

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
1500**

Première édition
First edition
1996-03

Centrales nucléaires –

**Systèmes de contrôle commande
importants pour la sûreté – Prescriptions
fonctionnelles pour la transmission
de données multiplexées**

Nuclear power plants –

**Instrumentation and control systems
important to safety – Functional
requirements for multiplexed data
transmission**



Numéro de référence
Reference number
CEI/IEC 1500: 1996

Numéros des publications

Depuis le 1^{er} janvier 1997, les publications de la CEI sont numérotées à partir de 60000.

Publications consolidées

Les versions consolidées de certaines publications de la CEI incorporant les amendements sont disponibles. Par exemple, les numéros d'édition 1.0, 1.1 et 1.2 indiquent respectivement la publication de base, la publication de base incorporant l'amendement 1, et la publication de base incorporant les amendements 1 et 2.

Validité de la présente publication

Le contenu technique des publications de la CEI est constamment revu par la CEI afin qu'il reflète l'état actuel de la technique.

Des renseignements relatifs à la date de reconfirmation de la publication sont disponibles dans le Catalogue de la CEI.

Les renseignements relatifs à des questions à l'étude et des travaux en cours entrepris par le comité technique qui a établi cette publication, ainsi que la liste des publications établies, se trouvent dans les documents ci-dessous:

- «Site web» de la CEI*
- **Catalogue des publications de la CEI**
Publié annuellement et mis à jour régulièrement (Catalogue en ligne)*
- **Bulletin de la CEI**
Disponible à la fois au «site web» de la CEI* et comme périodique imprimé

Terminologie, symboles graphiques et littéraux

En ce qui concerne la terminologie générale, le lecteur se reportera à la CEI 60050: *Vocabulaire Electrotechnique International* (VEI).

Pour les symboles graphiques, les symboles littéraux et les signes d'usage général approuvés par la CEI, le lecteur consultera la CEI 60027: *Symboles littéraux à utiliser en électrotechnique*, la CEI 60417: *Symboles graphiques utilisables sur le matériel. Index, relevé et compilation des feuilles individuelles*, et la CEI 60617: *Symboles graphiques pour schémas*.

* Voir adresse «site web» sur la page de titre.

Numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series.

Consolidated publications

Consolidated versions of some IEC publications including amendments are available. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Validity of this publication

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology.

Information relating to the date of the reconfirmation of the publication is available in the IEC catalogue.

Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is to be found at the following IEC sources:

- **IEC web site***
- **Catalogue of IEC publications**
Published yearly with regular updates (On-line catalogue)*
- **IEC Bulletin**
Available both at the IEC web site* and as a printed periodical

Terminology, graphical and letter symbols

For general terminology, readers are referred to IEC 60050: *International Electrotechnical Vocabulary* (IEV).

For graphical symbols, and letter symbols and signs approved by the IEC for general use, readers are referred to publications IEC 60027: *Letter symbols to be used in electrical technology*, IEC 60417: *Graphical symbols for use on equipment. Index, survey and compilation of the single sheets* and IEC 60617: *Graphical symbols for diagrams*.

* See web site address on title page.

**NORME
INTERNATIONALE
INTERNATIONAL
STANDARD**

**CEI
IEC
1500**

Première édition
First edition
1996-03

Centrales nucléaires –

**Systèmes de contrôle commande
importants pour la sûreté – Prescriptions
fonctionnelles pour la transmission
de données multiplexées**

Nuclear power plants –

**Instrumentation and control systems
important to safety – Functional
requirements for multiplexed data
transmission**

© CEI 1996 Droits de reproduction réservés — Copyright — all rights reserved

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'éditeur.

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 the publisher.

Bureau Central de la Commission Electrotechnique Internationale 3, rue de Varembe Genève, Suisse



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE

S

Pour prix, voir catalogue en vigueur
For price, see current catalogue

SOMMAIRE

	Pages
AVANT-PROPOS	4
INTRODUCTION	6
Articles	
1 Domaine d'application et objet	8
2 Références normatives	8
3 Définitions	10
4 Prescriptions générales	12
4.1 Séparation physique et séparation fonctionnelle des équipements	12
4.2 Détection des défaillances et reconfiguration	14
4.3 Signaux d'entrée et de sortie	18
4.4 Logiciel	18
4.5 Matériel	20
5 Prescriptions de performance	20
5.1 Fiabilité	20
5.2 Redondance interne et indépendance	20
5.3 Isolement électrique	22
5.4 Transmission de l'information	22
5.5 Maintenance et dispositifs d'essais	24
6 Essais	26
6.1 Essais fonctionnels	26
6.2 Qualification de l'équipement	28
Annexes	
A Extrait du Guide de sûreté 50-SG-D8 de l'AIEA	30
B Systèmes représentatifs de transmission de données multiplexées	32
C Réponses aux commandes	38
D Environnements représentatifs	40

CONTENTS

	Page
FOREWORD	5
INTRODUCTION	7
Clause	
1 Scope and object	9
2 Normative references	9
3 Definitions	11
4 General requirements	13
4.1 Physical separation and equipment functional separation	13
4.2 Failure detection and reconfiguration	15
4.3 Input and output signals	19
4.4 Software	19
4.5 Hardware	21
5 Performance requirements	21
5.1 Reliability	21
5.2 Internal redundancy and independence	21
5.3 Electrical isolation	23
5.4 Information transmission	23
5.5 Maintenance and test features	25
6 Testing	27
6.1 Functional testing	27
6.2 Equipment qualification	29
Annexes	
A IAEA Safety Guide 50-SG-D8 extract	31
B Representative multiplexed data transmission systems	33
C Control responses	39
D Representative environments	41

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

CENTRALES NUCLÉAIRES — SYSTÈMES DE CONTRÔLE COMMANDE IMPORTANTS POUR LA SÛRETÉ — PRESCRIPTIONS FONCTIONNELLES POUR LA TRANSMISSION DE DONNÉES MULTIPLEXÉES

AVANT-PROPOS

- 1) La CEI (Commission Electrotechnique Internationale) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI 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, la CEI, entre autres activités, publie des Normes internationales. 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant des questions techniques, représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux intéressés sont représentés dans chaque comité d'étude.
- 3) Les documents produits se présentent sous la forme de recommandations internationales; ils sont publiés sous forme de normes, rapports techniques ou guides et agréés comme tels par les Comités nationaux.
- 4) Dans le but d'encourager l'unification internationale, les Comités nationaux de la CEI s'engagent à appliquer de façon transparente, dans toute la mesure du possible, les Normes internationales de la CEI dans leurs normes nationales et régionales. Toute divergence entre la norme de la CEI et la norme nationale ou régionale correspondante doit être indiquée en termes clairs dans cette dernière.
- 5) La CEI n'a fixé aucune procédure concernant le marquage comme indication d'approbation et sa responsabilité n'est pas engagée quand un matériel est déclaré conforme à l'une de ses normes.
- 6) L'attention est attirée sur le fait que certains des éléments de la présente Norme internationale peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La Norme internationale CEI 1500 a été établie par le sous-comité 45A : Instrumentation des réacteurs, du comité d'études 45 de la CEI : Instrumentation nucléaire.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
45A/206 /FDIS	45A/219/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.

Les annexes A, B, C et D sont données uniquement à titre d'information.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

NUCLEAR POWER PLANTS —

INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY —
FUNCTIONAL REQUIREMENTS FOR MULTIPLEXED DATA TRANSMISSION

FOREWORD

- 1) The IEC (International Electrotechnical Commission) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of the IEC is to promote international cooperation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, the IEC publishes International Standards. 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 organisations liaising with the IEC also participate in this preparation. The 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 the 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 National Committees.
- 3) The documents produced have the form of recommendations for international use and are published in the form of standards, technical reports or guides and they are accepted by the National Committees in that sense.
- 4) In order to promote international unification, IEC National Committees undertake to apply IEC International Standards transparently to the maximum extent possible in their national and regional standards. Any divergence between the IEC Standard and the corresponding national or regional standard shall be clearly indicated in the latter.
- 5) The IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with one of its standards.
- 6) Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. IEC shall not be held responsible of identifying any or all such patent rights.

International Standard IEC 1500 has been prepared by sub-committee 45A: Reactor instrumentation, of IEC technical committee 45: Nuclear instrumentation.

The text of this standard is based on the following documents:

FDIS	Report on voting
45A/206/FDIS	45A/219/RVD

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

Annexes A, B, C and D are for information only.

INTRODUCTION

La présente Norme internationale définit les prescriptions fonctionnelles des systèmes de transmission de données multiplexées tirées du Guide de sûreté 50-SG-D8 de l'AIEA, section 4.12 (reproduit dans l'annexe A), et leur extension aux systèmes de catégorie A¹. Il sert également de guide aux fabricants pour l'application des prescriptions concernant les centrales nucléaires.

Les équipements de multiplexage peuvent être utilisés à des fins spécifiques, par exemple pour l'isolement électrique ou pour la réduction des risques de feu dus au câblage. L'équipement de multiplexage constitue une partie essentielle des systèmes programmés distribués. Il existe des applications dans les systèmes importants pour la sûreté des centrales nucléaires (catégories A, B et C¹). Les prescriptions de l'AIEA et de la CEI sur le multiplexage, le matériel et le logiciel des systèmes programmés sont, de ce fait, applicables.

Les aspects spécifiques importants étudiés dans cette norme sont les suivants:

- a) prescriptions fonctionnelles de l'équipement de multiplexage des systèmes de catégorie A, non couvertes par les Guides de sûreté 50-SG-D8 et 50-SG-D3 de l'AIEA;
- b) conditions de transmission de l'information multiplexée entre les systèmes de catégorie A et les systèmes de catégorie B ou C ou les systèmes non importants pour la sûreté;
- c) redondance interne et moyens de détection des pannes, nécessaires dans un sous-système centralisé de transmission de données multiplexées.

¹ Suivant la classification CEI 1226.

INTRODUCTION

This International Standard defines the functional requirements for multiplexed data transmission systems arising from IAEA Safety Guide 50-SG-D8, section 4.12 (reproduced in annex A), and its extension to category A¹ systems. It also provides manufacturers with guidance on nuclear power plant requirements.

Multiplexing equipment can be used for special purposes, for example for electrical isolation or for reduction of fire loads due to cabling. In a distributed computer-based system, multiplexing equipment is an essential part of the system. Applications exist in the systems of nuclear power plants important to safety (categories A, B and C¹). Requirements of the IAEA and IEC for multiplexing and for digital computer hardware and software are therefore applicable.

Specific aspects of importance considered in this standard are:

- a) the functional requirements for multiplexing equipment for category A systems, which were not considered by IAEA 50-SG-D8 and IAEA 50-SG-D3;
- b) the conditions for transmission of multiplexed information between a category A system and a category B or C system or to a system not important to safety;
- c) the internal redundancy and failure detection features necessary within a multiplexed data transmission subsystem.

¹ According to IEC 1226 classification.

CENTRALES NUCLÉAIRES —

SYSTÈMES DE CONTRÔLE COMMANDE IMPORTANTS POUR LA SÛRETÉ —

PRESCRIPTIONS FONCTIONNELLES POUR LA TRANSMISSION DE DONNÉES MULTIPLEXÉES

1 Domaine d'application et objet

La présente Norme internationale définit les prescriptions fonctionnelles pour la transmission de données multiplexées utilisées entre des équipements de systèmes de catégorie A² ou entre des équipements de ces systèmes et des équipements de systèmes de catégorie B ou C ou entre des équipements de ces systèmes et des équipements de systèmes non importants pour la sûreté, dans les centrales nucléaires. La présente norme sert de guide pour l'interprétation des prescriptions de multiplexage données en 4.12 dans le Guide de sûreté 50-SG-D8 de l'AIEA. L'AIEA définit le multiplexage comme étant la transmission d'un point à un autre de deux ou plusieurs signaux ou messages sur une seule voie de transmission de données par modulation temporelle, modulation de fréquences ou modulation par impulsions et codage, ou autres techniques similaires. La présente norme suit la définition de l'AIEA. Elle donne des prescriptions concernant la transmission de données avec envoi répétitif de messages, dans une direction principale, selon un cycle déterminé, sans variation notable en quantité. Elle s'applique seulement aux équipements de multiplexage, démultiplexage et transmission de données utilisés pour envoyer des données d'un équipement à un autre, en mode point à point.

La présente norme ne comprend pas de spécifications sur la technologie des équipements. Elle ne couvre pas non plus les équipements de transmission de données multiplexées utilisés entre des systèmes non importants pour la sûreté ou utilisés directement pour le fonctionnement des unités de visualisation (tubes à rayonnement cathodique). Les réseaux locaux ne font pas partie du domaine d'application de cette norme. La présente norme ne s'applique pas aux liaisons internes et à la transmission de données entre une unité de traitement, sa mémoire et la logique de commande. Elle ne concerne pas le fonctionnement interne des systèmes informatiques de contrôle commande³.

2 Références normatives

Les documents normatifs suivants contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions valables pour la présente Norme internationale. Au moment de la publication, les éditions indiquées étaient en vigueur. Tout document normatif est sujet à révision et les parties prenantes aux accords fondés sur la présente Norme internationale sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 68: *Essais d'environnement*

CEI 231A: 1969, *Principes généraux de l'instrumentation des réacteurs nucléaires – Premier complément*

AIEA Code 50-C-D: 1988, *Conception pour la sûreté des centrales nucléaires*

² Les catégories A, B, C mentionnées dans cette norme sont définies dans la CEI 1226.

³ Les diagrammes fournis en annexe B illustrent les liaisons multiplexées couvertes par cette norme.

NUCLEAR POWER PLANTS —

INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY — FUNCTIONAL REQUIREMENTS FOR MULTIPLEXED DATA TRANSMISSION

1 Scope and object

This International Standard establishes the functional requirements for multiplexed data transmission which is used between equipment of category A² systems or between equipment of these systems and equipment of category B or C systems or between equipment of these systems and equipment of systems not important to safety, in nuclear power plants. This standard gives guidance on interpretation of the requirements for multiplexing stated in 4.12 of IAEA Safety Guide 50-SG-D8. The IAEA defines multiplexing as the transmission from one location to another of two or more signals or messages over a single data channel by use of time division, frequency division, pulse code techniques or the like. This standard follows the IAEA definition. It gives requirements for data transmission where a fixed cycle of messages is sent, mainly in one direction, repeatedly with no significant variation of quantity. It covers only multiplexing, demultiplexing and data transmission equipment used to send data from one equipment to another, in a point-to-point mode.

This standard does not include detailed equipment specifications. It also does not cover multiplexed data transmission equipment used between systems not important to safety, or used directly for operation of VDUs (CRT displays). Local Area Networks (LAN) are not in the scope of this standard. This standard is not applicable to the internal connections and data transmission of a processor unit, its memory and control logic. It does not concern internal processing of instrumentation and control computer systems³.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. At the time of publication, the editions indicated were valid. All normative documents are subject to revision, and parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 68: *Environmental testing*

IEC 231A: 1969, *General principles of nuclear reactor instrumentation – First supplement*

IAEA Code 50-C-D: 1988, *Code on the safety of nuclear power plants: Design*

² The categories A, B, C referenced in this standard are defined in IEC 1226.

³ Diagrams are shown in annex B to illustrate multiplexed connections discussed in the standard.

AIEA Guide de sûreté 50-SG-D3: 1981, *Système de protection et dispositifs associés dans les centrales nucléaires*

NOTE – Les paragraphes 7.9, 7.10 et 9.2 sont tout particulièrement applicables.

AIEA Guide de sûreté 50-SG-D8: 1985, *Systèmes d'instrumentation et de commande liés à la sûreté dans les centrales nucléaires*

NOTE – Les paragraphes 3.2, 3.3, 4.3 et 4.12 sont tout particulièrement applicables.

CEI 639: 1979, *Réacteurs nucléaires – Utilisation du système de protection à d'autres fins que la sécurité*

CEI 709: 1981, *Séparation dans le système de protection des réacteurs*

CEI 721: *Classification des conditions d'environnement*

CEI 780: 1984, *Qualification des constituants électriques du système de sûreté des centrales électronucléaires*

CEI 801: *Compatibilité électromagnétique pour les matériels de mesure et de commande dans les processus industriels*

CEI 880: 1986, *Logiciel pour les calculateurs utilisés dans les systèmes de sûreté des centrales nucléaires*

CEI 964: 1989, *Conception des salles de commande des centrales nucléaires de puissance*

CEI 965: 1989, *Points de commande supplémentaires pour l'arrêt des réacteurs sans accès à la salle de commande principale (salle de commande de repli)*

CEI 980: 1989, *Pratiques recommandées pour la qualification sismique du matériel électrique du système de sûreté dans les centrales électronucléaires*

CEI 987: 1989, *Calculateurs programmés importants pour la sûreté des centrales nucléaires*

CEI 1226: 1993, *Centrales nucléaires – Systèmes d'instrumentation et de contrôle-commande importants pour la sûreté – Classification*

3 Définitions

Pour les besoins de la présente Norme internationale, les définitions de la CEI 880 et du Guide de sûreté 50-SG-D8 de l'AIEA s'appliquent, ainsi que les définitions suivantes:

- 3.1 **transmission de données multiplexées:** Transmission d'un point à un autre de deux ou plusieurs signaux ou messages sur une seule voie de transmission de données par modulation temporelle, modulation de fréquences ou modulation par impulsions et codage ou autres techniques similaires (issue du Guide de sûreté 50-SG-D8 de l'AIEA).
- 3.2 **multiplexage:** Centralisation de données provenant de plusieurs voies et traitement de ces données pour la transmission par une unité de transmission de données multiplexées.
- 3.3 **démultiplexage:** Reconstitution de données provenant d'un système de transmission de données multiplexées dans le but de former un ensemble de signaux maintenant ses valeurs ou ses états jusqu'à leur régénération par une nouvelle transmission.

IAEA Safety Guide 50-SG-D3: 1980, *Protection system and related features in nuclear power plants*

NOTE – Subclauses 7.9, 7.10 and 9.2 are of specific relevance.

IAEA Safety Guide 50-SG-D8: 1984, *Safety-related instrumentation and control systems for nuclear power plants*

NOTE – Subclauses 3.2, 3.3, 4.3 and 4.12 are of specific relevance.

IEC 639: 1979, *Nuclear reactors – Use of the protection system for non-safety purposes*

IEC 709: 1981, *Separation within the reactor protection system*

IEC 721: *Classification of environmental conditions*

IEC 780: 1984, *Qualification of electrical items of the safety system for nuclear power generating stations*

IEC 801: *Electromagnetic compatibility for industrial-process measurement and control equipment*

IEC 880: 1986, *Software for computers in the safety systems of nuclear power stations*

IEC 964: 1989, *Design for control rooms of nuclear power plants*

IEC 965: 1989, *Supplementary control points for reactor shutdown without access to the main control room*

IEC 980: 1989, *Recommended practices for seismic qualification of electrical equipment of the safety system for nuclear generating stations*

IEC 987: 1989, *Programmed digital computers important to safety for nuclear power stations*

IEC 1226: 1993, *Nuclear power plants – Instrumentation and control systems important for safety – Classification*

3 Definitions

For the purpose of this International Standard, the definitions of IEC 880, IAEA 50-SG-D8 and the following definitions are applicable:

- 3.1 **multiplexed data transmission:** Transmission from one location to another of two or more signals or messages over a single data channel by use of time division, frequency division, pulse code techniques or the like (based on IAEA 50-SG-D8).
- 3.2 **multiplexing:** Collection of data from many channels and its processing for transmission by a multiplexed data transmission unit.
- 3.3 **demultiplexing:** Restoration of data from a multiplexed data transmission system to form a set of signals which maintains its values or states until refreshed by a new transmission.

- 3.4 système de transmission de données multiplexées:** Comprend les équipements de multiplexage, les câbles et les logiciels destinés à la transmission des signaux, la vérification des transmissions et le démultiplexage des signaux en vue d'une utilisation ultérieure. Il exclut le matériel et le logiciel destinés au prétraitement des signaux, et au traitement des signaux après multiplexage.

NOTES

- 1 Une centrale nucléaire comprend des fonctions de protection, de commande et de multiplexage de données avec transmission à d'autres systèmes. Une centrale peut être équipée de systèmes multiplexés séparés pour chacune de ces fonctions, ou regrouper plusieurs fonctions dans un seul système. Les systèmes peuvent être connectés au moyen de liens point à point ou multipoints. Un réseau local (LAN) peut relier plusieurs systèmes communiquant entre eux en vue d'une fonction importante pour la sûreté.
 - 2 L'annexe B décrit et illustre des exemples de multiplexage couverts par le domaine d'application de la présente norme.
- 3.5 redondance:** Présence d'autres éléments ou systèmes (identiques ou différents) de sorte que l'un d'entre eux puisse remplir la fonction requise indépendamment de l'état de fonctionnement ou de la défaillance d'un autre. (AIEA 50-SG-D8)
- 3.6 voie:** Chemin par lequel circule l'information dans un système. Cette voie peut également nécessiter une redondance.

4 Prescriptions générales

4.1 Séparation physique et séparation fonctionnelle des équipements

4.1.1 Séparation physique

Les prescriptions de la CEI 709 s'appliquent aux câbles d'un système de transmission de données multiplexées important pour la sûreté. Il n'est pas nécessaire d'appliquer les prescriptions de la CEI 709 traitant de la séparation entre câbles de puissance et les câbles de signaux, si l'on utilise des câbles à fibre optique pour la transmission des signaux.

La méthode recommandée de séparation physique et de protection des câbles d'un système de transmission de données multiplexées transportant des signaux électriques ou optiques, consiste à utiliser de préférence des canalisations ou goulottes de câbles adaptées, fournissant une protection totale contre les risques.

4.1.2 Séparation fonctionnelle des équipements

Si la séparation des équipements est nécessaire, il convient d'utiliser un matériel distinct pour les fonctions de multiplexage, les fonctions de réception et transmission et les fonctions d'application. Il convient que le logiciel d'application soit séparé du logiciel système pour le multiplexage, la réception et la transmission.

Il convient que la conception prévoie une séparation entre le matériel et le logiciel destinés aux fonctions de transmission de données et les fonctions associées de prétraitement et de post-traitement des signaux. Il convient que la conception prévoie une séparation entre les modules du logiciel destinés aux opérations numériques et logiques réalisées sur le contenu des signaux et des messages et ceux utilisés pour la transmission de données et la vérification des messages. Cela dans le but de réduire la complexité et de simplifier la vérification et la validation.

- 3.4 multiplexed data transmission system:** Includes multiplexing equipment, cables and software for transmitting signals, for checking the transmissions and for demultiplexing the signals for subsequent use. It excludes hardware and software for preprocessing the signals, and for processing the signals after demultiplexing.

NOTES

- 1 A nuclear power plant includes functions for protection, control, and data multiplexing with transmission to other systems. A nuclear power plant might include separate multiplexed data transmission systems for each of the above functions, or integrate several functions into one system. Systems may be connected by point-to-point or multidrop links. A local area network (LAN) may connect several units which communicate with each other for a function important to safety.
 - 2 Examples of multiplexing within the scope of this standard are illustrated and described in annex B.
- 3.5 redundancy:** Provision of alternative (identical or diverse) elements or systems, so that any one can perform the required function regardless of the state of operation or failure of any other. (IAEA 50-SG-D8)
- 3.6 channel:** Path along which information flows through a system. That path may also require redundancy.

4 General requirements

4.1 Physical separation and equipment functional separation

4.1.1 Physical separation

The requirements of IEC 709 are applicable to the cables of a multiplexed data transmission system important to safety. The IEC 709 requirement for separation of power cables from signal cables need not apply if fibre optic cables are used for signal transmission.

The preferred method of physical separation and protection of the cables of a multiplexed data transmission system, whether carrying electrical or optical signals, is the use of dedicated cable enclosures or trunking, providing full protection against hazards.

4.1.2 Equipment functional separation

If equipment separation is needed, separate hardware should be used for multiplexing functions, receive and transmit functions and application functions. Application software should be separated from the system software for multiplexing, receiving and transmitting.

The design should separate the hardware and the software for data transmission functions from the associated signal preprocessing and post-processing functions. The design should separate software modules for the numerical and logical operations performed on signals and message contents, from those used for data transmission and message checking. This will reduce complexity and simplify verification and validation.

Il convient qu'une liaison multiplexée entre des systèmes de catégorie A envoie des informations dans une seule direction. La défaillance de retour d'accusé réception ou d'autres signaux envoyés par le système récepteur ne doit pas empêcher le système émetteur de fonctionner de façon correcte. Le contrôle de ces liaisons doit être inclus dans le système émetteur.

Il convient qu'une liaison multiplexée partant d'un système de catégorie A envoie uniquement des informations. Il convient qu'en utilisation normale ce système ne reçoive pas d'information des systèmes de moindre importance pour la sûreté. La défaillance de retour d'accusé réception ou d'autres signaux envoyés par le système récepteur ne doit pas empêcher le système émetteur de fonctionner correctement. La supervision de ces liaisons doit résider dans le système de plus grande importance pour la sûreté.

Il convient que les liaisons multiplexées en provenance de systèmes de catégories B ou C ou entre ceux-ci envoient uniquement des informations à partir du système de plus haute importance pour la sûreté vers les systèmes d'importance égale ou inférieure pour la sûreté. La défaillance de retour d'accusé réception ou d'autres signaux envoyés par le système récepteur ne doit pas empêcher le système émetteur de fonctionner de façon correcte. La supervision de ces liaisons doit résider dans le système émetteur.

La connexion entre des systèmes d'importance différente pour la sûreté doit comprendre un tampon d'isolement afin d'éviter toute interférence électrique et fonctionnelle avec le système d'importance supérieure pour la sûreté.

4.2 Détection des défaillances et reconfiguration

4.2.1 Détection des défaillances

Le Guide de sûreté 50-SG-D8, 4.12(2) de l'AIEA prescrit des dispositifs de détection d'erreurs. L'équipement de multiplexage doit être équipé de moyens de détection d'erreurs correspondant aux prescriptions de 4.2(d) de la CEI 987, et de 4.8 de la CEI 880. Il convient que les défauts suivants soient détectés et signalés au personnel d'exploitation.

- a) défaillance des bits simples ou groupes de bits à transmettre ou à recevoir;
- b) défaillance d'un bloc simple de message à transmettre, ou à recevoir;
- c) transmission répétée d'un bloc de message sans modification due à des défaillances;
- d) monopolisation du moyen de transmission par l'émetteur ou le récepteur, due à des défaillances ou à d'autres raisons;
- e) différences dans les messages transmis sur des voies redondantes;
- f) erreurs dans les dates et les temps de réponse.

La section 4.12(5) du Guide de sûreté 50-SG-D8 de l'AIEA prescrit la vérification du fonctionnement des dispositifs de détection d'erreurs, dans le cas où ceux-ci sont prévus pour l'amélioration de la transmission des signaux. Cette prescription s'applique dans le cas de dispositifs automatiques de correction d'erreur. Il convient que la méthode de transmission, l'équipement et les câbles soient suffisamment immunisés aux perturbations pour utiliser seulement la détection d'erreurs, sans correction. Il convient que les corrections automatiques d'erreurs ne soient pas permises pour les systèmes de catégorie A.

A multiplexed link between category A systems should send information in only one direction. Failure of acknowledgement or other signals sent by the receiving system shall not prevent the sending system from functioning correctly. The control of such links shall be in the sending system.

A multiplexed link from a category A system should only send information. It should not receive information from systems of lower importance to safety when operating normally on-line. Failure of acknowledgement or other signals sent by the receiving system shall not prevent the sending system from functioning correctly. The control of such links shall be in the system of higher importance to safety.

Multiplexed links from or between systems at category B or C should only send information from the system with higher importance to safety to systems with equal or lower importance to safety. Failure of acknowledgement or other signals sent by the receiving system shall not prevent the sending system from functioning correctly. The control of such links shall be in the sending system.

Connection between systems of different importance to safety shall include an isolating buffer unit to prevent electrical and functional interference with the system of higher importance to safety.

4.2 Failure detection and reconfiguration

4.2.1 Failure detection

IAEA Safety Guide 50-SG-D8, 4.12(2) requires error detection features. The multiplexing equipment shall be provided with error detection facilities according to the requirements of 4.2(d) of IEC 987, and 4.8 of IEC 880. The following should be detected and warnings given to operating staff:

- a) failure of single bits or groups of bits to be transmitted, or to be received;
- b) failure of a single message block to be transmitted, or to be received;
- c) transmission of a message block repeatedly, without change, due to failures;
- d) monopoly of transmission facilities by the transmitter or receiver due to failures or other reasons;
- e) differences in messages transmitted on redundant paths;
- f) scheduling and response time errors.

IAEA 50-SG-D8, 4.12(5) requires verification of the operation of error detection features, if they are provided to improve signal transmission. This requirement applies if automatic error correction facilities are included. The transmission method, equipment and cables should be sufficiently immune to interference to use error detection only, without error correction. Category A systems should not permit automatic error correction.

A l'initialisation du multiplexage ou du démultiplexage, il convient qu'un cycle de détection de défaillances soit initié avant connexion. Il convient que le processus de détection d'erreurs identifie le bon fonctionnement de chaque multiplexeur ou démultiplexeur ou sa défaillance, et fournisse, le cas échéant, des informations ou des alarmes.

4.2.2 Réponse aux défaillances

Il convient que l'équipement de multiplexage fournisse des signaux à l'équipement associé en cas de détection de la défaillance des entrées, ou dans le cas d'une mauvaise réception des messages. Le contrôle commande (I&C) important pour la sûreté peut alors prendre des actions appropriées, choisies de façon à améliorer la sûreté de la centrale.

Lorsque l'on détecte des défaillances de l'équipement de multiplexage ou de ses entrées, il convient que l'équipement de transmission et de réception entreprenne les actions appropriées, incluant:

- a) la reconfiguration permettant la poursuite de l'exploitation, avec indication de la défaillance à l'opérateur;
- b) l'isolement des voies de transmissions défectueuses;
- c) la fourniture de marqueurs de validité des signaux pour identifier les signaux d'entrée défectueux, ou rendus indisponibles par suite de la défaillance de l'équipement. Ces signaux peuvent être ensuite indiqués sur des affichages et des journaux de bord;
- d) la fourniture de marqueurs de validité des signaux afin de permettre aux opérations de commande ou aux mises en action de protection de conduire à une action prédéfinie;
- e) la fourniture de marqueurs de validité des signaux permettant aux indicateurs ou aux alarmes d'indiquer un état identifiable. Les états appropriés peuvent être « pleine échelle » ou à échelle au-dessous de zéro pour les indicateurs, les alarmes ou les témoins lumineux réglés de manière à indiquer directement la défaillance, ou destinés à avertir les opérateurs d'une défaillance en cas de passage d'une commande.

4.2.3 Causes de défaillances du système

Un système de transmission de données multiplexées pourrait être affecté par des conditions provoquant la défaillance simultanée de plusieurs parties redondantes du système. De façon à éliminer ou minimiser la possibilité de défaillance simultanée de plusieurs modules, la conception doit prendre en compte les pannes communes dues à un événement externe à l'équipement, tel que:

- a) perturbation sismique ou autre risque externe;
- b) effet d'incendie ou de fumée dans les équipements ou les zones de câbles;
- c) dysfonctionnement de l'équipement provoqué par une perte de contrôle de l'environnement, chauffage et ventilation, des rayonnements excessifs ou d'autres facteurs affectant l'équipement de multiplexage,

et les pannes dues à des causes internes à l'équipement lui-même, telles que:

- d) une défaillance de mode commun du matériel ou du logiciel du système de transmission de données multiplexées.

Les défaillances prises en compte pendant la conception doivent être documentées.

At multiplexing or demultiplexing initiation, a failure detection cycle of operation should take place before the multiplexer or the demultiplexer is brought on-line. The failure detection process should identify each multiplexer or demultiplexer as operable or failed and provide information and alarms appropriately.

4.2.2 Response to failure

Multiplexing equipment should provide signals to the equipment it serves if inputs are detected to have failed, or messages are not correctly received. Instrumentation and control (I&C) important to safety can then take suitable actions, chosen to enhance the safety of the station.

When failures of multiplexing equipment or its inputs are detected, the transmission and receiving equipment should take actions which include:

- a) reconfiguration to enable continued operation, with indication of failure to the operator;
- b) isolation of failed transmission paths;
- c) providing signal validity markers to identify input signals which have failed, or have become not available due to equipment failure. Those signals can then be indicated on displays and logs;
- d) providing signal validity markers to enable control operations or protection actuations to take a pre-defined action;
- e) providing signal validity markers to enable indicators or alarms to show an identifiable state. Suitable states may be full-scale or below-zero scale for indicators, and alarms or lamps set to a state which directly shows the failure, or which would warn operators of failure if a control were operated.

4.2.3 Causes of system failures

A multiplexed data transmission system could be affected by conditions which cause several redundant parts of the system to fail at the same time. In order to eliminate or minimize the possibility of simultaneous failures of several modules, consideration shall be given during design to common failures due to an event external to the equipment, such as:

- a) seismic disturbance or other external hazards;
- b) effect of fire or smoke in equipment or cable areas;
- c) equipment malfunction caused by loss of environmental control, heating and ventilation, excessive radiation or other factors affecting the multiplexing equipment,

and failures due to causes internal to the equipment itself, such as:

- d) common mode failure of the hardware or software of the multiplexed data transmission system.

The failures taken into account during design shall be documented.

4.3 Signaux d'entrée et de sortie

L'équipement de multiplexage pour la collecte de données doit être capable de fonctionner pour des signaux d'instrumentation standard choisis (par exemple 4 mA à 20 mA, thermocouple de 0 V à 5 V) et pour la détection d'état standard (par exemple fermetures de contact, 0 mA à 10 mA); il doit également être capable de fonctionner directement sur transmissions de signaux venant de capteurs intelligents utilisant un protocole standard reconnu. Il convient que l'équipement de multiplexage permette le fonctionnement de dispositifs de sortie comprenant des lampes à filament, des LED, des relais standards pour les interfaces d'appareillage et des électrovannes. Il convient que l'équipement de multiplexage permette le fonctionnement d'indicateurs ou d'enregistreurs au moyen de convertisseurs numériques-analogiques (DAC) à un niveau de signaux standard (par exemple 4 mA à 20 mA).

Il convient que les signaux et les circuits de sortie de l'équipement de multiplexage soient arrangés de façon à avoir des états de sortie définis lors de coupure d'alimentation. Une lecture des sorties peut être utilisée pour fournir un signal de confirmation de l'état de chaque sortie.

4.4 Logiciel

4.4.1 Prescriptions générales

Les prescriptions de la CEI 880 s'appliquent au logiciel des systèmes de transmission de données multiplexées importants pour la sûreté, en fonction de leur catégorie de sûreté définie par la CEI 1226.

L'utilisation d'un logiciel système ayant fait ses preuves peut être approprié pour:

- a) le contrôle de la transmission de données multiplexées;
- b) le séquençement des tâches d'un groupe de multiplexage;
- c) les fonctions spécifiques uniquement définies par des tableaux de données. Ceux-ci peuvent inclure des données de configuration et d'étalonnage des caractéristiques des signaux, ou des données de configuration pour les modules de conduite, de verrouillage ou de logique séquentielle.

La défaillance du logiciel d'un système de transmission de données multiplexées non important pour la sûreté ne doit pas être capable d'affecter la sûreté de l'équipement important pour la sûreté. La défaillance du logiciel dans un système de transmission de données multiplexées d'une catégorie de sûreté inférieure définie par rapport à la CEI 1226 ne doit pas être capable d'affecter la sûreté des systèmes de catégorie supérieure.

Les données de configuration définissant l'étalonnage, les seuils, la disposition et les fonctions du système, doivent être soumises au même degré de vérification et de validation que le logiciel, selon la classe de sûreté correspondante de la CEI 1226.

4.4.2 Systèmes de catégorie B ou C

La section 4.11 du Guide de sûreté 50-SG-D8 de l'AIEA sur les systèmes informatisés donne les principes à suivre pour les systèmes de catégorie B ou C.

Le logiciel (y compris le logiciel embarqué) pour le multiplexage utilisé dans les systèmes de catégorie B doit être développé selon la démarche structurée en accord avec la CEI 880. Cependant, d'après la CEI 1226, pour la catégorie B, l'application des exigences les plus sévères de la CEI 880 n'est pas imposée.

4.3 *Input and output signals*

Multiplexing equipment for data gathering shall be able to operate for the chosen standard instrument signals (e.g. 4 mA to 20 mA, and 0 V to 5 V thermocouple) and for standard state detection (e.g. contact closures, 0 mA to 10 mA), or shall be able to operate directly from signal transmission from smart sensors using a recognized standard protocol. Multiplexing equipment should allow for operation of output devices including filament lamps, LEDs, standard relays for switchgear interfaces, and solenoid valves. Multiplexing equipment should allow for operation of indicators or recorders by digital to analogue converters (DACs) at a standard signal level (e.g. 4 mA to 20 mA).

Multiplexing equipment output signals and circuits should be arranged to have a defined output state on failure of the power supply. Read-back signals may be used to provide a signal to confirm the state of each output.

4.4 *Software*

4.4.1 *General requirements*

The requirements of IEC 880 are applicable to the software in multiplexed data transmission systems important to safety, according to the categorization defined in IEC 1226.

The use of previously proven system software may be appropriate for:

- a) control of multiplexed data transmission;
- b) scheduling tasks of a multiplexing group;
- c) specific functions which are defined only by data tables. These may include configuration and calibration data on signal characteristics, or configuration data for modules of control, interlock or sequence logic.

Software failure of a multiplexed data transmission system not important to safety shall not be able to affect the safety of equipment important to safety. Software failure in a multiplexed data transmission system of a lower safety category according to IEC 1226 shall not be able to affect the safety of higher category systems.

Data which define calibration, thresholds, system arrangement and functions shall be subjected to a comparable degree of verification and validation as software, at the corresponding safety category of IEC 1226.

4.4.2 *Category B or C systems*

Section 4.11 of IAEA Safety Guide 50-SG-D8, on digital computer systems gives principles to be followed for category B or C systems.

Software (including firmware) for multiplexing used in category B systems shall be developed in a systematic structured fashion in accordance with the intent of IEC 880. However, according to IEC 1226, full application of the most rigorous requirements of IEC 880 is not required.

4.5 Matériel

L'équipement de multiplexage d'un système de catégorie A doit satisfaire aux prescriptions de la CEI 987.

L'équipement de transmission de données multiplexées pour les applications de catégorie B ou C et pour la transmission de systèmes importants pour la sûreté vers des systèmes non importants pour la sûreté doit être évalué conformément à la CEI 987. Toutes les différences par rapport à ces exigences doivent être justifiées en fonction des défaillances potentielles dans l'accomplissement de la fonction liée à la sûreté.

5 Prescriptions de performance

5.1 Fiabilité

Les exigences du système doivent être considérées pour identifier des groupes modulaires adaptés de sorties analogiques et logiques, de même pour les entrées.

Pour un système de transmission de données multiplexées d'un système de catégorie A, une exigence quantifiée sur le taux de fiabilité doit être définie. Ce taux doit être cohérent avec la fiabilité exigée du système concerné. Il convient qu'une estimation soit faite pour montrer que cette fiabilité est atteinte.

Un système de transmission de données multiplexées se comporte comme un seul équipement traversé par de nombreux signaux. Il convient que sa fiabilité soit donc bien meilleure que celle des boucles d'instrumentation ou des voies de commande uniques. Pour chaque système de transmission de données multiplexées utilisé, l'effet des défaillances doit être analysé. En conséquence de cette prescription, pour un système de transmission de données multiplexées utilisé pour rassembler plus d'une cinquantaine de signaux d'entrée, il convient que les défaillances uniques ne provoquent pas la perte de toute l'information.

NOTE – Sur la base d'un jugement d'expert, il peut être considéré qu'une façon possible d'obtenir la modularité du matériel consiste en ce que:

- a) toute défaillance unique du contrôle ou des alimentations conserve la disponibilité de toutes les entrées et sorties. Au minimum, 50 % de toutes les entrées et de toutes les sorties sont toujours disponibles après ce type de défaillance;
- b) la défaillance d'un seul module d'entrée multiplexée ne cause pas de perte supérieure à huit signaux analogiques ou seize signaux numériques;
- c) la défaillance d'un seul module de sortie multiplexée ne cause pas de perte supérieure à huit signaux.

Il convient que le remplacement simple des modules par enfichage soit possible pour restaurer complètement la disponibilité.

5.2 Redondance interne et indépendance

Il convient que l'équipement de multiplexage soit conçu de telle sorte que les défauts ne se propagent pas d'un point à l'autre de l'équipement ou vers un autre système.

La redondance interne doit être déterminée en fonction de la fiabilité requise. Pour atteindre ce niveau de fiabilité, il peut être nécessaire qu'un système de multiplexage comporte lui-même des canaux redondants.

4.5 Hardware

Category A system multiplexing equipment shall meet the requirements of IEC 987.

Multiplexed data transmission equipment for category B or C applications, and for transmission from systems important to safety to systems not important to safety, shall be assessed in relation to IEC 987. Differences from those requirements shall be justified in regard to potential failure to perform the safety-related function.

5 Performance requirements

5.1 Reliability

The system requirements shall be considered to identify suitable modular groups for analogue and contact outputs, and for inputs.

For a multiplexed data transmission system in a category A system, a requirement for a reliability figure shall be defined. This figure shall be consistent with the required reliability of the system concerned. Assessment to show that this reliability is achieved should be done.

A multiplexed data transmission system forms a single set of equipment through which many signals pass. Therefore its reliability should be substantially better than the reliability of any single instrument loop or control path. For each multiplexed data transmission system used, the effects of failures shall be analyzed. Following from this requirement, for a multiplexed data transmission system used to gather more than about 50 input signal, single failures should not cause loss of all information.

NOTE – On the basis of engineering judgement, it may be considered that a possible means of obtaining hardware modularity would be that:

- a) any single failure of control or power supplies leaves all inputs and outputs available. As a minimum, 50 % of all inputs and all outputs continue to be available after such failures;
- b) failure of a single multiplexing input module does not cause loss of more than eight analogue or sixteen digital signals;
- c) failure of a single multiplexing output module does not cause loss of more than eight signals.

Simple plug-in replacement of single modules should be possible to restore full availability.

5.2 Internal redundancy and independence

The multiplexing equipment should be designed such that faults are not propagated from one part of the equipment to another, or to another system.

The internal redundancy shall be determined on the basis of the required reliability. To reach this level of reliability, a multiplexing system may need redundant channels within itself.

Quand un équipement de multiplexage est utilisé dans un système de vote majoritaire, la redondance interne des canaux doit être déterminée en tenant compte de la fréquence d'actionnement intempestive ainsi que de la probabilité de défaillance d'actionnement. Cette évaluation doit être réalisée en fonction de la logique de vote.

5.3 *Isolement électrique*

L'isolement électrique d'un système de transmission de données multiplexées important pour la sûreté par rapport à tout autre système doit être considéré conformément à l'article 6 de la CEI 639 et à 5.6 de la CEI 231A. Les valeurs spécifiques de l'isolement électrique requis dépendent des alimentations électriques de puissance, des pratiques nationales et des prescriptions spécifiques d'une centrale. Les liaisons par fibres optiques ou les isolateurs opto-électroniques sont recommandés pour l'isolement des signaux d'information et de commande.

Un isolement mutuel doit être établi entre les équipements de transmission de données multiplexées et les autres équipements raccordés. Cela doit suffire à éviter que les défaillances des équipements et des câbles raccordés n'affectent par erreur le fonctionnement des équipements de transmission de données multiplexées. Les équipements raccordés comprennent les capteurs, les contacteurs, les alimentations et d'autres équipements de multiplexage.

La tension la plus élevée capable d'affecter les équipements et les câbles raccordés doit être évaluée. S'il peut être montré qu'elle est inférieure à 150 V, il convient de prévoir un isolement mutuel pour une tension crête à crête de 150 V c.a. ou c.c. Si tel n'est pas le cas, il convient de prévoir un isolement mutuel pour une tension crête à crête de 1 000 V c.a. ou c.c.

La tension doit être considérée comme appliquée directement aux bornes des équipements ou aux bornes de connexion de prises, ou due à des défauts de câbles. Cela doit concerner à la fois les systèmes de transmission de données multiplexées et les équipements raccordés. Une démonstration théorique peut être utilisée si les circuits comportent un isolement optique et par transformateur, et un isolement par des bobines de relaying et des contacts appropriés, mais il convient de les confirmer par des essais types.

Aucune perte de fonction du système de transmission de données multiplexées ne doit résulter de tensions définies appliquées aux équipements raccordés. Il convient qu'aucune perte de fonction des équipements raccordés ne résulte de tensions définies appliquées au système de transmission de données multiplexées.

Les câbles électriques raccordés au système de transmission de données multiplexées ou utilisés par celui-ci doivent impérativement être placés à 300 mm au moins d'un câble de tension supérieure à 600 V crête à crête c.a. ou c.c.

5.4 *Transmission de l'information*

5.4.1 *Caractéristiques des messages*

Il convient que les messages envoyés par les systèmes de transmission de données multiplexées soient conformes à un protocole et un format agréés au niveau international. Il convient d'être particulièrement attentif aux messages de longueur maximale, à leur cycle de répétition et à la capacité des systèmes de transmission en relation avec le temps de réponse et la largeur de bande de communication. Il convient que la capacité des modules de calcul utilisés dans les liaisons soit évaluée avec soin pour les charges anormales et les pics de charge. Il convient que la charge des modules de calcul utilisés dans les liaisons ne change pas de façon notable pour différentes conditions de la centrale ou à cause de défaillances de l'équipement de multiplexage.

Where multiplexing equipment is used in a majority voting system, the internal redundancy within channels shall be determined on the basis of the frequency of spurious actuation as well as the failure probability to actuate when required. This evaluation shall be performed in conjunction with the voting logic.

5.3 Electrical isolation

The electrical isolation of a multiplexed data transmission system important to safety from any other system shall be considered in accordance with IEC 639, clause 6, and IEC 231A, 5.6. The specific values of electrical isolation needed will depend on the station power supply voltages present, national practice, and plant-specific requirements. The preferred method of isolation for information and control is by means of optical fibre connections or opto-electronic isolators.

Mutual isolation shall be shown between multiplexed data transmission equipment and connected equipment. This shall be sufficient to prevent faults of the connected equipment and cables affecting the operation of the multiplexed data transmission equipment adversely. Connected equipment includes sensors, contacts, supplies and other multiplexing equipment.

The highest voltage able to affect the equipment and connected cables shall be assessed. If it can be shown to be below 150 V, mutual isolation should be provided for 150 V peak-to-peak a.c. or d.c. If it cannot be shown to be below 150 V, mutual isolation should be provided for 1 000 V peak-to-peak a.c. or d.c.

The voltage shall be considered as applied to any equipment terminal or plug/socket connection point directly or due to cable faults. This shall be considered for both the multiplexed data transmission system and the connected equipment. Theoretical demonstration may be used, if circuits include optical and transformer isolation, and isolation by suitable relay coils and contacts, but it should be supported by type tests.

No loss of function of the multiplexed data transmission system shall result from voltages applied, as defined, to the connected equipment. No loss of function of connected equipment should result from voltages applied, as defined, to the multiplexed data transmission system.

No electrical cable connected to the multiplexed data transmission system or used by it shall be closer than 300 mm to a cable used for voltages above 600 V peak-to-peak a.c. or d.c.

5.4 Information transmission

5.4.1 Message characteristics

The messages sent on the multiplexed data transmission system should follow an internationally agreed format and protocol. Special consideration should be paid to maximum length messages, message repeat cycles, and transmission system capacity in relation to communication bandwidth and response time. The capacity of computing modules used with the links should be assessed carefully for peak and abnormal loads. The load on computing modules used within the links should not change significantly under different plant conditions or due to multiplexer equipment failures.

5.4.2 Temps de réponse et durées de cycle

Les équipements de multiplexage doivent fonctionner selon un cycle continu régulier sans variation importante du nombre ou de la longueur des transmissions. Les conditions et les défaillances de la centrale et des équipements ne doivent pas causer d'incohérence chronologique ou de surcharges de messages.

Les durées de cycles de répétition des messages doivent être adaptées aux prescriptions temporelles des fonctions des systèmes connectés.

La réponse du système de transmission de données multiplexées à des opérations telles que les changements d'état des contacteurs de commande et des indicateurs ou des voyants correspondant à un état de la centrale doit être évaluée en accord avec la CEI 964 et la CEI 965. Des informations sur des exigences typiques sont données dans l'annexe C.

5.5 Maintenance et dispositifs d'essais

5.5.1 Prescriptions générales

Les prescriptions de maintenance et d'essais de l'article 10 de la CEI 987 doivent s'appliquer aux systèmes de transmission de données multiplexées importants pour la sûreté. Les sections 7.10 (aptitude aux essais), 7.11 (inhibitions d'exploitation) et 7.12 (contrôle de l'accès aux équipements du système de protection) du Guide de sûreté 50-SG-D3 de l'AIEA s'appliquent aux systèmes de transmission de données multiplexées de catégorie A. Les sections 4.5 (aptitude aux essais) et 4.6 (maintenabilité) du Guide de sûreté 50-SG-D8 de l'AIEA s'appliquent aux systèmes de transmission de données multiplexées de catégorie B ou C.

5.5.2 Prescriptions d'essais

La CEI 880 et la CEI 987 prescrivent que le système de transmission de données multiplexées soit doté de moyens d'autocontrôle. L'essai des systèmes de transmission de données multiplexées doit être possible pendant le fonctionnement de la centrale. Il convient d'effectuer les essais de fonctionnement correct de l'équipement de multiplexage une fois par an au moins, à moins qu'un intervalle différent ne soit défini par une analyse de fiabilité des fonctions de sûreté de la centrale.

Le Guide de sûreté de l'AIEA 50-SG-D8, 4.12(2), (3), (4) et (5), prescrit que des moyens doivent être fournis pour tester l'équipement de multiplexage. Il convient que les essais suivants soient possibles avec l'équipement non en service:

- a) modification de l'état ou de la valeur de tous les signaux d'entrée, et surveillance des modifications au niveau de l'équipement récepteur;
- b) interruption de la transmission, et confirmation de la détection de cette interruption par l'équipement récepteur ainsi que du déclenchement d'une action appropriée;
- c) essais et étalonnage des capteurs destinés aux systèmes importants pour la sûreté, conformément au Guide de sûreté de l'AIEA 50-SG-D3, 7.10.2;
- d) essais des actionneurs de sortie pour les systèmes importants pour la sûreté, conformément au Guide de sûreté de l'AIEA 50-SG-D3, 7.10.3.

5.4.2 Response times and cycle times

Multiplexing equipment shall operate on a continuous regular cycle with no significant variation of number or length of transmissions. Plant and equipment conditions and failures shall not cause timing inconsistency or message overloads.

Message repeat cycle times shall be suitable for the timing requirements of functions of the connected systems.

The response of the multiplexed data transmission system to operations such as control switch change and lamp or indicator changes in response to plant state shall be assessed in accordance with IEC 964 and IEC 965. Guidance on typical requirements is given in annex C.

5.5 Maintenance and test features

5.5.1 General requirements

The maintenance and testing requirements of IEC 987, clause 10, shall apply to multiplexed data transmission systems important to safety. Sections 7.10 (testability), 7.11 (operational bypasses) and 7.12 (control of access to protection system equipment) of IAEA Safety Guide 50-SG-D3 apply to category A multiplexed data transmission systems. Sections 4.5 (testability) and 4.6 (maintainability) of IAEA Safety Guide 50-SG-D8 apply to multiplexed data transmission systems which are of category B or C.

5.5.2 Testing requirements

IEC 880 and IEC 987 require that the multiplexed data transmission system shall have self-test capabilities. Testing of multiplexed data transmission systems shall be possible during operation of the plant. Testing of the correct operation of the multiplexing equipment should be done at least once per year, unless a different interval is defined by reliability analysis of the plant safety functions.

IAEA Safety Guide 50-SG-D8, 4.12(2), (3), (4) and (5), require that means shall be provided to test multiplexing equipment. The following tests should be possible with the equipment not in service:

- a) alteration of the state or value of any input signal, and monitoring of the alteration at the receiving equipment;
- b) interruption of transmission, and confirmation that the receiving equipment will detect this and take a correct action;
- c) testing and calibration of sensors for systems important to safety, in accordance with IAEA Safety Guide 50-SG-D3, 7.10.2;
- d) testing of output actuators for systems important to safety, in accordance with IAEA Safety Guide 50-SG-D3, 7.10.3.

La section 4.12(3) du Guide de sûreté de l'AIEA 50-SG-D8 prescrit que des moyens doivent être fournis pour contrôler la dérive par rapport à l'étalonnage des convertisseurs analogiques-numériques. Des moyens doivent être prévus pour contrôler, les équipements étant en service, la dérive par rapport à l'étalonnage des convertisseurs analogiques-numériques (ADC) et numériques-analogiques (DAC). On peut utiliser pour cela des tensions de référence régulièrement balayées et un dispositif de surveillance qui déclenchera une alarme sur les ADC ou DAC. Il convient de prévoir une compensation automatique pour la dérive d'étalonnage à court terme.

La section 4.12(4) du Guide de sûreté de l'AIEA 50-SG-D8 prescrit que des moyens doivent être fournis pour contrôler l'équipement de transmission multiplexée entrée par entrée. Citons à titre d'information sur les méthodes permettant cela:

- a) les moyens de détecter, l'équipement étant en service, si les signaux analogiques d'entrée sont en dehors de l'intervalle de mesure. Il convient alors que la méthode détecte les états d'ouverture de ligne et de court-circuit, que les états défectueux et hors intervalle de mesure donnent une identification avec la valeur fournie par l'ADC et les valeurs traitées de chaque signal concerné, et que cette indication soit fournie à tout traitement ultérieur des signaux en question;
- b) les moyens de détection et d'indication de contacts défectueux des signaux et des groupes de signaux d'entrée, l'équipement étant en service. Il convient que la méthode détecte les défauts de mise à la terre des câbles et des contacts, ainsi que les défaillances du traitement d'entrée, que les groupes de signaux défectueux fournissent une indication de l'existence de défaut et que cette indication puisse être fournie lors de tout traitement ultérieur des signaux concernés;
- c) les essais des signaux d'entrée à partir des bornes de l'équipement de multiplexage. Il convient de prévoir une méthode utilisant une unité de visualisation à cet effet. Cela est d'une importance particulière lors de l'installation et de la maintenance.

6 Essais

6.1 Essais fonctionnels

L'équipement de multiplexage doit être qualifié pour une utilisation opérationnelle au moyen d'essais fonctionnels, conformément à la section 4.4 du Guide de sûreté de l'AIEA 50-SG-D8 et à la section 7.9 du Guide de sûreté de l'AIEA 50-SG-D3. Dans ce processus, il faut effectuer des essais de type des modules des équipements, ou fournir la preuve d'essais de type préalables conformes à la CEI 780 (5.3).

Il convient que les essais fonctionnels comprennent des essais de conditions limites dues à une vitesse de transmission et un taux de messages élevés. Il convient que la capacité de transfert des messages soit conforme aux évaluations réalisées lors de la conception. Lors de l'utilisation de méthodes de demandes aléatoires, des essais spécifiques destinés à simuler des conditions aléatoires et des sollicitations maximales doivent être effectués.

Section 4.12(3) of IAEA Safety Guide 50-SG-D8 requires that means shall be provided to check for calibration drift of analogue-to-digital converters. Means shall be provided to check for calibration drift of analogue-to-digital converters (ADCs) and digital-to-analogue converters (DACs) with the equipment in service. Reference voltages which are regularly scanned and provided with alarms on the ADC or DAC reading may be used for this purpose. Automatic compensation for short-term drift of calibration should be provided.

Section 4.12(4) of IAEA Safety Guide 50-SG-D8 requires that means shall be provided to check multiplexed transmission equipment one input at a time. As guidance, methods to allow this are:

- a) means for detecting that input analogue signals are out of range with the equipment in service. The method should then detect open- and short-circuit states. Faulty and out-of-range states should give identification with the value provided by the ADC and the processed values of each involved signal. This indication should be provided to all subsequent processing of the signals involved;
- b) means for detecting and indicating faulty contact input signals and groups of signals with the equipment in service. The method should detect earth faults of contacts and cables, and failures of input processing. Defective groups of signals should give an indication that a fault exists and this indication should be provided to all subsequent processing of the signals involved;
- c) method of testing input signals from the multiplexing equipment terminals. A VDU (Visual Display Unit) method should be provided for this. This is of specific importance during installation and maintenance.

6 Testing

6.1 Functional testing

The multiplexing equipment shall be qualified for operational use by functional testing in accordance with 4.4 of IAEA Safety Guide 50-SG-D8 and 7.9 of IAEA Safety Guide 50-SG-D3. In this process, type testing of the equipment modules shall be performed, or evidence of previous type testing in accordance with IEC 780 (5.3) shall be provided.

Functional testing should include tests of limiting conditions due to high message contents and transfer rates. The message transfer capacity should be shown to be in accordance with assessments made during design. Where random demand methods are used, specific tests to simulate transient conditions and peak loading shall be done.

6.2 Qualification de l'équipement

Les systèmes de transmission de données multiplexées doivent être classés conformément à la CEI 1226 et leur qualification au plan de l'environnement doit être réalisée pour leur classe assignée. L'équipement de multiplexage des systèmes de catégorie A doit être qualifié conformément à la CEI 780 et à la CEI 980. Ces documents demandent que des tests de qualification de l'équipement sur des configurations représentatives soient effectués pour montrer que les équipements de multiplexage pour les systèmes de catégorie A sont capables

- d'effectuer leurs fonctions de sûreté dans les pires conditions de température et d'humidité qui pourraient se présenter, pendant la durée nécessaire pour amener le réacteur dans un état sûr;
- de réaliser leurs fonctions dans les limites des conditions normales d'environnement contrôlé. Il convient de montrer qu'il sont capables de fonctionner aux limites de ces conditions, sans dysfonctionnement.

L'annexe D comprend une note sur les environnements représentatifs.

6.2 *Equipment qualification*

Multiplexed data transmission systems shall be classified in accordance with IEC 1226 and appropriate environmental qualification performed for its assigned class. Multiplexing equipment of category A systems shall be qualified in accordance with IEC 780 and IEC 980. These documents call for equipment qualification tests of representative configurations to show that the multiplexing equipment for category A systems is able

- to perform its safety functions in the worst extreme conditions of temperature and humidity which could exist, for the time necessary to allow the reactor to be brought to a safe state;
- to perform its functions in the normal controlled environmental range. It should be shown to be able to operate in the extreme conditions of that range without malfunction.

A note on representative environments is given in annex D.

Annexe A

(informative)

Extrait du Guide de sûreté 50-SG-D8 de l'AIEA

Le texte ci-dessous est extrait de la section 4.12 du Guide de sûreté 50-SG-D8 de l'AIEA.

« Multiplexage

Dans le présent guide, le terme multiplexage désigne la transmission d'un point à un autre de deux ou plusieurs signaux ou messages sur une seule voie de transmission de données par modulation temporelle, modulation de fréquences ou modulation par impulsions et codage ou autres techniques de ce genre.

Le multiplexage réalisé dans le matériel numérique tels les ordinateurs de conduite du processus, ou qui fait partie intégrante de la conception du matériel I&C lié à la sûreté (ordinateur spécialisé ou systèmes de traitement numérique), doit également satisfaire à toutes les exigences pertinentes du présent guide.

Lorsqu'on utilise le multiplexage, celui-ci doit satisfaire aux exigences supplémentaires suivantes:

- 1) Les voies de transmission multiplexée de données doivent satisfaire aux exigences d'isolement fonctionnel et de séparation physique entre canaux redondants des systèmes I&C liés à la sûreté. Cela implique que les sources d'alimentation en énergie doivent être indépendantes.
- 2) La conception du système multiplexé doit prévoir la détection, dans l'information transmise, d'erreurs dues à des défaillances dans le matériel commun de transmission de données.
- 3) Il faut prévoir des moyens de contrôler la dérive par rapport à l'étalonnage dans les convertisseurs analogique-numérique.
- 4) Il faut prévoir des moyens de contrôler le matériel de transmission multiplexée entrée par entrée.
- 5) Si des dispositifs de détection d'erreurs sont prévus pour améliorer la transmission des signaux afin d'atteindre les objectifs de fiabilité, il faut avoir la possibilité de vérifier le fonctionnement de ces dispositifs de détection.
- 6) Le logiciel doit être conçu et vérifié conformément aux exigences relatives au logiciel des systèmes informatiques numériques ayant un rôle de sûreté. Ces exigences sont décrites sous 4.11 dans le présent guide. »

Annex A

(informative)

IAEA Safety Guide 50-SG-D8 extract

The relevant extract from section 4.12 of IAEA Safety Guide 50-SG-D8 is given below.

"Multiplexing

Multiplexing as used in this guide is the transmission from one location to another of two or more signals or messages over a single data channel by use of time division, frequency division, pulse code techniques or the like.

The multiplexing undertaken inside digital equipment such as central process computers, or which is part of the integral design of safety-related I&C equipment (dedicated computer or digital processing systems), shall also meet all relevant requirements of this guide.

When multiplexing is used, the following additional requirements apply:

- 1) The multiplexed data channels shall satisfy requirements for functional isolation and physical separation between redundant channels of safety-related I&C systems. This shall include independent power sources.
- 2) The design of the multiplexing system shall provide for detection of errors in the information transmitted which are due to faults in the common data transmission equipment.
- 3) Means shall be provided to check for calibration drift in the analogue-to-digital converters.
- 4) Means shall be provided to check multiplexed transmission equipment one input at a time.
- 5) If error detection features are provided to improve signal transmission so as to meet reliability goals, it shall be possible to verify the operation of these detection features.
- 6) The software shall be designed and verified in accordance with the requirements for software of safety-related digital computer systems as presented in section 4.11 of this guide."

Annexe B

(informative)

Systèmes représentatifs de transmission de données multiplexées

B.1 *Les exemples de systèmes représentatifs de transmission de données multiplexées décrits ci-dessous comprennent:*

- 1) Un multiplexeur du système de protection (système de catégorie A) et utilisé:
 - a) pour rassembler les valeurs de mesure de l'instrumentation;
 - b) pour transmettre les consignes de protection aux actionneurs;
 - c) pour transmettre les commandes des contacteurs de la salle de commande aux actionneurs;
 - d) pour transmettre les valeurs de signaux de protection à un système de commande.
- 2) Un multiplexeur de commande, inclus dans un système utilisé:
 - a) pour acquérir des grandeurs variables de la centrale, les traiter et transmettre les valeurs et les états à la salle de commande;
 - b) pour acquérir l'état des contacteurs de la salle de commande, les traiter et déclencher les actionneurs.

Les fonctions a) et b) peuvent être assurées par un même système de transmission de données duplex multiplexées.
- 3) Un multiplexeur de données, inclus dans un système qui rassemble les valeurs des signaux de l'instrumentation et leurs états, les traite et les transmet, pour les systèmes importants pour la sûreté.
- 4) Une unité de transmission de données utilisée pour transmettre des informations à partir des systèmes importants pour la sûreté vers d'autres systèmes non importants pour la sûreté.

Annex B

(informative)

Representative multiplexed data transmission systems

B.1 *Examples of representative multiplexed data transmission systems outlined in the following include:*

- 1) A protection system multiplexer (category A system) and used:
 - a) to gather instrumentation measurement values;
 - b) to transmit protection requirements to actuators;
 - c) to transmit control room switch demands to actuators;
 - d) to transmit protection signals values to a control system.
- 2) A control multiplexer, forming part of a system used:
 - a) to read plant conditions, process them, and transmit values and states to the control room;
 - b) to read control room switches, process them, and operate actuators.

The functions of both a) and b) may be performed in a single duplex transmission multiplexed data transmission system.
- 3) A data multiplexer, forming part of a system to gather instrumentation signal values and states, process them, and transmit them, for plant systems important to safety.
- 4) A data transmission unit used to transmit information from systems important to safety to other systems not important to safety.