



IEC 63208

Edition 1.0 2025-08

# NORME INTERNATIONALE

Appareillages et ensembles d'appareillages à basse tension - Exigences de sécurité

**ITEH Standards**  
<https://standards.iteh.ai>  
Document Preview

[IEC 63208:2025](#)

<https://standards.iteh.ai/catalog/standards/iec/358225d2-dea9-46f0-8912-b7be8bb0f6fc/iec-63208-2025>



## THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2025 IEC, Geneva, Switzerland

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

IEC Secretariat  
3, rue de Varembé  
CH-1211 Geneva 20  
Switzerland

Tel.: +41 22 919 02 11  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

### A propos de l'IEC

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

### A propos des publications IEC

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

#### Recherche de publications IEC -

[webstore.iec.ch/advsearchform](https://webstore.iec.ch/advsearchform)

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

#### IEC Just Published - [webstore.iec.ch/justpublished](https://webstore.iec.ch/justpublished)

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

#### Service Clients - [webstore.iec.ch/csc](https://webstore.iec.ch/csc)

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

#### IEC Products & Services Portal - [products.iec.ch](https://products.iec.ch)

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

#### Electropedia - [www.electropedia.org](https://www.electropedia.org)

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Également appelé Vocabulaire Electrotechnique International (IEV) en ligne.

**Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

## SOMMAIRE

AVANT-PROPOS .....	8
INTRODUCTION .....	10
1    Domaine d'application .....	12
2    Références normatives .....	13
3    Termes, définitions et abréviations .....	13
3.1    Termes et définitions .....	13
3.2    Abréviations .....	20
4    Généralités .....	21
5    Objectifs de sécurité .....	21
6    Gestion du cycle de vie de la sécurité .....	21
6.1    Généralités .....	21
6.2    Appréciation du risque pour la sécurité .....	23
6.2.1    Généralités .....	23
6.2.2    Relation entre sécurité et sécurité humaine .....	24
6.2.3    Appréciation de l'impact .....	25
6.2.4    Résultat de l'appréciation du risque pour la sécurité .....	25
6.3    Réponse au risque pour la sécurité .....	26
6.4    Spécification des exigences de sécurité .....	26
6.5    Rôles et responsabilités .....	26
6.6    Données importantes .....	27
6.7    Architecture du système de commande .....	27
6.7.1    Système de commande .....	27
6.7.2    Niveaux des fonctionnalités de communication .....	28
6.7.3    Niveaux de connectivité .....	30
6.7.4    Niveaux d'exposition de l'équipement .....	32
6.7.5    Niveaux de sécurité de l'équipement .....	32
6.7.6    Profil de protection de la sécurité .....	33
7    Exigences de sécurité .....	34
7.1    Généralités .....	34
7.2    Accès physique et environnement .....	34
7.2.1    PA – Exigence relative à l'accès physique et à l'environnement .....	34
7.2.2    Justification pour l'accès physique et l'environnement .....	34
7.2.3    PA-e – Amélioration des accès physiques et de l'environnement .....	35
7.2.4    Mise en œuvre type de l'accès physique et de l'environnement .....	36
7.3    Exigences relatives à l'équipement .....	37
7.3.1    Généralités .....	37
7.3.2    FR 1 – Contrôle d'identification et d'authentification .....	38
7.3.3    FR 2 – Contrôle d'utilisation .....	42
7.3.4    FR 3 – Intégrité du système .....	47
7.3.5    FR 4 – Confidentialité des données .....	53
7.3.6    FR 5 – Transfert de données limité (RDF) .....	54
7.3.7    FR 6 – Réponse appropriée aux événements .....	55
7.3.8    FR 7 – Disponibilité des ressources .....	55
8    Instructions d'installation, de fonctionnement et de maintenance .....	59
8.1    Exigences relatives aux instructions pour l'utilisateur .....	59
8.2    Amélioration des instructions pour l'utilisateur .....	60

8.3	Mise en œuvre des instructions pour l'utilisateur .....	60
9	Vérification et essais de conformité .....	60
9.1	Généralités .....	60
9.2	Documentation de conception .....	60
9.3	Accès physique .....	61
9.3.1	Vérification de l'accès physique et de l'environnement .....	61
9.3.2	Critère de décision .....	61
9.3.3	Amélioration des accès physiques et de l'environnement .....	61
9.3.4	Critère de décision .....	61
9.4	FR 1 – Contrôle d'identification et d'authentification .....	61
9.4.1	CR 1.1 – Identification et authentification d'un utilisateur humain .....	61
9.4.2	CR 1.2 – Identification et authentification des logiciels et équipements .....	62
9.4.3	CR 1.5 – Gestion d'authentifiant .....	62
9.4.4	CR 1.7 – Force de l'authentification par mot de passe .....	63
9.4.5	CR 1.8 – Certificats d'infrastructure à clés publiques .....	63
9.4.6	CR 1.9 – Force de l'authentification par clé publique .....	63
9.4.7	CR 1.10 – Retour de l'authentifiant .....	64
9.4.8	CR 1.11 – Tentatives infructueuses de connexion .....	64
9.4.9	CR 1.14 – Force de l'authentification par clés symétriques .....	64
9.5	FR 2 – Contrôle d'utilisation .....	65
9.5.1	CR 2.1 – Mise en œuvre d'autorisation .....	65
9.5.2	CR 2.2 – Contrôle d'utilisation sans fil .....	65
9.5.3	EDR 2.4 – Code mobile .....	65
9.5.4	CR 2.5 – Verrouillage de session .....	66
9.5.5	CR 2.6 – Fermeture de la session à distance .....	66
9.5.6	CR 2.7 – Contrôle de sessions simultanées .....	67
9.5.7	CR 2.8 – Événements auditables .....	67
9.5.8	CR 2.9 – Capacité de stockage des données d'audit .....	67
9.5.9	CR 2.10 – Réponse aux défaillances de traitement des audits .....	68
9.5.10	CR 2.11 – Horodatages .....	68
9.5.11	CR 2.12 – Non-répudiation .....	69
9.5.12	EDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai .....	69
9.6	FR 3 – Intégrité du système .....	69
9.6.1	CR 3.1 – Intégrité de la communication .....	69
9.6.2	EDR 3.2 – Protection contre les programmes malveillants .....	70
9.6.3	CR 3.3 – Vérification de la fonctionnalité de sécurité .....	70
9.6.4	CR 3.4 – Intégrité des logiciels et des informations .....	70
9.6.5	CR 3.5 – Validation d'entrée .....	71
9.6.6	RC 3.6 – Sortie déterministe .....	71
9.6.7	CR 3.7 – Traitement des erreurs .....	71
9.6.8	CR 3.8 – Intégrité de la session .....	72
9.6.9	CR 3.9 – Protection des informations d'audit .....	72
9.6.10	EDR 3.10 – Support pour les mises à jour .....	72
9.6.11	EDR 3.11 – Résistance aux violations physiques et détection .....	73
9.6.12	EDR 3.12 – Fourniture des racines de confiance du fournisseur de produit .....	73
9.6.13	EDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif .....	73
9.6.14	EDR 3.14 – Intégrité du processus d'amorçage .....	74
9.7	FR 4 – Confidentialité des données .....	74

9.7.1	CR 4.1 – Confidentialité des informations .....	74
9.7.2	CR 4.3 – Utilisation de la cryptographie .....	74
9.8	FR 6 – Réponse appropriée aux événements .....	75
9.8.1	CR 6.1 – Accessibilité au journal d'audit .....	75
9.9	FR 7 – Disponibilité des ressources .....	75
9.9.1	CR 7.1 – Protection contre le refus de service .....	75
9.9.2	CR 7.2 – Gestion des ressources .....	75
9.9.3	CR 7.3 – Sauvegarde du système de commande .....	76
9.9.4	CR 7.4 – Reprise et reconstitution du système de commande .....	76
9.9.5	CR 7.6 – Paramètres de configuration du réseau et de la sécurité .....	76
9.9.6	CR 7.7 – Fonctionnalité minimale .....	77
9.9.7	CR 7.8 – Inventaire des composants du système de commande .....	77
Annexe A (informative)	Cybersécurité et architecture des systèmes électriques .....	78
A.1	Généralités .....	78
A.2	Architecture type comprenant des appareillages et ensembles d'appareillages .....	78
A.2.1	Bâtiment .....	78
A.2.2	Installation de fabrication .....	79
Annexe B (informative)	Études de cas d'utilisation .....	81
B.1	Généralités .....	81
B.2	Cas d'utilisation 1 – Protection contre les attaques par déni de service (DoS) .....	82
B.3	Cas d'utilisation 2 – Protection contre les modifications non autorisées d'un dispositif de détection .....	83
B.4	Cas d'utilisation 3 – Protection contre les modifications non autorisées d'un équipement sans fil .....	84
B.5	Cas d'utilisation 4 – Protection contre les agents menaçants qui prennent le contrôle à distance d'un ensemble intelligent "de gestion" .....	85
Annexe C (informative)	Méthodes de développement de mesures de cybersécurité .....	87
Annexe D (informative)	Instructions relatives à la sécurité dans la documentation du produit .....	88
D.1	Généralités .....	88
D.2	Appréciation du risque et planification de la sécurité .....	88
D.2.1	Appréciation du risque .....	88
D.2.2	Plan de sécurité .....	89
D.3	Recommandations pour la conception et l'installation du système intégrant des appareillages et ensembles d'appareillages .....	89
D.3.1	Contrôle d'accès général .....	89
D.3.2	Recommandations pour l'accès local .....	89
D.3.3	Recommandations pour l'accès à distance .....	90
D.3.4	Recommandations pour les mises à niveau du microprogramme .....	91
D.3.5	Recommandations pour la fin de vie .....	91
D.4	Instructions pour un ensemble .....	91
Annexe E (normative)	Profil de protection de la sécurité d'un démarreur progressif et d'un contrôleur à semiconducteurs .....	92
E.1	Introduction .....	92
E.1.1	Référence du profil de protection de la sécurité .....	92
E.1.2	Vue d'ensemble de la cible d'évaluation .....	92
E.1.3	Objectifs généraux de la mission .....	93
E.1.4	Caractéristiques .....	93
E.1.5	Utilisation du produit .....	93

E.1.6	Utilisateurs .....	93
E.2	Hypothèses.....	94
E.3	Revendications de conformité et déclaration de conformité .....	94
E.4	Définition du problème de sécurité.....	94
E.4.1	Actifs essentiels de l'environnement .....	94
E.4.2	Actifs essentiels de la ToE .....	95
E.4.3	Modèle de menaces .....	95
E.5	Objectifs de sécurité .....	96
E.6	Exigences de sécurité .....	96
E.6.1	Exigences fonctionnelles de sécurité .....	96
E.6.2	Exigences d'assurance de sécurité .....	97
Annexe F (normative) Profil de protection de la sécurité d'un démarreur de moteur raccordé au réseau.....		98
F.1	Introduction.....	98
F.1.1	Référence du profil de protection de la sécurité .....	98
F.1.2	Vue d'ensemble de la cible d'évaluation.....	98
F.1.3	Objectifs généraux de la mission .....	99
F.1.4	Caractéristiques .....	99
F.1.5	Utilisation du produit .....	99
F.1.6	Utilisateurs .....	99
F.2	Hypothèses.....	100
F.3	Revendications de conformité et déclaration de conformité .....	100
F.4	Définition du problème de sécurité.....	100
F.4.1	Actifs essentiels de l'environnement .....	100
F.4.2	Actifs essentiels de la ToE .....	101
F.4.3	Modèle de menaces .....	101
F.5	Objectifs de sécurité .....	102
F.6	Exigences de sécurité .....	102
F.6.1	Exigences fonctionnelles de sécurité .....	102
F.6.2	Exigences d'assurance de sécurité .....	103
Annexe G (normative) Profil de protection de la sécurité d'un disjoncteur.....		104
G.1	Introduction.....	104
G.1.1	Référence du profil de protection de la sécurité .....	104
G.1.2	Vue d'ensemble de la cible d'évaluation.....	104
G.1.3	Objectifs généraux de la mission .....	105
G.1.4	Caractéristiques .....	105
G.1.5	Utilisation du produit .....	105
G.1.6	Utilisateurs .....	105
G.2	Hypothèses.....	106
G.3	Revendications de conformité et déclaration de conformité .....	106
G.4	Définition du problème de sécurité.....	106
G.4.1	Actifs essentiels de l'environnement .....	106
G.4.2	Actifs essentiels de la ToE .....	107
G.4.3	Modèle de menaces .....	107
G.5	Objectifs de sécurité .....	108
G.6	Exigences de sécurité .....	108
G.6.1	Exigences fonctionnelles de sécurité .....	108
G.6.2	Exigences d'assurance de sécurité .....	109
Annexe H (normative) Profil de protection de la sécurité d'un commutateur de transfert ...		110

H.1	Introduction.....	110
H.1.1	Référence du profil de protection de la sécurité .....	110
H.1.2	Vue d'ensemble de la cible d'évaluation.....	110
H.1.3	Objectifs généraux de la mission .....	111
H.1.4	Caractéristiques.....	111
H.1.5	Utilisation du produit .....	111
H.1.6	Utilisateurs .....	112
H.2	Hypothèses.....	112
H.3	Revendications de conformité et déclaration de conformité .....	112
H.4	Définition du problème de sécurité.....	113
H.4.1	Actifs essentiels de l'environnement .....	113
H.4.2	Actifs essentiels de la ToE .....	113
H.4.3	Modèle de menaces .....	114
H.5	Objectifs de sécurité .....	114
H.6	Exigences de sécurité .....	115
H.6.1	Exigences fonctionnelles de sécurité .....	115
H.6.2	Exigences d'assurance de sécurité .....	115
Annexe I (normative)	Profil de protection de la sécurité pour un appareillage de commande sans fil avec son interface de communication .....	116
I.1	Introduction.....	116
I.1.1	Référence du profil de protection de la sécurité .....	116
I.1.2	Vue d'ensemble de la cible d'évaluation.....	116
I.1.3	Objectifs généraux de la mission .....	117
I.1.4	Caractéristiques.....	117
I.1.5	Utilisation du produit .....	117
I.1.6	Utilisateurs .....	117
I.2	Hypothèses.....	117
I.3	Revendications de conformité et déclaration de conformité .....	118
I.4	Définition du problème de sécurité.....	118
I.4.1	Actifs essentiels de l'environnement .....	118
I.4.2	Actifs essentiels de la ToE .....	119
I.4.3	Modèle de menaces .....	119
I.5	Objectifs de sécurité .....	120
I.6	Exigences de sécurité .....	120
I.6.1	Exigences fonctionnelles de sécurité .....	120
I.6.2	Exigences d'assurance de sécurité .....	121
Annexe J (informative)	Exigences relatives à l'équipement par niveau d'exposition .....	122
Annexe K (informative)	Établissement de références aux systèmes de management de la cybersécurité .....	124
Annexe L (informative)	Mapping avec les dispositions relatives aux exigences essentielles de cybersécurité des annexes du règlement européen sur la cyberrésilience .....	130
Bibliographie .....	133	
Figure 1 – Paysage normatif .....	11	
Figure 2 – Exemple d'interfaces physiques d'un dispositif intégré dans un équipement pouvant faire l'objet d'une attaque.....	23	
Figure 3 – Exemple de relation entre sécurité et sécurité humaine .....	24	
Figure 4 – Architecture du système de commande avec appareillages .....	29	