NORME INTERNATIONALE

INTERNATIONAL STANDARD

CEI
IEC
60834-1

Deuxième édition
Second edition
1999-10

Matériels de téléprotection des réseaux d'énergie électrique – Performances et essais –

Partie 1: Systèmes de commande

Teleprotection equipment of power systems – Performance and testing –

Part 1: Command systems

Numéro de référence
Reference number
CEI/IEC 60834-1:1999

Numéros des publications

Depuis le 1er 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: S*ymboles 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
60834-1

Deuxième édition
Second edition
1999-10

Matériels de téléprotection des réseaux d'énergie électrique – Performances et essais –

Partie 1: Systèmes de commande

Teleprotection equipment of power systems – Performance and testing –

Part 1: Command systems

International Electrotechnical Commission 3, rue de Varembé Geneva, Switzerland
Telefax: +41 22 919 0300 e-mail: inmail@iec.ch IEC web site http://www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

CODE PRIX
PRICE CODE XA

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

SOMMAIRE

CONTENTS

Pages

Page

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

MATÉRIELS DE TÉLÉPROTECTION DES RÉSEAUX D'ÉNERGIE ÉLECTRIQUE – PERFORMANCES ET ESSAIS –

Partie 1: Systèmes de commande

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 les 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'études.
3) Les documents produits se présentent sous la forme de recommandations internationales. Ils sont publiés comme 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 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 60834-1 a été établie par le comité d'études 57 de la CEI: Conduite des systèmes de puissance et communications associées.

La présente deuxième édition annule et remplace la première édition publiée en 1988.

Le texte de cette norme est issu des documents suivants:

FDIS	Rapport de vote
57/406/FDIS	57/425/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.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 3.

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

Le comité a décidé que cette publication reste valable jusqu'en 2004. A cette date, selon décision préalable du comité, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

TELEPROTECTION EQUIPMENT OF POWER SYSTEMS – PERFORMANCE AND TESTING –

Part 1: Command systems

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 co-operation 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 organizations 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. The IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 60834-1 has been prepared by IEC technical committee 57: Power system control and associated communications.

This second edition cancels and replaces the first edition published in 1988.

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

FDIS	Report on voting
57/406/FDIS	57/425/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.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 3.

Annexes A, B and C are for information only.

The committee has decided that this publication remains valid until 2004. At this date, in accordance with the committee's decision, the publication will be

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

MATÉRIELS DE TÉLÉPROTECTION DES RÉSEAUX D'ÉNERGIE ÉLECTRIQUE – PERFORMANCES ET ESSAIS –

Partie 1: Systèmes de commande

1 Généralités

1.1 Domaine d'application

La présente partie de la CEI 60834 s'applique aux systèmes de commande de téléprotection utilisés pour transmettre les informations de commande, en principe en conjonction avec le matériel de protection. Elle a pour objectif d'établir les exigences relatives aux performances et aux méthodes d'essai recommandées pour le matériel de commande de téléprotection. L'information transmise par le matériel de commande de téléprotection peut être sous forme analogique ou numérique.

Le matériel de commande de téléprotection concerné par la présente norme peut être un matériel à fréquence porteuse sur ligne d'énergie ou à fréquences vocales utilisé avec divers systèmes de télécommunications, tels que courant porteur sur ligne d'énergie (CPL), liaisons radioélectriques, fibres optiques, circuits loués et câbles concédés ou privés. De plus, il peut être du matériel numérique utilisé avec un système de télécommunication numérique ou des médias tels que fibres optiques, liaisons radioélectriques, liaisons numériques louées ou concédées.

Le matériel de commande de téléprotection peut être séparé ou fourni comme partie intégrante du matériel de protection.

En plus des essais de performances du matériel de téléprotection, il faut effectuer les essais de l'alimentation du matériel de téléprotection. Il convient de considérer tous les essais en tant qu'essais de type.

NOTE – Le Vocabulaire Electrotechnique International (VEI) définit un essai de type comme un essai effectué sur un ou plusieurs dispositifs réalisés selon une conception donnée pour vérifier que cette conception répond à certaines spécifications.

1.2 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 partie de la CEI 60834. Pour les références datées, les amendements ultérieurs ou les révisions de ces publications ne s'appliquent pas. Toutefois, les parties prenantes aux accords fondés sur la présente partie de la CEI 60834 sont invitées à rechercher la possibilité d'appliquer les éditions les plus récentes des documents normatifs indiqués ci-après. Pour les références non datées, la dernière édition du document normatif en référence s'applique. Les membres de la CEI et de l'ISO possèdent le registre des Normes internationales en vigueur.

CEI 60050(151):1978, *Vocabulaire Electrotechnique International (VEI) – Chapitre 151: Dispositifs électriques et magnétiques*

CEI 60050(448):1995, *Vocabulaire Electrotechnique International (VEI) – Chapitre 448: Protection des réseaux d'énergie*

TELEPROTECTION EQUIPMENT OF POWER SYSTEMS – PERFORMANCE AND TESTING –

Part 1: Command systems

1 General

1.1 Scope

This part of IEC 60834 applies to teleprotection command systems used to convey command information, generally in conjunction with protection equipment. It aims at establishing performance requirements and recommended testing methods for command type teleprotection equipment. The information conveyed by the teleprotection equipment can be in analogue or digital form.

The command type teleprotection equipment referred to in this standard can be power line carrier equipment or voice frequency equipment which is used in connection with various telecommunication systems, such as power line carrier (PLC), radio links, optical fibre, rented circuits, leased or privately owned cables. In addition the command type teleprotection can be digital equipment which is used with a digital telecommunication system or media such as optical fibres, radio links, leased or privately owned digital links.

The command type teleprotection equipment may be separate or provided as an integral part of the protection equipment.

In addition to teleprotection equipment performance tests, tests have to be carried out on the power supply of the teleprotection equipment. All the tests should be regarded as type tests.

NOTE – According to the International Electrotechnical Vocabulary (IEV), a type test is defined as a test of one or more devices made to a certain design to show that the design meets certain specifications.

1.2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this part of IEC 60834. For dated references, subsequent amendments to, or revisions of any of these publications do not apply. However, parties to agreements based on this part of IEC 60834 are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of IEC and ISO maintain registers of currently valid International Standards.

IEC 60050(151):1978, *International Electrotechnical Vocabulary – Chapter 151: Electrical and magnetic devices*

IEC 60050(448):1995, *International Electrotechnical Vocabulary – Chapter 448: Power system protection*

CEI 60060-1:1989, *Techniques des essais à haute tension – Première partie: Définitions et prescriptions générales relatives aux essais*

CEI 60870-2-1:1995, *Matériels et systèmes de téléconduite – Partie 2: Conditions de fonctionnement – Section 1: Alimentation et compatibilité électromagnétique*

CEI 60870-2-2:1996, *Matériels et systèmes de téléconduite – Partie 2: Conditions de fonctionnement – Section 2: Conditions d'environnement (influences climatiques, mécaniques et autres influences non électriques)*

CEI 61000-4-1:1992, *Compatibilité électromagnétique (CEM) – Partie 4: Techniques d'essai et de mesure – Section 1: Vue d'ensemble sur les essais d'immunité – Publication fondamentale en CEM*

UIT-T G.823:1993, *Régulation de la gigue et du dérapage dans les réseaux numériques fondés sur la hiérarchie à 2048 kbit/s*

CISPR 22:1997, *Appareils de traitement de l'information – Caractéristiques des perturbations radioélectriques – Limites et méthodes de mesure*

1.3 Conditions de service

En référence à la CEI 60870-2-1 et à la CEI 60870-2-2, les spécifications suivantes doivent être appliquées.

Des exigences spécifiques ou des spécifications détaillées correspondant à d'autres conditions d'environnement (climatiques, mécaniques ou toute autre influence non électrique), non couvertes par ce qui suit mais considérées comme pertinentes pour l'exploitation correcte et la vie du matériel, doivent être convenues entre utilisateur et fabricant en se référant préférentiellement aux classes spécifiques mentionnées dans les références CEI citées ci-dessus.

Pour les environnements sévères, il est préférable de spécifier la classe C2 (gamme de température: –25 °C à +55 °C), si ce n'est que l'humidité relative forte doit être spécifiée à 95 %.

1.3.1 Conditions ambiantes

Les exigences stipulées de performance doivent être satisfaites dans les conditions correspondantes à la classe d'emplacement B3 (emplacement dans un lieu fermé – température de l'air contrôlée), dont la caractéristique principale est:

- gamme de température: +5 °C à +40 °C

1.3.2 Tension d'alimentation pour fonctionnement sur batterie

La tension continue nominale d'alimentation est typiquement 250 V, 220 V, 125 V, 110 V, 60 V, 48 V ou 24 V.

Les exigences spécifiées de performance doivent être satisfaites dans la classe de tolérance de la tension suivante:

- tolérances sur la tension: DC3 –20 % à +15 %

IEC 60060-1:1989, *High voltage test techniques – Part 1: General definitions and test requirements*

IEC 60870-2-1:1995, *Telecontrol equipment and systems – Part 2: Operating conditions – Section 1: Power supply and electromagnetic compatibility*

IEC 60870-2-2:1996, *Telecontrol equipment and systems – Part 2: Operating conditions – Section 2: Environmental conditions (climatic, mechanical and other non-electrical influences)*

IEC 61000-4-1:1992, *Electromagnetic compatibility (EMC) – Part 4: Testing and measurement techniques – Section 1: Overview of immunity tests. Basic EMC publication*

ITU-T G.823:1993, *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*

CISPR 22:1997, *Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement*

1.3 Service conditions

With reference to IEC 60870-2-1 and IEC 60870-2-2, the following specifications shall apply.

Special requirements or detailed specifications for other environmental conditions (climatic, mechanical or other non-electrical influences), not covered in the following but considered relevant for the proper operation and life of the equipment, shall be agreed between user and manufacturer, preferably referring to specific classes mentioned in the IEC references above.

Class C2 is the preferred specification for severe environments (temperature range: –25 °C to +55 °C) except that high relative humidity shall be specified as 95 %.

1.3.1 Ambient conditions

The stated performance requirements shall be satisfied for the conditions corresponding to location class B3 (enclosed locations – air temperature controlled), the main characteristic being the following:

- temperature range +5 °C to +40 °C

1.3.2 Supply voltage with battery operation

The nominal d.c. voltage is typically 250 V, 220 V, 125 V, 110 V, 60 V, 48 V or 24 V.

The stated performance requirements shall be satisfied for the following voltage tolerance class:

- voltage tolerance DC3 –20 % to +15 %

1.3.3 Tension d'alimentation pour fonctionnement sur réseau alternatif

La tension alternative nominale doit être choisie parmi les valeurs préférentielles de 230 V eff. ou 110 V eff., monophasé, 50 Hz ou 60 Hz.

Les exigences stipulées de performances doivent être satisfaites pour les classes suivantes de tolérances:

- tolérances sur la tension AC2 +10 % à –15 %
- tolérances sur la fréquence F3 ±5 %
- taux d'harmoniques H1 <5 %

1.3.4 Conditions de stockage

Le matériel ne doit pas être endommagé pendant le stockage ou le transport lorsque les conditions correspondent à un emplacement de classe C3 pour le stockage et à un emplacement de classe C2 pour le transport, les principales caractéristiques étant:

- gamme de température –40 °C à +70 °C

1.4 Système de télécommunication utilisé

Le système de télécommunication peut être:

a) une liaison sur câble pour la transmission à fréquence vocale;

b) une liaison à courant porteur pour les câbles électriques et les lignes aériennes;

c) une liaison à fréquence porteuse sur câble aérien supporté par ligne d'énergie;

d) une liaison à courant porteur sur ligne d'énergie (CPL);

e) un faisceau hertzien point à point;

f) un circuit loué;

g) une fibre optique.

Il convient de choisir avec soin les systèmes de télécommunication, car ils subissent l'influence du bruit, des variations de paramètres et de toutes sortes de perturbations qui peuvent entraver ou empêcher le fonctionnement du matériel de téléprotection.

La figure 1 présente un matériel de téléprotection qui fonctionne dans une configuration audiofréquence (c'est-à-dire qui utilise une partie de la bande 4 kHz). Les signaux sont transmis à partir de l'émetteur vers le récepteur par un système de télécommunication.

La figure 2 présente une configuration utilisant une liaison à courant porteur sur ligne d'énergie.

Les figures 1 et 2 s'appliquent à la fois aux systèmes de téléprotection qui émettent et reçoivent des porteuses à déplacement de fréquences et aux systèmes normalement au repos (silencieux).

La figure 3 présente une configuration dans laquelle une téléprotection numérique est connectée directement sur une fibre optique.

La figure 4 présente une autre disposition dans laquelle la téléprotection numérique est connectée à un système de téléprotection par un matériel de multiplexage.

1.3.3 Supply voltage with a.c. mains operation

The nominal a.c. voltage shall be chosen from the preferred values of 230 V r.m.s. or 110 V r.m.s single-phase 50 Hz or 60 Hz.

The stated performance requirements shall be satisfied for the following tolerance classes:

- voltage tolerance AC2 +10 % to –15 %
- frequency tolerance F3 ±5 %
- harmonic content H1 <5 %

1.3.4 Storage conditions

During storage or shipment, the equipment shall not suffer any damage when the ambient conditions correspond to location class C3 for storage and to class C2 for transportation, the main characteristic being:

- temperature range –40 °C to +70 °C

1.4 Telecommunication system used

The telecommunication system can be

a) cable links for voice frequency transmission;
b) carrier frequency links for cables and overhead lines;
c) carrier frequency links on aerial cables on power lines;
d) power line carrier (PLC) links;
e) point-to-point radio links (microwave);
f) leased circuits;
g) optical fibres.

The telecommunication systems should be chosen with care since they can be influenced by noise, change of parameters and other types of interference which may cause unwanted operation or the non-operation of the teleprotection equipment.

Figure 1 shows teleprotection equipment working in an audio-frequency configuration (e.g. using part of a 4 kHz band). The signals are conveyed from the transmitter to the receiver via a telecommunication system.

Figure 2 shows a configuration using a power line carrier link.

Figures 1 and 2 apply to teleprotection systems transmitting and receiving frequency shift keyed carrier or normally quiescent signals.

Figure 3 shows a configuration in which digital teleprotection is directly connected via an optical fibre.

Figure 4 is an alternative arrangement where the digital teleprotection is connected to a digital telecommunication system via multiplexing equipment.

La figure 3 et la figure 4 concernent des systèmes de téléprotection émettant et recevant de l'information numérique.

Les figures 1 à 4 sont seulement des exemples. D'autres configurations sont possibles mais elles ne sont pas représentées.

1.5 Définitions

Pour les besoins de la présente partie de la CEI 60834, les définitions suivantes s'appliquent. Se reporter également à la figure 5, qui clarifie les relations entre les termes utilisés.

1.5.1
protection
ensemble des dispositions destinées à détecter les défauts ou les autres situations anormales dans un réseau d'énergie, à permettre l'élimination des défauts, à mettre fin aux situations anormales et à lancer des ordres ou des signalisations

NOTE 1 – Le terme «protection» est un terme générique pour les dispositifs de protection ou les systèmes de protection.

NOTE 2 – Le terme «protection» peut être utilisé pour décrire la protection d'un réseau d'énergie dans son ensemble ou la protection d'ouvrages individuels d'un réseau d'énergie, par exemple la protection d'un transformateur, la protection d'une ligne, la protection d'un générateur.

NOTE 3 – La protection ne comprend pas les dispositifs d'un réseau d'énergie destinés, par exemple, à limiter les surtensions dans le réseau d'énergie. Toutefois, elle comprend les dispositifs destinés à contrôler les variations de tension ou de fréquence du réseau d'énergie tels que la connexion automatique d'une bobine d'inductance, le délestage, etc.

[VEI 448-11-01]

1.5.2
dispositif de protection
dispositif comportant un ou plusieurs relais de protection ainsi que, si nécessaire, un ou plusieurs éléments logiques, et destiné à assurer une ou plusieurs fonctions spécifiées de protection

NOTE – Un dispositif de protection fait partie d'un système de protection.

Exemples: Dispositifs de protection de distance, dispositif de protection à comparaison de phases. (Un dispositif de protection à comparaison de phases fait partie, à une extrémité de ligne, d'un système de protection à comparaison de phases.)

[VEI 448-11-03]

1.5.3
système de protection
ensemble d'un ou de plusieurs dispositifs de protection et autres appareils destinés à assurer une ou plusieurs fonctions spécifiées de protection

NOTE 1 – Un système de protection comprend un ou plusieurs dispositifs de protection, un ou des transformateurs de mesure, une filerie, un ou plusieurs circuits de déclenchement, une ou plusieurs alimentations auxiliaires ainsi que, le cas échéant, une ou plusieurs liaisons de transmission. Selon le ou les principes du système de protection, celui-ci peut comprendre une seule extrémité ou toutes les extrémités de la section protégée et, éventuellement, un dispositif de réenclenchement automatique.

NOTE 2 – Les disjoncteurs sont exclus de cette définition.

[VEI 448-11-04]

Figures 3 and 4 apply to teleprotection systems transmitting and receiving digital data.

Figures 1 to 4 serve only as examples. Other configurations are possible but are not shown.

1.5 Definitions

For the purposes of this part of IEC 60834, the following definitions apply. Refer also to figure 5 which clarifies the relationship between terms in use.

1.5.1
protection
the provisions for detecting faults or other abnormal conditions in a power system, for enabling fault clearance, for terminating abnormal conditions, and for initiating signals or indications

NOTE 1 – The term "protection" is a generic term for protection equipments or protection systems.

NOTE 2 – The term "protection" may be used to describe the protection of a complete power system or the protection of individual plant items in a power system e.g. transformer protection, line protection, generator protection.

NOTE 3 – Protection does not include items of power system plant provided, for example, to limit overvoltages on the power system. However, it includes items provided to control the power system voltage or frequency deviations such as automatic reactor switching, load-shedding, etc.

[IEV 448-11-01]

1.5.2
protection equipment
an equipment incorporating one or more protection relays and, if necessary, logic elements intended to perform one or more specified protection functions

NOTE – A protection equipment is part of a protection system.

Example: Distance protection equipment, phase comparison protection equipment. (One-phase comparison equipment is part of one line-end of a phase comparison protection system.)

[IEV 448-11-03]

1.5.3
protection system
an arrangement of one or more protection equipments, and other devices intended to perform one or more specified protection functions

NOTE 1 – A protection system includes one or more protection equipments, instrument transformer(s), wiring, tripping circuit(s), auxiliary supply(s) and, where provided, communication system(s). Depending upon the principle(s) of the protection system, it may include one end or all ends of the protected section and, possibly, automatic reclosing equipment.

NOTE 2 – The circuit-breaker(s) are excluded.

[IEV 448-11-04]

1.5.4
sélectivité d'une protection
aptitude d'une protection à identifier la section et/ou la ou les phases qui sont en défaut dans un réseau d'énergie

[VEI 448-11-06]

1.5.5
protection à sélectivité absolue de section
protection dont le fonctionnement et la sélectivité de section dépendent de la comparaison de grandeurs électriques entre chaque extrémité de la section protégée

NOTE – Aux Etats-Unis d'Amérique, le terme anglais «unit protection» désigne la protection destinée à un générateur électrique.

[VEI 448-11-09]

1.5.6
protection à sélectivité relative de section
protection dont le fonctionnement et la sélectivité de section dépendent de la mesure de grandeurs électriques par les relais de mesure à une seule extrémité de la section protégée et, dans certains cas, de l'échange de signaux logiques entre les extrémités

NOTE – La sélectivité de section d'une protection à sélectivité relative de section peut dépendre de son réglage, en particulier par rapport au temps.

[VEI 448-11-10]

1.5.7
protection de distance
protection à sélectivité relative de section dont le fonctionnement et la sélectivité dépendent de la mesure locale de grandeurs électriques à partir desquelles la distance équivalente du défaut est évaluée par comparaison avec des réglages de zones

[VEI 448-14-01]

1.5.8
portée réduite
situation de protection, en général une protection de distance, dont le réglage de la zone la plus courte correspond à une portée plus courte que la section protégée

[VEI 448-14-05]

1.5.9
portée étendue
situation d'une protection, en général une protection de distance, dont le réglage de la zone la plus courte correspond à une portée plus longue que la section protégée

[VEI 448-14-07]

1.5.10
matériel de téléprotection
matériel spécialement conçu pour être utilisé en conjonction avec un système de protection. Le matériel de téléprotection connecté à une liaison de télécommunication entre les deux extrémités du circuit protégé transforme les informations fournies par le dispositif de protection en une forme convenant à la transmission

1.5.4
selectivity of protection
the ability of a protection to identify the faulty section and/or phase(s) of a power system

[IEV 448-11-06]

1.5.5
unit protection
a protection whose operation and section selectivity are dependent on the comparison of electrical quantities at each end of the protected section

NOTE – In the USA, the term "unit protection" designates the protection provided for an electrical generator.

[IEV 448-11-09]

1.5.6
non-unit protection
a protection whose operation and section selectivity are dependent on the measurement of electrical quantities at one end of the protected section by the measuring relays and, in some cases, on the exchange of logic signals between the ends

NOTE – The section selectivity of non-unit protection may depend upon its setting, particularly with regard to time.

[IEV 448-11-10]

1.5.7
distance protection
a non-circuit protection whose operation and selectivity depend on local measurement of electrical quantities from which the equivalent distance to the fault is evaluated by comparing with zone settings

[IEV 448-14-01]

1.5.8
underreach
the condition of a protection, generally distance protection, when the shortest zone setting corresponds to a reach shorter than the protected section

[IEV 448-14-05]

1.5.9
overreach
the condition of a protection, generally distance protection, when the shortest zone setting corresponds to a reach longer than the protected section

[IEV 448-14-07]

1.5.10
teleprotection equipment
equipment specially designed to be used in conjunction with a protection system. The teleprotection equipment, which is connected to a telecommunication link between both ends of the protected circuit, transforms the information given by the protection equipment into a form suitable for transmission

1.5.10.1
système de téléprotection
système composé des matériels de téléprotection et du système de télécommunication associé entre les extrémités du circuit protégé

1.5.10.2
voie de téléprotection
bande de fréquences ou débit binaire du système de télécommunication disponible pour la transmission des signaux de protection

NOTE – La voie de téléprotection peut être analogique ou numérique. Dans une voie de téléprotection analogique, le signal instantané varie de façon continue, même si l'information est de nature numérique. Dans une voie de téléprotection analogique, seuls certains niveaux discrets (habituellement deux ou trois) sont possibles. Dans une voie de téléprotection numérique, il est commun de transmettre les informations de séquencement du débit binaire de façon synchrone avec les données. Cette information de séquencement peut être soit intégrée aux données, soit transmise séparément sous la forme d'un signal d'horloge dépendant du type d'interface. Il convient que l'information de séquencement soit considérée en tant que partie de la voie de télécommunication.

1.5.10.3
système de télécommunication – liaison de télécommunication
système composé du matériel de télécommunication et de la liaison physique associée nécessaire pour transmettre les signaux d'information à distance

1.5.11
protection à fils pilotes
protection à liaison de transmission utilisant des fils métalliques

[VEI 448-15-04]

1.5.12
protection à liaison par courant porteur sur ligne d'énergie
protection à liaison de transmission utilisant une liaison à courant porteur sur ligne d'énergie

[VEI 448-15-05]

1.5.13
protection à faisceau hertzien
protection à liaison de transmission utilisant un faisceau hertzien

[VEI 448-15-06]

1.5.14
protection de distance à transmission de signaux
protection de distance utilisant la communication pour améliorer sa performance

1.5.15
protection à autorisation
protection, en général une protection de distance, dans laquelle la réception d'un signal autorise la protection locale à commander le déclenchement

[VEI 448-14-09]

1.5.16
protection à portée réduite et à autorisation
protection, en général une protection de distance, à liaison de transmission, avec une protection à portée réduite à chaque extrémité de la section, et dans laquelle un signal est transmis lors de la détection d'un défaut par la protection à portée réduite. A l'autre extrémité, la réception de ce signal commande le déclenchement si une autre protection locale à autorisation a détecté le défaut

[VEI 448-15-11]

1.5.10.1
teleprotection system
system composed of teleprotection equipment and an associated telecommunication system between the ends of a protected circuit

1.5.10.2
teleprotection channel
frequency band or bit rate provided by the telecommunication system in order to permit the transmission of protection signals

NOTE – The teleprotection channel may be either analogue or digital. In an analogue teleprotection channel the instantaneous signal varies continuously, even though the information is of a digital nature. In a digital teleprotection channel only certain discrete levels (usually two or three) are permitted. In a digital teleprotection system, it is usual to convey bit timing information synchronously with the data. This timing information can be either integrated with the data or transmitted as a separate clock signal depending on the interface type. Timing information should be regarded as part of the teleprotection channel.

1.5.10.3
telecommunication system – telecommunication link
system composed of telecommunication equipment and the associated physical link required to transmit information signals over a distance

1.5.11
pilot wire protection
protection associated with telecommunication using metallic wires

[IEV 448-15-04]

1.5.12
power-line-carrier protection
protection associated with telecommunication using power-line carrier

[IEV 448-15-05]

1.5.13
microwave link protection
protection associated with telecommunication using a microwave link

[IEV 448-15-06]

1.5.14
communication-aided distance protection
distance protection which utilises communication to improve its performance

1.5.15
permissive protection
a protection, generally distance protection, in which the receipt of a signal permits the local protection to initiate tripping

[IEV 448-14-09]

1.5.16
permissive underreach protection (PUP)
protection, generally distance protection, using telecommunication, with underreach protection at each section end and in which a signal is transmitted when a fault is detected by the underreach protection. Receipt of the signal at the other end initiates tripping if other local permissive protection at the other end has detected the fault

[IEV 448-15-11]

1.5.17
protection à portée étendue et à autorisation
protection, en général une protection de distance, à liaison de transmission, avec une protection à portée étendue à chaque extrémité de la section, et dans laquelle un signal est transmis lors de la détection d'un défaut par la protection à portée étendue. A l'autre extrémité, la réception de ce signal autorise la protection locale à portée étendue à commander le déclenchement

[VEI 448-15-16]

1.5.18
protection à portée réduite et à accélération de stade
protection, en général une protection de distance, à liaison de transmission, avec une protection à portée réduite à chaque extrémité de la section, et dans laquelle un signal est transmis lors de la détection d'un défaut par la protection à portée réduite. A l'autre extrémité, la réception de ce signal autorise une mesure à portée étendue à commander le déclenchement

[VEI 448-15-13]

1.5.19
protection à verrouillage
protection, en général une protection de distance, dans laquelle la réception d'un signal empêche la protection locale de commander le déclenchement

[VEI 448-14-10]

1.5.20
protection à portée étendue et à verrouillage
protection, en général une protection de distance, à liaison de transmission, avec une protection à portée étendue à chaque extrémité de la section, et dans laquelle un signal est transmis lors de la détection d'un défaut externe dans le sens opposé. A l'autre extrémité, la réception de ce signal empêche la protection à portée étendue située à cette extrémité de commander le déclenchement

[VEI 448-15-14]

1.5.21
protection différentielle longitudinale
protection dont le fonctionnement et la sélectivité dépendent de la comparaison des courants en amplitude, ou en phase et en amplitude, entre les extrémités de la section protégée

[VEI 448-14-16]

1.5.22
protection à comparaison de phases
protection dont le fonctionnement et la sélectivité dépendent de la comparaison des angles de phase des courants à chaque extrémité de la section protégée

[VEI 448-14-18]

1.5.23
télédéclenchement
déclenchement d'un ou de plusieurs disjoncteurs par des signaux émis par une protection éloignée, indépendamment de l'état de la protection locale

[VEI 448-15-08]

1.5.17
permissive overreach protection (POP)
protection, generally distance protection, using telecommunication, with overreach protection at each section end and in which a signal is transmitted when a fault is detected by the overreach protection. Receipt of the signal at the other end permits the initiation of tripping by the local overreach protection

[IEV 448-15-16]

1.5.18
accelerated underreach protection (AUP)
protection, generally distance protection, using telecommunication, with underreach protection at each section end and in which a signal is transmitted when a fault is detected by the underreach protection. Receipt of the signal at the other end permits a sequential measurement by an overreach zone to initiate tripping

[IEV 448-15-13]

1.5.19
blocking protection
a protection, generally distance protection, in which the receipt of a signal blocks the local protection from initiating tripping

[IEV 448-14-10]

1.5.20
blocking overreach protection (BOP)
protection, generally distance protection, using telecommunication, with overreach protection at each section end and in which a signal is transmitted when a reverse external fault is detected. Receipt of the signal at the other end blocks the overreach protection at that end from initiating tripping

[IEV 448-15-14]

1.5.21
longitudinal differential protection
protection the operation and selectivity of which depend on the comparison of magnitude or the phase and magnitude of the currents at the ends of the protected section

[IEV 448-14-16]

1.5.22
phase comparison protection
protection whose operation and selectivity depend on the comparison of the phase of the currents at each end of the protected section

[IEV 448-14-18]

1.5.23
intertripping
the tripping of circuit-breaker(s) by signals initiated from protection at a remote location independent of the state of the local protection

[IEV 448-15-08]

2 Caractéristiques des systèmes de téléprotection de type commande

Les paragraphes suivants portent sur les termes utilisés pour définir ou spécifier les systèmes de téléprotection (voir également 3.3.1).

2.1 Types de dispositifs de commande de téléprotection

a) *Dispositifs à déclenchement avec autorisation (voir 1.5)*

Ce terme concerne les dispositifs pour lesquels la commande reçue initie le déclenchement en conjonction avec un matériel de protection local. Les voies de commande de ce type peuvent fonctionner dans une bande de fréquences vocales, dans une bande de fréquences CPL ou avec un débit binaire numérique. La voie est souvent conçue afin que la fiabilité d'exploitation soit élevée, y compris dans les conditions où, en raison de perturbations de l'alimentation, la voie de télécommunication peut se trouver affectée.

b) *Dispositifs à télédéclenchement (direct ou transféré) (voir 1.5)*

Ce terme concerne les dispositifs pour lesquels la commande reçue initie le déclenchement sans qu'il soit conditionné par la protection locale. Les voies à télédéclenchement utilisent des principes similaires à ceux des voies de déclenchement à autorisation, à la différence que l'immunité contre les commandes intempestives et l'absence de commande défaillante constituent des prescriptions primordiales. La vitesse de fonctionnement est habituellement sacrifiée pour répondre aux prescriptions de sécurité et de fiabilité, particulièrement pour les systèmes analogiques.

c) *Dispositifs de protection à verrouillage (voir 1.5)*

Ce terme concerne les dispositifs pour lesquels la commande reçue inhibe le fonctionnement de la protection locale. Ces voies sont similaires aux voies de déclenchement à autorisation, à la différence que les prescriptions régissant la fiabilité de fonctionnement et la vitesse sont plus strictes.

2.2 Temps global de fonctionnement des systèmes de téléprotection (circuit de télécommunication compris)

Le temps global de fonctionnement T est le temps écoulé entre le moment d'un changement d'état à l'entrée de la commande et le moment du changement d'état correspondant à la sortie de la commande, le temps de propagation et le retard additionnel dû au bruit étant inclus.

Le temps global de fonctionnement d'un système de téléprotection influe sur le temps d'élimination de défaut (voir figure 6).

NOTE – Le temps d'élimination de défaut T_c indiqué à la figure 6 n'est donné qu'à titre indicatif.

2.3 Temps de transmission (circuit de télécommunication non compris)

Le temps de transmission d'un système de téléprotection est le temps écoulé entre le moment d'un changement d'état à l'entrée de la commande et le moment du changement d'état correspondant à la sortie de la commande, le temps de propagation étant exclu.

Le temps de transmission nominal T_0 correspond à une transmission exempte de bruit (voir aussi 4.3.3).

Le temps mesuré de transmission maximal T_{ac} est le temps maximal obtenu dans une transmission avec bruit pour une fiabilité définie et pour un rapport signal sur bruit (S/B) défini ou un taux d'erreur de bit (BER) défini.

2 Characteristics of command type teleprotection systems

The following subclauses deal with the terms used in the description and/or specification of teleprotection systems (see also 3.3.1).

2.1 Types of teleprotection command schemes

a) *Permissive tripping schemes (see 1.5)*

This term refers to schemes where the received command initiates tripping in conjunction with a local protection equipment. Command channels of this type can operate in an audio frequency band, a PLC frequency band or at a digital bit rate. The channel is often designed with the premise that dependability of operation should be high even under conditions when, due to a power system disturbance, the telecommunication medium may be adversely affected.

b) *Intertripping schemes (direct or transfer tripping) (see 1.5)*

This term refers to schemes where the received command initiates tripping without qualification by local protection. Intertrip channels utilise similar principles to permissive trip channels; however, security against unwanted operation and dependability of correct operation are prime requirements. Speed of operation is usually sacrificed to meet security and dependability requirements, particularly in analogue systems.

c) *Blocking protection schemes (see 1.5)*

This term refers to schemes where the received command blocks the operation of local protection. These channels utilise similar principles to permissive trip channels; however, dependability of operation and speed are prime requirements.

2.2 Overall operating time of teleprotection systems (telecommunication circuit included)

The overall operating time T is the time elapsed between the instant of change in state at the command input and the instant of the corresponding change in state at the command output, including propagation time and additional delay due to noise.

The overall operating time of a teleprotection system influences the fault clearance time (see figure 6).

NOTE – Fault clearance time T_c as shown in figure 6 is typical only.

2.3 Transmission times (telecommunication circuit excluded)

The transmission time of a teleprotection system is the time elapsed between the instant of change in state at the command input and the instant of the corresponding change in state at the command output, excluding propagation time.

The nominal transmission time T_0 is the transmission time measured under noise-free transmission conditions (see also 4.3.3).

The maximum actual transmission time T_{ac} is the maximum transmission time encountered under noisy conditions for a defined dependability and signal-to-noise (S/N) ratio or bit error rate (BER).

Ce temps de transmission est mesuré en appliquant, selon le type de téléprotection, un bruit blanc continu ou des erreurs aléatoires de bits à la voie de transmission. Pour diverses valeurs du rapport signal sur bruit (S/B) ou du taux d'erreur de bits (BER), le temps réel maximal de transmission T_{ac} (typiquement 2 ms – 65 ms comme représenté à la figure 6) est déterminé.

Cette méthode d'essai correspond d'aussi près que possible à des conditions réelles.

Des fonctions d'alignement de niveau ou d'inhibition utilisées dans certains matériels de téléprotection peuvent, en raison du bruit, jouer sur le temps de transmission.

2.4 Sécurité

La sécurité est l'aptitude, lorsque aucune commande n'est émise, d'éviter la restitution de commandes en sortie du récepteur, en présence de perturbations et de bruit.

Par commodité, on mesure normalement la probabilité de commande intempestive P_{uc} (voir 4.3.1.1 et 4.3.2.1).

La sécurité est alors donnée par:

$$1 - P_{uc}$$

Une commande intempestive est une commande qui se produit à l'extrémité réceptrice pendant un temps supérieur à une valeur donnée, alors qu'aucune commande correspondante n'a été transmise.

Si la durée de la commande intempestive T_{uc} est supérieure à une durée spécifiée, elle est considérée comme une commande réelle. Pour les dispositifs à déclenchement à autorisation, le risque de déclenchement intempestif est en général faible, tandis que, dans les applications de télédéclenchement direct, chaque commande intempestive entraînera un déclenchement intempestif.

Pour les dispositifs à verrouillage, une commande intempestive peut entraîner, selon sa durée T_{uc}, un retard de déclenchement ou empêcher que le déclenchement voulu se produise (manque de fiabilité du dispositif de protection).

Pour les systèmes de téléprotection analogiques, on mesure la probabilité de commandes intempestives en appliquant des salves de bruit blanc à la voie de transmission; on détermine la probabilité de commandes intempestives pour la valeur pire cas du rapport signal/bruit (S/B) comme le rapport du nombre de commandes intempestives reçu par rapport au nombre de salves de bruit de durée spécifiée qui ont été appliquées.

Cette méthode correspond d'aussi près que possible aux conditions réelles (par exemple fonctionnement de disjoncteur et de sectionneurs, bruit d'arc, etc.) et permet la comparaison de résultats obtenus avec différents matériels (voir 4.3). Il est essentiel que la probabilité de commandes intempestives soit mesurée avec des salves de bruit puisque le récepteur peut bloquer sa sortie après un certain temps de présence de bruit continu. L'intervalle de temps entre des salves de bruit successives doit être suffisant pour permettre au récepteur de se reconfigurer.

The transmission time is measured with continuous white noise or with random bit errors applied to the transmission path depending upon the type of teleprotection system. For various S/N ratios or BERs the maximum actual transmission time T_{ac} (typically 2 ms to 65 ms, as shown in figure 6) is determined.

This method of testing corresponds as closely as possible to actual conditions.

Clamping or inhibit actions used in some teleprotection equipment may influence the transmission time due to noise.

2.4 Security

Security relates to the ability to prevent interference and noise from generating a command state at the receiving end when no command signal is transmitted.

For practical reasons the probability of an unwanted command P_{uc} is normally measured (see 4.3.1.1 and 4.3.2.1).

Security is then given by

$$1 - P_{uc}$$

An unwanted command is a command that occurs at the receiving end for a time longer than a specified duration when no such command has been transmitted.

If the duration of an unwanted command state, T_{uc}, is longer than a specified duration, it will be seen as an actual command. With permissive trip schemes, the risk of an unwanted tripping action is generally low, while in intertripping (direct tripping) schemes each unwanted command will lead to an unwanted tripping action.

With blocking schemes, an unwanted command may lead, depending upon its duration T_{uc}, either to a delayed trip or to a failure to trip (lack of dependability of the protection scheme).

For analogue teleprotection systems, the probability of an unwanted command is measured by applying bursts of white noise to the transmission path. The probability of an unwanted command P_{uc} is determined, for the worst case S/N ratio, from the ratio of the number of unwanted commands received to the number of noise bursts of specified duration that have been applied.

The application of noise bursts corresponds as nearly as possible to actual conditions (e.g. circuit-breaker and disconnector operations, arcing noise, etc.) and enables a comparison of the results obtained with different equipment (see 4.3). It is essential that the unwanted command rate is measured with bursts of noise since the receiver may block its output after a certain time in the presence of continuous noise. The interval between successive noise bursts shall be sufficient so as to allow the receiver to recover.

Pour les systèmes de téléprotection numériques, la sécurité est essayée à l'aide de salves d'erreurs aléatoires. Cette méthode est nécessaire afin d'essayer les matériels de téléprotection qui contiennent des circuits d'inhibition conçus pour fonctionner à une certaine valeur mesurée du taux d'erreur de bit. L'intervalle entre les salves peut être réduit pour essayer le matériel de téléprotection qui ne contient pas de circuit d'inhibition ou de verrouillage. Un essai supplémentaire est nécessaire pour s'assurer que les commandes intempestives apparaissent à la suite de la perte complète ou de la remise en service de la voie de téléprotection numérique. La probabilité d'une commande intempestive P_{uc} est déterminée, pour plusieurs valeurs du taux d'erreur de bit (BER), à partir du rapport du nombre de commandes intempestives au nombre de salves d'erreur.

2.5 Fiabilité

La fiabilité est l'aptitude à émettre et recevoir une commande valable en présence de perturbation et/ou de bruit.

Par commodité, on mesure normalement la probabilité de commandes défaillantes P_{mc} (voir 4.3.1.2 et 4.3.2.2).

La fiabilité est alors donnée par:

$$1 - P_{mc}$$

Quand une commande est produite à l'extrémité émettrice, elle est considérée comme défaillante dans les trois cas suivants:

a) absence totale d'état de commande à l'extrémité réceptrice ou l'état de commande se produit à l'extrémité réceptrice avec un retard excessif;

b) l'état de commande à l'extrémité réceptrice est plus court qu'une durée spécifiée.

Les cas a) et b) donnent évidemment lieu à une défaillance ou à un retard du déclenchement pour les dispositifs à télédéclenchement direct et pour les dispositifs de déclenchement à autorisation.

Pour un dispositif à verrouillage, un fonctionnement intempestif peut apparaître lors de conditions de défaut extérieures (manque de sécurité du dispositif de protection).

La probabilité de commande défaillante est mesurée en appliquant des impulsions de bruit blanc ou des impulsions d'erreurs aléatoires de bits sur la voie de transmission. La probabilité de commande défaillante P_{mc} est alors déterminée, pour diverses valeurs du rapport signal sur bruit (S/B) ou du taux d'erreur de bits (BER) comme le rapport des commandes non reçues à un instant spécifié (et d'une durée spécifiée, voir b) ci-dessus) au nombre de commandes transmises. Il est possible d'utiliser pour l'essai du bruit blanc continu ou des erreurs aléatoires de bits en continu lorsque le mécanisme de blocage du récepteur de téléprotection n'est pas utilisé ou lorsqu'il est inhibé.

Cette méthode correspond d'aussi près que possible aux conditions réelles; de plus, elle présente l'avantage de permettre la comparaison des résultats obtenus sur différents matériels.

For digital teleprotection systems, security is tested with bursts of random errors. This method is required in order to test teleprotection equipment that incorporate inhibit circuits designed to operate at certain measured BERs. The interval between bursts can be reduced to test teleprotection equipment without inhibit or blocking circuits. An additional test is required in order to ascertain whether unwanted commands occur following the complete loss or reintroduction of the digital teleprotection channel. The probability of an unwanted command P_{uc} is determined, for various BERs, from the ratio of the number of unwanted commands received to the number of error bursts.

2.5 Dependability

Dependability relates to the ability to issue and receive a valid command in the presence of interference and/or noise.

For practical reasons the probability of a missing command P_{mc} is normally measured (see 4.3.1.2 and 4.3.2.2).

Dependability is then given by

$$1 - P_{mc}$$

When a command is sent from the transmitting end, it is considered a missing command in the following cases:

a) command state at the receiving end is absent or takes place with an excessive delay;

b) command state at the receiving end is shorter than a specified duration.

Cases a) and b) give rise to a failure to trip or a delayed trip in an intertripping (direct tripping) or permissive tripping scheme.

In a blocking scheme, an unwanted operation is likely to occur in the presence of an external fault condition (lack of security of the protection scheme).

The probability of a missing command is measured by applying pulsed white noise or pulsed random bit errors to the transmission path. The probability of a missing command P_{mc} is then determined, at various S/N ratios or BERs, from the ratio of the number of commands which are not received within a specified time (and are of a specified duration, see b) above) to the number of transmitted commands. Continuous white noise, or continuous random bit errors, may be used for the test when the blocking mechanism of the teleprotection receiver is not employed or is disabled.

This method corresponds as far as possible to actual conditions; furthermore, it offers the advantage that results obtained with different equipment can be easily compared.

2.6 Bande de fréquences nominale/Débit binaire nominal

Pour les systèmes de téléprotection analogique, la bande de fréquences nominale est la largeur de bande nécessaire au matériel de téléprotection pour exécuter ses fonctions spécifiées, y compris toute exigence d'immunité au bruit. La largeur de bande utilisée affecte le temps de transmission. Dans les systèmes de téléprotection analogiques, la bande de fréquences utilisée a une influence sur les autres services qui utilisent la même voie de communication.

Pour les systèmes de téléprotection numérique, la largeur de bande de la voie doit être suffisamment large pour supporter le débit binaire utilisé par le matériel. Le débit binaire utilisé affecte le temps de transmission.

2.7 Impédance nominale

L'impédance nominale d'un matériel de téléprotection est définie comme étant l'impédance d'entrée ou de sortie du matériel dans sa bande de fréquence nominale. L'impédance du matériel de téléprotection à fréquence vocale est normalement de 600 Ω. Dans le cas de voies utilisant une liaison à courant porteur sur ligne d'énergie, l'impédance nominale doit être la même que celle des autres matériels à courant porteur sur ligne d'énergie. Des valeurs typiques sont 50 Ω et 75 Ω non équilibrés et 150 Ω équilibrés.

Pour les matériels de téléprotection numérique, l'impédance nominale dépend de la spécification de l'interface numérique utilisée.

2.8 Signaux de garde/Signaux de commande

Le signal de garde est le signal émis pour surveiller l'intégrité du système de téléprotection et il supervise effectivement la voie de communication en ce qui concerne la qualité du signal. D'autres surveillances sont souvent employées. Lorsqu'il est présent, le signal de garde inhibe toute sortie de commande du récepteur de téléprotection.

Le signal de commande est le signal émis pour provoquer un changement d'état à distance. Les exigences relatives au signal de commande dépendent du type de dispositif, comme défini en 2.1.

2.9 Niveaux des signaux de garde (pour les systèmes analogiques seulement)

Dans le cas de matériels réservés spécifiquement à la téléprotection, le niveau du signal de garde est lié à la puissance de sortie de l'émetteur, de manière à se conformer à sa puissance en crête de modulation (PEP). Pour les matériels CPL à fréquences vocales, une même voie peut acheminer d'autres signaux en assurant plusieurs fonctions avec des signaux d'exploitation mixte. Quand un relais de mise en route se trouve actionné, le signal de garde peut être émis à la pleine puissance de l'émetteur, en coupant les autres signaux.

L'augmentation du signal de garde est également utilisée sur des systèmes non partagés, comme les systèmes silencieux ou ceux qui utilisent des équipements CPL de protection à haute fréquence.

2.10 Niveaux des signaux de commande (pour les systèmes analogiques seulement)

Dans le cas de matériels spécifiques à la téléprotection, le niveau des signaux de commande, comme celui des signaux de garde, est lié à la puissance en crête de modulation de l'émetteur (PEP).

2.6 Nominal frequency band or bit rate

For analogue teleprotection equipment, the nominal frequency band is given by the bandwidth required by the teleprotection equipment to perform its stated functions, including any noise sensing requirement. The bandwidth used affects the transmission time. In analogue teleprotection, the frequency band used has a bearing on other services using the same communication channel.

For digital teleprotection equipment, the bandwidth of the channel needs to be sufficiently large to support the bit rate which the particular equipment utilises. The bit rate used affects the transmission time.

2.7 Nominal impedance

The nominal impedance of teleprotection equipment is defined as the input and output impedance of the equipment measured at its nominal frequency band. The impedance of voice frequency teleprotection equipment is normally 600 Ω. In the case of power line carrier channels the nominal impedance shall be the same as that for other power line carrier equipment. Typical values are 50 Ω and 75 Ω unbalanced, and 150 Ω balanced.

For digital teleprotection equipment the nominal impedance will depend on the specified digital interface being used.

2.8 Guard signals/Command signals

The guard signal is a signal that is transmitted to monitor the integrity of the teleprotection system and it effectively supervises the channel in terms of the signal quality. Other monitoring is often also employed. When present, the guard signal inhibits any command output of the teleprotection receiver.

The command signal is a signal that is transmitted to produce a change of state at a remote location. The requirements for the command signal are dependent upon the type of scheme as defined in 2.1.

2.9 Levels of guard signals (analogue systems only)

In the case of equipment dedicated to teleprotection, the level of a guard signal is related to the power output of the transmitter in order to comply with its peak envelope power (PEP). In the case of PLC voice frequency equipment, other services may be carried on the same link on a multi-purpose basis. When a starting relay operates, the guard signal may be boosted to the full power of the transmitter, cutting other signals.

Boosting of the guard signal is also employed on some dedicated systems, such as quiescent systems or those employing PLC high-frequency teleprotection equipment.

2.10 Levels of command signals (analogue systems only)

In the case of equipment dedicated to teleprotection the level of the command signal, as well as the level of the guard signal, are related to the PEP of the transmitter.

Dans tous les cas où l'augmentation de puissance est appliquée pour les signaux de garde, les signaux de commande sont traités de la même façon. Dans de nombreux cas, le signal de commande, seulement, peut être augmenté en puissance.

3 Exigences relatives aux systèmes de commande de téléprotection

3.1 Exigences générales relatives aux interfaces du matériel

Les exigences suivantes s'appliquent à l'interface entre le matériel de protection et le matériel de téléprotection aussi bien qu'à l'interface entre le matériel de téléprotection et le système de télécommunication. Ces interfaces a) et b) sont définies par les figures 1, 2, 3 et 4. Ces exigences s'appliquent tout aussi bien lorsque les matériels sont intégrés ou séparés les uns des autres.

Si le matériel de protection et le matériel de téléprotection forment un système combiné installé dans la même enveloppe et dans le même lieu, les exigences relatives à l'interface a) peuvent ne pas être applicables. Si le matériel de téléprotection et le matériel de télécommunication font partie du même appareil et sont installés dans la même baie et dans le même lieu, les exigences relatives à l'interface b) peuvent ne pas être applicables.

3.1.1 Isolement

Les essais de tenue à l'isolement sont couverts en 3.1.2.

3.1.2 Tensions de tenue d'isolement

Les exigences relatives aux tensions de tenue d'isolement sont en accord avec la CEI 60870-2-1.

Tous les circuits d'entrée et de sortie (y compris les bornes d'alimentation) doivent supporter sans être endommagés les tensions de tenue d'isolement correspondant aux classes suivantes:

VW1 pour toutes les bornes d'émission et de réception (interface b) indiquées aux figures 1 et 4.

VW2 pour toutes les bornes d'alimentation en courant continu, au-dessous de 60 V.

VW3 pour toutes les autres bornes de tension de fonctionnement inférieure à 250 V.

Pour la clarté, les spécifications des classes ci-dessus sont citées.

Tableau 1

Classe	Tension de tenue à la fréquence de l'alimentation (kV eff. pendant 60 s)	Tension de choc 1,2/50 µs (kV crête)
VW1	0,5	1
VW2	1	2
VW3	2,5	5

In all cases, where power boosting is applied to the guard signal, the command signal is treated in the same fashion. In many cases the command signal only may be boosted.

3 Requirements for command type teleprotection systems

3.1 General equipment interface requirements

The following requirements apply to the interface between protection equipment and teleprotection equipment as well as to the interface between teleprotection equipment and the telecommunication system. These interfaces a) and b) are defined in figures 1, 2, 3 and 4. The requirements apply equally when the various types of equipment are integrated as well as separated from each other.

If the protection equipment and the teleprotection equipment form a combined system installed in the same enclosure in the same location, the requirements for interface a) may not be applicable. If the teleprotection equipment and the telecommunication equipment are part of a common apparatus and are installed in the same bay in the same location, the requirements for interface b) may not be applicable.

3.1.1 Insulation

The insulation withstand tests are covered in 3.1.2.

3.1.2 Insulation withstand voltages

The requirements for insulation withstand voltages are in accordance with IEC 60870-2-1.

All input and output circuits (including power supply terminals) shall sustain without any damage the withstand voltages reported for the following classes:

VW1 for all transmit and receive terminals (interface b) shown in figures 1 and 4.

VW2 for all d.c. terminals below 60 V.

VW3 for all other terminals up to 250 V.

For the sake of clarity the specifications of the aforesaid classes are given below.

Table 1

Class	Power frequency withstand voltage (kV r.m.s. for 60 s)	1,2/50 µs impulse voltage (kV peak)
VW1	0,5	1
VW2	1	2
VW3	2,5	5

Des classes différentes doivent faire l'objet d'un accord entre utilisateur et fabricant.

La résistance d'isolement des circuits en essai ne doit pas être inférieure à 100 MΩ pour toute température inférieure à 35 °C et pour toute humidité relative inférieure à 75 %.

Les essais doivent être effectués le matériel en état de fonctionnement mais les bornes d'alimentation non raccordées.

3.1.3 Niveau de perturbation en ondes oscillatoires amorties

Afin d'essayer l'immunité du matériel aux perturbations provoquées par des phénomènes de commutation ou des défauts du réseau haute tension, l'essai suivant, correspondant à l'essai A.2.5 de la CEI 60870-2-1, doit être effectué.

Tous les circuits d'entrée et de sortie, y compris les bornes d'alimentation, doivent supporter sans être endommagés ou sans commande intempestive, des ondes oscillatoires amorties appliquées aux bornes correspondantes, en mode différentiel et en mode commun. En ce qui concerne les interfaces de communication, seuls les essais en mode commun doivent être appliqués.

La valeur crête normalisée de la tension d'essai doit être de 2,5 $kV_{crête}$, correspondant à un niveau 3 de sévérité selon le tableau 12 de la CEI 60870-2-1.

[Niveau de sévérité 3: matériel installé dans un environnement non particulièrement protégé; matériel de postes satellites ou équipements terminaux de postes éloignés situés en zone résidentielle et industrielle.]

Les essais en mode différentiel doivent être effectués à un niveau moitié des essais en mode commun.

Les essais doivent être effectués dans les conditions de service.

3.1.4 Niveau de perturbation des transitoires rapides en salve

Afin d'essayer l'immunité du matériel aux perturbations provoquées par la commutation de petites charges inductives, par les rebonds de contacts de relais ou par la commutation d'appareillage haute tension, l'essai suivant, correspondant à l'essai A.2.3 de la CEI 60870-2-1, doit être effectué.

Tous les circuits d'entrée et de sortie (y compris les bornes d'alimentation) doivent supporter sans être endommagés ou sans commande intempestive, des transitoires rapides en salves appliqués aux bornes correspondantes, en mode différentiel et en mode commun. En ce qui concerne les interfaces de communication, seuls les essais en mode commun doivent être effectués.

Les modes de défaillance doivent être évalués selon le critère de la CEI 60870-2-1 et la classe de défaillance doit être convenue entre fabricant et utilisateur.

La valeur crête normalisée de la tension d'essai doit être de 2,0 $kV_{crête}$ correspondant à un niveau 3 de sévérité selon le tableau 12 de la CEI 60870-2-1.

[Niveau de sévérité 3: matériel installé dans un environnement non particulièrement protégé; matériel de postes satellites ou équipements terminaux de postes éloignés situés en zone résidentielle ou industrielle.]

Other classes shall be agreed between user and manufacturer.

The insulation resistance of the circuits under test shall not be less than 100 MΩ for any temperature less than 35 °C and relative humidity less than 75 %.

The tests shall be carried out with the equipment under test turned on, but with the power connections disconnected.

3.1.3 Damped oscillatory waves- disturbance level

In order to test the immunity of the equipment to disturbances caused by switching phenomena or faults on the HV network, the following test, which corresponds to test A.2.5 of IEC 60870-2-1, shall be carried out.

All input and output circuits (including power supply terminals), shall sustain, without any damage or unwanted command, damped oscillatory waveforms applied to the relative terminals, both in differential and in common mode. For communication interfaces, only the common mode tests shall be carried out.

The standard peak value of the test voltage shall be 2,5 kV_{peak}, corresponding to a severity level 3 according to table 12 of IEC 60870-2-1.

[Severity level 3: equipment installed in an environment which has no special protection; equipment of controlled stations or remote terminal units located in residential and in industrial areas.]

Differential mode tests shall be carried out at half common mode level.

The tests shall be carried out under operating conditions.

3.1.4 Fast transient bursts – disturbance level

In order to test the immunity of the equipment to disturbances caused by the switching of small inductive loads, relay contact bouncing or switching of HV switchgear, the following test, which corresponds to test A.2.3 of IEC 60870-2-1, shall be carried out.

All input and output circuits (including power supply terminals) shall sustain, without any damage or unwanted command, fast transient bursts applied to the relative terminals both in differential and in common mode. For communication interfaces, only the common mode tests shall be carried out.

Failure modes shall be evaluated in accordance with the criteria given in IEC 60870-2-1 and the class of failure shall be agreed between manufacturer and user.

The standard peak value of the test voltage shall be 2,0 kV_{peak}, corresponding to a severity level 3 according to table 12 of IEC 60870-2-1.

[Severity level 3: equipment installed in an environment which has no special protection: equipment of controlled stations or remote terminal units located in residential and in industrial areas.]

Toutefois, lorsque cela est convenu entre fabricant et utilisateur, la valeur crête de la tension d'essai sera de 4 $kV_{crête}$ conformément au niveau de sévérité 4 du tableau 12 de la CEI 60870-2-1.

Les essais en mode différentiel doivent être effectués avec une tension d'essai d'une valeur crête de 1 $kV_{crête}$ ou 2 $kV_{crête}$ selon le niveau de sévérité spécifié.

Les essais doivent être effectués dans les conditions de service.

3.1.5 Niveaux de perturbation des décharges électrostatiques

Afin d'essayer l'immunité du matériel aux décharges électrostatiques entre un opérateur chargé et le matériel ou entre deux objets proches, l'essai suivant, correspondant à l'essai A.3.1 de la CEI 60870-2-1, doit être effectué.

La valeur crête normalisée de la tension d'essai (au contact) doit être de 8,0 $kV_{crête}$ correspondant à un niveau 4 de sévérité selon le tableau 13 de la CEI 60870-2-1. La décharge dans l'air doit être utilisée lorsque la décharge au contact ne peut pas être appliquée. La valeur crête de la tension d'essai pour les décharges dans l'air est de 15 $kV_{crête}$ pour un niveau 4 de sévérité.

[Niveau de sévérité 4: matériels de postes satellites ou équipements terminaux de postes installés dans des zones non contrôlées.]

Le matériel doit supporter, sans être endommagé ou sans commande intempestive, l'application de la tension d'essai.

L'essai doit être effectué dans les conditions de service.

3.1.6 Champ électromagnétique rayonné

Afin d'essayer l'immunité du matériel aux perturbations provoquées par les champs électromagnétiques produits par les émetteurs radio portables ou tout autre appareil, l'essai suivant, correspondant à l'essai A.5.1 de la CEI 60870-2-1, doit être effectué.

La valeur d'essai du champ électromagnétique doit être de 10 V/m, correspondant à un niveau 3 de sévérité, conformément au tableau 15 de la CEI 60870-2-1.

[Niveau de sévérité 3: matériel installé dans un environnement de rayonnement sévère; matériel de postes satellites ou équipements terminaux de postes éloignés situés en zone résidentielle ou industrielle ou dans les usines électriques.]

Le matériel doit supporter, sans être endommagé ou sans commande intempestive, l'application du champ électromagnétique d'essai.

L'essai doit être effectué dans les conditions de service, dans une configuration d'armoire ouverte.

3.1.7 Emissions RF

Il est admis qu'il est nécessaire de vérifier les limites des perturbations électromagnétiques produites par le matériel et qui peuvent affecter les performances d'autres éléments du système ou influencer l'environnement extérieur.

However, where agreed between manufacturer and user, the peak value of the test voltage shall be 4,0 kV_{peak} corresponding to a severity level 4 according to table 12 of IEC 60870-2-1.

Differential mode tests shall be 1 kV_{peak} or 2 kV_{peak} depending on the severity level specified.

The tests shall be carried out under operating conditions.

3.1.5 Electrostatic discharge – disturbance levels

In order to test the immunity of the equipment to electrostatic discharges between a charged operator and the equipment or between two nearby objects, the following test, which corresponds to test A.3.1 of IEC 60870-2-1, shall be carried out.

The standard peak value of the test voltage (contact discharge) shall be 8,0 kV_{peak} corresponding to a severity level 4 according to table 13 of IEC 60870-2-1. Air discharge shall be used where contact discharge cannot be applied. The peak value of the test voltage for air discharge is 15 kV_{peak} for severity level 4.

[Severity level 4: equipment of controlled stations and remote terminal units installed in uncontrolled areas.]

The equipment shall sustain, without any damage or unwanted command, the application of the test voltage.

The test shall be carried out under operating conditions.

3.1.6 Radiated electromagnetic field disturbances

In order to test the immunity of the equipment to disturbances caused by electromagnetic fields generated by portable radio transceivers or any other device, the following test, which corresponds to test A.5.1 of IEC 60870-2-1, shall be carried out.

The test value of the electromagnetic field shall be 10 V/m, corresponding to severity level 3 according to table 15 of IEC 60870-2-1.

[Severity level 3: equipment installed in an environment with severe radiation; equipment of controlled stations or remote terminal units located in residential and industrial areas, or in electrical plants.]

The equipment shall sustain, without any damage or unwanted command, the application of the test electromagnetic field.

The test shall be carried out under operating conditions in an open rack configuration.

3.1.7 RF disturbance emission

It is considered necessary to verify the limits of electromagnetic disturbance generated by the equipment that may affect the performance of other components of the system or influence the external environment.

Une tension d'essai correspondant à une perturbation RF doit être émise sur toutes les bornes des circuits d'entrée et de sortie (y compris les bornes d'alimentation) selon la classe A de la CEI 60870-2-1 (tableau 17).

Un essai de champ RF rayonné doit être effectué selon la classe A de la CEI 60870-2-1 (tableau 17).

[Classe A: matériels des postes de conduite, des postes satellites ou équipements terminaux de postes situés dans des installations industrielles ou des usines électriques.]

Les essais doivent être effectués dans les conditions de service, dans une configuration d'armoire ouverte.

3.2 Prescriptions spécifiques à l'alimentation

3.2.1 Variations d'alimentation

Tous les appareils de téléprotection doivent supporter (sans être endommagés ou sans commande intempestive) des variations lentes de la tension d'alimentation de sa valeur nominale à zéro et de zéro à sa valeur nominale. Les variations doivent durer au moins 10 s. Pendant l'essai, il faut vérifier le fonctionnement correct du dispositif d'alarme.

3.2.2 Coupures

Afin d'essayer l'aptitude du matériel à supporter des creux ou des coupures de la tension d'alimentation provoquées par des perturbations ou par interruption de connexions dans le câblage de l'alimentation, l'essai suivant, correspondant à l'essai A.1.5 de la CEI 60870-2-1, doit être effectué.

La valeur d'essai des creux de tension doit être égale à 100 % de l'amplitude de la tension nominale et doit durer 10 ms, pour un niveau de sévérité 1, conformément au tableau 11 de la CEI 60870-2-1.

[Niveau de sévérité 1: matériel, systèmes et équipements terminaux de postes avec des dispositifs d'alimentation spécifiques: alimentation sans interruption, sources continues stabilisées avec des batteries, sont des exemples de sources d'alimentation spécifiques.]

Tous les matériels de téléprotection doivent supporter, sans aucune commande intempestive, de brèves coupures de la tension d'alimentation de durée inférieure à 10 ms se produisant en séquences aléatoires sur des périodes inférieures ou égales à 20 s.

De même, si l'alimentation est coupée pour une durée plus longue, puis remise sous tension, aucune commande intempestive ne doit se produire.

Lorsqu'une source d'alimentation alternative est utilisée, des coupures plus longues peuvent se produire. Dans ce cas, il peut être nécessaire d'utiliser une alimentation sans interruption (ASI).

3.2.3 Emissions basses fréquences

Afin de vérifier les limites des perturbations basses fréquences générées par le matériel, qui peuvent affecter d'autres matériels connectés à la même source d'alimentation, un essai de tension de perturbation basse fréquence doit être effectué conformément à la CEI 60870-2-1.

An RF disturbance voltage test shall be carried out on all input and output circuits (including power supply terminals) according to IEC 60870-2-1 (table 17), class A.

An RF radiated field test shall be carried out according to IEC 60870-2-1 (table 17), class A.

[Class A: equipment of control centres, controlled stations and remote terminal units located in industrial or electrical plants.]

The tests shall be carried out under operating conditions in an open rack configuration.

3.2 Specific power supply requirements

3.2.1 Power supply variations

All teleprotection apparatus shall withstand, without damage or unwanted command, slow variations of the power supply voltage from its nominal value to zero and from zero to its nominal value (not faster than 10 s). During the test the alarm device shall be checked for correct operation.

3.2.2 Interruptions

In order to test the ability of the equipment to withstand voltage dips and interruptions on the power supply, caused by disturbances or by loose connections in the power supply wiring, the following test, which corresponds to test A.1.5 of IEC 60870-2-1, shall be carried out.

The test value of the voltage dips shall be 100 % in amplitude with reference to the nominal value and 10 ms in duration, corresponding to a severity level 1 according to table 11 of IEC 60870-2-1.

[Severity level 1: Equipment, systems and remote terminal units with dedicated power supply devices; uninterruptible power supply systems or stabilized d.c. sources with batteries are examples of dedicated power sources.]

All teleprotection equipment shall sustain, without any unwanted command, short interruptions of the power supply voltage lasting not longer than 10 ms and occurring in a random sequence over a period not longer than 20 s.

Similarly, if the power is switched off for a longer period of time and then switched on, no unwanted command shall occur.

When an a.c. power supply is used, longer interruptions can occur. In this case an uninterruptible power supply (UPS) may be required.

3.2.3 LF disturbance emission

In order to verify the limits of LF disturbance generated by the equipment, which may affect other equipment connected to the same d.c. power source, a LF disturbance voltage test shall be carried out according to IEC 60870-2-1.

Le bruit mesuré aux bornes de l'alimentation du matériel en essai ne doit pas être supérieur à 3 mV de bruit psophométrique.

3.2.4 Inversion de polarité

Si le matériel de téléprotection est alimenté par une source d'alimentation continue, il doit comprendre une protection contre les inversions de polarité afin de la prémunir contre une inversion de polarité de la tension d'alimentation.

3.3 Prescriptions applicables aux performances des systèmes de téléprotection

3.3.1 Relations mutuelles entre les prescriptions

La fiabilité, la sécurité et le temps de transmission d'un matériel de téléprotection sont des paramètres qui dépendent mutuellement les uns des autres; pour une largeur de bande constante par exemple, il n'est possible d'améliorer la sécurité qu'au détriment de la fiabilité ou du temps de transmission.

Les prescriptions qu'un matériel de téléprotection doit satisfaire et, par suite, le compromis optimal à retenir entre les paramètres, dépendent de l'utilisation visée (verrouillage, déclenchement à autorisation ou télédéclenchement) et du type de voie de transmission utilisé.

Les performances des matériels de téléprotection doivent être représentées sous forme de courbes qui montrent.

– Pour la sécurité

  P_{uc}: la probabilité de commande intempestive en fonction du rapport S/B donné en décibels pour un système analogique ou du taux d'erreur binaire (BER) pour un système numérique. Le rapport S/B ou le BER pour lequel P_{uc} est maximale est appelé «rapport signal sur bruit pire cas» ou «taux d'erreur binaire (BER) pire cas»;

– Pour la fiabilité

  P_{mc}: la probabilité de commande défaillante en fonction du rapport S/B donné en décibels pour un système analogique ou du taux d'erreur binaire pour un système numérique, pour diverses valeurs de T_{ac}.

Pour un système numérique, la valeur théorique de P_{uc} est normalement très faible et en conséquence nécessiterait une période d'essai très longue pour la mesure de ces probabilités avec un niveau de confiance élevé. Il est donc acceptable de faire une démonstration analytique de la valeur de P_{uc} pour une gamme de valeur du taux d'erreur binaire (BER) afin de compléter les essais lorsqu'il semble raisonnable, pour des raisons pratiques, de procéder ainsi.

Des exemples de courbes de fiabilité et de sécurité pour des systèmes analogiques et numériques sont donnés aux figures 9, 14, 22 et 23.

Des chiffres typiques de performance de fiabilité et de sécurité sont donnés, à titre d'ordres de grandeur, pour les différents dispositifs de téléprotection décrits ci-dessous, à la figure 21.

3.3.1.1 Système à verrouillage

Cette classe de protection se fonde sur le principe de la détection de la valeur du courant de défaut vers «l'extérieur» à l'une des extrémités du circuit protégé si le défaut est externe. Cela engendre l'émission d'une commande de verrouillage qui évite un déclenchement éventuel à l'autre extrémité où le courant débite vers «l'intérieur».

The noise measured across the power supply terminals of the equipment under test shall not be greater than 3 mV, psophometrically weighted.

3.2.4 Reverse polarity

If the teleprotection equipment is supplied from a d.c. source, reverse polarity protection shall be provided in order to protect against the inadvertent inversion of power supply voltage.

3.3 Teleprotection system performance requirements

3.3.1 Interrelationship of requirements

Dependability, security and transmission time of a given teleprotection command system are interdependent parameters; for a constant bandwidth, for instance, security can only be improved at the expense of dependability or transmission time.

The requirements to be met by teleprotection command systems, and therefore the optimum compromise of the above parameters, depend on the particular application (permissive tripping, intertripping or blocking) and on the type of transmission path used.

The performance of the teleprotection equipment shall be given in the form of probability curves.

– For security

  P_{uc}: probability of unwanted command as a function of the S/N ratio given in decibels for an analogue system or of the BER for a digital system. The S/N ratio or BER at which P_{uc} has its maximum is referred to as "worst case S/N ratio" or "worst case BER".

– For dependability

  P_{mc}: probability of missing command as a function of the S/N ratio given in decibels for an analogue system or of the BER for a digital system for different values of T_{ac}.

For a digital system, the theoretical value of P_{uc} is normally very low and would consequently require a lengthy testing period to measure these probabilities to a high degree of confidence. It is therefore acceptable to make an analytical proof of P_{uc} for a range of BERs to supplement testing where it is reasonably practical to do so.

Examples of dependability and security curves for analogue and digital systems are given in figures 9, 14, 22 and 23.

Typical performance guidance figures for the various teleprotection schemes described below are given in figure 21.

3.3.1.1 Blocking

This class of protection is based on the principle of detecting "outward" fault current flow at one end of the protected circuit if the fault is external. This causes transmission of a blocking command which prevents a possible tripping action at the other end where the current flow is "inward".

Chaque extrémité peut verrouiller l'autre (ou les autres), et il n'est pas exigé que le matériel de téléprotection soit capable de recevoir pendant qu'il émet.

Dans les réseaux à verrouillage, la liaison d'information constitue l'élément essentiel pour éviter les déclenchements intempestifs provoqués par des défauts externes. Pour obtenir le verrouillage correct, le déclenchement à l'extrémité qui fournit le courant vers «l'intérieur» doit être suffisamment retardé pour que l'on soit sûr que la commande de verrouillage de l'extrémité fournissant le courant vers «l'extérieur» puisse être reçue.

Pour les défauts internes, le courant de défaut débite vers «l'intérieur» aux deux extrémités et les commandes de verrouillages sont supprimées. La défaillance de la liaison d'information n'affecte généralement pas l'aptitude de la protection à déclencher correctement.

Par suite, la prescription générale applicable à un matériel de téléprotection dans les applications de verrouillage est la rapidité et la fiabilité, car une vitesse trop faible ou une fiabilité insuffisante peuvent causer des déclenchements intempestifs en présence de défauts externes. Une sécurité inadéquate peut engendrer des déclenchements retardés en présence de défauts internes.

3.3.1.2 Système de déverrouillage

Les dispositifs de protection à déverrouillage se fondent sur les mêmes principes que les dispositifs à verrouillage, mais avec des critères de commande opposés: dans les conditions normales, une commande de verrouillage est émise en permanence.

Les dispositifs à déverrouillage sont quelquefois utilisés en plus de dispositifs CPL à déclenchement à autorisation pour améliorer la fiabilité globale dans des conditions limites telles qu'un affaiblissement additionnel extrême dû au défaut en ligne.

Les prescriptions générales qui s'appliquent à la fiabilité et à la sécurité sont les mêmes que pour les applications à verrouillage, alors que le temps de transmission nominal peut être légèrement supérieur.

3.3.1.3 Déclenchement à autorisation (à portée réduite)

Ce dispositif de protection se fonde sur le principe de la détection de la valeur du courant de défaut vers «l'intérieur», au moins à l'une des extrémités du circuit protégé, pour un défaut interne.

La détection d'un défaut à l'une au moins des extrémités provoque un déclenchement à cette extrémité, et de plus, un signal de commande à autorisation est transmis à l'extrémité éloignée. A l'autre extrémité, la réception de la commande provoque le déclenchement en conjonction avec un dispositif détecteur de défaut local.

Chaque extrémité peut envoyer une commande de déclenchement à autorisation aux autres, et le matériel de téléprotection n'a pas à être capable de recevoir pendant l'émission.

Dans les dispositifs à autorisation à portée réduite, la liaison d'information constitue un élément supplémentaire pour obtenir le déclenchement rapide aux deux extrémités pour toutes les origines de défauts internes. La défaillance de la liaison d'information n'affecte pas la sélectivité, mais retarde le déclenchement à une extrémité pour certains emplacements du défaut.

Either end may block the other(s), and the teleprotection equipment need not be able to receive while transmitting.

In blocking systems the information link is an essential feature for avoiding unwanted tripping due to external faults. To obtain correct blocking action, the tripping at the end feeding "inward" current must be delayed sufficiently to ensure that the blocking command from the end feeding "outward" current can be received.

For internal faults the fault current flow is "inward" at both ends and blocking commands are suppressed. Failure of the information link does not generally affect the ability of the protection to trip correctly.

The general requirement for a teleprotection equipment operating in blocking applications is, therefore, that it should be fast and dependable, since inadequate speed or dependability can cause spurious tripping for external faults. Inadequate security can cause delayed tripping for internal faults.

3.3.1.2 Unblocking

Unblocking protection schemes are based on the same principles as blocking schemes, but with opposite command criteria: under normal conditions a blocking command is continuously transmitted.

Unblocking schemes are sometimes used in addition to PLC permissive tripping schemes to improve the overall dependability under marginal conditions, such as extreme additional attenuation due to a line fault.

The general requirements in respect of dependability and security are the same as in blocking applications, although the nominal transmission time may be slightly longer.

3.3.1.3 Permissive tripping (underreach)

This protection scheme is based on the principle of detecting "inward" fault current flow from at least one end of the protected circuit for an internal fault. Detection of a fault from at least one end results in a tripping action at that end, and in addition, a permissive command signal is transmitted to the remote end. At the other end the received command initiates tripping action in conjunction with a local fault detecting device.

Either end may send a permissive tripping (or command) signal to the other(s), and the teleprotection equipment need not be able to receive while transmitting.

In permissive underreach schemes, the information link is a supplementary feature for obtaining fast tripping at both ends for all internal fault positions. Failure of the information link does not affect the selectivity, but delays tripping at one end for certain fault locations.

Aucune commande de déclenchement n'est émise en cas de défaut externe, et la défaillance de la liaison d'information n'affecte généralement pas l'aptitude de la protection à se stabiliser correctement. Toutefois, les perturbations et le bruit peuvent donner des déclenchements intempestifs.

3.3.1.4 Déclenchement à autorisation (à portée étendue)

Cette classe de protection se fonde sur le principe de la détection de la valeur du courant de défaut vers «l'intérieur» aux deux extrémités du circuit protégé, ce qui entraîne l'émission d'une commande de déclenchement à partir des deux extrémités; à l'autre extrémité, la réception de la commande provoque le déclenchement en conjonction avec le dispositif local de détection de défaut.

Chaque extrémité peut envoyer une commande de déclenchement à autorisation aux autres, et le matériel de téléprotection doit être en mesure de recevoir quand il émet.

Dans les dispositifs à autorisation à portée étendue, la liaison d'information constitue l'élément essentiel pour obtenir le déclenchement rapide aux deux extrémités pour tous les défauts internes. La défaillance de la liaison d'information peut affecter la sélectivité et le délai de déclenchement, au moins à une extrémité pour tous les emplacements de défauts au sein du circuit protégé.

En cas de défaut externe, l'extrémité qui alimente le courant vers «l'extérieur» n'émet pas de commande de déclenchement. Cela évite un déclenchement éventuel à l'autre extrémité qui fournit le courant vers «l'intérieur» et la défaillance de la liaison d'information n'affecte généralement pas l'aptitude de la protection à se stabiliser correctement. Toutefois, les perturbations et le bruit peuvent causer des déclenchements intempestifs.

La prescription générale qui s'applique à un matériel de téléprotection utilisé dans un dispositif de déclenchement à autorisation est la fiabilité et la rapidité; pour les dispositifs à portée étendue, la fiabilité est prépondérante. Un défaut de sécurité peut causer des déclenchements intempestifs en présence de défauts externes; le manque de rapidité ou de fiabilité peut entraîner des retards de déclenchement pour tous les défauts internes, ou même un fonctionnement intempestif avec les dispositifs à portée étendue.

3.3.1.5 Télédéclenchement

Dans certaines conditions, un réseau de puissance peut imposer le déclenchement d'un disjoncteur à distance de la protection. Cela s'applique par exemple dans des transformateurs ou des bobines d'inductance sont raccordés au réseau sans disjoncteurs ou pour assurer le déclenchement à distance de la protection à la suite du fonctionnement en cas de défaillance du disjoncteur.

Le signal de commande reçu possède la capacité complète de déclencher sans commande additionnelle, et c'est pourquoi la sécurité du matériel de téléprotection est très importante pour éviter les déclenchements intempestifs. Comme il peut être nécessaire d'émettre des commandes en présence de défaut, la fiabilité a également une grande importance pour obtenir le déclenchement désiré en présence de perturbation et de bruit.

La prescription générale qui s'applique au matériel de téléprotection utilisé en télé-déclenchement est, en conséquence, qu'il soit très fiable et très sûr, car une sécurité et une fiabilité défectueuses peuvent provoquer un fonctionnement intempestif. Avec certaines applications, le matériel doit pouvoir recevoir tout en émettant, et les signaux de commande peuvent être émis pendant une durée plus longue en comparaison à d'autres systèmes de commande de téléprotection.

For external faults no permissive commands are transmitted, and failure of the information link generally does not affect the ability of the protection to stabilize correctly. However, interference and noise can cause unwanted tripping.

3.3.1.4 Permissive tripping (overreach)

This protection scheme is based on the principle of detecting "inward" fault current flow at both ends of the protected circuit. This causes transmission of a permissive command from each end. At the remote ends the received commands initiate tripping action in conjunction with a local fault detecting device.

Each end must send a permissive tripping (or command) to the other(s), and the teleprotection equipment shall be able to receive while transmitting.

In permissive overreach schemes, the information link is an essential feature for obtaining fast tripping at both ends for all internal faults. Failure of the information link may affect the selectivity and delay tripping at one end at least, for faults anywhere along the protected circuit.

For external faults, the end feeding "outward" current does not transmit a permissive command. This prevents a possible tripping action at the other end feeding "inward" current. Failure of the information link does not generally affect the ability of the protection to stabilize correctly. However, interference and noise can cause unwanted tripping.

The general requirement for a teleprotection equipment operating in a permissive tripping application is that it should be secure and fast. In overreach schemes there is a further emphasis on dependability. Inadequate security can cause unwanted tripping for external faults; inadequate speed or dependability can cause delayed tripping for internal faults or even unwanted operation in overreach schemes.

3.3.1.5 Intertripping (transfer tripping)

Various conditions on a power system may require a circuit-breaker to be tripped remotely from a protection relay. This applies, for instance, where transformers or reactors are connected to the system without circuit-breakers or for remote tripping following operation of the circuit-breaker failure protection.

The received command has the complete ability to trip without any additional qualification and, therefore, the security of the teleprotection equipment is of most importance to avoid unwanted tripping. Since intertripping command transmission is likely to be required during fault conditions, dependability is also very important if correct tripping is to be obtained in the presence of noise and interference.

The general requirement for a teleprotection equipment operating in intertripping applications is, therefore, that it should be very secure and very dependable, since both inadequate security and dependability may cause unwanted operation. In some applications the equipment shall be able to receive while transmitting, and commands may be transmitted over a longer period of time than for other teleprotection command systems.

3.3.2 Surveillance et alarmes

La conception des systèmes de téléprotection et la façon d'utiliser les liaisons d'information obligent à tenir compte de limitations pratiques provenant du fait que l'influence des perturbations, du bruit et des défaillances de communication ne peut être totalement négligée.

Quand les signaux de garde ou de commande sont émis ou reçus, ils doivent servir à surveiller la voie de transmission, ainsi que la plus grande partie possible de l'équipement terminal. L'absence de réception d'un signal transmis par suite de la défaillance de la voie de transmission ou de l'équipement terminal doit être détectée par les circuits de surveillance associés au récepteur et à l'émetteur. En outre, une alarme doit être mise en service si la durée de la défaillance dépasse une valeur spécifiée (habituellement ajustable dans une gamme définie). Les circuits de surveillance peuvent encore réagir aux excès de bruit et de perturbations qui pourraient entraver le bon fonctionnement. De nouveau, une alarme doit être émise si la durée de perturbation dépasse le temps spécifié.

De plus, pour les systèmes de téléprotection numériques, les messages de garde ou de commande transmis par un matériel particulier ne doivent pas être reçus en tant que signaux valides de garde ou de commande par le matériel dont ils proviennent ou par un matériel auquel ils ne sont pas destinés. Si le système de communication, par erreur, retourne les messages au matériel dont ils proviennent ou à un matériel auquel ils ne sont pas destinés, une alarme doit être déclenchée. Il convient qu'un tel mécanisme puisse être inhibé pour le besoin des essais.

On doit avoir prévu des moyens pour maintenir à niveau ou inhiber la sortie du récepteur quand les circuits de surveillance ont réagi à une situation anormale. La sortie du récepteur doit être maintenue à niveau ou inhibée selon l'état qui existait avant le défaut de signal ou à un état permanent «commande coupée» ou «commande active». Les différentes options doivent pouvoir être choisies par l'utilisateur. Ce maintien à niveau ou cette inhibition peut être immédiat ou retardé (par exemple commandé par le circuit d'alarme).

Les fonctions propres aux circuits de surveillance et d'alarme doivent être vérifiées à l'occasion des essais des performances (voir article 4).

3.3.3 Gigue

Lorsqu'un système de téléprotection numérique est utilisé dans un réseau numérique, il faut effectuer des mesures pour s'assurer que la gigue à la sortie de l'émetteur de téléprotection n'affecte pas le réseau et que la gigue à l'entrée du récepteur de téléprotection ne provoque pas un mauvais fonctionnement ou un fonctionnement intempestif.

Les exigences suivantes s'appliquent.

3.3.3.1 Gigue à la sortie de l'émetteur

La gigue à la sortie de l'émetteur de téléprotection doit rester dans les limites suivantes, déduites de la Recommandation G.823 de l'UIT-T section 2.1:

3.3.2 Monitoring and alarms

The design of teleprotection systems and the way in which information links are used need to take account of the practical limitations arising from the fact that the influence of interference, noise and communication failures cannot be completely avoided.

While transmitting and receiving either guard or command signals, the teleprotection equipment shall monitor the transmission path and as much of the terminal equipment as possible. Failure to receive the transmitted signal, whether by failure of the transmission path or the terminal equipment, shall be detected by monitoring circuits associated with the receiver and transmitter. In addition, an alarm shall be given, provided that the period of failure exceeds a specified time (usually settable within a defined range). The monitoring circuits may further respond to excessive interference and noise at a level that could impair correct operation. Again, an alarm shall then be given, should the period of interference exceed a specified time.

Furthermore, for digital teleprotection systems, the command or guard messages transmitted by a particular equipment shall not be received as valid guard or command messages by the originating equipment or by the wrong equipment. If the communication system mistakenly directs messages back to the originating equipment or to the wrong equipment, then an alarm shall be given. It should be possible to disable such a mechanism for test purposes.

Facilities shall be provided for clamping or inhibiting the receiver output once the monitoring circuits have responded to abnormal conditions. The receiver output shall be clamped or inhibited either in the state that existed prior to the signal failure, or in a steady "command off" or "command on" state. The various options shall be selectable by the user. The clamping or inhibit action may be immediate or delayed (e.g. controlled by the alarm circuit).

The correct functioning of monitoring and alarm circuits shall be checked during the performance tests (see clause 4).

3.3.3 Jitter

When a digital teleprotection system is used in a digital network, measurements shall be carried out to ensure that jitter at the output of the teleprotection transmitter does not affect the network and that jitter at the input of the teleprotection receiver does not result in any type of malfunctioning or unwanted operation.

The requirements given hereafter apply.

3.3.3.1 Jitter at the transmitter output

Jitter at the output of the teleprotection transmitter shall meet the following limits, derived from ITU-T Recommendation G.823, section 2.1:

Tableau 2

Débit binaire kbits/s	**B1** **(intervalles unité, crête-crête)**	**B2** **(intervalles unité, crête-crête)**	**Largeur de bande du filtre de mesure**		
			f1	f3	f4
64	0,25	0,05	20 Hz	3 kHz	20 kHz

NOTE 1 – Les limites ci-dessus se réfèrent à une interface codirectionnelle.

NOTE 2 – Le filtre de mesure est défini comme étant un filtre passe-bande de fréquence de coupure basse f1 ou f3, de fréquence de coupure haute f4 et d'une atténuation hors bande de 20 dB/décade.

NOTE 3 – L'amplitude de «l'intervalle unité» est définie par:

UI = 1 / Rd

où Rd est le débit binaire (bits/s). Par exemple, si Rd = 64 kbits/s, alors UI = 15,6 µs.

La figure 24 présente le principe de ce type de mesure. L'essai doit être effectué dans un état de garde permanent, dans un état de commande permanent, et pendant un essai de fiabilité (transitions répétitives de l'état de garde à l'état de commande).

3.3.3.2 Gigue à l'entrée du récepteur

Le récepteur de téléprotection doit supporter un signal d'entrée modulé par une gigue sinusoïdale sans que n'apparaisse un mauvais fonctionnement quel qu'il soit, ou une commande intempestive. Pour les besoins de l'essai, l'amplitude et la fréquence de la gigue sont données par les courbes présentées à la figure 25, déduites de la Recommandation G.823 de l'UIT-T, section 3.1.1, dont les limites sont les suivantes:

Tableau 3

Amplitude (intervalles unité, crête à crête)			**Fréquence** Hz				
A0	A1	A2	f0	f1	f2	f3	f4
1,15	0,25	0,05	$1{,}2 \times 10^{-5}$	20	600	3×10^{3}	2×10^{4}

La gigue est la seule contrainte à prendre en compte pendant cet essai. Aucune erreur ne doit être injectée dans le flux de données reçu.

Lorsque le fonctionnement a lieu au-dessous des limites présentées à la figure 25, il convient que la performance de la téléprotection ne soit altérée en aucune façon; il convient que la gigue n'affecte pas la sécurité, la fiabilité ou le temps de transmission.

4 Méthodes applicables au contrôle des performances

4.1 Contrôle général d'interface du matériel

Les essais suivants doivent être effectués conformément aux publications de la CEI citées.

Les exigences sont données à l'article 3.

Table 2

Digit rate kbit/s	B1 (unit intervals, peak-to-peak)	B2 (unit intervals, peak-to-peak)	Bandwidth of measuring filter		
			f1	f3	f4
64	0,25	0,05	20 Hz	3 kHz	20 kHz

NOTE 1 – The above limits relate to a co-directional interface.

NOTE 2 – The measuring filter is defined as a passband filter with lower cut-off frequency f1 or f3, upper cut-off frequency f4 and an out-of-band characteristic of 20 dB/decade.

NOTE 3 – The magnitude of the "Unit Interval" is defined as follows:

UI = 1 / Rd

where Rd is the digit rate in bits/s. For example; if Rd = 64 kbits/s, then UI = 15,6 µs.

The test set-up for this type of measurement is shown in figure 24. The test shall be carried out in a permanent guard state, a permanent command state and during a dependability test (repetitive transitions from guard to command).

3.3.3.2 Jitter at the receiver input

The teleprotection receiver shall withstand an input signal modulated by a sinusoidal jitter without it resulting in any type of malfunctioning or unwanted command. For test purposes the amplitude and frequency of the jitter are given in figure 25, derived from ITU-T Recommendation G.823, section 3.1.1, whose limits are given hereafter.

Table 3

Amplitude (unit intervals, peak-to-peak)			Frequency Hz				
A0	A1	A2	f0	f1	f2	f3	f4
1,15	0,25	0,05	$1{,}2 \times 10^{-5}$	20	600	3×10^{3}	2×10^{4}

Jitter is the only impairment to be taken into account during this test. No errors shall be introduced into the received data flow.

When operating below the limits shown in figure 25, the teleprotection performance should not be altered in any way; jitter should not affect security, dependability or transmission time.

4 Methods for performance testing

4.1 General equipment interface tests

The following tests shall be carried out according to the IEC publications quoted.

The requirements are given in clause 3.

4.1.1 Essais d'isolement

Les essais de tenue à la tension d'isolement sont couverts au 4.1.2.

4.1.2 Essais de tenue à la tension d'isolement

La procédure d'essai est donnée dans la CEI 60060-1, sections 5 et 6.

Après les essais, un contrôle est effectué à l'aide d'un ohmmètre 500 V c.c. afin de vérifier que la résistance d'isolement entre les bornes réunies ensemble et la terre est supérieure à la valeur spécifiée de 100 MΩ.

En final, le matériel est mis sous tension pour vérifier le fonctionnement correct et l'absence de fonctionnement intempestif.

4.1.3 Essai de perturbation aux ondes oscillatoires amorties

La procédure d'essai est celle de la CEI 61000-4-1, article A.2.5.

Pendant l'essai, on vérifie le fonctionnement correct du matériel et l'absence de fonctionnement intempestif.

4.1.4 Essai de perturbation aux transitoires rapides en salves

La procédure d'essai est celle de la CEI 61000-4-1, article A.2.3.

Pendant l'essai, on vérifie le fonctionnement correct du matériel et l'absence de fonctionnement intempestif.

4.1.5 Essai de perturbation aux décharges électrostatiques

La procédure d'essai est celle de la CEI 61000-4-1, article A.3.1.

4.1.6 Essai de champ électromagnétique rayonné

La procédure d'essai est celle de la CEI 61000-4-1, article A.5.1.

4.1.7 Essai d'émissions RF

La procédure d'essai est celle du CISPR 22, article 10.

4.2 Essais spécifiques à l'alimentation

4.2.1 Variations d'alimentation

Dans cet essai, on tient compte des variations lentes de la tension d'alimentation qui dépassent la limite inférieure de tolérance de cette tension.

Des essais de variation de l'alimentation doivent être effectués séparément sur l'émetteur et sur le récepteur d'un système de téléprotection.

4.1.1 Insulation tests

The insulation voltage withstand tests are covered in 4.1.2.

4.1.2 Insulation voltage withstand tests

The test procedure is given in sections 5 and 6 of IEC 60060-1.

After testing a check is run with an ohmmeter at 500 V d.c. in order to verify that the insulation resistance between the terminals in parallel and earth is higher than the prescribed value of 100 MΩ.

Finally the equipment is switched on and checked for correct operation and absence of unwanted operation.

4.1.3 Damped oscillatory waves disturbance test

The test procedure is given in A.2.5 of IEC 61000-4-1.

During testing the equipment is checked for correct operation and absence of unwanted operation.

4.1.4 Fast transient bursts disturbance test

The test procedure is given in A.2.3 of IEC 61000-4-1.

During testing the equipment is checked for correct operation and absence of unwanted operation.

4.1.5 Electrostatic discharge disturbance test

The test procedure is given in A.3.1 of IEC 61000-4-1.

4.1.6 Radiated electromagnetic field test

The test procedure is given in A.5.1 of IEC 61000-4-1.

4.1.7 RF disturbance emission test

The test procedure is given in clause 10 of CISPR 22.

4.2 Specific power supply tests

4.2.1 Power supply variations

In this test slow power supply voltage variations which exceed the lower limit of supply tolerances are taken into account.

Separate power supply variation tests shall be performed on the transmitter and the receiver of a teleprotection system.

4.2.2 Coupures

Cet essai est effectué grâce à une coupure brève de 10 ms et, afin de mieux simuler la situation réelle, avec une séquence aléatoire de coupures générées par un dispositif de commutation, comme cela est indiqué à la figure 7.

Afin de s'approcher le plus possible d'une séquence aléatoire réelle des coupures, le générateur de trame pseudo-aléatoire utilisé pour les essais de transmission de données, peut être mis en oeuvre pour piloter le dispositif de commutation.

Pour une trame de 2 047 bits, il est possible de réaliser les durées de coupure suivantes:

Débit binaire (bits/s)	*Durée des coupures (ms)*
1 200	0,83 à 8,3

De même, la déconnexion de la source d'alimentation suivie d'une reconnexion après 1 min ne doit pas provoquer de commande intempestive.

Des essais de coupures d'alimentation doivent être effectués séparément sur l'émetteur et sur le récepteur d'un système de téléprotection.

4.2.3 Emissions basses fréquences

Le principe de la mesure du bruit généré par le matériel et réinjecté dans la source d'alimentation externe est indiqué à la figure 8.

Le filtre passe-bas découple le matériel de la source d'alimentation.

4.2.4 Inversion de polarité

Aucun montage spécial n'est nécessaire pour l'essai d'inversion de polarité.

4.3 Contrôle de performance des systèmes de téléprotection

Une voie de téléprotection peut être exposée à diverses sortes de bruits suivant le moyen de transmission utilisé.

Les essais de sécurité comme, dans une certaine mesure, les essais de fiabilité font appel à des procédures qui prennent du temps. Il est donc très important de choisir une procédure qui donne une bonne indication des performances d'une voie sur une durée raisonnable de temps. La procédure choisie doit également être facile à reproduire et les instruments d'essai doivent être faciles à se procurer. De plus, les essais ne représentent qu'un compromis par rapport aux conditions réelles de fonctionnement, et il convient de reconnaître que des conditions d'essai plus onéreuses peuvent se présenter en pratique. En conséquence, il convient de présenter les résultats comme un moyen d'obtenir des performances comparatives et non pas absolues.

4.3.1 Systèmes de téléprotection analogiques

L'une des façons de remplir toutes les prescriptions précitées consiste à utiliser une procédure d'essai à base de bruit blanc. La sécurité et la fiabilité peuvent toutes deux être contrôlées en fonction du rapport signal/bruit quand le bruit est du bruit blanc. Dans certains cas spéciaux, les résultats ne se comparent pas avec les mesures effectuées avec du bruit impulsionnel.

4.2.2 Interruptions

The test is carried out with a single short interruption of 10 ms and, in order to give a better approximation of the real situation, with a random sequence of interruptions generated by a switching device, as indicated in figure 7.

In order to approach the random sequence of real interruptions, the pseudo-random pattern generator of a data transmission test set can be used to drive the switching device.

For a 2 047 bit pattern the following interruption duration can be achieved:

Bit rate (bits/s)	*Interruption duration (ms)*
1 200	0,83 to 8,3

Disconnection of the power source followed by reconnection after 1 min shall not cause any unwanted command either.

Separate power supply interruption tests shall be performed on the transmitter and the receiver of a teleprotection system.

4.2.3 LF disturbance emission

The test circuit used for measuring the noise generated by the equipment and introduced into the external power supply source is indicated in figure 8.

The low-pass filter decouples the equipment from the power supply source.

4.2.4 Reverse polarity

No special test set-up is needed for the reverse polarity test.

4.3 Teleprotection system performance tests

A teleprotection channel may be exposed to various kinds of noise depending on the transmission medium used.

Testing the security and to some degree also testing the dependability is a time-consuming operation. It is therefore very important to choose a procedure which will give a good measure of the performance of the channel within a reasonable time frame. The chosen procedure shall also be easy to repeat and the test instruments easy to obtain. Furthermore, the tests represent only a compromise on actual operating conditions and it should be recognized that more onerous conditions will occur in practical situations. The results should, therefore, be presented as indicative of comparative, and not absolute, performance.

4.3.1 Analogue teleprotection systems

One way to fulfil all the above-mentioned requirements for analogue systems is to adopt a test procedure using white noise. Both the security and the dependability can be tested in relation to the S/N ratio when the noise is white noise. In some special cases, the results are not comparable with measurements made with impulse noise.

Le bruit doit être rapporté à une largeur de bande fixe de 4 kHz (voir A.1). Il ne faut pas utiliser des largeurs de bande inférieures à 1 kHz environ, car elles entraînent des incertitudes sur le niveau mesuré. La largeur de bande choisie est utilisée sans tenir compte de la voie en essai. Les mesures de bruit ne doivent pas être pondérées.

Des essais complémentaires peuvent être effectués avec des fréquences variables.

4.3.1.1 Sécurité

Le bruit le plus critique pour une voie de téléprotection consiste en des salves de bruit impulsionnel de niveau élevé. A la place, on utilisera des salves de bruit blanc pour essayer la sécurité, la durée des salves T_B constituant la référence dans le domaine temps. Une durée de 200 ms et un intervalle suffisamment long entre les salves doivent être choisis pour assurer le déverrouillage du récepteur entre des salves successives.

On applique, dans un temps donné, un certain nombre de salves de bruit pour provoquer l'apparition d'un certain nombre de commandes intempestives à la sortie du récepteur.

La sécurité est définie par $1 - P_{uc}$.

P_{uc} peut s'estimer de la manière suivante:

$$P_{uc} \approx \frac{N_{uc}}{N_B}$$

où

N_B est le nombre de salves appliquées;

N_{uc} est le nombre de commandes intempestives à la sortie du récepteur.

Pour mesurer la sécurité, il est recommandé d'utiliser un montage d'essai comme celui de la figure 12.

Le nombre de commandes intempestives et le nombre total de salves de bruit doivent être consignés en fonction du rapport signal/bruit, où le signal (S) est le niveau de garde. Il en découle une caractéristique semblable à la courbe *a* de la figure 14 si le récepteur ne comporte aucun dispositif de verrouillage.

On ne doit compter qu'une seule commande intempestive par salve et seulement si sa durée est supérieure à une valeur spécifiée, par exemple 1 ms.

On peut obtenir une caractéristique semblable à celle de la courbe *b* de la figure 14 quand le récepteur utilise des dispositifs de verrouillage. Suivant le niveau du seuil du dispositif de verrouillage, mesurer une caractéristique réelle comme celle de la courbe *b* peut prendre du temps, car la valeur mesurée de P_{uc} devient très faible.

Il convient de mesurer les courbes de probabilité de commande intempestive P_{uc} pour une valeur nominale du niveau de garde reçu.

On donnera une courbe pour chaque réglage recommandé pour la voie.

4.3.1.2 Fiabilité

Le bruit peut entraver le fonctionnement d'une voie de téléprotection en retardant les signaux réels de commande ou en empêchant le récepteur de restituer les commandes.

The noise shall be referred to a fixed 4 kHz bandwidth (see A.1). Bandwidths smaller than approximately 1 kHz shall not be used since this will result in uncertainty as to the measured level. The chosen bandwidth is used irrespective of the channel tested. All noise measurements shall be unweighted.

Additional tests may be carried out using variable tones.

4.3.1.1 Security

The most serious noise for a teleprotection channel consists of bursts of impulse noise of high level. Bursts of white noise are used instead when testing the security, the duration of the noise bursts T_B being used as a time reference. A duration of 200 ms and an interval sufficiently long between bursts to ensure deblocking of the receiver between subsequent bursts shall be chosen.

Within a given time a number of noise bursts are applied and a number of unwanted commands appear at the receiver output.

Security is defined as $1 - P_{uc}$.

The estimate of P_{uc} can be stated as follows:

$$P_{uc} \approx \frac{N_{uc}}{N_B}$$

where

N_B is the number of noise bursts applied;

N_{uc} is the number of unwanted commands at the receiver output.

When measuring security a test set-up similar to that shown in figure 12 is recommended.

The number of unwanted commands recorded and the total number of noise bursts applied shall be recorded in relation to the S/N ratio, where the signal S is the guard level. This will result in a characteristic similar to curve *a* in figure 14 if no blocking device is included in the receiver.

Only one unwanted command per burst shall be counted and only if its duration is longer than a specified time, e.g. 1 ms.

When using blocking devices in the receiver a characteristic similar to curve *b* of figure 14 may result. Depending on the threshold level and response time of the blocking device it will be time-consuming to measure an actual characteristic similar to curve *b*, because the measured P_{uc} is very low.

Curves for the probability of unwanted command P_{uc} should be measured at the nominal received guard level.

Curves may be given for each setting recommended for the channel.

4.3.1.2 Dependability

Noise may disrupt a teleprotection channel by delaying a genuine command signal or by preventing the receiver from delivering a command.

Il est donc important d'essayer le récepteur pour divers rapports signal/bruit S/B, où le niveau S est le niveau de commande reçu. La fiabilité doit être mesurée en fonction du rapport signal/bruit en comparant le nombre de commandes fournies par le récepteur pendant une période raisonnable de transmission avec le nombre de commandes envoyées par l'émetteur.

La fiabilité augmente quand on peut accepter une durée de transmission plus longue. Un certain nombre de commandes sont envoyées et reçues pendant un temps donné.

La probabilité estimée de commande défaillante peut s'écrire:

$$P_{mc} \approx \frac{N_T - N_R}{N_T} = 1 - \frac{N_R}{N_T}$$

où

N_T est le nombre de commandes envoyées;

N_R est le nombre de commandes reçues.

La fiabilité est alors égale à $1 - P_{mc}$.

On construit une famille de courbes semblables à celles de la figure 9 en mesurant la fiabilité en fonction du rapport signal/bruit pour diverses valeurs de la durée de transmission.

On utilise du bruit blanc gaussien en impulsions. Le bruit doit commencer 10 ms avant la commande et doit se terminer en même temps que la commande.

Du bruit blanc continu peut être utilisé pour l'essai lorsque le verrouillage du récepteur de téléprotection n'est pas employé ou lorsqu'il est inhibé.

Un montage semblable à celui de la figure 10 est recommandé pour mesurer la fiabilité.

Pour obtenir une famille de courbes comme à la figure 9, il est nécessaire d'envoyer un nombre suffisant de commandes pour avoir une mesure statistiquement significative. Plus la fiabilité à mesurer a une valeur élevée et plus il sera nécessaire d'envoyer un nombre de commandes élevé (voir A.2).

Chaque commande doit avoir une durée minimale cohérente avec la durée maximale de transmission tolérable. L'intervalle entre commandes successives doit être suffisant pour permettre le rétablissement du récepteur. Il en découlera normalement une vitesse de récurrence de 1 à 10 commandes par seconde.

Pour toutes les applications, la commande reçue doit avoir une durée supérieure à une valeur spécifiée, par exemple 10 ms.

Pour chaque réglage de la voie, on peut donner des courbes représentant la fiabilité en fonction du rapport signal/bruit. Il revient au constructeur de donner ces courbes.

Les courbes doivent au moins être données dans la plage comprise entre T_0 et $3 \times T_0$.

It is therefore important to test the receiver for various S/N ratios, where the signal S is the received command level. Dependability versus S/N ratio shall be measured by comparing the number of commands delivered from the receiver within an acceptable actual transmission time with the number of commands sent from the transmitter.

If a longer transmission time can be accepted, dependability will increase. Within a given time a number of commands are sent and received.

The estimated probability of a missing command can be stated as follows:

$$P_{mc} \approx \frac{N_T - N_R}{N_T} = 1 - \frac{N_R}{N_T}$$

where

N_T is the number of commands sent,

N_R is the number of commands received.

The dependability is then given by 1 – P_{mc}.

When measuring the dependability versus S/N ratio for various transmission times a family of curves similar to that given in figure 9 is obtained.

Pulsed Gaussian white noise is used. The noise shall be initiated 10 ms before the command and shall terminate at the same time as the command.

Continuous white noise may be used for the test when the blocking mechanism of the teleprotection receiver is not employed or is disabled.

When measuring dependability a test set-up similar to that shown in figure 10 is recommended.

To obtain a family of curves similar to that shown in figure 9, it is necessary to send a sufficient number of commands in order to obtain a statistically significant measurement. The higher the dependability one intends to measure, the higher the number of commands it is necessary to send (see A.2).

Each command shall have a minimum duration consistent with the maximum tolerable transmission time. The interval between successive commands shall be sufficient to allow the receiver to recover. This will normally result in a repetition rate of 1 to 10 commands per second.

For all applications the received command shall be longer than a specified duration, e.g. 10 ms.

For each setting recommended for the channel, curves showing the dependability versus S/N ratio shall be given. The manufacturer shall produce these curves.

The curves shall at least be given within the range T_0 and 3 × T_0.

4.3.1.3 Temps de rétablissement

Le temps que le matériel met pour se rétablir de salves de bruit de courte durée et de niveau élevé peut avoir un effet sur son aptitude à transmettre avec succès une commande permanente dans une courte période de temps. Ce temps de rétablissement peut être affecté par la durée de remise à zéro de l'un des mécanismes utilisés pour l'inhibition de déclenchement.

Un montage d'essai pour le temps de rétablissement est présenté à la figure 20.

Une commande permanente est initialisée dans la voie de façon synchrone à une salve de bruit de courte durée (20 ms). La salve de bruit est ajustée pour obtenir un rapport signal/bruit (S/B) de 0 dB. Le temps d'émission de la commande est alors mesuré. Cet essai est répété un certain nombre de fois pour déterminer la plage des retards qui ont été relevés.

La différence entre le temps de transmission nominal (T_0) (sans bruit) et le temps de transmission réel mesuré pendant l'essai, tenant compte de la durée des salves de bruit, donne une bonne indication du temps de rétablissement.

4.3.1.4 Perturbations dues à des fréquences discrètes

Un montage d'essai semblable à celui de la figure 16 est recommandé pour mesurer la sensibilité des récepteurs de téléprotection aux perturbations produites par des fréquences discrètes. L'essai doit être effectué dans les conditions suivantes:

a) L'émetteur envoie un signal de garde

   Les conditions en sortie de commande doivent être surveillées quant aux commandes intempestives quand le signal perturbateur est balayé sur toute la bande de fréquences utilisée. On doit utiliser au moins les niveaux suivants pour le signal perturbateur: le rapport entre le niveau du signal de garde et le niveau du signal perturbateur doit être de –6 dB, 0 dB et +6 dB. On peut faire des balayages complémentaires avec d'autres niveaux de signal perturbateur dans l'intention de vérifier la dépendance en fréquence et par rapport au niveau de la perturbation.

b) Selon agrément entre fabricant et utilisateur, d'autres essais peuvent être effectués (par exemple, le signal de garde étant coupé en présence de bruit).

4.3.1.5 Perturbation par écart de fréquence

Les matériels de téléprotection utilisent quelquefois des circuits de télécommunication où des écarts de fréquence peuvent se produire.

Un essai de perturbation par écart de fréquence ne doit être effectué que sur accord entre utilisateur et constructeur.

Un montage semblable à celui de la figure 17 peut être utilisé.

La basse fréquence de l'émetteur de téléprotection est transformée en une fréquence plus élevée par la fréquence f_S. Une seule bande latérale est transmise par le filtre passe-bande qui suit le modulateur. Du côté récepteur, la fréquence f_r démodule la fréquence élevée pour retrouver la basse fréquence à la sortie du démodulateur. Le filtre passe-bas placé à la sortie du démodulateur permet uniquement aux fréquences basses d'atteindre le récepteur de téléprotection.

4.3.1.3 Recovery time

The time required by the equipment to recover from a short duration burst of noise at a high level can have an effect on its ability to successfully convey persistent command information within a short period of time. This recovery time can be affected by the reset time of any trip-inhibiting mechanisms utilised.

A test set-up for recovery time measurement is shown in figure 20.

A persistent command is initiated synchronously with a short duration (20 ms) burst of noise into the channel. The noise burst is pre-set to a S/N ratio of 0 dB. The actual command transmission time is then measured. The test is repeated a number of times to determine the spread of delays incurred.

The difference between the nominal (noise-free) transmission time (T_0) and the actual transmission time measured during the tests, allowing for the duration of the noise burst, gives a fairly accurate indication of the recovery time.

4.3.1.4 Interference by discrete frequencies

When measuring the sensitivity of teleprotection receivers to interference from discrete frequencies, a test set-up similar to that shown in figure 16 is recommended. The test shall be carried out for the conditions given below.

a) The transmitter sends a guard signal

   Command output conditions shall be monitored for unwanted commands when the interfering signal is swept over the whole frequency band used. At the very least, the following levels of the interfering signal shall be used: the ratio of the guard signal level to the level of the interfering signal shall be –6 dB, 0 dB and +6 dB. Additional sweeps with other interfering signal levels may be made, in order to verify both the frequency and level dependence of this interference.

b) Other tests may be carried out by agreement between the user and the manufacturer (for instance, with the guard signal removed in the presence of noise).

4.3.1.5 Interference by frequency deviation

The teleprotection equipment sometimes uses a telecommunication circuit where frequency deviation may occur.

Only when agreed upon between the user and manufacturer shall a frequency deviation test be carried out.

A test set-up similar to that shown in figure 17 may be used.

The low frequency from the teleprotection transmitter is translated to a higher frequency by the frequency f_s. Only one sideband is transmitted through the band-pass filter placed after the modulator. At the receive side, the frequency f_r will demodulate the high frequency back to low frequency in the demodulator. A low-pass filter connected to the output of the demodulator will only allow low frequencies to arrive at the teleprotection receiver.

Le générateur de fréquence f_r doit être conçu de manière à produire une variation de fréquence en fonction d'une tension de commande continue variable (oscillateur commandé en tension).

On effectue les mesures suivantes avec le montage de la figure 17, dans les conditions suivantes:

a) on doit faire varier la fréquence f_r en utilisant une tension de commande en dents de scie, de forme semblable à celle qui est représentée à la figure 18;

b) la variation de fréquence f_r va de 0 à $\pm B$ (B étant l'écart de fréquence convenu entre l'utilisateur et le constructeur). On surveille, sur le récepteur de téléprotection, le manque de signal de garde, la réception de commandes intempestives et le fonctionnement de l'alarme.

4.3.2 Systèmes de téléprotection numérique

Le bruit sur une voie de téléprotection numérique tend à dégrader l'information transmise en provoquant des erreurs sur les bits.

Ces erreurs peuvent retarder la réception d'une commande ou peuvent provoquer une commande intempestive. Généralement, en conséquence, le taux d'erreurs binaire (BER) va affecter la sécurité et la fiabilité du système. Le but principal des essais de performance est donc d'examiner la sécurité et la fiabilité du système en rapport avec le taux d'erreur binaire (BER).

Tant pour la sécurité que pour la fiabilité, il est préférable d'utiliser des erreurs binaires aléatoires.

Les raisons suivantes justifient cette approche:

a) l'utilisation d'une variable aléatoire pour le BER est en conformité avec la méthodologie principalement utilisée pour l'analyse mathématique des protocoles qui s'appuie généralement sur des techniques probabilistes utilisant des variables d'erreurs aléatoires;

b) il est souvent difficile d'introduire des erreurs non aléatoires sur les bits, dans une voie numérique de transmission.

Les propriétés statistiques de la voie de communication numérique perturbée doivent correspondre à celles du modèle de voie binaire symétrique (BSC, voir annexe B), c'est-à-dire à l'équivalent numérique d'une voie de communication analogique perturbée par la superposition d'un bruit blanc gaussien. Des erreurs de bits ayant cette propriété peuvent être introduites en injectant directement des erreurs binaires, pourvu que ces erreurs puissent être introduites de façon aléatoire et que les propriétés de la voie binaire symétrique s'appliquent. Les erreurs sur les bits peuvent également être appliquées en injectant du bruit blanc à l'entrée de la terminaison de ligne du système de télécommunication utilisé.

4.3.2.1 Sécurité

Dans les systèmes numériques, il peut apparaître à la fois des perturbations continues et par impulsions. L'effet sur la sécurité et la fiabilité du système lors de l'application de ces types de perturbations dépend du protocole utilisé et du mode de fonctionnement du matériel, par exemple y a-t-il un quelconque mécanisme utilisé dans le matériel de téléprotection qui inhibe la sortie «déclenchement» pour des débits d'erreurs binaires élevés. En conséquence, il est recommandé que les essais de sécurité soient effectués en appliquant des perturbations en salves, l'intervalle entre salves successives étant modifié en fonction de la conception du matériel de téléprotection.

On doit utiliser des erreurs de bits aléatoires.

Frequency generator f_r shall be designed in such a way that a variable control voltage will cause a change in frequency (voltage-controlled oscillator (VCO)).

When using the test set-up shown in figure 17, the following conditions apply:

a) the frequency f_r shall be changed by applying a sawtooth control voltage similar in form to that shown in figure 18;

b) the frequency f_r shall be varied from 0 to ± B (B being the frequency deviation agreed upon between the user and the manufacturer). The teleprotection receiver shall be monitored for loss of guard, receipt of unwanted commands and alarm performance.

4.3.2 Digital teleprotection systems

Noise on a digital teleprotection channel tends to corrupt the information being transferred by causing bit errors.

The bit errors may delay reception of a command, or may cause an unwanted command. Generally, therefore, the BER will alter the levels of security and dependability of the system. The main aim of the performance tests, therefore, is to examine the security and dependability characteristics of the system in relation to the BER.

For security and dependability tests, it is preferable to use random bit errors.

This approach is chosen for the following reasons:

a) the use of a random variable for the BER aligns with the main methodology used for mathematical analysis of the protocol, which generally relies on probabilistic techniques utilising random error variables;

b) it is often difficult to introduce non random bit errors into the digital transmission path.

The statistical properties of the disturbed digital communication channel shall correspond to those of the binary symmetric channel model (BSC), (see annex B), i.e. the digital equivalent of an analogue communication channel disturbed by additive white Gaussian noise. Bit errors with these properties may be introduced by injecting direct bit errors, provided the bit errors can be introduced randomly and the BSC properties apply. Bit errors may also be applied by injecting white noise into the input of the line terminal of the telecommunication system used.

4.3.2.1 Security

In digital systems both continuous and impulsive disturbances can occur. The effect on the security and dependability of the system during the application of these types of disturbances will depend on the protocol utilized and the mode of operation of the equipment, e.g. whether there is any mechanism employed within the teleprotection equipment which inhibits the "trip" output at high BERs. It is therefore recommended that security tests should be carried out with the application of burst disturbances, the interval between successive bursts varying according to the design of the teleprotection equipment.

Random bit errors shall be used.

En plus de l'application des perturbations ci-dessus, un essai au cours duquel la voie de communication est brusquement coupée doit être effectué. Ce dernier essai est considéré comme nécessaire afin d'évaluer le comportement transitoire du système de téléprotection.

4.3.2.1.1 Essai de sécurité avec des perturbations en salves

Ces essais sont effectués en appliquant des salves d'erreurs de bits aléatoires à des vitesses définies. Le montage d'essai est présenté à la figure 13.

Fréquemment, le matériel de téléprotection numérique utilise des protocoles complexes pour lesquels la probabilité d'une commande intempestive est très faible, et, en conséquence, difficile à mesurer lors d'essai sur une période d'essai insuffisamment longue. Il est donc recommandé que l'essai soit effectué pour vérifier qu'une certaine probabilité maximale de commande intempestive P_{uc} ne soit pas dépassée.

Les performances complètes, couvrant une large gamme de valeurs du BER, doivent être fournies. Selon accord entre fabricant et utilisateur, une analyse de sécurité du protocole peut être conduite afin de révéler les performances qui ne seraient pas couvertes par l'essai. Il convient que cette analyse, si elle est conduite, établisse à quelle valeur du BER apparaît la probabilité maximale P_{uc}. Un exemple d'analyse pour un protocole simple est fourni à l'annexe C. L'analyse dans le cas d'essais en salves est plus complexe et elle n'est pas incluse dans l'annexe C.

Les salves d'erreurs aléatoires sur les bits, à des vitesses définies, sont couplées à la voie de communication à des périodes définies. Il convient que la durée de la salve soit de 200 ms. L'intervalle entre les salves doit être suffisamment long pour assurer le déverrouillage du récepteur entre des salves successives. Lorsque la conception du système de téléprotection ne comprend pas de mécanisme de blocage, les intervalles entre salves peuvent être inexistants (c'est-à-dire: bruit continu). Cela réduira la durée de l'essai.

La probabilité d'une commande intempestive est approximée de la façon suivante:

$$P_{uc} \approx \frac{N_{uc}}{N_B}$$

où

N_{uc} est le nombre enregistré de commandes intempestives;

N_B est le nombre de salves d'erreurs sur les bits.

La sécurité est alors de $1 - P_{uc}$.

Il convient que les mesures ou calculs de P_{uc} soient représentés en fonction du BER, tel que cela apparaît à la figure 23. La gamme de BER utilisée s'étendra au moins de 0,5 jusqu'à 10^{-4}.

4.3.2.1.2 Essai de sécurité avec des coupures soudaines du signal

Il convient d'effectuer un essai supplémentaire en coupant brusquement la voie de téléprotection. Il convient de répéter ce dernier essai un certain nombre de fois et d'en noter les conséquences observées sur le matériel de téléprotection. Il convient que ces coupures soient effectuées alors que le matériel en essai fonctionne dans des conditions de référence (sans erreurs).

In addition to applying the above disturbances, a test in which the communication channel is suddenly interrupted shall be carried out. This latter test is deemed necessary in order to assess the transient behaviour of the teleprotection system.

4.3.2.1.1 Security test with burst disturbances

These tests are carried out with the application of bursts of random bit errors at defined rates. The test set-up is shown in figure 13.

Often, digital teleprotection equipment uses complex protocols where the probabilities of an unwanted command are very low, and consequently difficult to measure by test without a very long testing period. It is therefore recommended that testing is carried out to verify that a certain maximum probability of an unwanted command P_{uc} is not exceeded.

A full characteristic over a wide range of BERs shall be provided. When agreed between the manufacturer and the user a security analysis of the protocol may be carried out in order to reveal the characteristic not covered by testing. The analysis, if carried out, should establish the BER at which the maximum P_{uc} occurs. An example of an analysis for a simple protocol is contained in annex C. The analysis for burst tests is more complex and is not included in annex C.

Bursts of random bit errors at defined rates are coupled into the channel with defined periods. The duration of the error burst should be 200 ms. The interval between the bursts shall be sufficiently long to ensure deblocking of the receiver between subsequent bursts. Where the teleprotection design does not include a blocking mechanism, the intervals between the bursts may be reduced to zero (i.e. continuous bit errors). This will shorten the test period.

The probability of an unwanted command is approximated as follows:

$$P_{uc} \approx \frac{N_{uc}}{N_B}$$

where

N_{uc} is the number of unwanted commands recorded;

N_B is the number of error bursts.

The security is then given by $1 - P_{uc}$.

Measurements or calculation of P_{uc} should be recorded as a function of the BER similar to that shown in figure 23. The range of BERs used shall at least cover the range 0,5 to 10^{-4}.

4.3.2.1.2 Security test with sudden signal interruption

An additional test should be carried out where the teleprotection channel is suddenly interrupted. This should be repeated a number of times and the effect on the teleprotection equipment observed and noted. The interruptions should be made when the system under test is operating normally under reference (error-free) conditions.

4.3.2.2 Fiabilité

Les erreurs sur les bits peuvent perturber un système de téléprotection en retardant l'arrivée d'une commande à l'extrémité réceptrice. La raison en est que les messages pour lesquels une erreur a été détectée sont refusés. Il peut aussi apparaître une perte de l'information de synchronisation.

La fiabilité en fonction du BER doit être mesurée en comparant le nombre de commandes reçues en un temps réel de transmission acceptable au nombre de commandes émises.

Les commandes sont émises par une voie soumise à des impulsions d'erreurs aléatoires sur les bits, à des vitesses prédéterminées. Le bruit doit être initié 10 ms avant la commande et doit se terminer en même temps que la commande. Pour chaque taux d'erreur, un nombre fixé de commandes est envoyé et l'on compte le nombre de commandes reçues en un temps donné. La probabilité de commande défaillante P_{mc}, pour un temps de transmission réel fixé, est donnée par:

$$P_{mc} \approx \frac{N_T - N_R}{N_T}$$

où

N_T est le nombre de commandes émises;

N_R est le nombre de commandes reçues.

La fiabilité est donnée par $1 - P_{mc}$.

Du bruit blanc continu ou des erreurs aléatoires sur les bits continus peuvent être utilisées pour l'essai lorsque le verrouillage du système de téléprotection n'est pas utilisé ou est inhibé.

Le montage d'essai recommandé est présenté à la figure 11.

Pour obtenir une famille de courbes, il est nécessaire d'envoyer un nombre de commandes suffisant permettant un résultat statistique significatif. L'intervalle entre commandes successives doit être suffisant pour permettre un temps de rétablissement suffisant du récepteur.

Pour chaque réglage de la voie, les courbes présentant la fiabilité en fonction du BER doivent être tracées. Le fabricant doit fournir ces courbes.

Il convient que ces courbes soient fournies dans la gamme de T_0 à $3 \times T_0$.

4.3.2.3 Gigue

4.3.2.3.1 Gigue à la sortie de l'émetteur

La gigue à la sortie de l'émetteur doit être mesurée conformément au montage présenté à la figure 24. Cet essai doit être effectué dans un état de garde permanent, dans un état de commande permanent et pendant un essai de fiabilité (transitions répétitives de l'état de garde à l'état de commande). L'essai doit vérifier, pour chacun des états décrits ci-dessus, que la gigue obtenue ne dépasse pas les limites spécifiées en 3.3.3.1.

4.3.2.2 Dependability

Bit errors may disturb a teleprotection system by delaying the arrival of a command at the receiving end. This occurs because messages received with detected errors are rejected. A loss of message synchronisation may also occur.

Dependability versus BER shall be measured by comparing the number of commands delivered from the receiver within an acceptable actual transmission time with the number of commands sent from the transmitter.

Commands are transmitted through a channel subjected to pulsed random bit errors at pre-determined rates. The burst of bit errors shall be initiated 10 ms before the command and shall terminate at the same time as the command. For each error rate, a fixed number of commands is sent, and the number of commands received within a given time is counted. The probability of a missing command P_{mc} for a fixed actual transmission time, is given below.

$$P_{mc} \approx \frac{N_T - N_R}{N_T}$$

where

N_T is the number of commands sent;

N_R is the number of commands received.

The dependability is then given by $1 - P_{mc}$.

Continuous white noise, or continuous random bit errors, may be used for the test when the blocking mechanism of the teleprotection receiver is not employed or is disabled.

The recommended test set-up is shown in figure 11.

To obtain a family of curves, it is necessary to send a sufficient number of commands to give a statistically significant measurement. The interval between successive commands shall be sufficient to allow the receiver enough time to recover.

For each setting of the channel, curves showing dependability versus BER shall be plotted. The manufacturer shall provide these curves.

The curves should be given within the range T_0 to $3 \times T_0$.

4.3.2.3 Jitter

4.3.2.3.1 Transmitter output jitter

The jitter at the transmitter output shall be measured in accordance with the test set-up shown in figure 24. The test shall be carried out in a permanent guard state, a permanent command state and during a dependability test (repetitive transitions from guard to command). The testing shall verify for each of the above states that the jitter produced does not exceed the limits specified in 3.3.3.1.

4.3.2.3.2 Gigue à l'entrée du récepteur

L'effet de l'introduction d'une gigue sur le matériel de téléprotection, avec l'amplitude et à la fréquence spécifiées en 3.3.3.2, doit être mesuré de la façon suivante:

Lorsque le matériel donne accès aux statistiques sur le message d'erreur, ou annonce un «message erroné» par une alarme, il convient d'introduire la gigue en surveillant l'une ou l'autre des indications ci-dessus. Il convient qu'un contrôle soit effectué dans les limites de l'enveloppe spécifiée de la gigue (voir figure 25) et que l'effet soit enregistré. Si la gigue a pour conséquence la réception de messages erronés, il convient de mesurer la fiabilité et la sécurité et d'évaluer la dégradation de ces performances. Il convient de conduire l'essai de fiabilité pour T_0, sans apporter aucune autre contrainte. Il convient que cet essai soit effectué au point de l'enveloppe de la gigue pour lequel le message d'erreur est émis le plus souvent. Si ce point ne peut pas être déterminé, alors il convient d'effectuer l'essai à la limite de performance aux fréquences f0, f1, f2, f3 et f4, dans la limite d'amplitude de la gigue. Le nombre de commandes envoyées sur chaque point doit être convenu entre le fabricant et l'utilisateur. Si, toutefois, la gigue affecte la fiabilité et/ou le temps de transmission, il convient qu'un essai de sécurité soit effectué au point de la caractéristique où l'effet est le plus grave, ou bien au point où le débit de message d'erreur est le plus élevé. La durée de l'essai de sécurité doit être convenue entre le fabricant et l'utilisateur.

Lorsque le matériel ne donne pas accès aux statistiques sur le message d'erreur, il convient qu'un essai de fiabilité soit effectué aux fréquences f0, f1, f2, f3 et f4, dans la limite d'amplitude de la gigue, comme ci-dessus. Si la fiabilité et le temps de transmission ne sont pas affectés substantiellement par la gigue, alors il convient de ne pas effectuer d'essai de sécurité. Si, toutefois, la gigue affecte la fiabilité et/ou le temps de transmission, il convient qu'un essai de sécurité soit effectué au point de la caractéristique où l'effet est le plus grave.

4.3.2.4 Temps de rétablissement

Le temps mis par le matériel pour se rétablir d'une salve d'erreurs de courte durée, à vitesse élevée, peut avoir un effet sur son aptitude à transmettre une information de commande permanente dans une courte période de temps. Ce temps de rétablissement peut être affecté par le temps de remise à zéro d'un mécanisme quelconque utilisé pour inhiber le déclenchement ou par les techniques de synchronisation de message qui font partie de la conception du matériel.

Un montage d'essai pour la mesure du temps de rétablissement est présenté à la figure 19.

Une commande permanente est initiée de façon synchrone à une salve d'erreurs de courte durée (20 ms), dans la voie de communication. La salve d'erreurs est ajustée à un BER de 0,5. Le temps réel de transmission de la commande est mesuré. Cet essai est répété un certain nombre de fois pour déterminer l'étendue des retards induits.

La différence entre le temps de transmission nominal (sans bruit), T_0, et le temps de transmission réel mesuré lors des essais, tenant compte de la durée des salves d'erreurs, donne une indication sur le temps de rétablissement.

4.3.2.5 Matériel multiplexé

Certains matériels de téléprotection utilisent des techniques de multiplexage temporel en tant que partie intégrante du matériel lui-même. Un tel matériel peut aussi mettre en oeuvre des fonctions de téléprotection séparées qui partagent le même cheminement multiplexé. Un essai de vérification de l'alignement correct de la voie (fenêtre temporelle) dans des conditions d'erreur transitoires est donc nécessaire pour s'assurer qu'il n'y a pas un mauvais aiguillage des commandes qui pourrait affecter d'autres fonctions de téléprotection à l'intérieur du même matériel.

4.3.2.3.2 Receiver input jitter

The effect on the teleprotection equipment caused by introducing jitter, with the amplitude and frequency specified in 3.3.3.2 shall be measured as outlined below.

Where the equipment provides access to message error statistics or annunciates a "wrong message" alarm, then the jitter should be introduced whilst monitoring either of the above indications. A check should be carried out over the boundary of the specified jitter envelope (see figure 25) and the effects noted. If the jitter results in wrong messages being received, dependability and security should be measured and their degradation evaluated. The dependability test should be carried out for T_0, with no other impairment introduced. This test should be carried out at the point on the jitter envelope where the message error rate is greatest. If this point cannot be determined, then the test should be performed at the amplitude boundary of the characteristic at frequencies f0, f1, f2, f3 and f4. The number of commands sent at each point shall be agreed between manufacturer and user. The security test should be carried out at the point on the jitter envelope where the dependability/transmission time is most affected or where the message error rate is greatest. The duration of the security test shall be agreed between manufacturer and user.

Where the equipment does not incorporate any error statistics or "wrong message" indication, a dependability test should be performed at f0, f1, f2, f3 and f4 on the amplitude boundary as above. If dependability and transmission time are not substantially affected by jitter, then no security test should be made. If, however, jitter affects dependability and/or transmission time, a security test should be carried out at the point on the characteristic where the effect is worst.

4.3.2.4 Recovery time

The time required by the equipment to recover from a short duration burst of errors at a high rate may have an effect on its ability to successfully convey persistent command information within a short period of time. This recovery time can be affected by the reset time of any trip-inhibiting mechanisms utilised or by the message synchronisation techniques incorporated in its design.

A test set-up for recovery time measurement is shown in figure 19.

A persistent command is initiated synchronously with a short duration (20 ms) burst of errors into the channel. The error burst is preset to a BER of 0,5. The actual command transmission time is measured. The test is repeated a number of times to determine the spread of delays incurred.

The difference between the nominal (noise-free) transmission time T_0 and the actual transmission time measured in the tests, allowing for the duration of the error burst, gives an indication of the recovery time.

4.3.2.5 Multiplexed equipment

Some teleprotection equipment utilises time division multiplexing techniques as an integral part of the equipment itself. Such an equipment might also employ separate teleprotection functions which share the same multiplexed data path. A test which checks for correct channel (time slot) alignment under transient error conditions is therefore necessary to ensure there is no misdirection of commands which may affect other teleprotection functions within the same equipment.

Il est donc recommandé, pour les matériels de ce type, que l'essai de temps de rétablissement décrit plus haut soit effectué avec des compteurs supplémentaires sur les sorties de commandes des fonctions de téléprotection qui sont implantées sur des voies adjacentes à celle qui est en essai. Ces compteurs indiqueront alors si l'une des commandes a été mal aiguillée vers une destination erronée pendant les transitoires d'erreur. Ces transitoires peuvent affecter le processus de synchronisation de la voie au sein de la partie multiplexage du matériel de téléprotection. Aucun aiguillage de commande erroné n'est admis.

Il convient de noter, pour ce type de matériel, que les salves d'erreurs doivent être appliquées à la voie de multiplexage qui a le débit binaire le plus élevé (ce qui peut inclure un certain nombre de voies de téléprotection), et non à la voie individuelle uniquement.

4.3.3 Temps de transmission

Un montage d'essai pour le temps de transmission de systèmes de téléprotection est donné à la figure 15.

Le temps de transmission doit être mesuré pour des niveaux nominaux de signal à la sortie de l'émetteur et à l'entrée du récepteur. Le temps mesuré est noté T_0.

4.3.4 Matériel multicommande

Un matériel de téléprotection multicommande a normalement un signal ou un message de garde commun et deux, ou plus, signaux ou messages de commande. Cela est presque toujours le cas pour les téléprotections numériques.

L'essai de sécurité des signaux ou messages de commande doit être effectué de la même façon que décrit ci-dessus. Chaque signal ou message de commande doit être essayé en surveillant au cours de l'essai toutes les sorties de commande simultanément.

Il convient que l'essai de la fiabilité soit effectué comme indiqué ci-dessus pour chacun des signaux ou messages de commande. Lors de l'essai de la fiabilité d'un signal de commande, il convient que l'absence de commande intempestive sur chacun des autres signaux de commande soit essayée simultanément. En raison du temps nécessaire, il convient de considérer l'essai de chaque signal ou message de commande de cette façon seulement si une analyse du protocole utilisé semble le justifier. L'essai ne doit être effectué qu'avec l'accord du fabricant.

4.3.5 Vérification des fonctions d'alarme

Lorsque le matériel de téléprotection n'est pas en mesure de fonctionner correctement, il convient qu'une alarme soit émise à l'extérieur (voir A.3).

Il faut vérifier le matériel pour savoir si l'alarme fonctionne correctement. Une alarme doit être donnée dans les cas suivants:

a) lorsque le signal ou message de garde est coupé du récepteur et qu'aucun signal ou message de commande n'apparaît sur le récepteur dans un temps spécifié par le fabricant (en général, ce temps est ajustable à l'intérieur d'une gamme définie);

b) lorsqu'un bruit important verrouille le récepteur pour une durée plus longue supérieure à une durée spécifiée par le fabricant;

c) lorsque le fabricant spécifie d'autres situations (par exemple, défaillance de l'émetteur) dans lesquelles une alarme doit être émise. Dans ces cas-là, la fonction d'alarme doit également être essayée.

It is therefore recommended that, for equipment of this type, the recovery time test described above should be performed with additional separate counters on the command outputs of teleprotection functions which are installed on adjacent channels to the one under test. These counters would then indicate whether any commands have been misdirected to the wrong destination during error transients. These transients may affect the channel synchronisation process within the multiplexing part of the teleprotection equipment. No such misdirections are allowed.

It should be noted that, for this type of equipment, the error bursts will be applied to the higher bit rate multiplexed path (which may comprise a number of teleprotection channels), and not to the individual channel itself.

4.3.3 Transmission time

A test set-up for measuring transmission time for teleprotection systems is given in figure 15.

The transmission time shall be measured with nominal signal levels at the transmitter output and the receiver input. The measured time is T_0.

4.3.4 Multi-command equipment

A multi-command teleprotection equipment usually has a common guard signal or message and two or more command signals or messages. This is nearly always the case for digital teleprotection.

Security testing for command signals or messages shall be carried out in the same way as described above. Each command signal or message shall be tested by monitoring all the command outputs simultaneously during the test.

Dependability testing should be carried out as described above for each of the command signals or messages. When testing the dependability of one command signal, the absence of unwanted commands at each of the other command signals should be tested at the same time. Because of the time involved, consideration to the testing of every command signal or message in this manner should only be given where analysis of the utilized protocol appears to justify it. The testing shall only be carried out with the agreement of the manufacturer.

4.3.5 Checking alarm functions

When the teleprotection equipment is unable to operate correctly, an external alarm should be given (see A.3).

The equipment shall be checked to see if the alarm is operating correctly. An alarm shall be given when the following occur:

a) the guard signal or message is cut off from the receiver and no command signal or message appears at the receiver within a specified time given by the manufacturer (usually settable within a defined range);

b) heavy noise blocks the receiver for a time longer than a specified time given by the manufacturer;

c) the manufacturer specifies other situations (e.g. transmitter failure) in which an alarm shall be given. In such situations the function of the alarm shall also be tested.

4.3.6 Essais supplémentaires

Des essais supplémentaires peuvent être convenus entre fabricant et utilisateur.

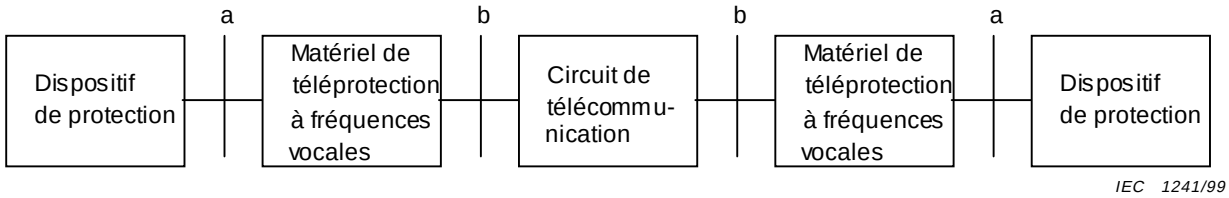


Figure 1 – Configuration de transmission à fréquences vocales

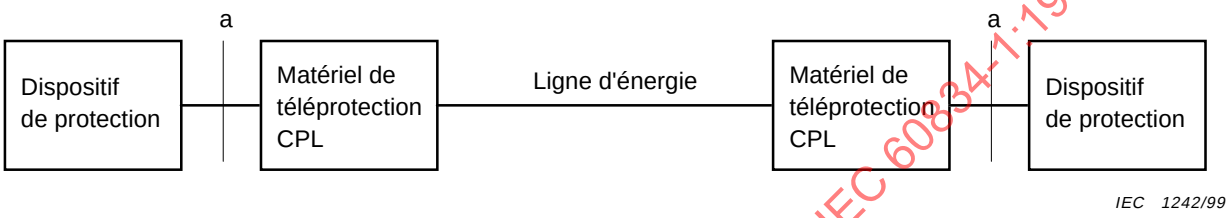


Figure 2 – Configuration de transmission à courants porteurs

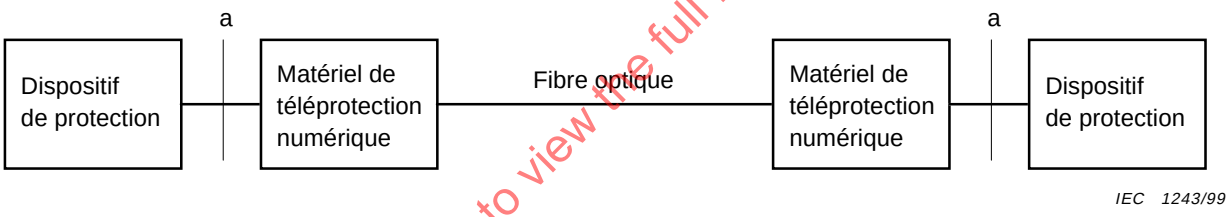


Figure 3 – Téléprotection numérique connectée directement (exemple)

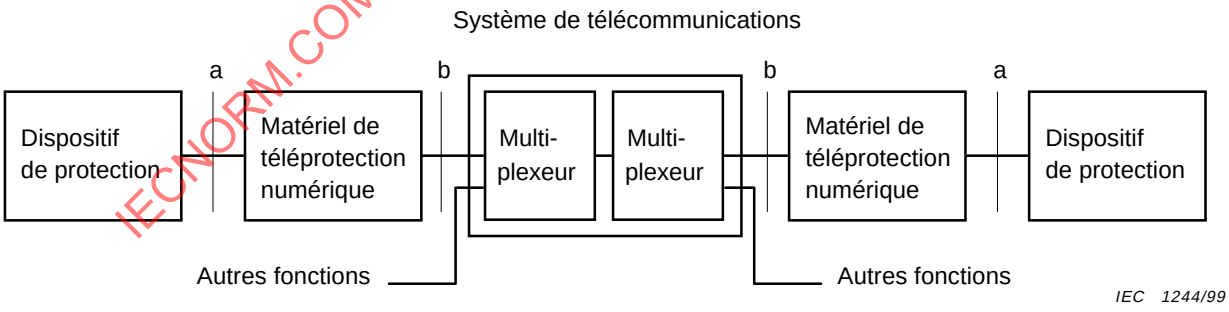


Figure 4 – Téléprotection numérique connectée à travers un système de communication multiplexé

4.3.6 Additional tests

Additional tests may be agreed between the manufacturer and the user.

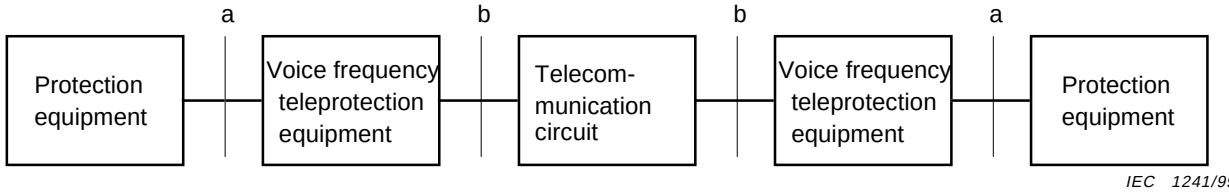


Figure 1 – Voice frequency configuration

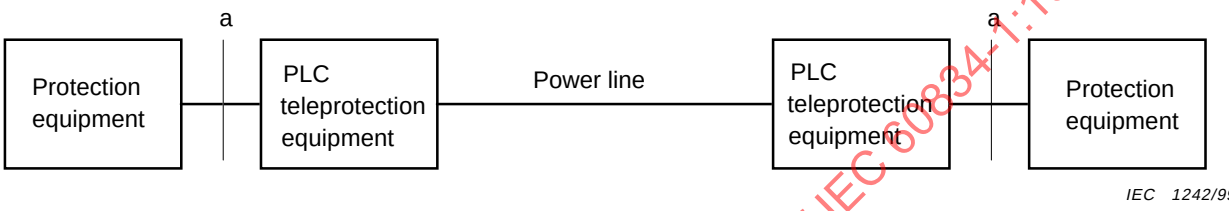


Figure 2 – Power line carrier frequency configuration

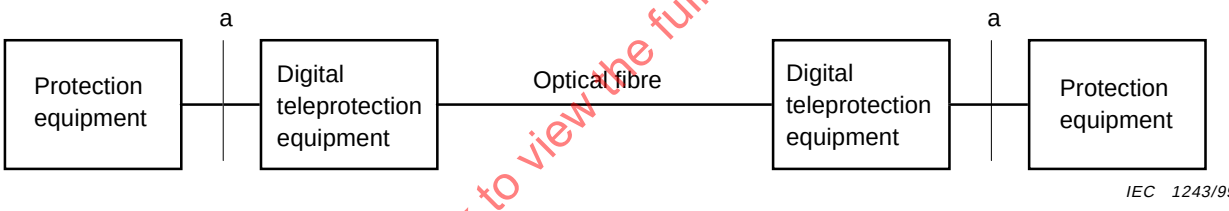


Figure 3 – Directly connected digital teleprotection (example)

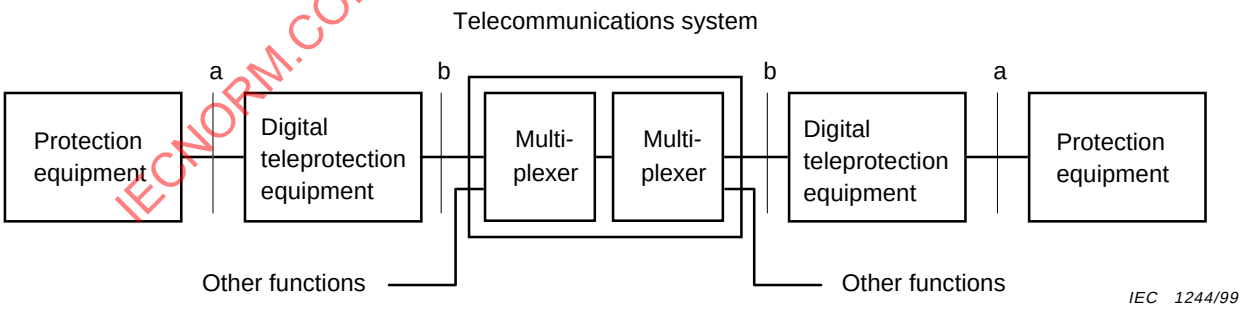


Figure 4 – Digital teleprotection connected via a multiplexed communication system

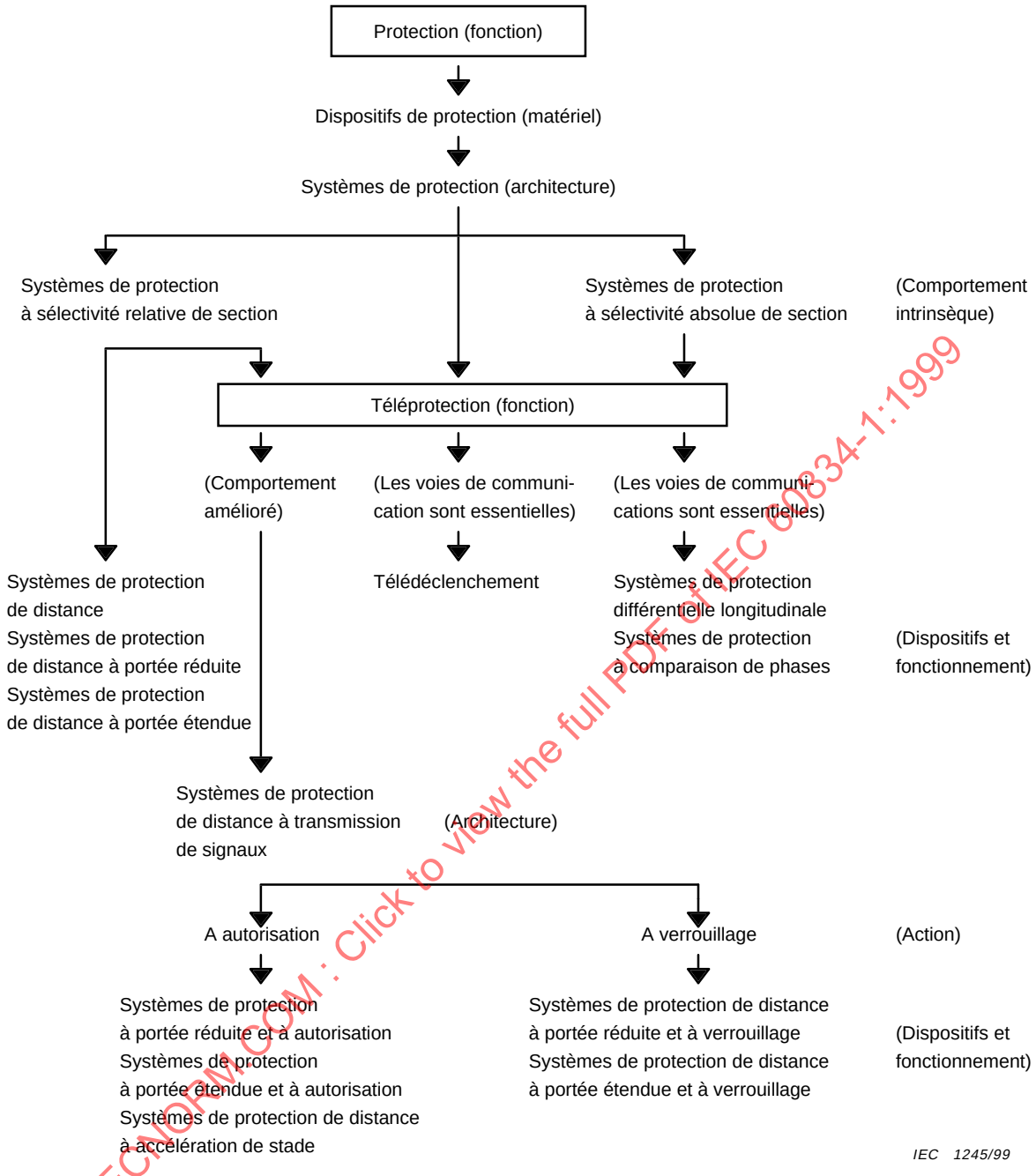


Figure 5 – Termes fondamentaux en protection et en téléprotection

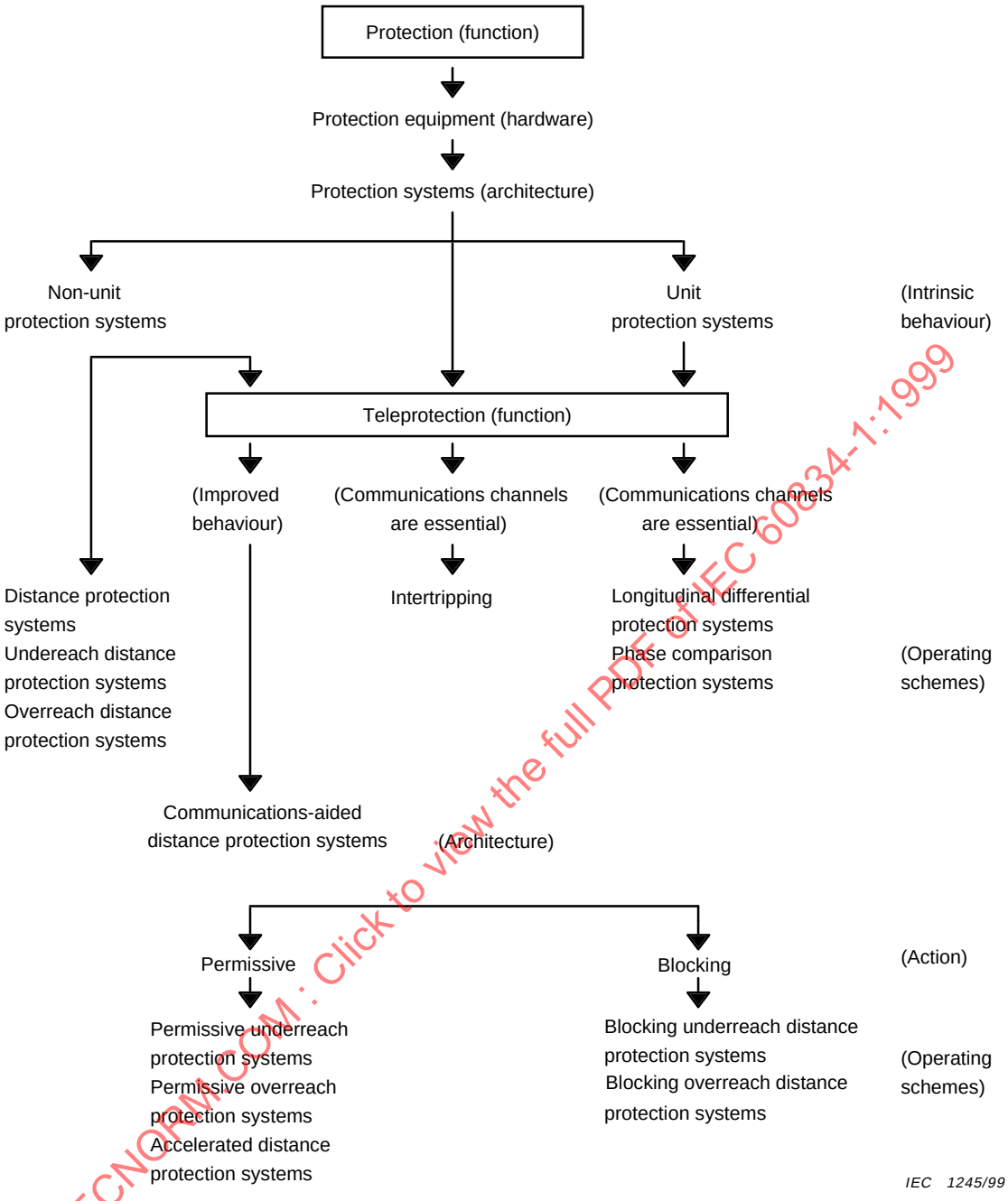
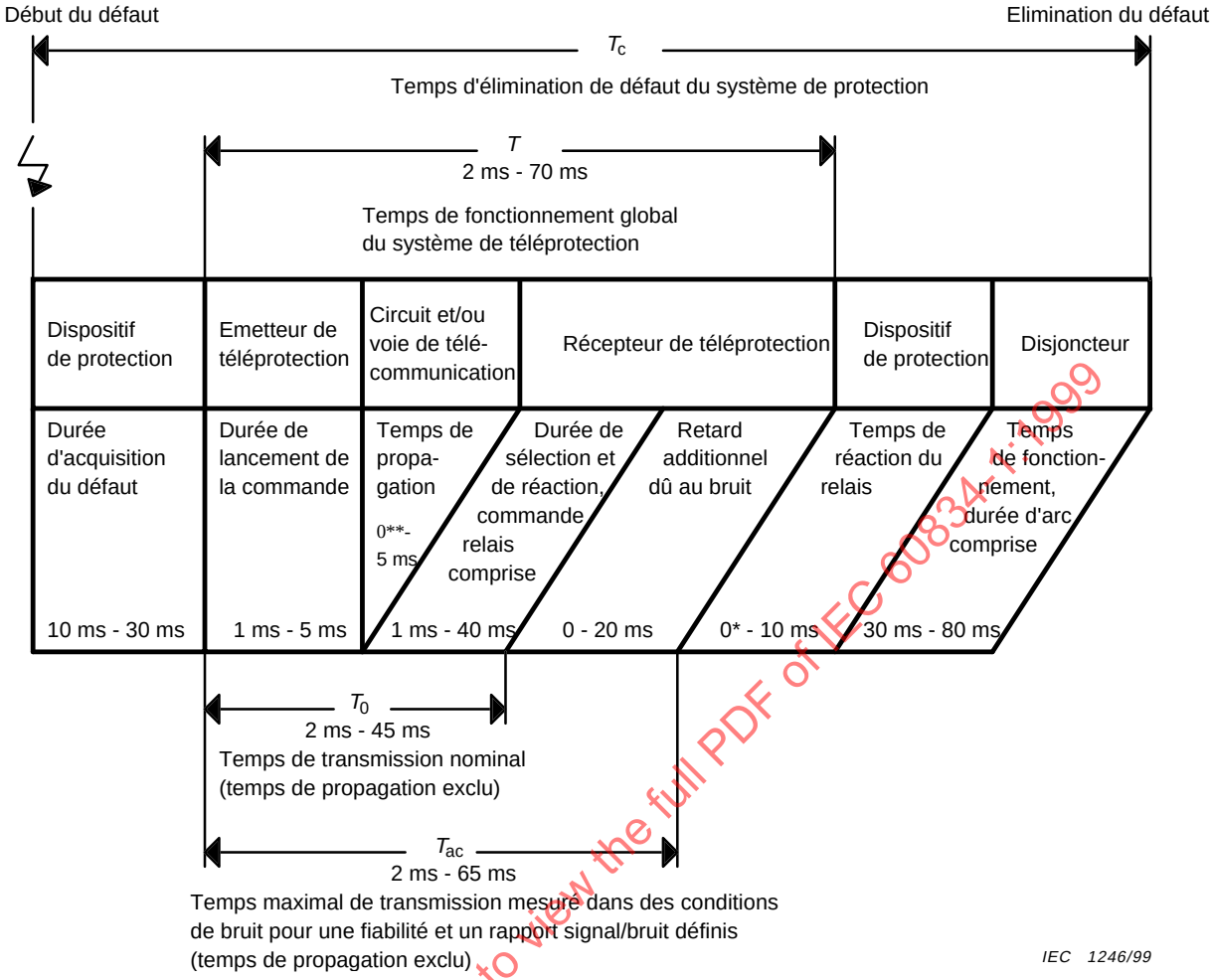


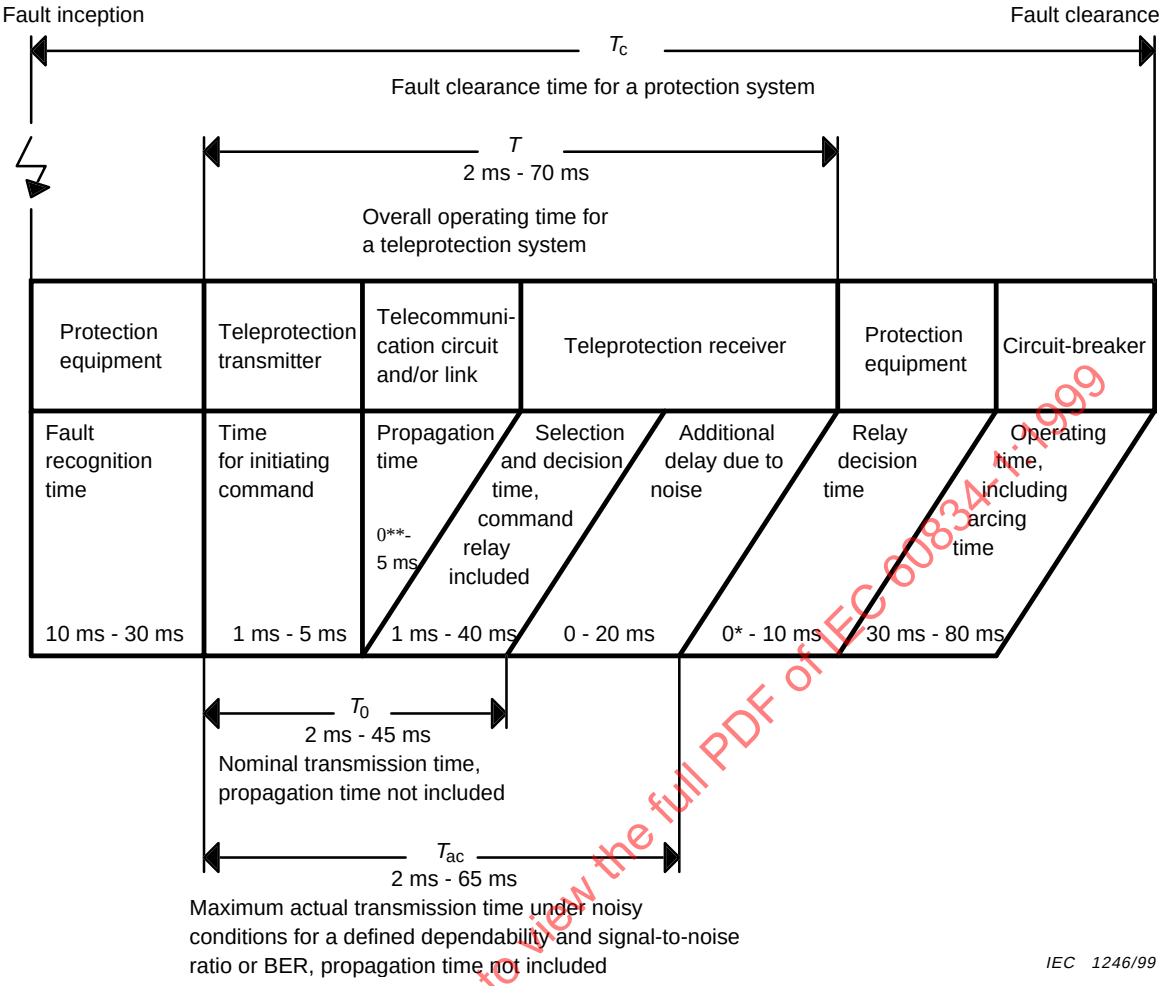
Figure 5 – Fundamental terms on protection and teleprotection



* Peut s'appliquer au télédéclenchement (matériel à déclenchement direct).

** S'applique lorsque le matériel est rebouclé sur lui-même.

Figure 6 – Temps de fonctionnement types des systèmes de protection qui comprennent une téléprotection



* Can apply to intertripping (direct tripping equipment).

** Applies when equipment is back to back.

Figure 6 – Typical operating times for protection systems incorporating teleprotection

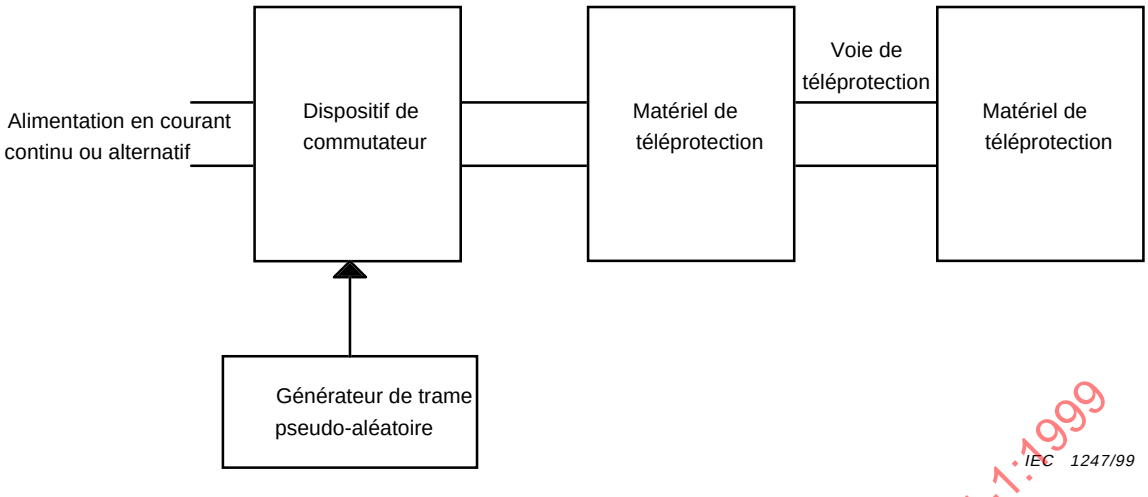


Figure 7 – Circuit pour l'essai des interruptions d'alimentation

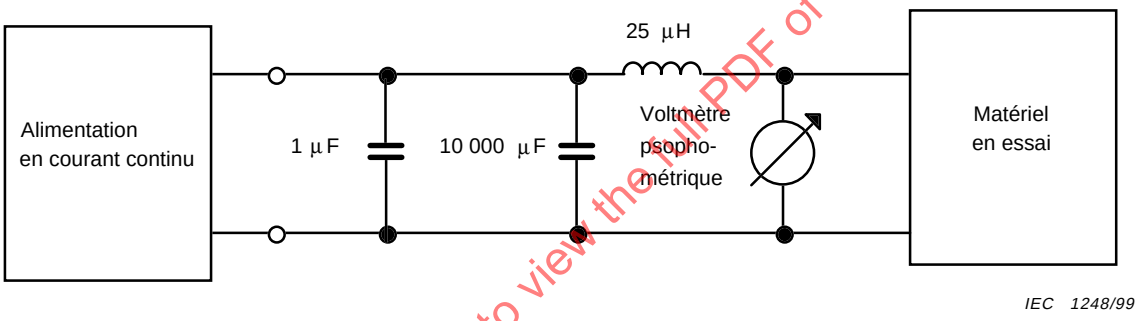


Figure 8 – Circuit d'essai pour la mesure de l'émission de perturbations BF

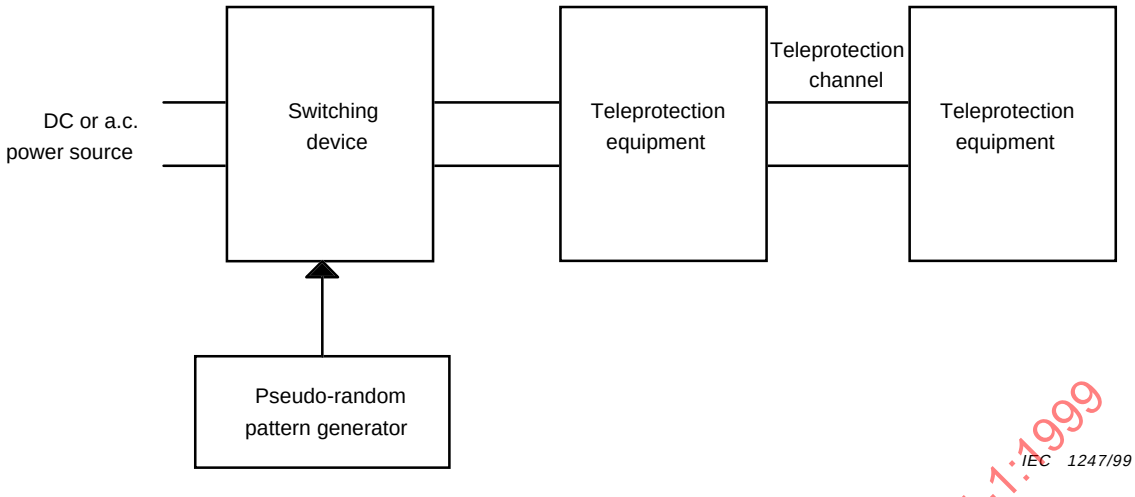


Figure 7 – Test circuit for testing power supply interruptions

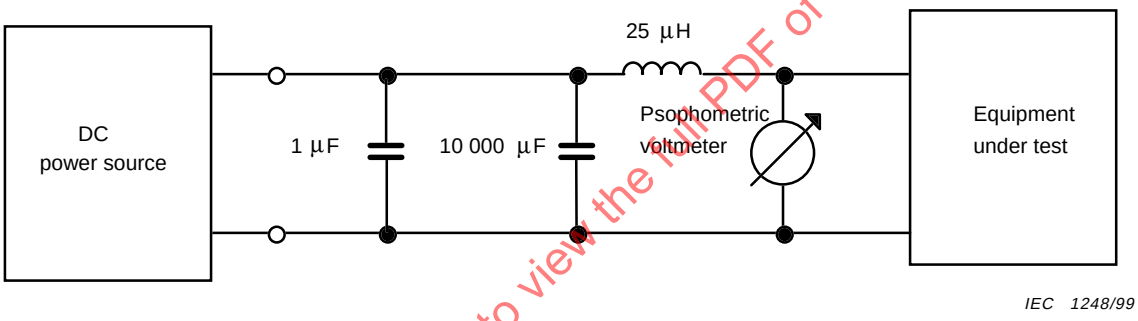


Figure 8 – Test circuit for LF disturbance emission measurement

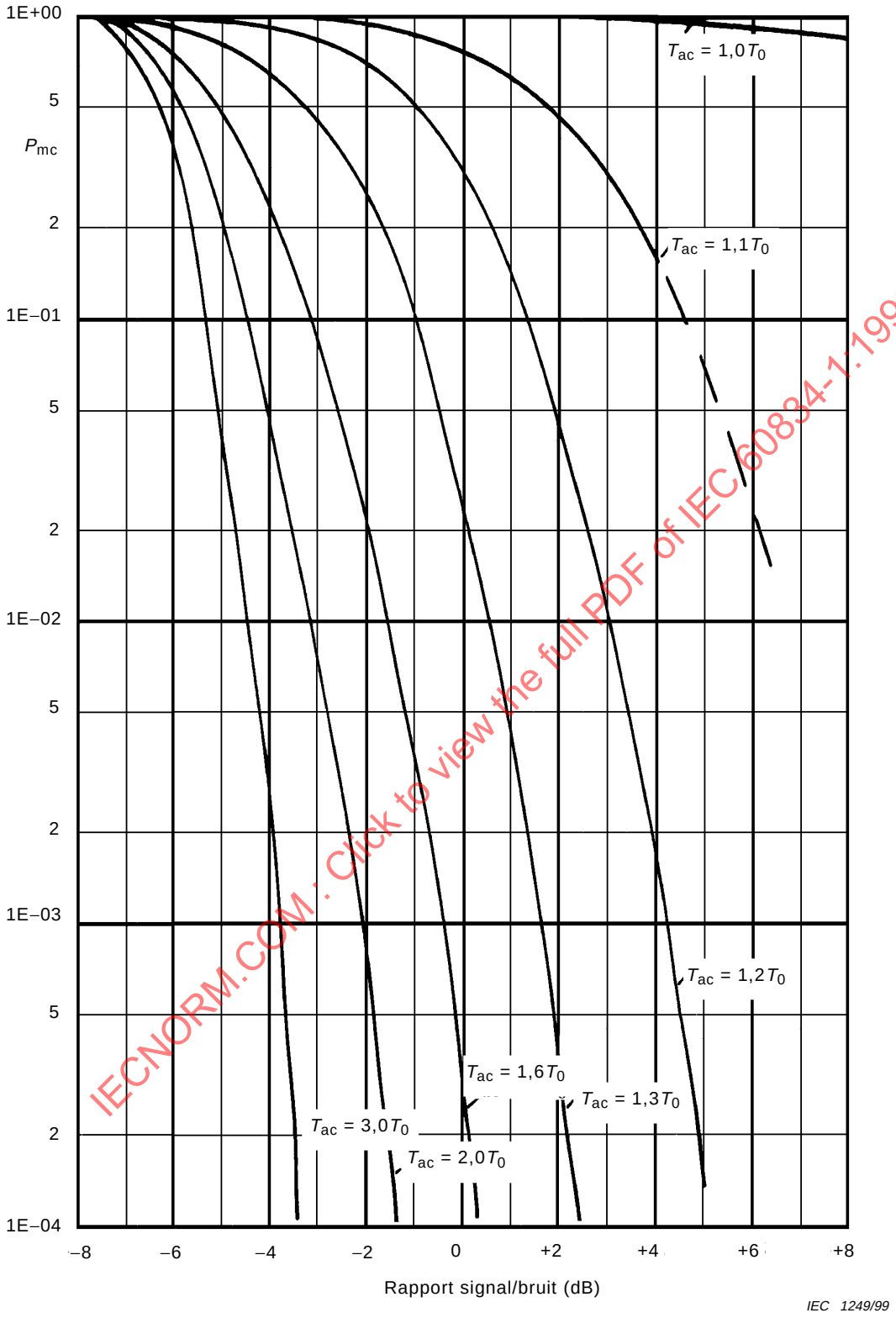


Figure 9 – Exemples de probabilité de commande défaillante en fonction du rapport signal/bruit

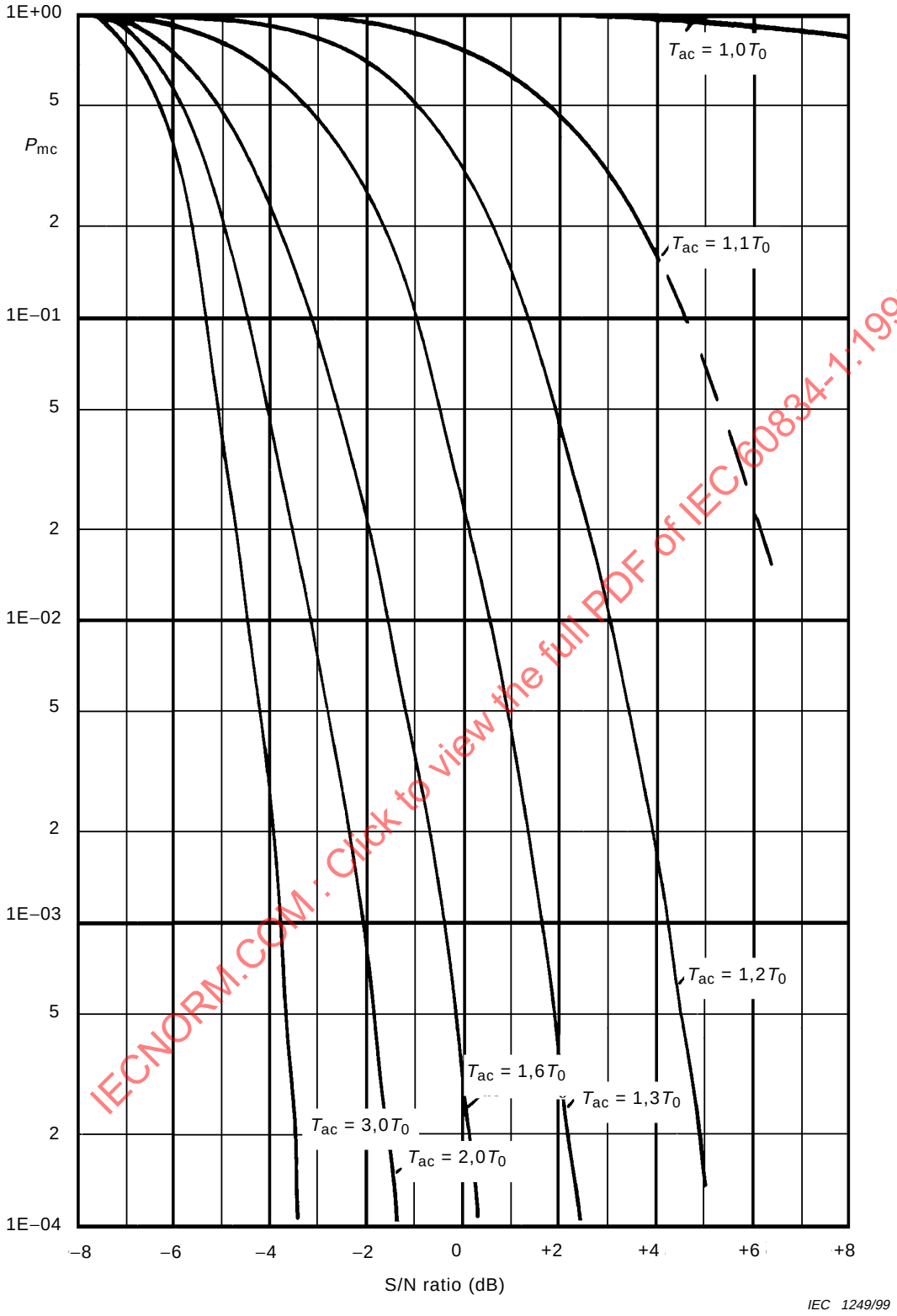


Figure 9 – Examples of the probability of missing command versus signal-to-noise ratio

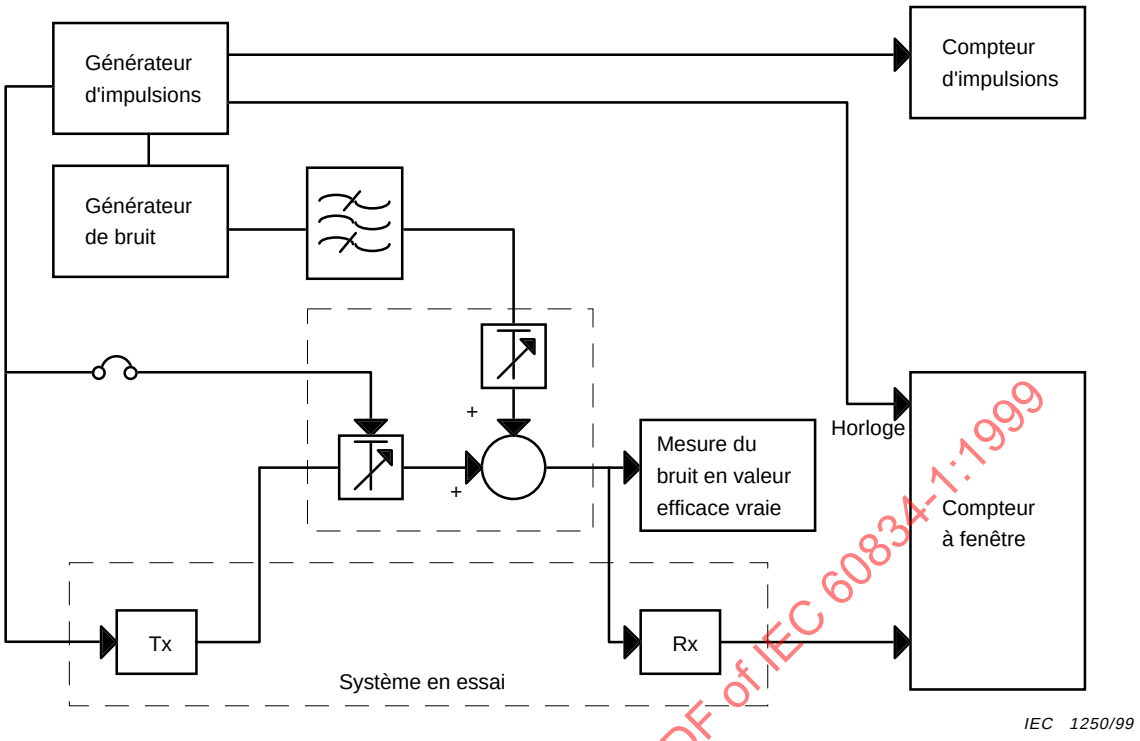


Figure 10 – Montage d'essai pour la mesure de la fiabilité (téléprotection analogique)

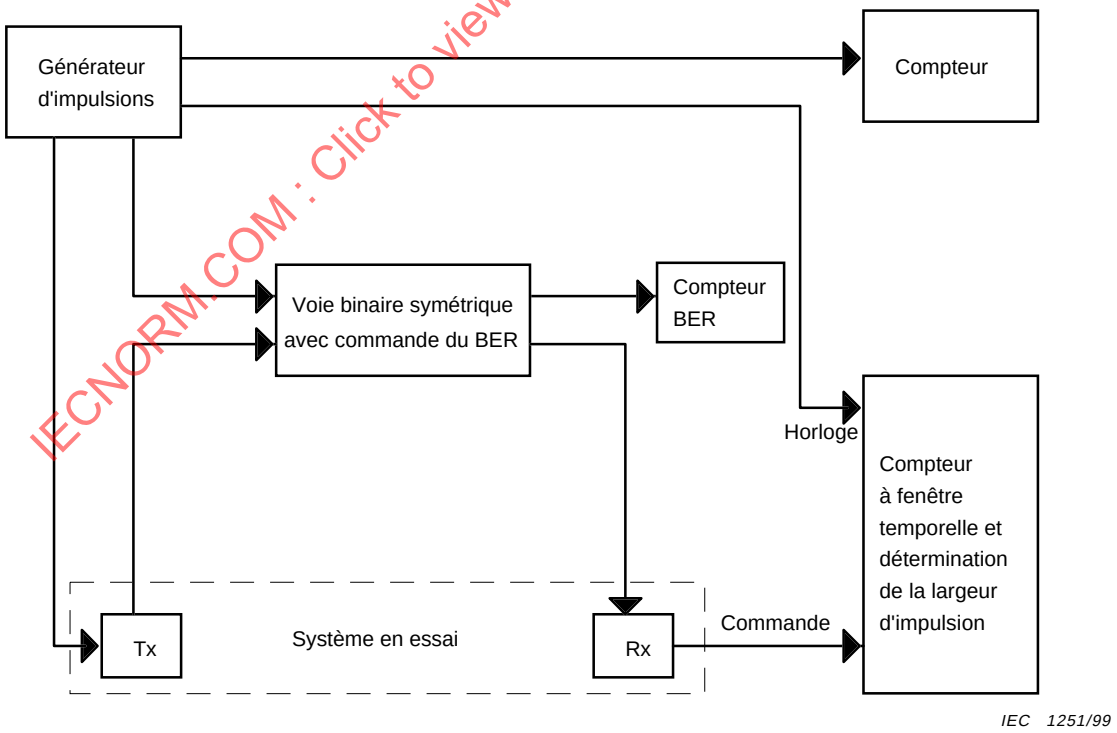


Figure 11 – Montage d'essai pour la mesure de la fiabilité (téléprotection numérique)

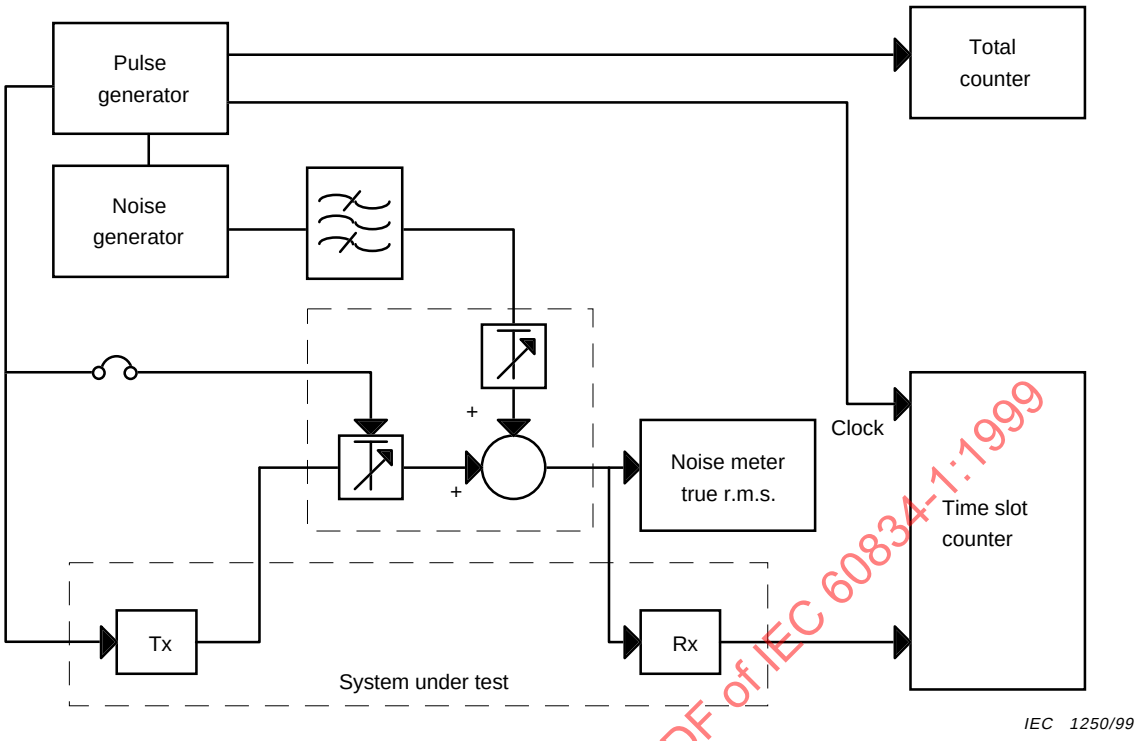


Figure 10 – Test set-up for dependability measurement (analogue teleprotection)

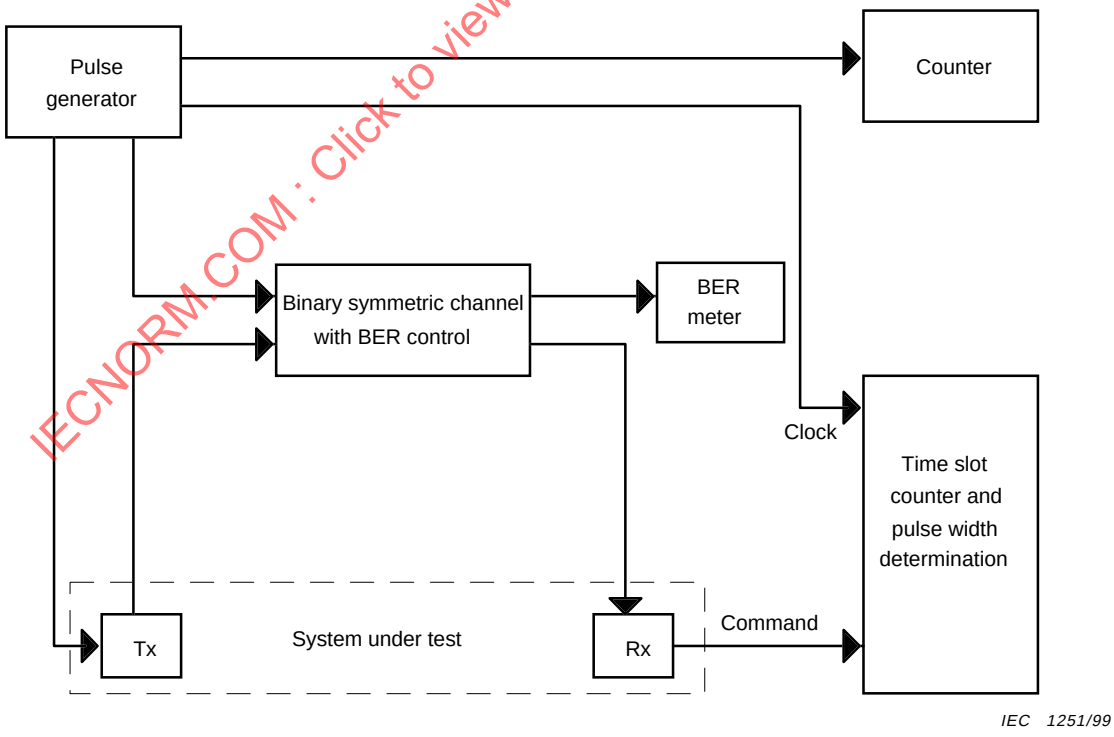


Figure 11 – Test set-up for dependability measurement (digital teleprotection)

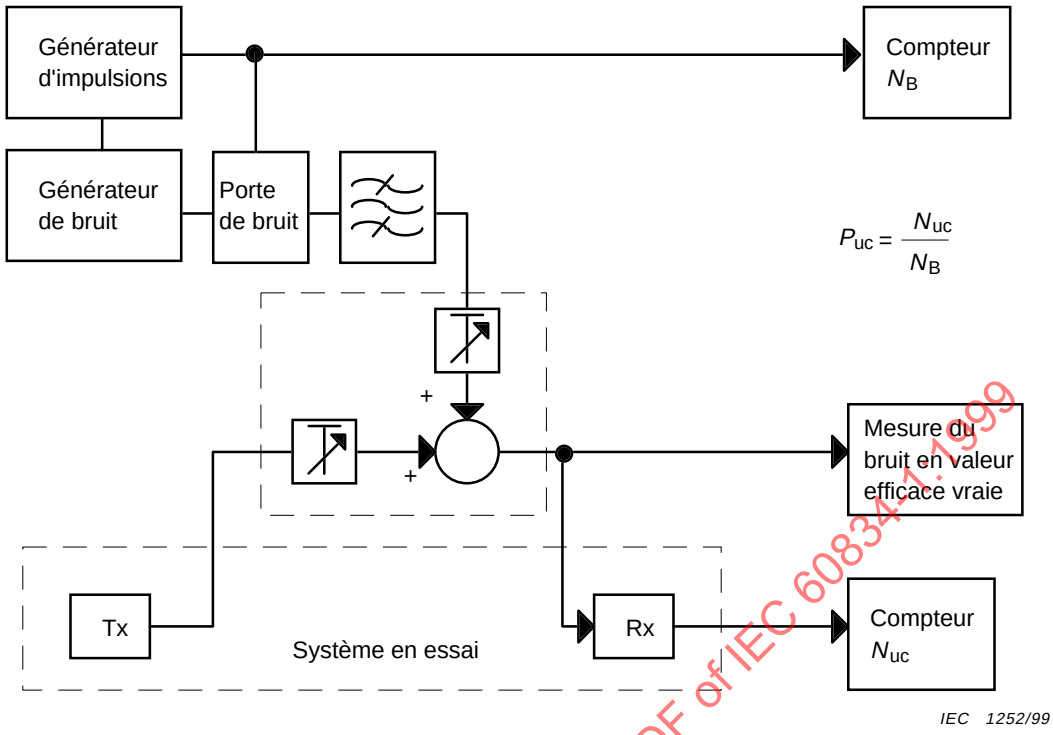


Figure 12 – Montage d'essai pour la mesure de la sécurité (téléprotection analogique)

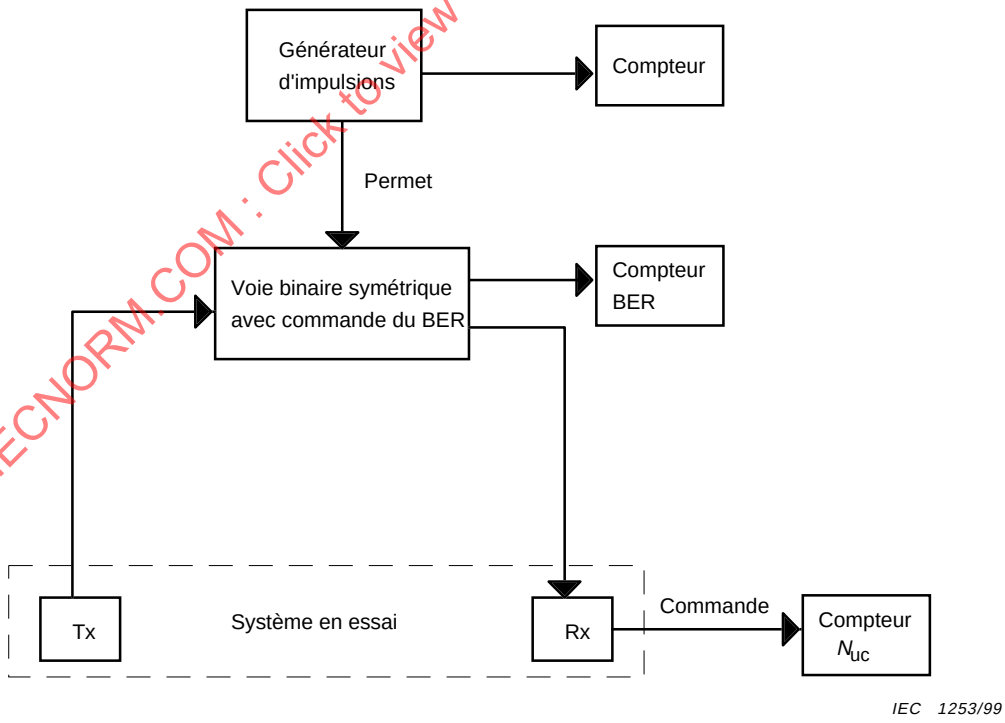


Figure 13 – Montage d'essai pour la mesure de la sécurité (téléprotection numérique)

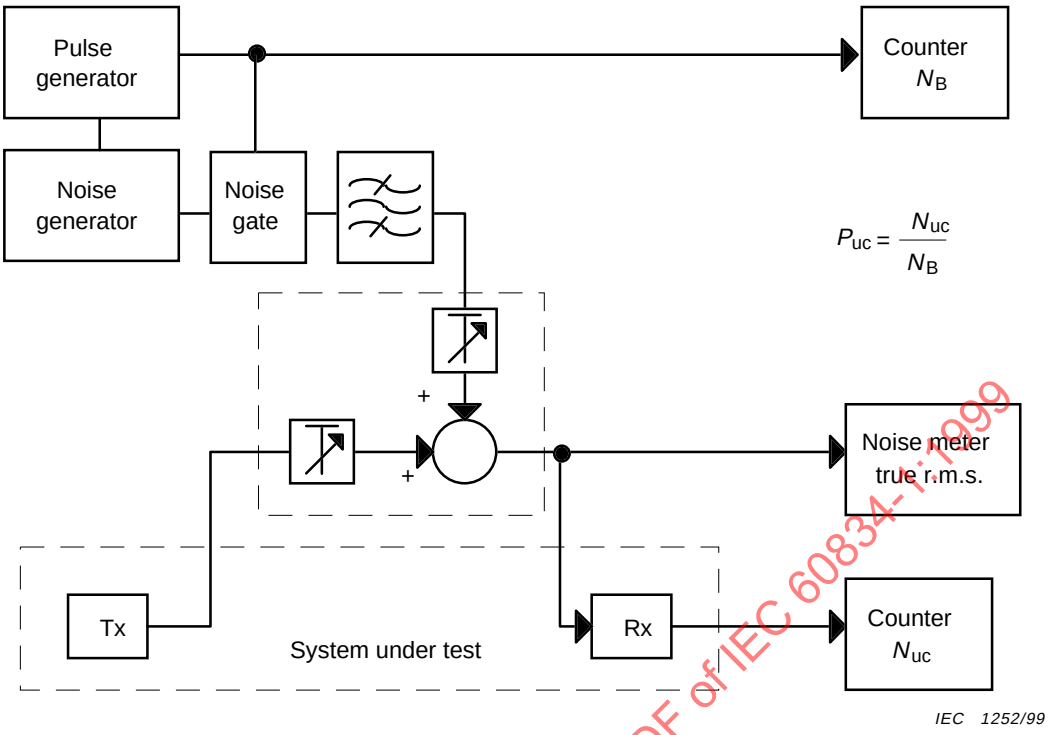


Figure 12 – Test set-up for security measurement (analogue teleprotection)

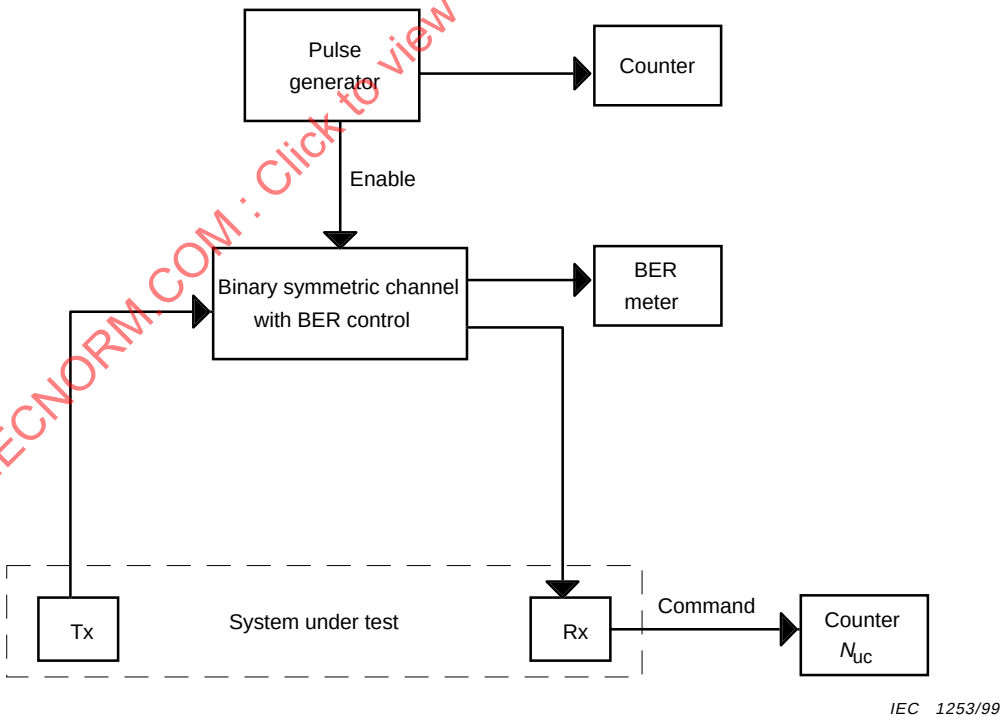


Figure 13 – Test set-up for security measurement (digital teleprotection)

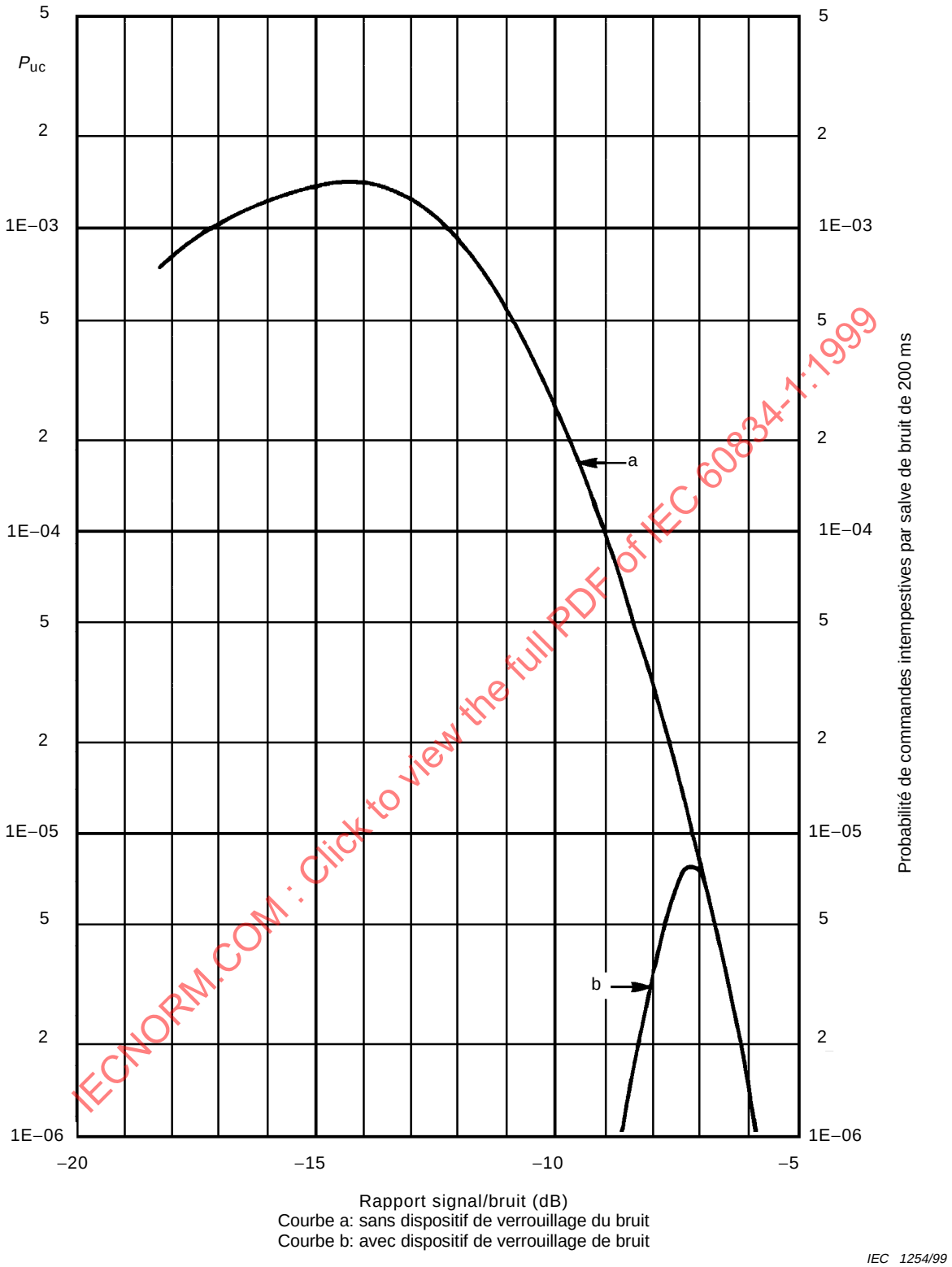


Figure 14 – Exemples de probabilité de commandes intempestives en fonction du rapport signal/bruit pour un canal de 200 Bd

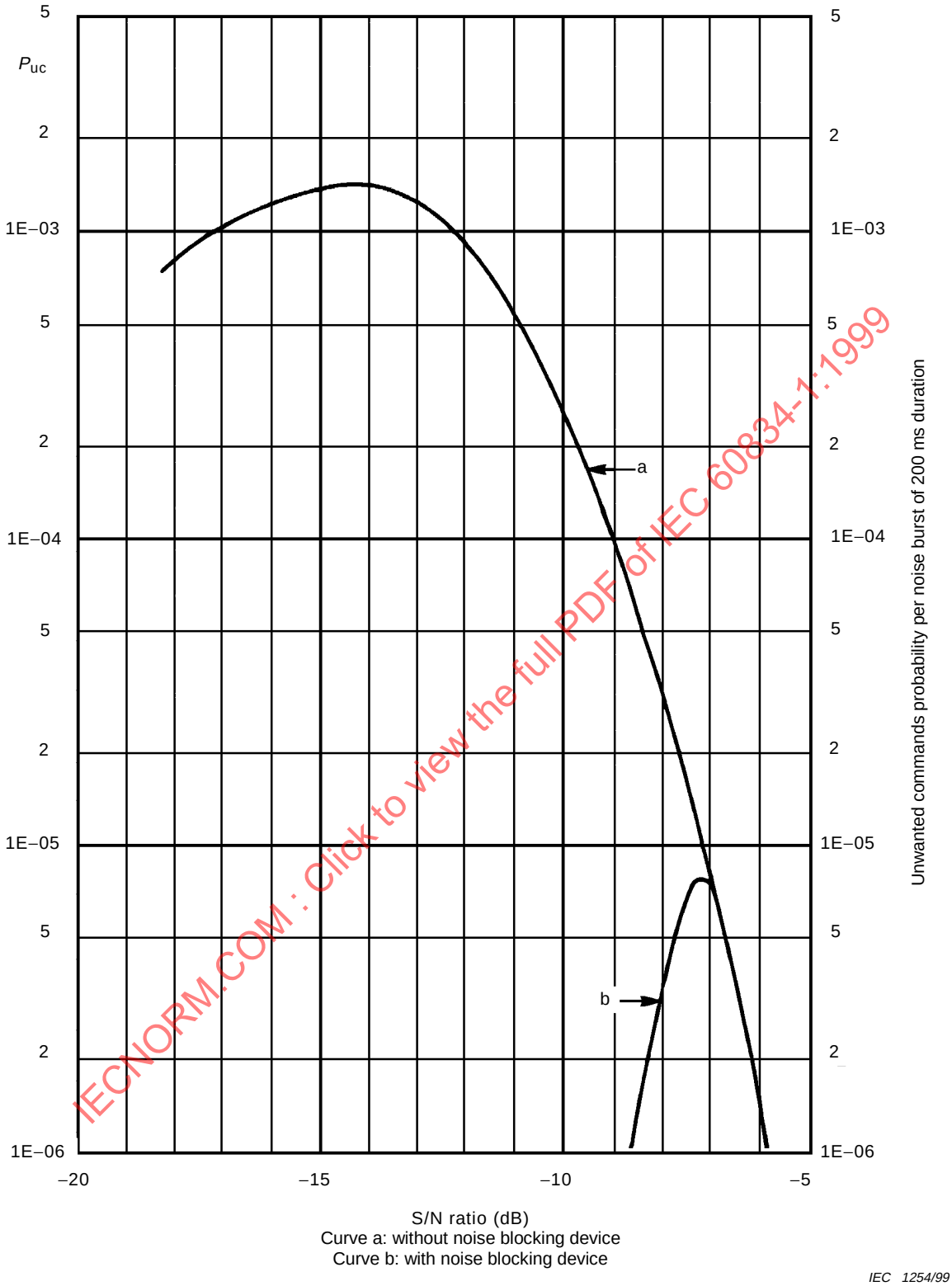


Figure 14 – Examples of probability of unwanted commands versus signal-to-noise ratio for 200 Bd channel

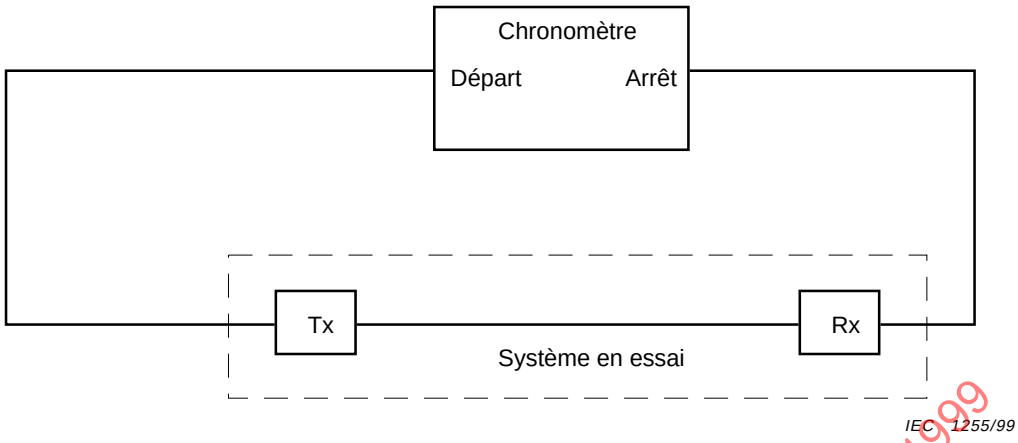


Figure 15 – Montage d'essai pour la mesure du temps de transmission

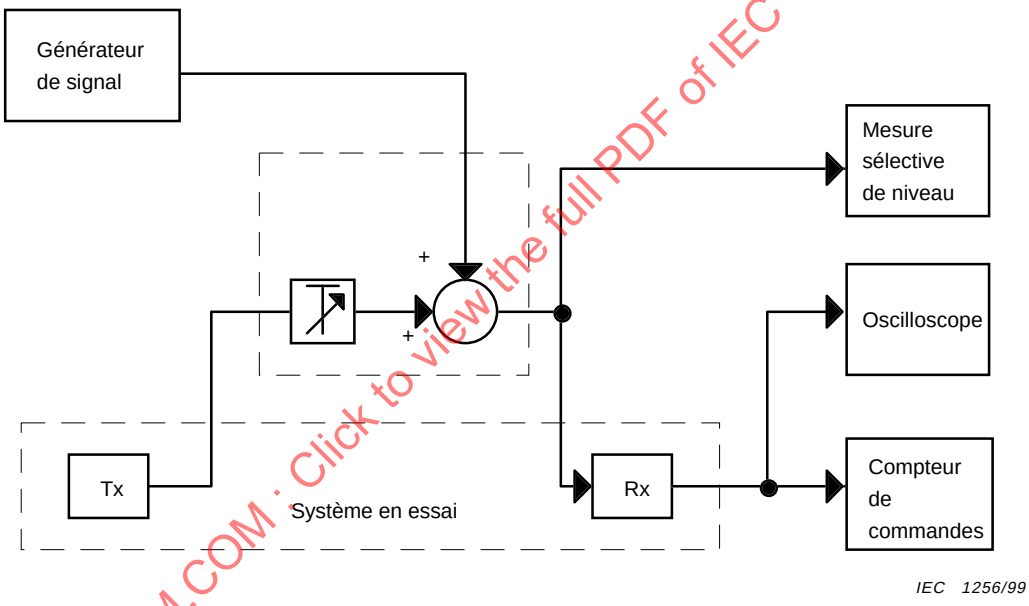


Figure 16 – Montage d'essai pour la mesure des perturbations par fréquences discrètes

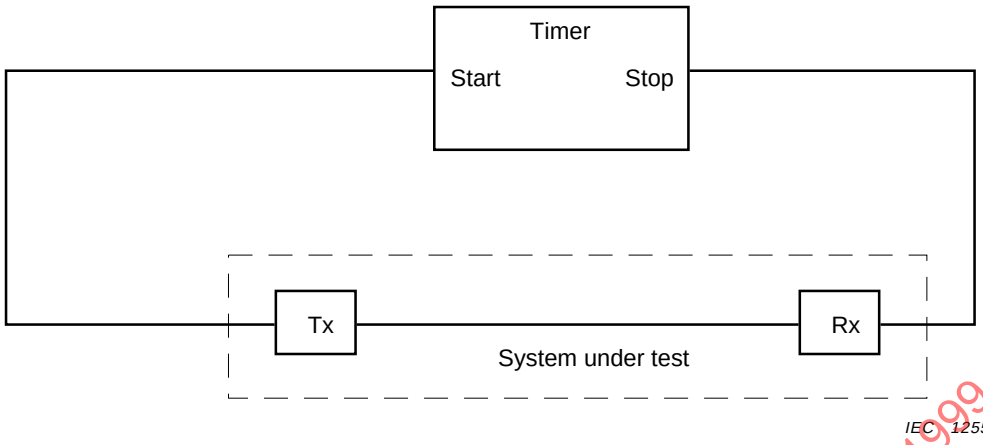


Figure 15 – Test set-up for measuring transmission time

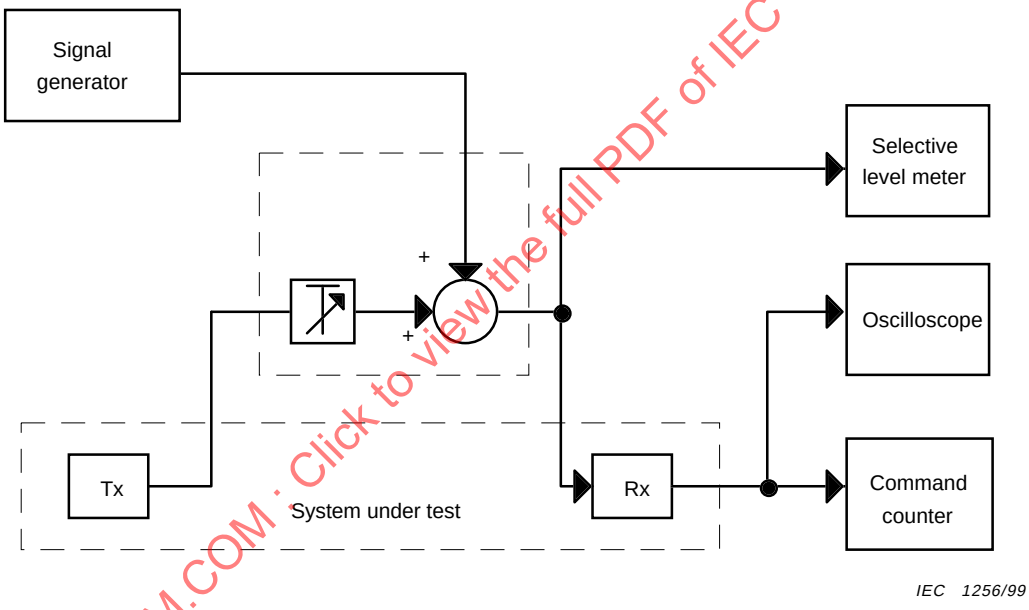


Figure 16 – Test set-up for measuring interference by discrete frequencies

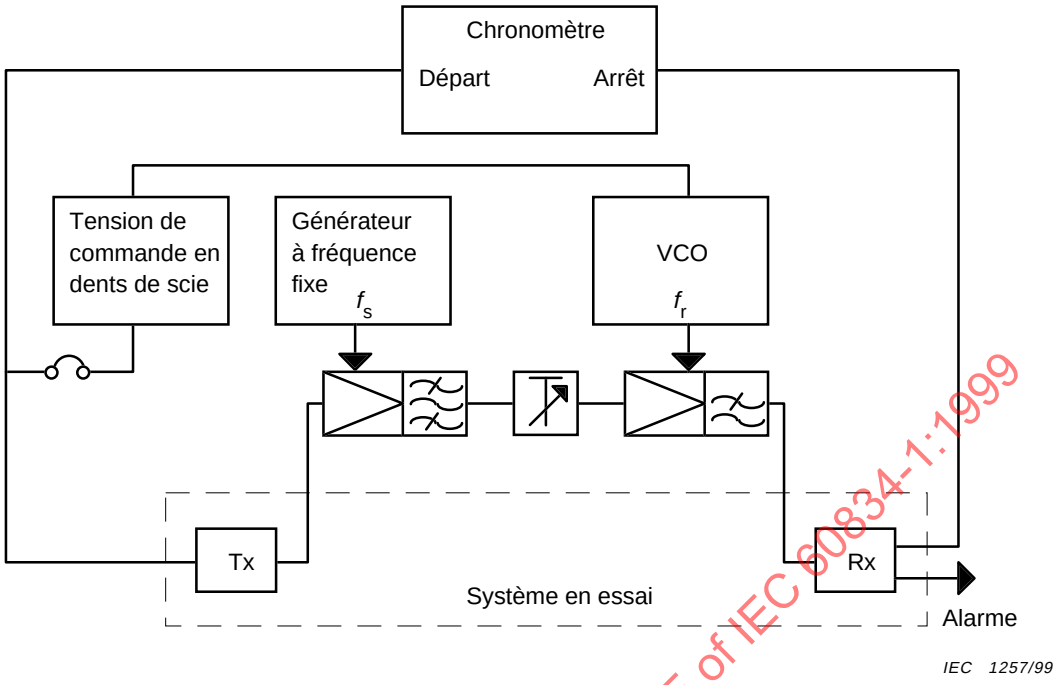


Figure 17 – Montage d'essai pour la mesure des perturbations par écart de fréquence

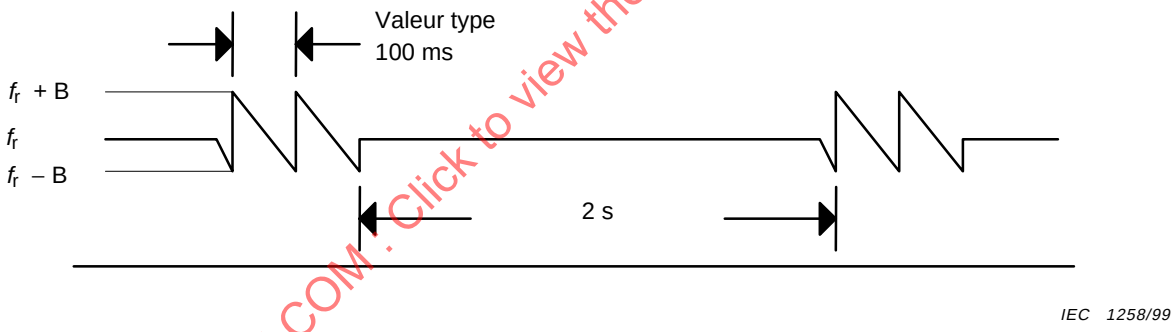


Figure 18 – Ecart de fréquence en fonction du temps pour le montage de la figure 17

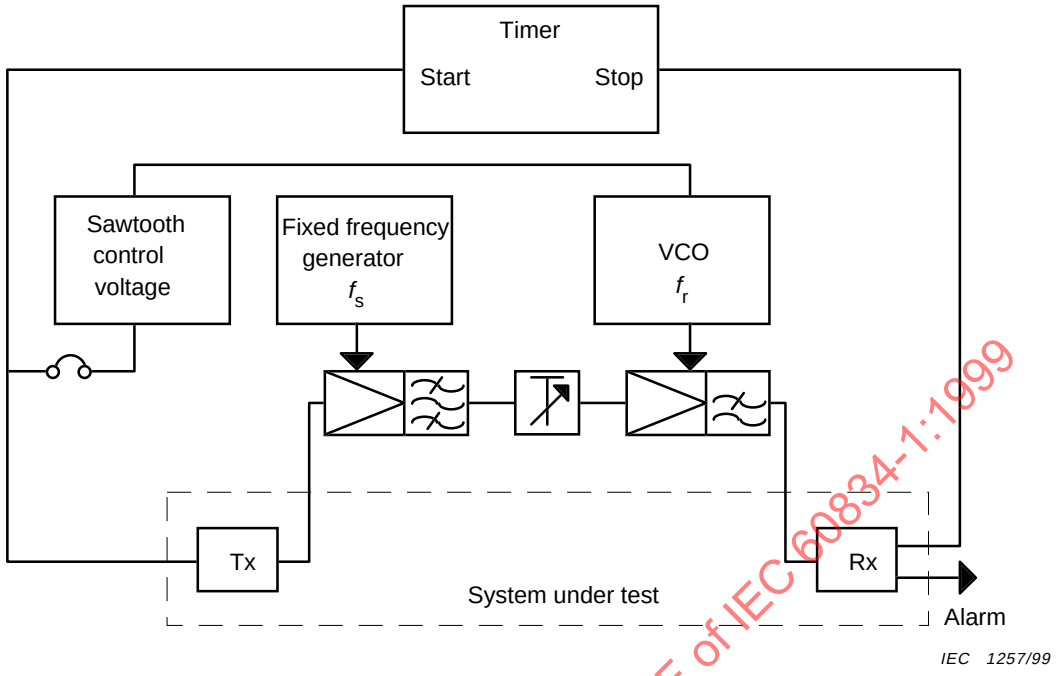


Figure 17 – Test set-up for measuring interference by frequency deviation

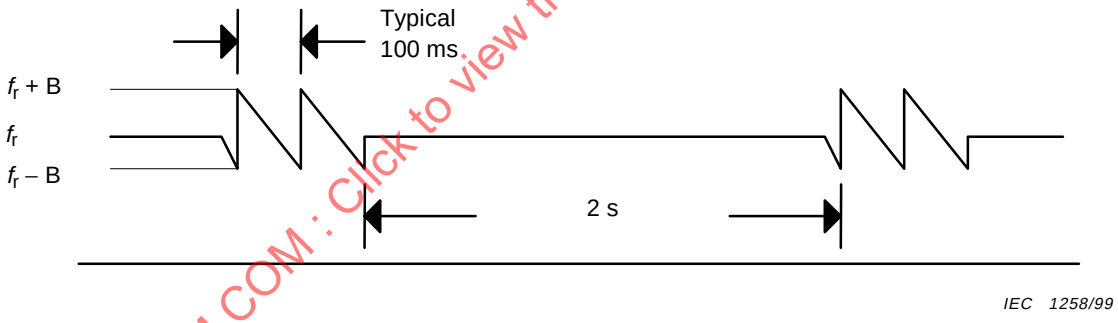


Figure 18 – Frequency deviation versus time for test set-up in figure 17