissance

puissance active et puissance réactive exigées en régime établi par le système d'alimentation électrique

3.32 alimentation préférentielle

alimentation à partir du réseau de transport du système d'alimentation électrique classé de sûreté

Note 1 à l'article: Certaines parties du système d'alimentation préférentielle ne sont pas classées de sûreté.

Note 2 à l'article: Dans le contexte de la norme, le réseau de transport est hors du domaine d'application. Les limites de l'alimentation préférentielle correspondent au poste raccordant la CNP au réseau.

[SOURCE: Définition du guide de sûreté SSG-34 de l'AIEA]

3.33 étude probabiliste de sûreté

EPS

approche détaillée, structurée, utilisée pour élaborer les scénarios de défaillance, constituant un outil conceptuel et mathématique servant à établir des estimations chiffrées du risque

Note 1 à l'article: Il est généralement reconnu qu'il existe trois niveaux d'étude probabiliste de sûreté.

Le niveau 1 comprend l'évaluation des défaillances de la centrale, qui permet de déterminer la fréquence d'endommagement du cœur.

Le niveau 2 comprend l'évaluation de la réaction du confinement, qui permet, avec les résultats du niveau 1, de déterminer les fréquences des défaillances du confinement et de rejets dans l'environnement d'un pourcentage donné de la quantité de radionucléides contenue dans le cœur du réacteur.

Le niveau 3 comprend l'évaluation des conséquences hors site, qui permet, avec les résultats du niveau 2, d'estimer les risques pour le public.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.34 qualité

niveau auquel l'ensemble des caractéristiques intrinsèques d'un objet satisfont à des exigences

[SOURCE: ISO 9000, édition 2015, 3.6.2]

3.35

assurance qualité

activité de la gestion de la qualité dont l'objectif est de donner confiance quant au niveau de satisfaction à des exigences qualité

[SOURCE: ISO 9000, édition 2015, 3.3.6]

3.36

gestion de la qualité

gestion concernant la qualité

[SOURCE: ISO 9000, édition 2015, 3.3.4]

3.37

redondance

mise en place de structures, systèmes ou composants (identiques ou différents) supplémentaires, afin qu'une structure, qu'un système ou qu'un composant quelconque puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de défaillance d'un autre élément

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.38

temps de rétablissement

temps maximal nécessaire à un équipement électrique appartenant à un système pour être à nouveau alimenté par une source d'alimentation électrique

3.39

robustesse du système d'alimentation électrique

capacité du système d'alimentation électrique à accomplir ses missions de sûreté en résistant aux défaillances et/ou perturbations électriques

3.40

évaluation de sûreté

évaluation de tous les aspects d'une pratique pertinents pour la protection et sûreté ; pour une installation autorisée, ceci comprend le choix du site, la conception et le fonctionnement de l'installation

analyse visant à prévoir la performance de l'ensemble d'un système et son impact et dans laquelle la performance est mesurée par l'impact radiologique ou une autre mesure globale de l'impact sur la sûreté

processus systématique mis en œuvre tout au long de la conception pour s'assurer que la conception proposée (ou effective) satisfait à toutes les prescriptions de sûreté pertinentes. L'évaluation de la sûreté comprend, mais pas seulement, une analyse de la sûreté formelle

Note 1 à l'article: Dans le contexte de la conception du système d'alimentation électrique, c'est une analyse qui indique pour tous les types de conditions, les charges requises.

[SOURCE: Glossaire de sûreté de l'AIEA édition 2018]

3.41

argumentaire de sûreté

ensemble d'arguments et d'éléments d'information relatifs à la sûreté d'une installation ou d'une activité

Note 1 à l'article: Il comprend normalement les conclusions d'une évaluation de la sûreté et une déclaration de confiance dans ces conclusions.

Note 2 à l'article: Pour un dépôt, l'argumentaire de sûreté peut concerner un stade particulier de la mise en place. En pareil cas, il devrait indiquer s'il existe des questions non résolues et donner des orientations pour tenter de résoudre celles-ci à des stades ultérieurs.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.42

classement de sûreté

pour les centrales nucléaires de puissance, affectation des systèmes, composants et autres équipements à un nombre limité de classes de sûreté sur la base de leurs fonctions et de leur importance pour la sûreté

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.43

groupe de sûreté

ensemble d'équipements prévus pour accomplir toutes les actions requises si un événement initiateur particulier se produit afin que les limites spécifiées dans la base de conception pour les incidents de fonctionnement prévus et les accidents de dimensionnement ne soient pas dépassées

Note 1 à l'article: La note de l'IEEE 308-2001 précise: Un groupe de sûreté peut comprendre une ou plusieurs divisions. Dans une conception où chaque division peut accomplir une fonction de sûreté, chaque division est un groupe de sûreté. Toutefois, une conception présentant trois systèmes d'une capacité de 50 % séparés en trois divisions comprend trois groupes de sûreté; il est exigé que deux divisions sur trois fonctionnent pour accomplir la fonction de sûreté.

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.44

système lié à la sûreté

système important pour la sûreté qui ne fait pas partie d'un système de sûreté

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.45

système de sûreté

système important pour la sûreté destiné à garantir la mise à l'arrêt sûr du réacteur ou l'évacuation de la chaleur résiduelle du cœur, ou à limiter les conséquences des incidents de fonctionnements prévus et des accidents de dimensionnement

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.46

défaillance unique

défaillance qui rend un système unique ou un composant impropre à remplir sa (ses) fonction(s) de sûreté prévue(s) et toute autre défaillance qui peut en résulter

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.47

critère de défaillance unique

critère (ou contrainte) appliqué à un système, en vertu duquel ce dernier doit être capable de remplir sa (ses) fonction(s) en cas de défaillance unique

[SOURCE: Glossaire de sûreté de l'AIEA, édition 2018]

3.48**source interne de secours en courant alternatif**

source de puissance pouvant fournir, en cas de perte des sources externes et du générateur principal, la puissance nécessaire à l'alimentation des auxiliaires classés de sûreté lors d'incidents de fonctionnement prévus ainsi que lors de conditions accidentelles

3.49**manque de tension généralisé**

situation de l'alimentation ou des alimentations électriques de la centrale en courant alternatif comprenant la perte des sources externes, du générateur principal et des sources internes de secours en courant alternatif classées de sûreté pour les tableaux d'appareillages essentiels et non essentiels

[SOURCE: Guide de sûreté SSG-34 de l'AIEA: 2016]

3.50**perturbation du réseau**

perturbation électrique

variation brusque non programmée de l'état de fonctionnement d'un réseau d'énergie électrique qui occasionne des problèmes ou des interruptions généralisés de la qualité de l'énergie

Note 1 à l'article: Dans ce document, le terme perturbation électrique est utilisé.

Note 2 à l'article: Une perturbation du réseau peut avoir pour origine une panne du réseau de transport, le déclenchement d'un groupe de production, des pertes de charge ou toute combinaison de ces phénomènes. La perturbation du réseau peut entraîner des plages anormales de fréquence ou de tension, une perte de stabilité du réseau d'énergie ou des indisponibilités en cascade des circuits de transport de l'énergie, ainsi qu'une interruption généralisée de la consommation.

Note 3 à l'article: Les perturbations électriques peuvent générer des perturbations électromagnétiques qui peuvent compromettre le système électrique.

[SOURCE: IEC 60050-692:2017, 692-1-10]

3.51**gestionnaire de réseau de transport**

entité chargée de fournir et de gérer les réseaux de transport et de répartition d'électricité. Elle est également en charge de la sûreté du système avec un niveau élevé de qualité et de fiabilité

3.52**système d'alimentation électrique sans interruption**

alimentation de charges exigées pour assurer la disponibilité fonctionnelle en cas d'indisponibilité de l'alimentation interruptible

Note 1 à l'article: Les charges spécifiques exigeant une stabilité à haute tension peuvent également être alimentées par le système d'alimentation électrique sans interruption.

Note 2 à l'article: Les vannes d'isolement, les amortisseurs, les systèmes d'I&C et de surveillance représentent des charges types des systèmes d'alimentation électrique sans interruption.

4 Termes abrégés

NOTE Elaborés à partir des symboles et abréviations des systèmes d'alimentation électrique, l'AIEA et de l'IEC et à adapter au domaine électrique.

CA	courant alternatif
BIL	basic insulation level (niveau d'isolement de base)
DCC	défaillance de cause commune
CDF	core damage frequency (fréquence d'endommagement du cœur)
GC	gestion de la configuration
DBA	design basis accident (accident de dimensionnement)

DBC	design basis conditions (conditions de dimensionnement)
EDD	événement de dimensionnement
CC	Courant continu
DEC	design extension conditions (conditions du domaine de conception étendu)
DiD	defense in depth (défense en profondeur)
DSO	distribution system operator (Distributeur)
E/E/EP	système électrique/électronique/électronique programmable
IEM	interférence electro magnétique
EMIT	examination, maintenance, in-service inspection and surveillance testing (examen, maintenance, contrôle en service et essais de surveillance)
EQ	environmental qualification (qualification environnementale)
ETS	equipment technical specification (spécification technique des équipements)
IHM	interface homme-machine
HT	haute tension
CVC	système de chauffage, ventilation et climatisation
I&C	instrumentation et contrôle-commande
AIEA	Agence internationale de l'énergie atomique
INSAG	International Nuclear Safety Group (Groupe consultatif international pour la sûreté nucléaire)
E/S	entrée/sortie
LEP	loss of electrical power (perte totale des alimentations électriques)
LoDiD	level of defence in depth (niveau de défense en profondeur)
LOOP	loss of offsite power (perte des sources d'alimentation externes)
BT	basse tension
CNP	centrale nucléaire de puissance
EIP	événement initiateur postulé
PPS	preferred power supply (alimentation préférentielle)
EPS	étude probabiliste de sûreté
AQ	assurance qualité
SBO	station black out (manque de tension généralisé)
SF	single failure (défaillance unique)
SFC	single failure criterion (critère de défaillance unique)
SSC	structure, système et composant
SLD	single line diagram (schéma unifilaire)
SSG	specific safety guide (guide de sûreté)
SSR	specific safety requirement (prescription de sûreté particulière)
GRT	gestionnaire de réseau de transport
ASI	alimentation sans interruption

5 Cycle de vie de l'ensemble du système d'alimentation électrique

Les phases d'un cycle de vie type de l'ensemble du système d'alimentation électrique comprennent:

- a) la revue des exigences applicables au système d'alimentation électrique (voir Article 6):
 - les exigences de sûreté applicables (voir 6.2);
 - les exigences électriques (voir 6.3);
 - les exigences fonctionnelles et de performances (voir 6.4);
 - les exigences de maintenance (voir 6.5);
- b) la conception de l'architecture électrique (voir Article 7):
 - les dispositions relatives à la conception de sûreté (voir 7.2);
 - les dispositions relatives à la conception électrique (voir 7.3);
 - les dispositions fonctionnelles et de performances relatives à la conception (voir 7.4);
 - les dispositions relatives à la maintenance (voir 7.5);
- c) les exigences relatives aux sous-systèmes électriques (voir Article 8);
- d) la vérification de l'architecture du système d'alimentation électrique (voir Article 9);
- e) l'intégration et la mise en service de l'ensemble des systèmes (voir Article 10);
- f) l'exploitation et la maintenance d'ensemble (voir Article 11);

Les liens entre ce cycle de vie et les cycles de vie des sous-systèmes sont représentés de manière simplifiée sur la Figure 3.

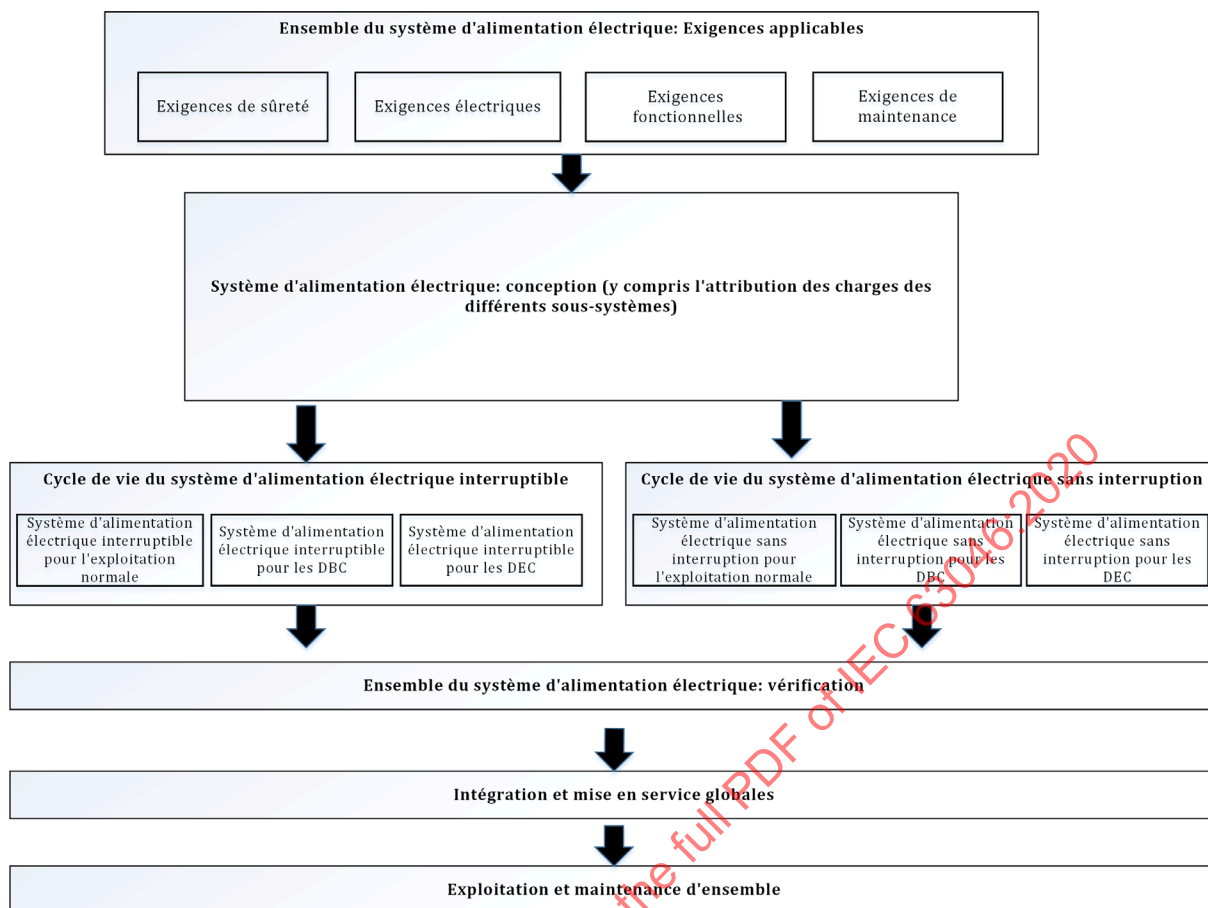


Figure 3 – Liens entre le cycle de vie de l'ensemble du système d'alimentation électrique et les cycles de vie des sous-systèmes d'alimentation électrique

6 Architecture du système d'alimentation électrique: identification des exigences

6.1 Objectifs

Le présent article a pour objet de définir les exigences applicables à la conception du système d'alimentation électrique.

L'architecture du système d'alimentation électrique doit:

- satisfaire aux exigences de sûreté applicables à la CNP, telles que:
 - la mise en place d'une approche de défense en profondeur cohérente avec celle des systèmes supportés et avec leur importance pour la sûreté conformément aux bases de conception de la centrale;
 - l'application du critère de défaillance unique;
 - la gestion des défaillances de cause commune;
 - les conditions de perte des sources d'alimentation électrique externe;
 - les conditions de manque de tension généralisé;
 - les conditions de perte totale d'alimentation électrique;
 - la robustesse contre les agressions internes et externes;
 - les exigences de catégorisation et de classement;
 - les exigences de fiabilité pour les études probabilistes de sûreté;

- satisfaire aux exigences électriques applicables à la CNP, telles que:
 - les exigences coordonnées avec le gestionnaire du réseau électrique;
 - la robustesse du système d'alimentation électrique face aux perturbations électriques;
- satisfaire aux exigences fonctionnelles applicables au système d'alimentation électrique (en tant que système support);
- satisfaire aux exigences liées à la stratégie de maintenance;
- prendre en charge le cycle de vie complet de la centrale nucléaire de puissance (mise en service, exploitation et mise hors service).

Les exigences de sûreté et leur application au système d'alimentation électrique doivent être décomposées et dérivées en exigences relatives à l'architecture de l'alimentation électrique, aux sous-systèmes d'alimentation électrique et aux équipements.

NOTE Par hypothèse, concernant la conception des systèmes d'alimentation électrique des CNP qui sont supports de fonctions de sûreté conventionnelle (par exemple pour garantir la sécurité des travailleurs, la protection des biens, la prévention contre les risques chimiques, la prévention contre les risques liés au procédé énergétique) des normes nationales ou internationales pour les équipements électriques conventionnels s'appliquent.

Il convient que le cumul des exigences applicables en matière de stratégie de sûreté et de maintenance soit établi comme une donnée d'entrée.

6.2 Exigences de sûreté applicables à la conception de l'architecture électrique

6.2.1 Défense en profondeur

Il convient que le processus de conception électrique développe le concept de défense en profondeur conformément aux bases de conception de sûreté de la centrale.

Il convient de spécifier la stratégie relative à la mise en œuvre des différents LoDiD du projet comme une donnée d'entrée afin de préciser:

- les niveaux de défense en profondeur pour chacune des conditions d'exploitation;
- les limites entre les niveaux de défense en profondeur;
- les exigences concernant l'indépendance entre ces niveaux.

6.2.2 Application du critère de défaillance unique

Le critère de défaillance unique doit être appliqué à un système de sorte que ce dernier doive être capable de remplir sa tâche définie en cas de défaillance unique.

L'applicabilité du critère de défaillance unique doit être spécifiée pour chaque LoDiD comme une donnée d'entrée issue de l'évaluation de la sûreté pour la conception électrique.

NOTE Usuellement, le SFC est applicable pour le niveau DBC

6.2.3 Gestion des défaillances de cause commune

Lors de la conception du système d'alimentation électrique, la résilience face aux défaillances de cause commune doit être évaluée en vue de satisfaire aux exigences de sûreté des fonctions prises en charge.

Il convient que les exigences de robustesse du système soient établies et justifiées sur la base de données de fiabilité pertinentes issues soit de la centrale, soit d'un ensemble de bases de données de centrales nationales et internationales.

6.2.4 Conditions de perte des sources d'alimentation externe

Le système d'alimentation électrique doit être conçu de manière à réduire le risque de perte des sources d'alimentation externes lors de conditions de dimensionnement, pour tous les états et conditions d'exploitation spécifiés de la centrale.

La conception doit inclure des dispositions adéquates afin d'éviter tout dommage au niveau combustible-cœur pendant les conditions de perte des sources d'alimentation externe de façon à maintenir les capacités du système d'alimentation électrique à supporter les fonctions de sûreté de la centrale.

6.2.5 Conditions de manque de tension généralisé

Le système d'alimentation électrique doit être conçu de manière à réduire le risque de perte d'alimentation électrique lors de conditions du domaine de conception étendu, pour tous les états et conditions d'exploitation spécifiés de la centrale.

La conception doit inclure des dispositions adéquates afin d'éviter tout dommage significatif du combustible en cas manque de tension généralisé et de maintenir la capacité de la centrale à assurer les fonctions de sûreté et à évacuer la puissance résiduelle lors de conditions hors dimensionnement.

6.2.6 Conditions de perte totale des alimentations électriques

Le système d'alimentation électrique doit être conçu de manière à réduire le risque de perte totale d'alimentation électrique lors de conditions de dimensionnement et de conditions hors dimensionnement, pour tous les états d'exploitation spécifiés de la centrale.

Une condition de perte d'alimentation électrique est une situation correspondant à un manque de tension généralisé de la centrale cumulé à la perte de l'alimentation ou des alimentations de secours en courant alternatif diversifiées.

La robustesse face à une condition de perte d'alimentation électrique doit être spécifiée comme une donnée d'entrée pour la conception électrique.

6.2.7 Prise en compte des agressions internes et externes

6.2.7.1 Généralités

Le système d'alimentation électrique important pour la sûreté doit être robuste face aux agressions applicables pour la centrale nucléaire de puissance.

Il convient de prendre en compte au minimum la liste suivante d'agressions:

6.2.7.2 Agressions externes

- tremblement de terre;
- inondation externe;
- conditions climatiques;
- foudre;
- IEM (sources externes);
- missiles;
- chute d'avion;
- environnement industriel (par exemple, installation industrielle à proximité du site de la CNP présentant un risque pour la CNP).

L'évaluation de chaque agression doit prendre en compte:

- les conditions de dimensionnement;
- les conditions hors dimensionnement;
- les exigences spécifiques au site.

NOTE Exemples de conditions climatiques: basse et haute température (température de l'air et de la source froide), neige, vents violents, tempête de verglas.

6.2.7.3 Agressions internes

- agressions liées à l'eau provenant de sources directes et indirectes, telles que la pulvérisation et l'infiltration par les toits, les murs, les chemins de roulement et les conduites;
- incendie;
- missiles;
- jets de vapeur;
- effet de fouet des tuyaux;
- explosions chimiques;
- inondation;
- défaillance de l'équipement adjacent;
- IEM (sources internes).

Les agressions et les règles de cumul d'agressions à prendre en compte doivent être identifiées comme des données d'entrée pour la conception électrique.

6.2.8 Exigences de sécurité nucléaire

La conception d'un système d'alimentation électrique important pour la sûreté doit tenir compte des exigences de sécurité nucléaire applicables (protection physique de la centrale).

Ces exigences doivent être identifiées comme données d'entrée pour la conception électrique.

6.2.9 Exigences de classement

La norme IEC 61226 définit une méthode d'affectation des fonctions spécifiées de la centrale dans différentes catégories selon leur importance pour la sûreté.

Le classement subséquent des systèmes d'I&C et d'alimentation électrique qui exécutent ou supportent ces fonctions, selon la catégorie assignée, détermine ensuite les critères de conception pertinents.

La classe de sûreté de la partie des sous-systèmes d'alimentation électrique participant à la défense en profondeur ne doit pas être inférieure à la classe de sûreté des systèmes alimentés par le système d'alimentation électrique.

6.2.10 Exigences probabilistes

Les cibles des études probabilistes de sûreté doivent être identifiées comme données d'entrée pour la conception électrique.

6.3 Exigences électriques

6.3.1 Exigences coordonnées avec le gestionnaire de réseau

Le gestionnaire de réseau peut être un GRT (gestionnaire de réseau de transport) ou un GRD (gestionnaire de réseau de distribution) suivant la tension de branchement au réseau.

Il convient de prendre en compte les données d'entrée suivantes pour les connexions au réseau définies par le gestionnaire de réseau:

- la plage de tensions et de fréquences du réseau;
- la tenue au court-circuit minimale et maximale du réseau au point de connexion;
- la fiabilité du réseau;
- les exigences de comportement sur défaut;
- les exigences de réponse en fréquence;
- les exigences relatives au passage en îlotage (le cas échéant).
- il convient que la conception du système d'alimentation électrique prenne en compte les exigences particulières du gestionnaire de réseau (associées à la production d'énergie).

6.3.2 Perturbations électriques

Les perturbations électriques peuvent entraîner des variations par rapport aux valeurs assignées d'exploitation définies pour les trois principales grandeurs électriques:

- tension (U);
- courant (I);
- fréquence (f).

Les éléments suivants peuvent être à l'origine des perturbations électriques:

- l'installation électrique elle-même;
- l'activité humaine;
- les phénomènes naturels.

Des perturbations symétriques et asymétriques peuvent affecter la centrale. Ces événements peuvent être initiés:

- dans le réseau de transport ou à la suite de la séparation de la centrale du réseau en raison de défaillances prévues ou de variations de tension et de fréquence au-delà des niveaux acceptables définis;
- par le déclenchement du groupe turboalternateur, laissant les systèmes d'alimentation internes uniquement connectés aux systèmes d'alimentation externes ou aux systèmes d'alimentation internes de secours;
- dans les systèmes d'alimentation internes, à la suite d'un événement électrique tel que le démarrage d'un moteur, une défaillance de court-circuit ou des surtensions de manœuvre.

NOTE Des exemples de perturbations électriques peuvent être consultés dans l'IEC 62855.

Une perturbation électrique peut provoquer une défaillance de cause commune dans l'ensemble du système d'alimentation électrique, en raison du point électrique commun que constituent la connexion au réseau d'un côté et le groupe turboalternateur de l'autre côté.

Il convient que la robustesse du système d'alimentation électrique face aux DCC induisant des conditions de manque de tension généralisé ou de perte totale des alimentations électriques soit assurée par une protection efficace contre les perturbations électriques.

Il convient d'analyser les effets des perturbations électriques et des mesures de protection possibles conformément à l'IEC 62855 et de mettre en œuvre des mesures de protection appropriées.

6.4 Exigences fonctionnelles et de performances

En tant que système support, le système d'alimentation électrique alimente les systèmes de première ligne ou autres systèmes supports de la centrale (tels que les systèmes CVC ou d'I&C) selon les exigences des systèmes alimentés.

Le processus de conception électrique exige les données d'entrée suivantes, provenant des concepteurs des systèmes supportés:

- la liste consommateurs, ainsi que les données électriques associées, nécessaires pour accomplir les fonctions non importantes pour la sûreté et importantes pour la sûreté durant le fonctionnement normal, les DBC et les DEC;
- le type des alimentations exigées par consommateur (interruptibles ou sans interruption);
- les exigences fonctionnelles et de performances des fonctions importantes pour la sûreté nécessaires pour satisfaire aux exigences de sûreté générales de la centrale;
- la durée de mission et le temps de rétablissement maximal des consommateurs en cas d'alimentation interne (CA ou CC);
- les conditions d'ambiance de dimensionnement.

6.5 Exigences de maintenance

La maintenance de la centrale a deux objectifs principaux:

- entretenir les équipements importants pour la sûreté afin d'assurer la sûreté de la centrale et le respect des exigences fonctionnelles;
- atteindre les objectifs de production électrique (hors du domaine d'application de la présente norme).

Il convient de prendre en compte l'impact de la maintenance de la centrale dans la conception de l'architecture électrique.

La stratégie de maintenance doit être utilisée pour spécifier les exigences de maintenance. Il convient de déduire ces exigences de la conception de la centrale ainsi que des exigences de fonctionnement et de sûreté.

7 Conception de l'architecture électrique

7.1 Objectifs

Il convient que le concepteur tienne compte des exigences suivantes dans la conception de l'architecture du système d'alimentation électrique:

- dispositions visant à satisfaire aux exigences de sûreté nucléaire;
- dispositions visant à satisfaire aux exigences de performances électriques;
- dispositions visant à satisfaire aux exigences fonctionnelles;
- dispositions visant à satisfaire aux exigences de maintenance.

7.2 Disposition relative à la conception de sûreté

7.2.1 Défense en profondeur du système d'alimentation électrique

Le système d'alimentation électrique doit suivre une approche de défense en profondeur cohérente avec celle des systèmes pris en charge.

Pour assurer la robustesse face aux événements électriques identifiés (tels que les conditions de perte des sources d'alimentation externes ou de manque de tension généralisé), le système d'alimentation électrique doit comprendre:

- une conception électrique détaillée du système d'alimentation électrique et de ses sous-systèmes selon l'approche LoDiD en prenant en compte:
 - les caractéristiques intrinsèques;
 - l'emploi de mesures à un ou plusieurs niveaux de défense en cas de défaillances électriques (système de protection électrique).
- des sources de puissance associées aux différents LoDiD pour alimenter les équipements de première ligne et les systèmes supports.
- Suivant le SSG34, en général 3 alimentations électriques sont identifiées:
 - l'alimentation électrique préférentielle (couvrant les LoDiD 1&2);
 - l'alimentation électrique de sûreté (couvrant le LoDiD 3);
 - l'alimentation électrique de secours (couvrant le LoDiD 4);
- L'exigence portant sur l'intégration de chaque source d'alimentation dans la conception du système d'alimentation électrique doit être justifiée par des mesures de conception portant sur les performances (voir 7.2.5).

Le système électrique de sûreté prenant en charge les fonctions DBC doit être alimenté par l'alimentation préférentielle secourue par les sources de secours.

Il convient que le système électrique prenant en charge les fonctions DEC soit alimenté par le système électrique de sûreté prenant en charge les DBC ou par une alimentation de secours dédiée aux conditions hors dimensionnement.

Les alimentations préférentielles doivent être les alimentations normales pour tous les systèmes de la centrale importants pour la sûreté. Elles doivent toujours être choisies en priorité pour l'alimentation des systèmes électriques de sûreté.

Afin de satisfaire aux exigences de sûreté au regard de la résilience en cas d'indisponibilité prolongée des sources de puissance, il convient que la mise à disposition de sources mobiles ou d'alimentations supplémentaires soit envisagée.

Un exemple des considérations de base de conception des systèmes d'alimentation électrique est fourni pour information en Annexe A.

NOTE Les systèmes de secours spécifiques conçus uniquement pour la protection des équipements non liés à la sûreté ne sont pas listés dans cette description.

7.2.2 Défaillance unique du système d'alimentation électrique

La mise en place de la redondance dans la conception du système d'alimentation électrique est le principal facteur permettant de satisfaire au critère de défaillance unique.

Il convient que la mise en place de la redondance dans la conception du système d'alimentation électrique assure la robustesse relative au critère de défaillance unique et améliore la fiabilité du système.

Le principe de conception des systèmes de sûreté et du système d'alimentation électrique de support doit être cohérent, de sorte que les dispositions relatives à la redondance des systèmes de production et de distribution électriques correspondent à celles des systèmes alimentés.

Toutes les exceptions au SFC doivent être justifiées dans l'analyse de sûreté.

7.2.3 Défaillance de cause commune du système d'alimentation électrique

7.2.3.1 Types de DCC

7.2.3.1.1 Généralités

On doit prendre en compte la possibilité de défaillances de cause commune, susceptibles de rendre les systèmes électriques de sûreté indisponibles pour l'exécution de leurs fonctions de sûreté sur demande, lors de la conception, de la maintenance, des essais et de l'exploitation des systèmes électriques de sûreté et de leurs systèmes supports.

Plusieurs sources de DCC ont un impact potentiel sur le système d'alimentation électrique:

- DCC résultant d'agressions internes ou externes;
- DCC résultant de perturbations électriques internes ou externes;
- DCC des équipements et composants électriques;
- DCC provoquées par des erreurs logicielles dans les éléments numériques programmables;
- DCC provoquées par des facteurs humains (y compris les activités de conduite/exploitation et de maintenance).

7.2.3.1.2 DCC résultant d'agressions internes ou externes

On doit envisager les dispositions suivantes pour assurer la protection contre les agressions internes et externes:

- caractéristiques intrinsèques de conception de l'équipement (par exemple, niveau d'isolement de base (BIL) pour les équipements pouvant être soumis à l'agression foudre);
- isolations électriques (par exemple, parafoudres);
- séparation physique (par exemple, risque d'incendie).

7.2.3.1.3 DCC induites par des perturbations électriques

Les perturbations électriques peuvent provoquer une défaillance de cause commune sur l'ensemble du système d'alimentation électrique en raison de leur point électrique commun, le réseau d'un côté et le groupe turboalternateur de l'autre côté.

Il convient que les dispositions en vue de la protection contre ce type de DCC incluent:

- les caractéristiques intrinsèques de conception de l'équipement (par exemple, la tenue au court-circuit de l'équipement électrique);
- un système de protection bien conçu ;
- la séparation physique et les isolations électriques.

7.2.3.1.4 DCC des équipements et composants électriques

Il convient que les dispositions en vue de la protection contre ce type de DCC incluent:

- la diversité (au niveau fonctionnel ou au niveau de l'équipement).

Il convient que l'analyse des DCC électriques évalue les défaillances de cause commune potentielles des équipements composant le système d'alimentation électrique.

Il convient de porter une attention particulière aux équipements suivants:

- sources internes en courant alternatif (par exemple, ensembles de groupes diesel, ensembles de turbines à gaz);
- alimentations sans interruption, y compris:

- batteries;
- redresseurs, onduleurs, convertisseurs.

Il convient que les dispositions de protection contre les DCC soient justifiées par des données de fiabilité et des analyses des DCC.

7.2.3.1.5 DCC provoquées par des erreurs logicielles dans les éléments numériques programmables ou des cyberattaques des éléments numériques programmables du système d'alimentation électrique

Avec l'utilisation d'éléments numériques programmables intégrés aux composants du système d'alimentation électrique on doit évaluer les vulnérabilités aux DCC et cyberattaques associées afin de protéger ce dernier d'une condition de DCC.

Les dispositions applicables sont l'utilisation de normes dédiées (telle que l'IEC 62671) concernant les éléments numériques programmables, afin de réduire le plus possible le risque d'apparition de ce type de DCC.

Il convient de prendre en compte la sensibilité aux cyberattaques des systèmes contenant des éléments numériques programmables (suivant l'IEC 62859).

7.2.3.1.6 DCC provoquées par des facteurs humains

Il convient que les dispositions en vue de la protection contre ce type de DCC incluent:

- les choix au niveau de la conception des interfaces IHM;
- la séparation physique.

NOTE Du personnel différent peut aussi apporter de la robustesse au niveau de ce type de DCC (procédure administrative).

Des activités concomitantes (telles que des essais ou de la maintenance) sur des équipements redondants qui peuvent produire des conditions de DCC ne doivent pas être réalisées au même moment.

L'évaluation de l'aptitude au fonctionnement de l'équipement peut réduire le risque de DCC provoquées par des facteurs humains.

Il convient qu'une analyse des facteurs humains soit effectuée en ce qui concerne le système d'alimentation électrique, afin d'identifier les activités ou opérations pouvant provoquer une DCC.

7.2.3.2 Dispositions contre les défaillances de cause commune

7.2.3.2.1 Généralités

La protection de systèmes de sûreté redondants qui pourraient être affectés par un événement unique, des agressions internes, des agressions externes ou des perturbations électriques est procurée par l'indépendance.

Elle permet également d'empêcher qu'un événement unique ou une agression unique ou encore une perturbation unique n'affecte les systèmes fournissant différents niveaux de défense en profondeur.

Il convient d'inclure dans l'examen des processus de défaillance:

- les défaillances résultant d'événements de dimensionnement de référence;
- les perturbations électriques ou les agressions internes ou externes;

- la défaillance de systèmes supports;
- les erreurs de conception, de fabrication, d'exploitation ou de maintenance courantes;
- les DCC induites par:
 - les connexions électriques entre systèmes de différentes divisions ou de différents LoDiD;
 - l'échange de données entre systèmes de différentes divisions ou de différents LoDiD;

Les parties redondantes des groupes de sûreté doivent être indépendantes les unes des autres pour s'assurer que le groupe de sûreté peut accomplir ses fonctions de sûreté pendant et après tout événement.

Les exigences relatives à l'indépendance entre parties redondantes ou différentes de circuits contribuant à la même fonction de sûreté doivent être déterminées à partir des moyens de sûreté de première ligne pris en charge.

Il convient que la mise en place de la séparation physique, de la diversité et/ou de l'isolement électrique permette de satisfaire aux exigences d'indépendance.

Il convient d'envisager l'avantage présenté par l'utilisation de plusieurs systèmes supports diversifiés (à vapeur, à air comprimé, etc.) plutôt que d'un système support électrique commun.

7.2.3.2.2 Séparation physique

Les exigences relatives à la séparation physique des circuits et équipements doivent être respectées à l'aide d'une distance, de barrières ou de toute combinaison.

La norme de second niveau IEC 60709 définit les méthodes et dispositions permettant de réaliser la séparation.

Dans le cadre de l'application du critère de défaillance unique, on se doit d'appliquer la ségrégation pour réduire le risque de défaillance de cause commune des parties redondantes d'un système et de ses systèmes supports essentiels face à des agressions tels qu'un incendie, une inondation, une explosion, de sorte qu'une défaillance unique et ses conséquences n'entraînent pas la défaillance de plus d'une disposition redondante.

7.2.3.2.3 Diversité au sein des systèmes d'alimentation électrique et des équipements

L'application de la diversité au niveau de la conception réduit les possibilités de défaillances de causes communes des systèmes redondants en raison d'une défaillance de cause commune au niveau du système ou de l'équipement.

Après une analyse des DCC et si nécessaire, les systèmes d'alimentation électrique doivent être diversifiés conformément aux exigences des moyens de sûreté pris en charge.

Il convient de mettre en œuvre la diversité lors de la phase de conception, la phase de fabrication, la phase de configuration de l'exploitation et la phase de maintenance ou d'une combinaison de celles-ci.

Il convient également de prendre en compte la diversité humaine (différents personnels) dans la conception et l'exploitation du système d'alimentation électrique.

Il convient d'envisager les approches suivantes concernant la diversité:

a) diversité fonctionnelle:

- diversité fondée sur les principes physiques de la mise en œuvre de la conception, de la technologie ou des fonctions;

b) diversité matérielle (ou physique):

- diversité entre les systèmes qui remplissent la même fonction (utilisation d'un système diversifié, dédié et indépendant ou d'un système existant), par exemple: il convient que l'alimentation préférentielle soit différente de l'alimentation interne de secours;
- diversité entre les équipements ou composants redondants d'un même système (diversité intégrée au système), par exemple: utilisation de différentes technologies de batteries;
- diversité entre fabricants d'équipements ou lots de fabrication.

Il convient que l'adéquation des dispositions en matière de diversité soit établie et justifiée sur la base de données de fiabilité pertinentes issues soit de la base de données de la centrale, soit d'un ensemble de bases de données de centrales nationales et internationales.

La mise en œuvre de la diversité peut augmenter la complexité du système d'alimentation électrique et peut accroître le risque d'erreurs lors de l'exploitation et de la maintenance. Il convient que les mesures de la diversité reposent sur les exigences identifiées sur la base d'une analyse complète.

Lorsque le dimensionnement exige la diversité des dispositifs numériques programmables d'un système d'alimentation électrique, il convient que la mise en œuvre repose sur les exigences du 7.2.3.3.3.

Afin d'utiliser la diversité entre fabricants d'équipements, il convient que les différents équipements ne présentent pas de composants communs pouvant provoquer une DCC.

7.2.3.2.4 Isolement électrique

On doit mettre en place des dispositifs d'isolement électrique, afin de réduire le risque que les défaillances électriques d'un système ne compromettent les systèmes connectés. Il convient que les dispositifs de commande d'isolement électriques limitent les interactions dommageables entre équipements et composants, conséquences de facteurs tels que les interférences électromagnétiques, les piques électrostatiques, les courts-circuits, les ouvertures de circuits, les mises à la terre ou des conditions de surtension.

On doit obtenir l'isolement électrique au moyen de dispositifs d'isolement, de techniques de blindage et de câblage, ou d'une combinaison de ceux-ci.

L'isolement électrique mis en œuvre entre systèmes importants pour la sûreté doit satisfaire aux exigences de l'IEC 60709.

Lorsqu'il existe des interfaces entre des composants électriques de classement supérieur et inférieur, le composant au niveau de l'interface doit être conçu de manière à empêcher la propagation d'une défaillance ou des conséquences de conditions dégradées d'un composant classé de sûreté inférieure à des composants classés de sûreté supérieure. Ce composant doit être classé selon la classe de sûreté la plus élevée des équipements interconnectés.

Les dispositifs d'isolement des systèmes à très basse tension doivent être conçus conformément à l'IEC 62808. Les dispositifs d'isolement types sont: les amplificateurs, les commutateurs de contrôle, les transformateurs de courant, les coupleurs photo-optiques ou fibroniques, les relais, les transducteurs, les disjoncteurs, les fusibles.

Les dispositifs d'isolement des charges électriques doivent être conçus conformément aux normes IEC industrielles. Les dispositifs d'isolement types sont les disjoncteurs et les fusibles associés avec ou sans contacteurs ou commutateurs.

7.2.3.3 Gestion des exigences en matière de défaillance de cause commune du système d'alimentation électrique

7.2.3.3.1 Généralités

Le processus de conception du système d'alimentation électrique doit comprendre une analyse des DCC.

7.2.3.3.2 Mise en œuvre de l'indépendance du système d'alimentation électrique

7.2.3.3.2.1 Généralités

Il convient de justifier l'adéquation des caractéristiques de conception pour assurer l'indépendance.

7.2.3.3.2.2 Indépendance entre LoDiD

Le système d'alimentation électrique important pour la sûreté interruptible doit comporter des dispositions afin d'être alimenté à partir de différentes sources d'alimentation électrique suivant l'approche LoDiD.

Si des systèmes non électriques fournissent un moyen différent d'accomplir une fonction importante pour la sûreté donnée, leurs alimentations et systèmes d'instrumentation et de contrôle-commande associés doivent être indépendants des alimentations et systèmes d'instrumentation et de contrôle-commande desquels ils sont conçus pour être diversifiés.

La source de secours du système électrique important pour la sûreté prenant en charge les DEC doit être indépendante de la source de secours du système électrique de sûreté prenant en charge les DBC.

Il convient que l'alimentation électrique importante pour la sûreté prenant en charge les DEC soit indépendante de l'alimentation électrique de sûreté prenant en charge les DBC.

De plus, si l'alimentation de secours du niveau DEC est composée de plusieurs sources, chacune ayant une fonction spécifique (par exemple, éviter la fusion du cœur et gérer les accidents graves), l'alimentation dédiée de la fonction DEC spécifique doit être fonctionnellement indépendante du système électrique de sûreté prenant en charge les DBC et des autres alimentations prenant en charge les autres fonctions DEC.

Il convient d'empêcher la possibilité d'une mauvaise connexion, d'erreurs humaines ou d'une erreur de configuration (locale ou distante) entre les différents LoDiD (en particulier entre les sources) (sauf pour certaines configurations de maintenance ou d'essais de surveillance spécifiques). Toutes exceptions à cette exigence doivent être justifiées.

Les sources d'alimentation électrique de différents LoDiD ne doivent pas fonctionner en parallèle au niveau d'un même tableau de distribution (sauf pour un essai périodique accompagné d'une analyse de sûreté).

7.2.3.3.2.3 Indépendance entre divisions

La défaillance d'une division d'alimentation électrique redondante ne doit pas rendre d'autres divisions d'alimentation électrique redondantes inutilisables.

L'alimentation interne de sûreté d'une division donnée ne doit alimenter que cette division. Toutes les exceptions relatives à des cas particuliers doivent être justifiées.

Il convient que les systèmes électriques appartenant à une division soient alimentés en électricité par cette division. Toutes les exceptions à cette exigence doivent être justifiées par analyse.

Il convient que les équipements d'un même sous-système du process (pompe, vanne motorisée et régulateur du même système de processus, par exemple) soient alimentés par la même division d'alimentation électrique.

Une défaillance unique de l'alimentation de surveillance ne doit pas rendre la surveillance d'une division entière impossible.

Les équipements classés de sûreté dans différentes divisions doivent être isolés électriquement.

On doit prévoir des dispositifs de protection indépendants entre les divisions.

On ne doit pas interconnecter les divisions redondantes d'un système d'alimentation électrique de sûreté (sauf pour une opération de maintenance temporaire).

La propagation d'une défaillance électrique entre les divisions ne doit pas être possible.

7.2.3.3.2.4 Indépendance entre niveaux de classement

L'interface entre les systèmes importants pour la sûreté et des systèmes de classement de sûreté inférieur doit être conçue de manière à s'assurer qu'il n'y ait pas d'impact négatif des équipements de classement de sûreté inférieur sur les équipements importants pour la sûreté, résultant de perturbations dans les systèmes d'alimentation électrique de la centrale.

Les systèmes importants pour la sûreté doivent être indépendants des systèmes de classement de sûreté inférieur, afin de s'assurer que les systèmes importants pour la sûreté puissent accomplir leurs fonctions de sûreté pendant et après tout événement exigeant l'exécution de ces fonctions.

Dans la mesure du possible, il convient que les charges non importantes pour la sûreté ne soient pas alimentées par les systèmes électriques importants pour la sûreté.

S'il est nécessaire d'alimenter des charges non importantes pour la sûreté à partir de systèmes électriques importants pour la sûreté, les charges non importantes pour la sûreté doivent être équipées de dispositifs d'isolement de même classe de sûreté que les systèmes électriques supports importants pour la sûreté.

Lorsqu'il n'est pas possible de fournir une séparation et un isolement appropriés des défaillances électriques entre un circuit classé de sûreté et un circuit de fonction de classe de sûreté inférieure, le circuit de classe inférieure (circuit associé) doit être:

- analysé ou soumis à l'essai afin de démontrer que le circuit de classe de sûreté associé ne sera pas dégradé de façon inacceptable;
- identifié comme faisant partie de la division de sûreté associée;
- isolé électriquement des autres composants de la même manière que les circuits de la division de sûreté associée.

Il convient de déconnecter automatiquement lors d'un basculement de source électrique, les charges qui ne sont pas importantes pour la sûreté et qui sont susceptibles d'avoir un impact sur la capacité à fonctionner du système d'alimentation électrique important pour la sûreté.

7.2.3.3.3 Mise en œuvre de l'indépendance des éléments numériques programmables

Les éléments numériques programmables sont utilisés dans de nombreux équipements électriques et leur utilisation est croissante dans de nombreux éléments propriétaires, sans alternative disponible pour certains éléments.

Il convient qu'une étude soit réalisée afin d'identifier et d'enregistrer:

- l'emplacement des éléments numériques programmables intégrés à l'équipement et la fonction de ces dispositifs;
- les modes de défaillance et la possibilité d'une défaillance de cause commune des d'éléments numériques programmables.

Il convient d'évaluer les conséquences d'une DCC d'éléments numériques programmables.

La diversité doit être prise compte de lors de la conception du système électrique, afin de réduire la vulnérabilité du système aux DCC des éléments numériques programmables. La diversité de la conception du système électrique doit être prise en considération afin de réduire la vulnérabilité du système aux CCF provenant d'éléments numériques programmables

Il convient de porter une attention particulière aux propositions de mise en réseau des systèmes de protection électriques par des relais programmables de relais présentant une communication bidirectionnelle à partir de systèmes centralisés de commande.

Ces systèmes présentent un risque de DCC et il convient de les exclure si possible sur les centrales nucléaires de puissance.

Lorsque un système distribué utilisant une communication bidirectionnelle est mis en œuvre alors il convient qu'une validation et vérification complète des dispositifs programmables soit entreprise pour montrer que les mesures compensatrices contre les DCC potentielles que le risque de DCC due aux erreurs logiciel ou les cyberattaques soient acceptables conformément à l'argumentaire de sûreté d'ensemble de l'installation.

Lorsque l'installation d'éléments numériques programmables est prévue dans la conception du système électrique, leur mise en œuvre doit être validée en fonction de leur classement de sûreté.

Cette validation doit respecter les procédures définies dans l'IEC 62671.

Lorsque des éléments numériques programmables sont mis en œuvre, il convient d'évaluer la vulnérabilité du système en matière de cybersécurité ainsi que les conséquences associées pour le système d'alimentation électrique.

Il convient de fonder la justification d'un élément numérique programmable sur l'évaluation des fonctions de sûreté/modes de défaillance.

Il convient d'envisager les éléments numériques programmables des systèmes électriques dans le contexte de la conception électrique globale et de l'argumentaire de sûreté.

La mise en œuvre d'éléments numériques programmables dans les systèmes d'alimentation électriques exige une participation pluridisciplinaire.

7.2.4 Dispositions pour faire face à la perte des alimentations électriques

Il convient que la conception prévoie des dispositifs aptes à détecter cette condition de perte des alimentations électriques externes afin d'initier les actions automatiques ou manuelles appropriées.

Il convient que la conception comprenne des mesures pour faire face à la perte des alimentations électriques externes (en prenant en compte les exigences fonctionnelles applicables au système d'alimentation électrique et s'appuyant sur les besoins électriques des charges alimentées) telles que:

- mise en place d'un ensemble de batteries approprié pour alimenter les équipements d'instrumentation et de contrôle-commande classés de sûreté et les autres équipements vitaux nécessaires pour les conditions de dimensionnement;
- installation de sources de secours en courant alternatif qui satisfont aux exigences d'indépendance entre divisions (voir 7.2.3.3.2);
- conception de l'installation avec des moyens de sûreté passifs.

Il convient que le choix des dispositifs à utiliser se base sur les exigences en termes de bilans de puissance, de temps de restauration et de durée de mission des systèmes alimentés durant une perte des alimentations électriques externes.

7.2.5 Dispositions pour faire face au manque de tension généralisé

Il convient que la conception prévoie des dispositifs aptes à détecter cette condition de manque de tension généralisé afin d'initier les actions automatiques ou manuelles appropriées.

Il convient d'envisager les mesures de conception suivantes:

- la mise à disposition d'une capacité de batterie suffisante pour alimenter les équipements d'instrumentation et de contrôle-commande classés de sûreté ainsi que d'autres équipements vitaux exigés en DEC;
- l'installation d'une source d'alimentation de secours en courant alternatif, présentant une diversité de conception et protégée des agressions susceptibles de dégrader l'alimentation préférentielle et les sources internes de secours;
- l'utilisation de connexions CNP à CNP en l'absence de risque de DCC entre les deux unités de la source de puissance (lorsque des connexions sont réalisées entre CNP, il ne doit pas être possible qu'une défaillance de l'une des CNP ait un impact sur l'autre);
- une conception de la CNP présentant davantage de fonctionnalités passives.

Il convient que le choix des dispositifs à utiliser se base sur les exigences en termes de bilans de puissance, de temps de restauration et de durée de mission des systèmes alimentés durant un manque de tension généralisé.

7.2.6 Dispositions visant à éviter ou à réduire la perte totale des alimentations électriques

Il convient que la conception prévoie des dispositifs aptes à détecter cette condition de perte totale des alimentations électriques afin d'initier les actions automatiques ou manuelles appropriées.

Les dispositions pour éviter ou limiter ces conditions sont:

- la robustesse du système d'alimentation électrique face aux DCC;
- une fiabilité appropriée des équipements du système d'alimentation électrique.

Afin de faire face à une condition de LEP, il convient d'envisager les mesures de conception suivantes:

- une autonomie adéquate de la source d'alimentation sans interruption pour surveiller les paramètres d'accidents graves;
- la mise à disposition d'une source d'alimentation supplémentaire pour alimenter les fonctions d'accidents graves (y compris les points de connexion appropriés permettant ce type d'alimentation);

- une conception de la CNP présentant davantage de fonctionnalités passives.

Il convient que le choix des dispositifs à utiliser se base sur les exigences en termes de bilans de puissance, de temps de restauration et de durée de mission des systèmes alimentés durant une perte totale des alimentations électriques.

7.2.7 Considérations relatives au classement

7.2.7.1 Généralités

Chaque système électrique doit être classé suivant le classement des charges supportées. Tous les écarts doivent être justifiés.

Le classement des niveaux DBC et DEC doit être réalisé suivant l'IEC 61226.

Lorsque le système d'alimentation électrique a été classé conformément à l'IEC 61226, il convient d'appliquer deux méthodes principales afin de vérifier l'adéquation des exigences de performances et de fiabilité des systèmes et équipements électriques importants pour la sûreté:

- la qualification;
- la surveillance et les essais.

7.2.7.2 Qualification

Les éléments d'équipements électriques doivent être qualifiés en fonction de leurs exigences fonctionnelles et des conditions de service et d'environnement.

Les systèmes d'alimentation électrique et les composants importants pour la sûreté doivent être qualifiés en ce qui concerne leur fonction prévue pendant leur durée de vie en service dans les conditions d'environnement d'exploitation prévues.

L'objectif principal de la qualification est de démontrer, avec une assurance raisonnable, que les équipements importants pour la sûreté peuvent accomplir leurs fonctions de sûreté sans subir de défaillances dans toutes les conditions prévues.

L'IEC/IEEE 60780-323 décrit les exigences de base pour la qualification des équipements électriques importants pour la sûreté et les interfaces (électriques et mécaniques) qui doivent être utilisées dans les centrales nucléaires de puissance.

L'IEC/IEEE 60980-344 indique les pratiques recommandées pour la qualification sismique des équipements électriques des centrales nucléaires de puissance.

7.2.7.3 Essais de surveillance

Pour les systèmes électriques de sûreté, il convient de soumettre les paramètres suivants à des essais réguliers:

- le fonctionnement des sources de puissance du sous-système et de ses composants y compris les performances des sources de puissance associées;
- le basculement entre sources d'alimentation électriques;
- l'activation de la protection (et appareils de suppression des défauts associés);
- les performances des éléments d'équipements de conversion d'énergie, en particulier ceux comprenant de l'électronique de puissance.

Il convient que la conception électrique permette de surveiller et de soumettre à l'essai les paramètres énumérés ci-dessus.

L'IEC 60671 fournit des exigences techniques et des recommandations quant à la mise en œuvre des essais de surveillance pour les systèmes d'I&C importants pour la sûreté.

Il convient de suivre les exigences générales relatives aux essais de surveillance (Article 6) pour les systèmes d'alimentation électrique importants pour la sûreté.

7.2.8 Dispositions visant à atteindre l'objectif de fiabilité du système d'alimentation électrique

Les trois principales mesures visant à augmenter la fiabilité du système d'alimentation électrique sont:

- La spécification correcte des composants et approvisionnement de composants fiables;
- la mise en place de redondance au sein d'une division et entre divisions;
- la mise en place de diversification entre LoDiD et entre divisions.

Les systèmes d'alimentation électrique importants pour la sûreté doivent présenter le degré de redondance nécessaire pour satisfaire aux exigences de fiabilité du dimensionnement.

La fiabilité du système d'alimentation électrique doit être évaluée par rapport à l'objectif de sûreté global fondé sur l'analyse EPS.

Il convient de mettre en place des dispositions internes de secours des sources externes lorsque cela est nécessaire pour satisfaire aux exigences de sûreté de la centrale. Il convient que ces dispositions emploient des mesures telles que des sources internes supplémentaires et la mise en place d'une activation automatique des alimentations de secours.

Afin d'atteindre les objectifs de l'étude probabiliste de sûreté, il convient d'envisager la modification de l'architecture par la mise en place de la redondance face aux problèmes de fiabilité des composants et de la diversité face aux problèmes de DCC.

7.3 Disposition relative à la conception électrique

7.3.1 Généralités

Il convient que la conception électrique prenne en compte les données d'entrée principales suivantes afin de déterminer les performances du sous-système d'alimentation électrique:

- exigences et performances de l'alimentation du réseau;
- exigences de performances des charges alimentées (voir 7.4);
- perturbations électriques.

7.3.2 Coordination avec le réseau

La plage de tensions et de fréquences doit être dérivée du code réseau applicable.

Les exigences du réseau doivent faire l'objet d'une discussion et d'un accord avec le gestionnaire de réseau, de manière à ne pas compromettre les performances des équipements assurant des fonctions importantes pour la sûreté.

La contribution de la centrale nucléaire de puissance à la stabilité du réseau ne doit pas compromettre la capacité du système d'alimentation électrique pour prendre en charge les fonctions de sûreté de la centrale.

7.3.3 Conception conforme aux exigences électriques

7.3.3.1 Généralités

Les variations de la tension, du courant et de la fréquence du système d'alimentation électrique de la centrale nucléaire de puissance, quel que soit le mode de fonctionnement, ne doivent pas dégrader les performances des équipements du système important pour la sûreté.

Les variations et les transitoires de tension, de courant et de fréquence sur les tableaux électriques classés de sûreté, susceptibles de résulter d'événements sur l'alimentation préférentielle ou sur la source d'alimentation électrique interne, doivent être identifiées.

Il convient que la conception des différents sous-systèmes repose sur un équilibre entre la robustesse par la conception des équipements avec une capacité de tenue associée et un système ou un composant protégé par le système de protection électrique.

Il convient de prendre en compte dans les analyses tous les modes de fonctionnement ainsi que les événements symétriques et asymétriques. Un événement est susceptible de mettre en cause différents composants des systèmes d'alimentation électrique, en fonction du temps de montée, du temps de défaillance, de l'amplitude ou de l'asymétrie.

La norme IEC 62855 fournit les lignes directrices en matière d'ingénierie électrotechnique, afin d'effectuer cette analyse spécifique pour les systèmes d'alimentation électrique CA et CC des CNP.

Les caractéristiques de fréquence et de tension de l'alimentation des équipements doivent être spécifiées.

Il convient de fonder la spécification des caractéristiques de fréquence et de tension sur la configuration la plus défavorable.

Chaque caractéristique doit être définie par une valeur nominale et des plages de variation normales, exceptionnelles et très exceptionnelles (également appelées conditions d'exploitation).

Il convient que ces variations soient issues du réseau ou de sources d'alimentation internes.

La condition d'exploitation normale n'est pas limitée dans le temps, mais il convient de spécifier les conditions d'exploitation dégradées pour une durée maximale et un taux de fréquence maximal ou une durée minimale et maximale cumulée.

7.3.3.2 Conditions de régime établi du système d'alimentation électrique

Il convient de spécifier les paramètres suivants pour chaque sous-système et de chaque LoDiD:

- plage de tensions;
- plage de fréquences;
- plage de courants.

Il convient de déterminer ces valeurs:

- aux bornes de l'équipement pris en charge en régime établi, à l'exclusion des phénomènes transitoires;
- en fonction des caractéristiques des sources externes et internes.

Il convient de tenir compte des tolérances et des paramètres d'exploitation des équipements et systèmes pour la démonstration de la robustesse des systèmes électriques importants pour la sûreté face aux perturbations électriques.

7.3.3.3 Perturbations électriques

7.3.3.3.1 Généralités

Il convient de vérifier la capacité du système d'alimentation électrique à résister aux perturbations électriques par:

- des analyses complètes permettant d'identifier tous les événements possibles (initiateurs), susceptibles de se produire sur le système d'alimentation électrique, fondées sur des normes et des guides internationaux, des rapports réglementaires, l'expérience opérationnelle, des publications, études ou rapports internationaux;
- la définition des mesures préventives possibles visant à limiter ou éliminer l'événement initiateur;
- la caractérisation des phénomènes électriques (plage de fréquences, amplitude de tension et/ou courant);
- la définition des mesures de protection associées aux phénomènes électriques (par des dispositions relatives aux caractéristiques intrinsèques de l'équipement ou par un système de protection électrique).

7.3.3.3.2 Tension des systèmes d'alimentation électrique

7.3.3.3.2.1 Condition de sous-tension

Il convient de déterminer les points de consigne de la sous-tension et de la temporisation relatifs à la protection de la tension dégradée par analyse des exigences de tension des charges importantes ou non pour la sûreté à tous les niveaux du système d'alimentation électrique (limite d'exploitation électrique normale).

On doit spécifier la tension minimale d'opération et par analyse on doit montrer que la tension reste au-dessus de cette limite.

Il convient que l'évaluation de la chute de tension permette de confirmer que la tension aux bornes des matériels reste supérieure à la tension minimale susceptible d'entraîner la perte de fonctions.

a) Chute de tension acceptable

Cela correspond à une chute de tension transitoire présentant les caractéristiques suivantes:

- la tension est supérieure à la tension minimale nécessaire au fonctionnement de la charge sur une période continue;

ou

- la tension est inférieure à la tension minimale nécessaire au fonctionnement de la charge; **et** la durée de cette sous-tension est **inférieure** à la limite associée pour initier un basculement de source électrique.

Une chute de tension acceptable ne doit pas entraîner de basculement de source électrique.

b) Chute de tension inacceptable

Cela correspond à une chute de tension transitoire présentant les caractéristiques suivantes:

- la tension est inférieure à la tension minimale nécessaire au fonctionnement de la charge;

et

- la durée de cette sous-tension est **supérieure** à la limite associée pour initier un basculement de source électrique.

Il convient d'évaluer l'effet des transitoires électriques courts termes sur le basculement de source électrique.

Il convient que la stratégie de basculement de source électrique entre les différentes sources d'alimentation électriques permette l'utilisation des différentes sources de défense en profondeur disponible.

On doit initier un basculement de source électrique en cas de chute de tension inacceptable, après un délai suffisant pour permettre l'élimination des perturbations en amont ou en aval.

7.3.3.3.2.2 Conditions de surtension

Il convient d'analyser les surtensions pour s'assurer que les caractéristiques de tenue des équipements ne sont pas dépassées.

Il convient de prendre en compte dans l'analyse les surtensions provoquées par la foudre, la CEM, les surtensions de basculement et les surtensions résultant de défauts de terre dans les réseaux isolés.

Il convient de prévoir un plan de protection contre les surtensions entraînant le dépassement des caractéristiques de tenue de l'équipement (en considérant le niveau de priorité de la fonction exécutée par le système).

Il convient de réaliser une étude afin de justifier la coordination entre la valeur de surtension maximale, les durées et la coordination avec la conception des équipements du système d'alimentation électrique.

La Figure 4 n'est fournie qu'à titre d'exemple, les niveaux de tension et les durées de temps étant spécifiques à la centrale.

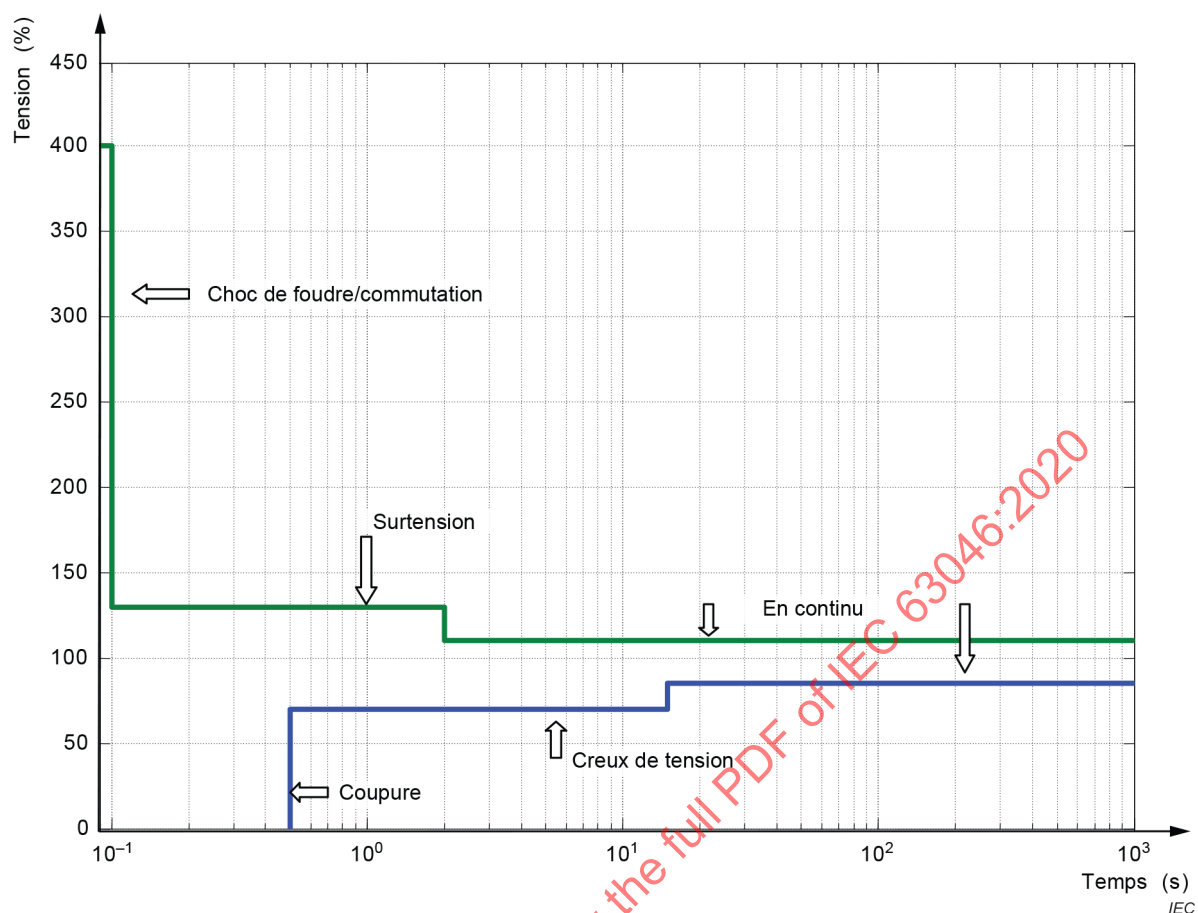


Figure 4 – Bases de conception de la tension classique (IEC 62855)

7.3.3.3.2.3 Tension déséquilibrée

Il convient de tenir compte, dans l'analyse des perturbations électriques, des tensions déséquilibrées et de leurs conséquences possibles sur le fonctionnement électrique.

7.3.3.3.3 Courant

Les études liées aux perturbations de courant doivent tenir compte:

- des défaillances électriques;
- des surcharges;
- des courants d'appel;
- des courants induits géomagnétiquement (si applicable).

7.3.3.3.4 Fréquence

L'impact des variations de fréquence doit être évalué.

Il convient que les groupes techniques responsables procèdent à une analyse de l'impact fonctionnel de la sous-fréquence et de la surfréquence sur les charges de process telles que les systèmes fluides.

Le fonctionnement du système d'alimentation électrique ne doit pas être compromis par les harmoniques (par exemple, risque d'activation de la protection contre les surcharges).

Il convient d'évaluer la distorsion harmonique totale (courant et tension).

Il convient d'évaluer les effets des harmoniques générés par le réseau ou les équipements de la centrale et de prendre des mesures appropriées pour assurer la robustesse face aux harmoniques.

Il convient de définir les limites des niveaux de production d'harmoniques par équipement et de s'assurer de la robustesse des équipements par rapport aux harmoniques produites.

7.3.3.4 Caractéristiques intrinsèques de l'équipement

Les systèmes d'alimentation électrique doivent être conçus et construits de manière à pouvoir résister aux tensions et aux courants maximums de conception dans n'importe quel état ou mode de fonctionnement de la centrale.

7.3.3.5 Système de protection électrique

7.3.3.5.1 Généralités

Un système de protection électrique doit être prévu pour:

- protéger l'équipement électrique contre des tensions, une fréquence et des courants en dehors des conditions d'exploitation définies (en plus des caractéristiques intrinsèques de l'équipement);
- assurer la continuité de l'alimentation par isolement des défaillances, de sorte qu'elles ne compromettent pas la disponibilité du système global.

Le système de protection électrique peut être divisé en deux parties:

- basculement de source électrique lorsque la source n'est plus en mesure d'alimenter les charges;
- un plan de protection du personnel et des équipements du site contre les perturbations électriques du système d'alimentation électrique.

Le plan de protection électrique de la centrale et la conception des composants de la centrale doivent être tels que les perturbations de l'alimentation ne compromettent pas le fonctionnement exigé des systèmes électriques de sûreté et des charges connectées.

Si la sous-tension ou la sous-fréquence/surfréquence et les limites sont dépassées, la charge doit être transférée aux sources d'alimentation de secours, en respectant les délais appropriés.

Le système d'alimentation électrique doit être robuste et capable de remplir sa tâche dans des conditions de défaut et en cas de transitoires électriques rapides et lents.

Il convient de réaliser une évaluation de l'impact des perturbations électriques sur tous les systèmes d'alimentation électrique internes (CA et CC) conformément à la méthode présentée en 7.3.3.3.1.

Il convient que les bases de conception couvrent tous les modes de fonctionnement et tous les événements possibles susceptibles d'avoir un impact sur le système d'alimentation électrique de la centrale nucléaire de puissance.

Il convient que la conception des différents sous-systèmes repose sur un équilibre entre la robustesse d'un équipement conçu avec une capacité de tenue adéquate et la protection des systèmes ou composants par le système de protection électrique.

Il convient qu'une analyse spécifique permette de confirmer que le système de protection satisfait à la protection des équipements et au maintien de l'alimentation du système d'alimentation électrique important pour la sûreté.

7.3.3.5.2 Conception de la surveillance et du basculement de source électrique

La qualité, l'étendue et les performances de l'alimentation électrique doivent être surveillées de manière continue sur chaque jeu de barres nécessitant un basculement de source électrique.

On doit déconnecter les bus tableaux par la dégradation de l'alimentation électrique à partir d'une source de puissance donnée de cette source de puissance si la dégradation dépasse les niveaux de conception spécifiés.

Il convient de réaliser des études afin d'analyser les performances du système d'alimentation électrique lors des basculements de sources électriques conformément à l'IEC 62855.

7.3.3.5.3 Conception du plan de protection électrique

7.3.3.5.3.1 Généralités

Le système de protection électrique doit assurer une protection contre le dépassement de la capacité de tenue graduée de l'équipement.

7.3.3.5.3.2 Facteurs à prendre en compte

Des études de coordination de la protection doivent être réalisées en tenant compte de toutes les conditions transitoires et d'exploitation.

Il convient d'inclure dans les études tous les types de défaillances en série et de défauts shunt, y compris les événements tels que la perte d'une ou deux phases et les défauts à la terre dans les systèmes fonctionnant avec un neutre isolé.

Il convient que la conception du plan de protection électrique tienne compte des défaillances symétriques et asymétriques.

Il convient que le plan de protection tienne compte des courants de réaccélération faisant suite à des creux de tension et à des basculements de source.

7.3.3.5.3.3 Mise en œuvre

Il convient que les exigences suivantes soient prises en compte afin d'assurer la coordination électrique du système:

- il convient que le temps de fonctionnement du système de protection soit compatible avec la capacité de tenue de l'équipement et les exigences de performances du système,
- une défaillance ou la maintenance d'une partie du système de protection.

Le plan de protection doit présenter les caractéristiques suivantes:

- rapidité d'action en vue de la protection du personnel et des biens:
 - activation des dispositifs exigés lorsque des conditions inacceptables sont détectées, afin de réduire la gravité et l'ampleur des perturbations du système d'alimentation électrique, l'endommagement de l'équipement, et les risques potentiels pour le personnel et les biens,
 - il convient que les dispositifs de protection soient conçus pour permettre à l'organe de coupure d'éliminer rapidement les courants de défaut afin d'éviter des agressions et d'empêcher les perturbations entraînant l'activation d'autres dispositifs de protection.
- sélectivité:
 - s'assurer que seuls les équipements défectueux sont déconnectés des alimentations électriques,

- en cas de courts-circuits et de surcharges, il convient que les dispositifs de protection soient conçus pour fonctionner de façon sélective dans toutes les configurations de connexion prévues du système d'alimentation électrique.

Il convient que le schéma de protection soit mis en œuvre de façon graduée pour éviter les déclenchements intempestifs des appareils en amont.

Il convient de concevoir les dispositifs de protection individuels installés pour protéger les composants pendant les essais de manière à ce que leur fonctionnement ne compromette pas la capacité d'un système à fonctionner.

Il convient que les appareils de protection qui protègent l'alimentation d'une source de secours contre une défaillance catastrophique immédiate soient en service dans tous les modes de fonctionnement.

NOTE De tels appareils incluent, par exemple la protection de la source de secours contre les défaillances catastrophiques, par exemple protection contre la survitesse et protection différentielle de générateur;

Il est possible de contourner les appareils de déclenchement qui protègent la source de secours contre les défaillances non catastrophiques, suivant une évaluation de la sûreté appropriée, quand la source de secours alimente les charges de sûreté lors d'opérations d'urgence, mais il convient qu'ils soient en service lors de l'exploitation normale et des essais de la source secours.

Il convient d'inclure dans les études de coordination une évaluation de la protection interne des équipements.

7.3.3.5.3.4 Exigences relatives aux dispositifs de protection

Il convient d'utiliser des dispositifs de détection et d'élimination des défauts pour permettre le retrait rapide du service de tout élément d'un système électrique lorsque des conditions anormales susceptibles d'entraîner une dégradation ou une défaillance de l'équipement d'exploitation se produisent.

Les dispositifs de protection numériques doivent être conçus, vérifiés et qualifiés pour une utilisation conforme à la fonction de sûreté qu'ils sont destinés à assurer et il convient qu'ils satisfassent aux exigences du 7.2.3.3.3 et de l'IEC 62671.

La conception des dispositifs de protection du système d'alimentation électrique et des composants des centrales nucléaires de puissance doit être conforme aux normes IEC et aux normes nationales relatives à la sûreté des équipements et des installations électriques, ainsi qu'aux autres réglementations applicables relatives aux équipements et installations électriques.

7.3.3.6 Mesure des paramètres électriques et enregistrement des événements

En plus du système de protection électrique (basculement de source électrique et plan de protection), il convient que la conception fournisse des exigences relatives à la mesure des paramètres électriques et à l'enregistrement des événements.

Il convient que le concepteur identifie et mette en œuvre toutes les mesures exigées pour l'analyse de tous les types d'événements électriques.

Il convient que les spécifications relatives aux équipements électriques de la centrale spécifient tous les signaux de sortie exigés.

Il convient que le système d'enregistrement des événements conserve le même horodatage pour toutes les mesures.

Il convient de tenir compte de la cybersécurité pour la mesure des paramètres électriques et l'enregistrement des événements.

7.4 Dispositions fonctionnelles et de performances relatives à la conception

7.4.1 Généralités

La conception du système électrique doit venir en support des exigences fonctionnelles des systèmes de la centrale importants pour la sûreté.

7.4.2 Etudes du système d'alimentation électrique

7.4.2.1 Généralités

Il convient que les systèmes d'alimentation électrique de la centrale nucléaire de puissance satisfassent à l'ensemble des exigences fonctionnelles en conditions de régime établi et en conditions dégradées définies dans l'étude de dimensionnement.

7.4.2.2 Affectation des charges aux sous-systèmes

Il convient que la conception affecte et assigne les charges (et spécialement les charges importantes pour la sûreté) aux différents sous-systèmes électriques en fonction de critères tels que la sensibilité à la perte de tension, les puissances actives et réactives, le temps de rétablissement et la durée de mission.

Deux sous-systèmes principaux sont définis:

- Alimentation interruptible;
- Alimentation sans interruption.

7.4.2.3 Marge

Il convient d'établir une stratégie de marge, et il convient qu'elle permette d'identifier les différentes marges applicables et le niveau de marge associé:

- marge visant à couvrir les modifications au cours des phases de conception du projet de CNP;
- marge visant à couvrir les modifications au cours de la durée de vie d'exploitation de la centrale;
- marge visant à couvrir les tolérances (pour les paramètres de protection, par exemple);
- marge de sûreté;
- marge visant à couvrir le fonctionnement transitoire.

Il convient de confirmer régulièrement l'adéquation des marges des caractéristiques assignées des équipements, en conjonction avec le remplacement des principaux composants, les modifications de la centrale et les examens périodiques de la sûreté.

Il convient de spécifier les équipements électriques avec une marge de conception suffisante pour s'assurer que les améliorations et modifications futures de la centrale puissent être mises en œuvre sans dépasser les caractéristiques assignées des équipements.

7.4.2.4 Bilan de puissance

Il convient que l'étude du bilan de puissance vienne à l'appui de la conception initiale des composants électriques principaux.

Il convient que les bilans de puissance soient:

- établis pour les régimes transitoires et permanents et pour les puissances actives et réactives;
- examinés en cas de modifications des consommateurs de la centrale.

Il convient que le bilan de puissance soit déterminé de manière individuelle pour chaque division.

Il convient d'établir les bilans de puissance des systèmes électriques selon une approche déterministe tenant compte des éléments suivants:

- la configuration fonctionnelle et opérationnelle:
 - tous les modes de fonctionnement;
 - le fonctionnement à partir de sources internes ou externes;
 - différents crans de charge (temps de réalimentation);
 - les configurations d'exploitation du système d'alimentation électrique (par exemple maintenance, essai, fonctionnement) et les installations de verrouillage;
- l'analyse de sûreté:
 - les différents états et accidents répertoriés dans l'analyse de sûreté;
 - les modes de fonctionnement faisant suite aux défaillances uniques des équipements électriques;
- les exigences de puissance électrique pour les conditions ambiantes maximale et minimale;
- les données entrées électriques:
 - exigences de puissance maximale et minimale;
 - plage de tensions;
 - plage de fréquences;
 - rendement et pertes.

Il convient de déterminer à partir d'une évaluation fonctionnelle, des facteurs de charges simultanées et de les appliquer aux charges intermittentes.

Lorsque des interconnexions sont prévues, les besoins de puissance des charges interconnectées doivent être pris en compte.

Lors d'un basculement de source électrique, une charge non classée de sûreté doit être prise en compte comme une charge permanente dans le bilan de puissance, si elle n'est pas déconnectée par un équipement de sûreté.

Il convient que le bilan de puissance prenne en compte:

- les charges actives et la puissance réactive;
- les charges motrices inductives;
- les événements initiateurs postulés;
- les états de fonctionnement et les équipements de secours;
- les temps de démarrage et les durées de mission;
- le type de réseau (interruption et sans interruption).

7.4.2.5 Niveau de tension

Il convient que les niveaux de tension nominaux pour l'alimentation de tous les systèmes, à l'exception du système du générateur principal, soient conformes aux Tableaux 1 et 3 et aux colonnes "préférentielles" du Tableau 6 de l'IEC 60038.

Il convient que le niveau de tension soit adapté à la puissance exigée et aux exigences de coordination électrique.

Il convient d'utiliser les exigences fonctionnelles pour optimiser les niveaux de tension.

7.4.2.6 Etudes relatives aux dispositifs de coupure

Il convient qu'une étude justifie la position dans le système de distribution et la mission de chaque dispositif de coupure.

Le choix du dispositif de coupure doit reposer sur cette étude.

7.4.2.7 Stratégie de distribution

Il convient que la stratégie de distribution (utilisation de sous-distribution) optimise la disposition de mise en œuvre des équipements électriques.

La stratégie de distribution ne doit pas diminuer la conformité du système électrique important pour la sûreté interruptible en courant alternatif aux exigences applicables (6.2, 6.3, 6.4 et 6.5).

La stratégie de distribution ne doit pas compromettre le fonctionnement exigé en cas de perturbations électriques.

7.4.2.8 Système de mise à la terre

Le système de mise à la terre doit fournir un chemin de faible impédance pour le raccordement des équipements électriques à la terre afin d'empêcher l'apparition de tensions dangereuses sur l'équipement et de contribuer à la gestion des interférences électromagnétiques, y compris du phénomène de foudre.

Pour chaque réseau du système d'alimentation interruptible et sans interruption, il convient de définir la connexion du système de mise à la terre selon:

- la fiabilité du réseau (en cas de court-circuit, par exemple);
- la capacité à détecter le premier défaut.

Il convient que la conception du plan de protection électrique tienne compte du système de mise à la terre.

7.4.2.9 Etude du verrouillage

Dans le cas des tableaux équipés d'installations pour le raccordement de différentes sources d'alimentation, un système de verrouillage doit être prévu.

Il convient de prévoir des verrouillages entre les disjoncteurs afin d'empêcher la connexion de circuits en parallèle, susceptible de provoquer des conditions de tension ou de courant dommageables sur les tableaux.

7.4.2.10 Etude de la perte de la tension de commande

Il convient de réaliser une étude de la perte de la tension de commande pour déterminer l'effet de la perte de la tension de commande sur le fonctionnement des systèmes.

7.4.3 Conception du système d'alimentation électrique interruptible

Le système d'alimentation électrique interruptible en courant alternatif peut être divisé en trois parties:

- le système d'alimentation électrique interruptible en courant alternatif alimentant les charges de la centrale lors de l'exploitation normale et des incidents de fonctionnement prévus;
- les systèmes électriques importants pour la sûreté interruptibles en courant alternatif comprenant:
 - le système électrique de sûreté interruptible prenant en charge les DBC;
 - le système d'alimentation électrique important pour la sûreté interruptible prenant en charge les DEC.

La conception du système d'alimentation interruptible doit couvrir:

- l'alimentation préférentielle;
 - la conception de l'alimentation externe;
 - la conception de l'alimentation interne préférentielle;
- des systèmes électriques importants pour la sûreté interruptibles en courant alternatif;
- des sources internes de secours.

NOTE Une norme de second niveau (IEC 63272) couvre la conception du système d'alimentation interruptible.

7.4.4 Conception du système d'alimentation électrique sans interruption

Le système d'alimentation sans interruption peut être divisé en trois parties:

- le système d'alimentation électrique sans interruption alimentant les charges de la centrale lors de l'exploitation normale et des incidents de fonctionnement prévus;
- les systèmes électriques importants pour la sûreté sans interruption comprenant:
 - le système électrique de sûreté sans interruption prenant en charge les DBC;
 - du système d'alimentation électrique important pour la sûreté sans interruption prenant en charge les DEC.

La conception du système d'alimentation sans interruption doit couvrir:

- les systèmes électriques importants pour la sûreté sans interruption;
- les sources électriques.

NOTE Une norme de second niveau (IEC 61225) couvre la conception du système d'alimentation sans interruption.

7.5 Maintenance

7.5.1 Considérations relatives à la maintenance lors de la conception électrique

Il convient d'envisager les dispositions suivantes afin de venir en appui de la continuité des alimentations pendant les activités de maintenance:

- redondance de la fonction ou de l'équipement concerné;
- interconnexion temporaire entre divisions.

Lors des coupures visant à faciliter les opérations de maintenance, le nombre de sources de puissance et de tableaux utilisables peut être réduit conformément aux limites et conditions d'exploitation de la centrale. La conception du système d'alimentation doit tenir compte de l'exigence relative à la maintenance de l'équipement électrique tout en respectant les limites d'exploitation définies.

En cas de maintenance au cours de demandes opérationnelles d'un système de sûreté, l'utilisation d'interconnexions convient d'être considérée pendant une période de maintenance définie.

Lorsqu'elles sont adoptées, des connexions temporaires entre les divisions redondantes peuvent être réalisées à l'arrêt si une évaluation de la sûreté confirme que:

- les interconnexions comportent des verrouillages qui ne peuvent pas être défaits par simple actionnement d'un organe de coupure;
- les effets de ces connexions sur la fiabilité des fonctions de sûreté de la centrale et sur leur vulnérabilité aux défaillances de cause commune sont acceptables.

Les interconnexions des systèmes de sûreté doivent satisfaire aux critères suivants:

- justification du caractère acceptable de l'interconnexion du point de vue de la sûreté;
- mise à disposition de deux dispositifs d'isolement électrique en série, un à chaque extrémité;
- preuve que l'utilisation de l'interconnexion ne provoquera pas de défaillance électrique sur la division alimentée, entraînant la perte de la division d'alimentation;
- les interconnexions ne doivent pas augmenter le niveau des défaillances possibles au-delà du niveau de résilience des équipements ;
- être mises hors tension lors de l'exploitation normale, sauf lorsque des activités de maintenance l'exigent.

Il convient d'inclure dans la conception des systèmes d'alimentation électrique des plans de maintenance pour tous les systèmes et composants.

Il convient de concevoir les systèmes d'alimentation électrique importants pour la sûreté de manière à faciliter les activités de surveillance et de maintenance, à permettre un accès rapide et, en cas de défaillance ou d'erreur, à permettre un diagnostic et une réparation faciles afin de réduire les risques pour le personnel de maintenance.

La stratégie de maintenance doit établir les éventuels besoins des équipements électriques en termes de système de surveillance d'état afin de faciliter la surveillance et la maintenance.

Les dispositions de conception visant à faciliter la maintenance, le dépannage et la réparation comprennent:

- le fait d'éviter de placer les équipements dans des zones soumises à des conditions de température ou d'humidité extrêmes;
- le fait d'éviter de placer les équipements dans des zones soumises à des niveaux de rayonnement élevés;
- la prise en compte des facteurs humains (capacités et limites) lors de l'exécution des activités de maintenance exigées;
- la mise à disposition d'un espace suffisant autour de l'équipement pour s'assurer que les équipes de maintenance puissent remplir leurs tâches en toute sécurité dans des conditions de travail normales.

Il convient d'évaluer les dispositions relatives à la maintenance des systèmes d'alimentation électrique importants pour la sûreté afin de confirmer que tous les effets sur la sûreté de la centrale sont acceptables.

NOTE Les essais périodiques sont traités en 7.2.7.3.

7.6 Systèmes d'alimentation électrique partagés sur un site à tranches multiples

Il convient qu'une agression ou une perturbation électrique dans une tranche ne perturbe pas une autre tranche.

7.7 Installation du système électrique

Il convient que l'installation du système électrique:

- assure l'indépendance entre:
 - les parties redondantes ou diversifiées d'une fonction importante pour la sûreté;
 - les systèmes électriques importants pour la sûreté et les autres systèmes:
 - a) équipements interconnectés:
 - i) classement;
 - ii) isolement;
 - b) équipements adjacents:
 - i) séparation;
 - ii) isolement électrique;
 - iii) barrières physiques;
- soit conforme aux:
 - réglementations nationales relatives aux issues de secours et à la gestion de la lutte contre les incendies;
 - exigences de la centrale concernant:
 - c) les règles d'installation des équipements électriques et des câbles, par exemple:
 - i) exigences de ségrégation;
 - ii) optimisation du cheminement des câbles, de leurs longueurs et de leurs sections;
 - iii) conception des chemins de câble avec différents composants (boîtiers, châssis, bornes); supports de câbles, types de câbles (cuivre, fibre), ouvertures électriques et d'I&C et locaux d'équipement;
 - iv) chemin de câble et implantation;
 - v) conception des locaux d'équipement;
 - d) la réduction des conséquences des agressions;
 - e) le choix des câbles pour les infrastructures de construction, les systèmes d'I&C et les systèmes d'alimentation;
 - f) l'accès facile pour la maintenance et l'installation des câbles.

7.8 Systèmes supports et associés au système d'alimentation électrique

Le classement de sûreté et la conception des systèmes associés et supports doivent permettre de s'assurer que les performances de ces systèmes sont cohérentes avec l'importance pour la sûreté du système ou du composant qu'ils desservent dans la centrale nucléaire de puissance.

a) Systèmes à air comprimé

La spécification de tout système à air comprimé desservant un élément important pour la sûreté du système électrique dans la centrale nucléaire de puissance doit définir les exigences en matière de qualité, de débit et de pureté de l'air.

b) Systèmes de climatisation et de ventilation.

Il convient de prévoir des systèmes de climatisation, de chauffage, de refroidissement et de ventilation, selon ce qui est approprié, dans les locaux auxiliaires ou autres zones de la centrale nucléaire de puissance afin de maintenir les conditions d'environnement exigées pour le système électrique et les composants importants pour la sûreté dans tous les états de la centrale.

Une attention particulière doit être accordée au système de ventilation des locaux électriques présentant un risque d'atmosphère explosive (locaux des batteries, par exemple).

c) I&C

Le système d'I&C qui permet de surveiller et de commander le système électrique important pour la sûreté doit être développé conformément à la norme IEC 61513.

Il convient de gérer durant la conception l'interface entre les signaux électriques et la salle de commande principale ou les indicateurs et alarmes locaux (IHM).

L'IEC 60964 établit des exigences pour l'interface homme-machine dans les salles de commande principales des centrales nucléaires.

Il convient d'évaluer la fiabilité des alimentations électriques des systèmes de surveillance et de commande.

d) Eclairage

Il convient que la stratégie relative à l'éclairage tienne compte des exigences applicables aux locaux électriques pour toutes les conditions afin d'affecter les charges requises à alimenter avec une source de secours.

e) Système de communication

Il convient de définir une stratégie pour le système de communication couvrant toutes les conditions.

f) Système de commande de la tension

Il convient d'évaluer la fiabilité de l'alimentation électrique des systèmes de commande de la tension.

Il convient d'accorder une attention particulière à ces systèmes supports afin de limiter le risque de perturbations lors de l'exploitation du système d'alimentation électrique ou le risque de DCC affectant l'ensemble du système d'alimentation électrique en raison d'une ou de plusieurs défaillances des systèmes supports. Il convient que la conception électrique définisse les exigences relatives aux systèmes supports.

7.9 Programmes d'assurance qualité d'ensemble

Cette norme part de l'hypothèse qu'un programme d'assurance qualité ou de préférence un système de gestion intégré de la qualité existe comme partie essentielle du projet de la centrale nucléaire de puissance et qu'il en assure un contrôle des activités constitutives.

Il convient que les composants classés de sûreté du système d'alimentation électrique soient conformes aux exigences des documents de l'AIEA partie 2 du GS-R et du GS-G 3.1.

- a) Les programmes d'assurance qualité doivent être établis et mis en œuvre pour chaque activité liée au cycle de vie d'ensemble du système d'alimentation électrique.
- b) Les programmes d'assurance qualité doivent comprendre toutes les activités qui sont nécessaires pour atteindre le niveau de qualité et les activités qui permettent de vérifier que le niveau de qualité exigée est atteint.
- c) Les activités de vérification doivent être définies dans les plans de vérification. Il convient que les plans de vérification couvrent les ressources, les procédés et les sorties des phases du cycle de vie d'ensemble du système d'alimentation électrique et il convient qu'ils définissent :
 - les procédures et les outils des activités de vérification;
 - les enregistrements à garder et à vérifier;
 - les aspects pertinents pour la sûreté à vérifier;
 - les procédures permettant la résolution des défaillances et des incompatibilités;
 - les critères pour déclarer chaque phase terminée;

- les rapports finaux à produire démontrant la conformité des sorties des phases aux exigences d'entrée et la résolution des anomalies.
- d) Les programmes d'assurance qualité doivent être planifiés et compris dans le programme d'assurance qualité général de la centrale nucléaire de puissance et leurs activités doivent être comprises dans le planning général des activités du projet de la centrale nucléaire.

7.10 Exigences relatives à la documentation produite

7.10.1 Généralités

Il convient de documenter et de contrôler les informations, les analyses et les calculs de support de la conception des systèmes électriques important pour la sûreté conformément au système d'enregistrements de qualité établi pour la centrale.

Il convient de prévoir des enregistrements de documentation aux fins du support de la conception des fonctions ou fonctionnalités d'un système individuel. Il convient de vérifier chaque enregistrement de documentation de conception conformément aux exigences de l'ISO 9001, complétées par les exigences de la partie 2 du GS-R de l'AIEA, et il convient que ces enregistrements contiennent suffisamment d'informations pour permettre un contrôle ou examen supplémentaire indépendant.

Il convient que les informations et les études soient conformes aux éléments répertoriés dans la documentation de support de la conception des systèmes d'alimentation électrique importants pour la sûreté.

Il convient d'inclure dans la documentation relative aux systèmes d'alimentation électrique:

- les bases de conception;
- une description de l'ensemble du système d'alimentation électrique, y compris:
 - des détails concernant la façon dont la centrale nucléaire de puissance est connectée au réseau;
 - une explication du degré de redondance du système d'alimentation électrique important pour la sûreté;
 - l'identification des interfaces avec les systèmes auxiliaires;
- une description des critères de séparation pour l'installation d'équipements, de câbles et de chemins de roulement, y compris le câblage et les composants internes des panneaux;
- des schémas unifilaires, des diagrammes de contrôle fonctionnel, des schémas, des diagrammes de connexion, des diagrammes de câblages de panneaux et des descriptions des systèmes;
- des plans d'implantation du système d'alimentation électrique interne, ainsi que l'agencement des équipements et des systèmes supports associés;
- des plans d'installation des chemins de câbles, y compris les trémies, goulottes et conduites, dans l'ensemble de la centrale et l'identification des divisions redondante ainsi que des câbles redondants et leur cheminement;
- des séquences par chemin de câble présentant les câbles contenus dans chaque tronçon de chemin de câble et le pourcentage de remplissage de chaque tronçon;
- des araignées de câblage identifiant, pour chaque câble, les points de connexion, le type de câble et le cheminement à travers le système de chemin de câble;
- une analyse des charges électriques présentant l'inventaire des charges électriques. Pour les systèmes électriques importants pour la sûreté, il convient que cela permette d'établir un taux de charge en fonction du temps à partir duquel les capacités des composants nécessaires des systèmes électriques sont calculées;
- les procédures d'exploitation et les manuels de maintenance des systèmes et équipements électriques;

- les exigences concernant les essais périodiques et la maintenance des systèmes et équipements électriques;
- la documentation des essais d'acceptation et de mise en service des systèmes et équipements électriques;
- les enregistrements de management de la qualité;
- l'analyse des perturbations de courant, de tension et de fréquence;
- des études électriques en régime établi et des études de profil de tension présentant les tensions dans l'ensemble du système électrique pour différents modes de fonctionnement de la centrale (et la charge de générateur en fonction du facteur de puissance), y compris les événements de dimensionnement, l'exploitation normale et les conditions de dégradation de tension;
- des études transitoires présentant le profil des charges appliquées de manière séquentielle aux alimentations préférentielles et aux sources de secours dans différents modes de fonctionnement de la centrale;
- une étude de basculement de source électrique analysant les effets de la tension, de l'angle de phase et de la fréquence, ainsi que les effets de la réaccélération d'un moteur sur les tableaux et les moteurs avant, pendant et immédiatement après les transferts automatiques;
- des études de court-circuit permettant de déterminer les courants de défaut maximaux et minimaux dans l'ensemble du système électrique pour différents modes de fonctionnement de la centrale, y compris les événements de dimensionnement, afin de les utiliser pour analyser l'élimination des défauts et la capacité de tenue de l'équipement électrique;
- des études de coordination des dispositifs de protection et des études des équipements de protection présentant le choix du point de consigne approprié pour tous les systèmes de protection;
- l'analyse des capacités de stockage de combustible des sources de secours;
- l'analyse des conséquences d'une perte partielle ou totale des alimentations;
- des plans de qualification des équipements, des analyses et des rapports d'essais;
- les spécifications des composants électriques.

7.10.2 Principes d'architecture

Il convient de produire un document relatif aux principes d'architecture du système d'alimentation électrique ainsi qu'un schéma afin d'identifier les caractéristiques principales des systèmes électriques importants pour la sûreté:

- Disposition de sûreté (voir 7.2):
 - l'analyse des règles déterministes de sûreté applicables;
 - les événements applicables de la centrale;
 - l'approche de défense en profondeur de la centrale et son application pour le système d'alimentation électrique;
 - le nombre de divisions électriques basé sur le cumul des exigences de sûreté et de maintenance applicables;
 - l'analyse des risques liés aux DCC;
 - les exigences de diversification applicables au système d'alimentation électrique et à ses équipements;
 - l'attribution des (groupes respectifs de) fonctions ou des charges principales;
 - le nombre et le type de sources internes (CA, CC);
 - le classement des systèmes électriques;
 - les dispositions applicables en matière d'indépendance au niveau sous-système.
- Disposition de conception électrique (voir 7.3):
 - conformité aux exigences de l'opérateur du réseau électrique;

- rapport d'identification des perturbations électriques (avec si possible des mesures) et les impacts associés sur les grandeurs électriques (tension, intensité et fréquence);
 - études des perturbations électriques (couvrant les études de transitoires et de défauts);
 - exigences de performance pour les charges électriques;
 - performances du système d'alimentation électrique prenant en compte les différentes sources électriques associées avec les différents niveaux de défense en profondeur (reposant sur les quatre articles précédents);
 - études des flux de charge (load flow);
 - études de basculement de source;
 - caractéristique en termes de tenue pour les équipements électriques du système d'alimentation électrique;
 - schéma de protection et études de coordination des protections électriques.
- Dispositions fonctionnelles (voir 7.4)
 - agencement des organes de coupure, sources de puissance et convertisseurs;
 - agencement des connexions au réseau;
 - tensions des systèmes d'alimentation électriques;
 - caractéristiques des sources internes;
 - caractéristiques des composants de conversion;
 - système de raccordement à la terre;
 - liste consommateur et répartition des charges sur le schéma unifilaire;
 - bilan de puissances pour les différents tableaux électriques;
 - rapport de sélection des niveaux de tension;
 - dimensionnement des principaux équipements électriques;
 - dimensionnement des appareils de protection;
 - étude des organes de coupure;
 - rapport de sélection du système de mise à la terre pour chaque réseau;
 - étude d'interverrouillage;
 - dispositifs de surveillance;
 - étude de la perte de la tension de commande.
 - Caractéristiques de maintenance (voir 7.5):
 - Il convient que l'exploitant puisse documenter les exigences de maintenance de la centrale et les mesures associées.
 - Il convient que les interconnexions soient identifiées dans les schémas unilaires.

7.10.3 Schémas unilaires

Il convient qu'un schéma unifilaire global identifie les caractéristiques principales du système d'alimentation électrique:

- l'agencement de la distribution avec les organes de coupure, sources de puissance et convertisseurs correspondants;
- l'agencement des connexions au réseau;
- la tension des systèmes d'alimentation électrique;
- la puissance des sources de secours;
- la puissance des convertisseurs de puissance;
- les connexions du système de mise à la terre;
- les dispositions relatives aux interconnexions.

8 Exigences relatives aux sous-systèmes

8.1 Exigences du système d'alimentation électrique

8.1.1 Généralités

Le présent article a pour objet de présenter une liste générique de sujets à traiter lors de la rédaction d'une norme de second niveau.

Les exigences suivantes sont en particulier applicables à deux sous-systèmes principaux:

- alimentation interruptible;
- alimentation sans interruption.

8.1.2 Conception du système

Les normes de second niveau relatives aux deux sous-systèmes électriques principaux suivent la même structure que le présent document (IEC 63046).

Les normes définissent:

- la conception des systèmes par rapport aux exigences de sûreté;
- la conception des systèmes en fonction des exigences électriques;
- la conception des systèmes en fonction des exigences fonctionnelles et de performances;
- la conception des systèmes en fonction des exigences de maintenance;
- les interfaces du système: identifier et spécifier les exigences relatives aux interfaces susceptibles de compromettre, par leur défaillance fonctionnelle, les fonctionnalités de support auxiliaires des systèmes d'alimentation électrique.

8.1.3 Schéma unifilaire

Il convient que le schéma unifilaire des alimentations interruptibles en courant alternatif et/ou des alimentations sans interruption définisse:

- les limites du système et les interfaces avec les systèmes en amont et en aval;
- la partie classée de sûreté (y compris la classe de sûreté associée) et la partie non classée de sûreté des circuits.

8.2 Spécification de conception des équipements

Il convient d'inclure les règles de conception applicables aux différents éléments des équipements électriques dans la norme de second niveau qui déterminera, à partir de la présente norme de premier niveau, les paramètres suivants:

- tension et fréquence assignées;
- régime établi (plage de tensions et plages de fréquences);
- caractéristiques de tenue en fonction des transitoires de tension et de courant maximales calculées;
- exigences de puissance dérivées de la liste consommateur ou du bilan de puissance;
- autonomie (des alimentations);
- conditions ambiantes d'environnement.