
**Engins de terrassement — Systèmes de
contrôle-commande utilisant des
composants électroniques — Critères et
essais de performances de sécurité
fonctionnelle**

*Earth-moving machinery — Machine-control systems (MCS) using
electronic components — Performance criteria and tests for functional
safety*
iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 15998:2008

<https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-770bf31bc612/iso-15998-2008>



PDF – Exonération de responsabilité

Le présent fichier PDF peut contenir des polices de caractères intégrées. Conformément aux conditions de licence d'Adobe, ce fichier peut être imprimé ou visualisé, mais ne doit pas être modifié à moins que l'ordinateur employé à cet effet ne bénéficie d'une licence autorisant l'utilisation de ces polices et que celles-ci y soient installées. Lors du téléchargement de ce fichier, les parties concernées acceptent de fait la responsabilité de ne pas enfreindre les conditions de licence d'Adobe. Le Secrétariat central de l'ISO décline toute responsabilité en la matière.

Adobe est une marque déposée d'Adobe Systems Incorporated.

Les détails relatifs aux produits logiciels utilisés pour la création du présent fichier PDF sont disponibles dans la rubrique General Info du fichier; les paramètres de création PDF ont été optimisés pour l'impression. Toutes les mesures ont été prises pour garantir l'exploitation de ce fichier par les comités membres de l'ISO. Dans le cas peu probable où surviendrait un problème d'utilisation, veuillez en informer le Secrétariat central à l'adresse donnée ci-dessous.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 15998:2008

<https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-770bf31bc612/iso-15998-2008>



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO 2008

Droits de reproduction réservés. Sauf prescription différente, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'ISO à l'adresse ci-après ou du comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax. + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	iv
Introduction	v
1 Domaine d'application	1
2 Références normatives	1
3 Termes, définitions et abréviations	1
4 Exigences générales de sécurité	4
5 Exigences supplémentaires relatives aux systèmes de contrôle-commande relatifs à la sécurité	6
6 Documentation	8
7 Essais pour les MCS relatifs à la sécurité	9
Annexe A (informative) Recommandations pour l'estimation du risque	12
Annexe B (informative) Exemple d'un schéma de défaillance d'une spécification du système	18
Annexe C (informative) Liste des composants éprouvés	19
Annexe D (informative) Recommandations pour systèmes bus pour la transmission de messages relatifs à la sécurité	22
Bibliographie	34

[ISO 15998:2008](https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-770bf31bc612/iso-15998-2008)

<https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-770bf31bc612/iso-15998-2008>

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO 15998 a été élaborée par le comité technique ISO/TC 127, *Engins de terrassement*, sous-comité SC 3, *Emploi et entretien*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 15998:2008
<https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-770bf31bc612/iso-15998-2008>

Introduction

Les systèmes électriques/électroniques sont utilisés depuis des années pour exécuter des fonctions liées à la sécurité dans la plupart des secteurs d'application. Des systèmes à base d'informatique [que l'on nommera de façon générique systèmes électroniques programmables (PES)] sont actuellement utilisés dans tous les secteurs d'application pour exécuter des fonctions non liées à la sécurité, mais aussi de plus en plus souvent, liées à la sécurité. Si l'on veut exploiter efficacement et en toute sécurité la technologie des systèmes informatiques, il est indispensable de fournir à tous les responsables suffisamment d'éléments liés à la sécurité pour les guider dans leurs prises de décisions.

La présente Norme internationale établit des recommandations pour les systèmes électriques et/ou électroniques et/ou avec des organes constitutifs électroniques programmables [systèmes électriques/électroniques/électroniques programmables (E/E/PES)] qui sont utilisés pour la sécurité fonctionnelle avec les engins de terrassement.

Dans la plupart des cas, la sécurité est obtenue par un certain nombre de systèmes de protection fondés sur diverses technologies (par exemple mécanique, hydraulique, pneumatique, électrique, électronique, électronique programmable). En conséquence, toute stratégie de sécurité doit non seulement prendre en compte tous les éléments d'un système individuel (par exemple les capteurs, les appareils de commande et les actionneurs), mais également tous les systèmes relatifs à la sécurité. C'est pourquoi la présente Norme internationale, bien que traitant essentiellement des systèmes électriques/électroniques/électroniques programmables (E/E/PES) relatifs à la sécurité, fournit néanmoins des orientations de sécurité susceptible de concerner les systèmes relatifs à la sécurité basés sur d'autres technologies.

La présente Norme internationale

- a été élaborée dans le souci de l'évolution rapide des technologies; le cadre fourni par la présente Norme internationale est suffisamment solide et étendu pour cette situation,
- fournit une méthode de développement des exigences de sécurité nécessaires pour définir la sécurité fonctionnelle requise des systèmes E/E/PE,
- donne la méthodologie afin de spécifier le niveau cible d'intégrité de sécurité des fonctions de sécurité devant être réalisées par les systèmes E/E/PE, en utilisant l'approche fondée sur le risque.

iTeh STANDARD PREVIEW **(standards.iteh.ai)**

ISO 15998:2008

<https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-770bf31bc612/iso-15998-2008>

Engins de terrassement — Systèmes de contrôle-commande utilisant des composants électroniques — Critères et essais de performances de sécurité fonctionnelle

1 Domaine d'application

La présente Norme internationale spécifie les critères et les essais de performances de sécurité fonctionnelle, relatifs au développement des systèmes de contrôle-commande de sécurité, utilisant des composants électroniques dans les engins de terrassement et leur équipement tels que définis dans l'ISO 6165. Les modes opératoires de l'ECE R79, Annexe 6, de l'ISO 13849-1 ou de la CEI 62061 peuvent être utilisées en alternative pour peu qu'une vérification et un essai soient menés par le constructeur en utilisant l'Article 7 de la présente Norme internationale.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO 6165:2006, *Engins de terrassement — Principaux types* — Identification et termes et définitions

[https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-](https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-70b1b1b1b1b1)

ISO 13766, *Engins de terrassement — Compatibilité électromagnétique*

ISO 14121-1, *Sécurité des machines — Appréciation du risque — Partie 1: Principes*

CEI 60529, *Degrés de protection procurés par les enveloppes (code IP)*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité — Partie 4: Définitions et abréviations*

CEI 61508-5:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité — Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

CEI 61508-7:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité — Partie 7: Présentation de techniques et mesures*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes, les définitions et les abréviations donnés dans la CEI 61508-4 ainsi que les suivants s'appliquent.

3.1 Termes et définitions

3.1.1

engin de terrassement

engin automoteur ou tracté, à roues, à chenilles ou à jambes, ayant un équipement, des accessoires (outil) ou les deux, principalement conçu pour assurer des opérations de creusement, de chargement, de transport, de forage, d'épandage, de compactage ou de tranchage de terre, de roche et d'autres matériaux

NOTE Adapté de ISO 6165:2006, définition 3.1.

3.1.2

systèmes de contrôle-commande

MCS

systèmes de contrôle-commande comprenant plusieurs composants nécessaires à l'exécution de la fonction du système comprenant généralement des capteurs, une unité de traitement des signaux, des commandes et des actionneurs

NOTE L'étendue du système ne se limite pas aux commandes électroniques, mais est définie par la fonction relative à la machine du système complet. Elle comprend par conséquent généralement des dispositifs électroniques, non électroniques et de connexion. Elle peut comprendre des composants/des systèmes qui peuvent être électroniques, mécaniques, hydrauliques, optiques ou pneumatiques.

3.1.3

unité système

partie d'un système de contrôle-commande comprenant tout nombre donné de composants et/ou de pièces intégrés en une ou plusieurs unités

EXEMPLE Unité de commande de la boîte automatique.

NOTE Les composants et/ou les pièces sont généralement disposés dans une enceinte commune, mais l'unité système peut également être constituée sous forme de composite mécanique avec plusieurs éléments fonctionnels.

3.1.4

dispositifs de connexion

dispositifs utilisés pour l'alimentation électrique et pour la transmission des signaux et des données

3.1.5

fonction de base

⟨système de contrôle-commande⟩ commande de la (des) tâche(s)

3.1.6

fonction de base

⟨unité système⟩ recevant les signaux et les données, les traitant et/ou les actionnant

3.1.7

fonction système

toute fonction devant être traitée par un système de contrôle-commande ou une unité système

NOTE Outre la fonction de base, les fonctions système comprennent le diagnostic, l'autosurveillance, le traitement des signaux et la transmission des données à d'autres systèmes.

3.1.8

concept de sécurité

concept contenu dans la description des méthodes intrinsèques au système traitant des performances de ce dernier et du fonctionnement en toute sécurité dudit système en cas de panne

3.1.9

systèmes de contrôle-commande relatifs à la sécurité

⟨systèmes de contrôle-commande⟩ régulant les fonctions de la machine relatives à la sécurité

3.1.10**état de sécurité**

état appliqué automatiquement ou manuellement après un dysfonctionnement du système de contrôle-commande lorsque l'équipement, le procédé ou le système commandé est interrompu ou commuté en mode sécurité afin de prévenir tout mouvement intempestif ou d'éviter l'accumulation d'énergie potentiellement dangereuse (par exemple électricité sous haute tension, pressions hydrauliques ou ressorts comprimés)

3.1.11**composant éprouvé**

composant pour utilisation relative à la sécurité qui a été largement utilisé dans le passé avec des résultats satisfaisants pour des utilisations similaires et qui a été fabriqué et vérifié en utilisant les principes qui démontrent qu'il est adapté et fiable pour les utilisations relatives à la sécurité

NOTE 1 Pour quelques composants éprouvés, certains défauts peuvent également être exclus car le taux de défaillance est connu pour être très faible.

NOTE 2 La décision d'accepter un composant particulier comme composant éprouvé dépend de son utilisation.

3.1.12**fonction de remplacement**

fonction permettant l'existence d'un procédé continu en cas de dysfonctionnement ou de défaillance du système

3.1.13**fonction de mouvement d'urgence**

fonction à adopter en cas de dysfonctionnement ou de défaillance du système afin de permettre à l'opérateur d'exécuter un mouvement d'urgence (de l'engin)

EXEMPLE Dégager un engin de la voie publique.

3.1.14**système programmable électronique
PES**

système de commande, de protection ou de surveillance basé sur un ou plusieurs dispositifs électroniques programmables, y compris tous les éléments du système tels que les alimentations en énergie, les capteurs et autres périphériques d'entrée, les bus de données et autres circuits de communication, et les actionneurs et autres dispositifs de sortie

3.2 Abréviations

PES	système programmable électronique
MCS	systèmes de contrôle-commande
FMEA	analyse des modes de défaillance et leurs effets
FTA	arbre des défaillances
ETA	arbre des événements
SIL	niveau d'intégrité de sécurité (voir la CEI 61508-4:1998, 3.5.6)
Code IP	degré de protection IP
CEM	compatibilité électromagnétique (voir l'ISO 13766:2006, 3.1)
OSI	dispositifs de connexion ouverts
ASIC	circuit intégré à application spécifique
RF	radiofréquence

4 Exigences générales de sécurité

4.1 Application

Les critères de performances suivants sont valables pour tous les systèmes de contrôle-commande, utilisant des composants électroniques, relatifs à la sécurité. Ces critères de performance peuvent être appliqués à tout type de MCS.

4.2 Description du système de contrôle-commande

La description et la définition générale du système doivent comprendre

- une liste de toutes les unités système qui sont utilisées pour des fonctions relatives à la sécurité, et
- un schéma des dispositifs de connexion et des unités système, représentatif des fonctions relatives à la sécurité du système de contrôle-commande.

Un exemple de la structure et du contenu de la description du système est donné dans l'Annexe B.

Les fonctions de base et leurs interfaces avec d'autres unités système doivent être spécifiées pour chaque unité système. Cette spécification peut se présenter sous la forme d'un schéma ou d'un organigramme.

La connexion doit être illustrée de manière appropriée; un schéma de circuits convient dans le cas du système électrique.

Le schéma doit classer sans aucune ambiguïté chaque dispositif de connexion (par exemple câbles) aux unités système (par exemple par l'identification des bornes).

Les unités système doivent être marquées par des codes d'identification (par exemple numéros, symboles, caractères) de manière à pouvoir vérifier la corrélation entre l'illustration des systèmes et le MCS installé sur la machine.

Le constructeur démontre, en utilisant les codes d'identification, que les unités système sont conformes à la documentation concernant la fonction de base, le concept de sécurité et les interfaces. La structure des codes d'identification (par exemple alphanumérique) peut être spécifiée par le constructeur mais doit être dépourvue de toute ambiguïté.

La description du système doit également comprendre les exigences relatives aux conditions ambiantes en cours d'exploitation prévue de la machine:

- conditions climatiques (température, humidité);
- conditions mécaniques (vibrations, choc);
- conditions de corrosion (brouillard salin, gaz polluant);
- conditions électriques (sur et sous-tension);
- conditions électromagnétiques;
- fluctuation de tension de la source d'alimentation.

4.3 Description de la fonction de base

La fonction de base du système de contrôle-commande doit être spécifiée dans une description succincte, pouvant être appuyée par des outils graphiques tels que des schémas fonctionnels ou des organigrammes. La description doit comprendre

- le recensement des types et valeurs d'entrée du MCS;
- le recensement des types et valeurs de sortie contrôlées du MCS;
- les objectifs de commande en boucle ouverte et en boucle fermée et données/capteurs utilisés;
- les plages de fonctionnement et de réglage admissibles.

4.4 Analyse et estimation du risque

Le MCS doit faire l'objet d'une analyse et d'une estimation du risque en utilisant la description du système conformément à 4.2 afin d'évaluer les phénomènes dangereux. Ces dernières peuvent être effectuées conformément à des méthodes d'estimation du risque telles que celles données dans l'ISO 14121-1 ou dans la CEI 61508-5:1998, Annexe D. Un exemple est donné dans l'Annexe A de la présente Norme internationale.

4.5 Critères de performances applicables au concept de sécurité

Le développement et la production du système de contrôle-commande doivent tenir compte du concept et des fonctions système de base spécifiés par le constructeur pour le concept de sécurité de la machine. Ledit concept comprend toutes les mesures qui permettent un fonctionnement en toute sécurité au-delà d'une exploitation normale (pour des conseils se reporter à la CEI 61508-2:2000, 7.2.3.1). Ces mesures doivent être énumérées d'une manière générale et compréhensible comme les exemples suivants:

- redondance; <https://standards.iteh.ai/catalog/standards/sist/82ae1070-ca7c-4d8a-adcb-770bf31bc612/iso-15998-2008>
- procédures de détection des anomalies;
- «état de sécurité», un état de sécurité peut par exemple déclencher une fonction de mouvement d'urgence (voir 5.4).

Ceci comprend une analyse documentée indiquant la réalisation effective du concept de sécurité tel que décrit. Cette analyse peut prendre la forme d'une analyse (par exemple FMEA, FTA, ETA) ou des méthodes similaires, qui sont appropriées au concept de sécurité du MCS.

Le constructeur doit documenter la méthode de validation de la logique du système au cours de la phase de développement.

La transition du mode de fonctionnement normal à un état de sécurité doit prendre en considération la stabilité de la machine et réduire au minimum le risque de blessure des personnes.

Il convient que le mouvement (actif ou passif) de la machine ou de son matériel/ses accessoires de service en dehors de la zone ou de la position dangereuse dans le cas d'un dysfonctionnement du MCS soit possible.

4.6 Environnement physique et conditions d'exploitation

4.6.1 Généralités

Il convient que les conditions environnementales dans lesquelles les engins sont utilisés soient la base de la spécification du MCS.

4.6.2 Température et humidité ambiantes

Le système de contrôle-commande des engins de terrassement doit fonctionner en toute sécurité dans les conditions décrites en 7.2.2.

Des restrictions, n'exerçant aucune influence sur la fonction de sécurité du MCS, peuvent être acceptées.

Pour des conditions de fonctionnement spéciales de l'engin et des conditions d'installation des pièces électroniques, d'autres conditions environnementales peuvent être spécifiées par le constructeur.

4.6.3 Degré de protection (Code IP)

Les pièces du MCS réalisant la sécurité fonctionnelle, sur la base des conditions d'installation, doivent satisfaire au moins aux degrés de protection suivants, conformément à la CEI 60529:

- IP 66¹⁾ pour toutes les pièces électroniques, installées à l'extérieur de la machine ou directement exposées aux influences de l'environnement.

Pour des conditions de fonctionnement de l'engin et des conditions d'installation des pièces électroniques, d'autres conditions environnementales peuvent être spécifiées par le constructeur.

4.6.4 Compatibilité électromagnétique (CEM)

Le système de contrôle-commande doit satisfaire aux exigences de l'ISO 13766.

4.6.5 Vibrations et chocs mécaniques

Les unités système, les composants et pièces du MCS utilisés sur les engins de terrassement doivent être conçus et installés de sorte que leur fonction de sécurité soit maintenue pour les charges dues aux vibrations et chocs pendant l'exploitation type de l'engin.

Voir 7.2.3 et 7.2.4 pour les conditions d'essai.

Pour des conditions de fonctionnement spéciales de l'engin et des conditions d'installation des pièces électroniques, d'autres conditions environnementales peuvent être spécifiées par le constructeur.

4.7 Fonction d'arrêt d'urgence

Une fonction d'arrêt d'urgence doit être prévue lorsque le concept de sécurité le requiert. L'arrêt d'urgence doit commuter le MCS, l'unité système ou la machine en un état de sécurité défini en cas de défaillance pouvant entraîner un mouvement ou un état dangereux de la machine.

5 Exigences supplémentaires relatives aux systèmes de contrôle-commande relatifs à la sécurité

5.1 Généralités

Le présent article s'applique aux systèmes de contrôle-commande avec des fonctions de sécurité ayant un niveau SIL = 1 ou équivalent (voir A.3.2).

Les systèmes de contrôle-commande avec fonctions relatives à la sécurité doivent satisfaire les exigences supplémentaires suivantes selon l'estimation des risques.

1) Pour des conditions spéciales d'installation, d'autres degrés de protection peuvent être sélectionnés, par exemple en cas de plus haute tension, dysfonctionnement dû à l'humidité, saletés ou particules extérieures conductrices qui pourraient entraîner une situation inacceptable (risque).

5.2 Évitement et maîtrise des anomalies

5.2.1 Les Annexes A et B de la CEI 61508-2:2000 ou d'autres méthodes comparables, doivent être utilisées comme un guide applicable aux mesures et aux techniques relatives à l'évitement et à la maîtrise des anomalies.

5.2.2 Les défaillances observées au niveau d'un système relatif à la sécurité varient essentiellement en fonction du moment de leur apparition (origine):

- a) défaillances dues à des anomalies apparaissant avant ou pendant l'installation du système (par exemple les anomalies logicielles comprennent des anomalies de spécification et de programme, les anomalies matérielles comprennent des anomalies de fabrication et une sélection de composants incorrecte);
- b) défaillances dues à des anomalies ou à des erreurs humaines apparaissant pendant la vie/l'exploitation de l'engin et généralement après l'installation du système (par exemple des défaillances aléatoires du matériel ou des défaillances dues à une utilisation incorrecte).

Les défaillances du type décrit en a) peuvent être décelées, corrigées et évitées par l'adoption de mesures lors des différentes phases du cycle de vie (voir la CEI 61508-2:2000, Annexe B). Les mesures applicables à l'évitement des défaillances sont des procédures essentiellement de conception et analytiques.

Les défaillances du type décrit en b) peuvent être maîtrisées uniquement lors d'une exploitation normale (voir CEI 61508-2:2000, Annexe A). Les mesures applicables à la maîtrise de ces défaillances doivent être intégrées au concept de sécurité.

Certaines mesures et techniques décrites dans la CEI 61508-2 sont d'une importance essentielle (voir les Annexes A et B), il convient qu'elles soient ainsi employées indépendamment du niveau d'intégrité de sécurité. Il convient d'employer d'autres mesures et techniques indépendamment du niveau d'intégrité de sécurité. Il convient que l'effort requis pour la réalisation effective de ces mesures permette d'obtenir l'efficacité exigée dans la CEI 61508-2:2000, Tableaux B.1 à B.5 (faible/moyenne/élevée). Toutes les autres mesures peuvent être remplacées en principe, soit de manière individuelle, soit associées à d'autres mesures.

5.3 Exigences relatives aux systèmes électroniques programmables (PES)

Le logiciel doit être développé et validé suivant les mesures appropriées (voir, par exemple, la CEI 61508-3:1998, Annexe A ou l'ISO 13849-1).

Les concepts et les méthodes, et les outils de développement applicables aux systèmes électroniques programmables (PES) utilisés dans les systèmes de contrôle-commande doivent être documentés.

5.4 Dysfonctionnement ou défaillance des composants électroniques utilisés avec les systèmes de contrôle-commande

L'adoption d'un état de sécurité doit être réalisée en cas de dysfonctionnement ou de défaillance des composants électroniques utilisés avec le système de contrôle-commande suivant l'estimation du risque. Une performance réduite du système ou l'utilisation de fonction(s) de substitution peuvent être utilisées pour parvenir à un état sûr en tant que partie du concept de sécurité.

L'état de sécurité peut être atteint par une permutation automatique vers une fonction de remplacement (voir la Figure 1). Si cette transition est appliquée par le MCS alors, il doit y avoir une forme quelconque d'indication pour l'opérateur telle que alarmes, indicateurs ou performance réduite (par exemple vitesse lente).