

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

# Maskinsikkerhed – Functional safety for sikkerhedsrelaterede styresystemer

Safety of machinery – Functional safety of safety-related control systems



**DANSK STANDARD**  
Danish Standards Association

Göteborg Plads 1  
DK-2150 Nordhavn  
Tel: +45 39 96 61 01  
[dansk.standard@ds.dk](mailto:dansk.standard@ds.dk)  
[www.ds.dk](http://www.ds.dk)

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

DS projekt: M333380  
ICS: 13.110; 25.040.99; 29.020

**Første del af denne publikations betegnelse er:**  
DS/EN IEC, hvilket betyder, at det er en international standard, der har status som europæisk og dansk standard.

**Denne publikations overensstemmelse er:**  
IDT med: IEC 62061:2021 ED2  
IDT med: EN IEC 62061:2021

DS-publikationen er på dansk og engelsk.

Denne publikation erstatter: [DS/EN 62061:2009](#), [DS/EN 62061/AC:2012](#), [DS/EN 62061/A1:2013](#), [DS/EN 62061:2005/A2:2015](#)

I tilfælde af tvivl om oversættelsens korrekthed henvises til den engelske version.

Der er i denne DS/EN IEC 62061:2021 indsat en DK-fodnote til tabel 9.

This DS/EN IEC 62061:2021 includes a DK footnote in Table 9.

---

### **DS-publikationstyper**

Dansk Standard udgiver forskellige publikationstyper.  
Typen på denne publikation fremgår af forsiden.

Der kan være tale om:

#### **Dansk standard**

- standard, der er udarbejdet på nationalt niveau, eller som er baseret på et andet lands nationale standard, eller
- standard, der er udarbejdet på internationalt og/eller europæisk niveau, og som har fået status som dansk standard

#### **DS-information**

- publikation, der er udarbejdet på nationalt niveau, og som ikke har opnået status som standard, eller
- publikation, der er udarbejdet på internationalt og/eller europæisk niveau, og som ikke har fået status som standard, fx en teknisk rapport, eller
- europæisk præstandard

#### **DS-håndbog**

- samling af standarder, eventuelt suppleret med informativt materiale

#### **DS-hæfte**

- publikation med informativt materiale

Til disse publikationstyper kan endvidere udgives

- tillæg og rettelsesblade

### **DS-publikationsform**

Publikationstyperne udgives i forskellig form som henholdsvis

- fuldttekstpublikation (publikationen er trykt i sin helhed)
- godkendelsesblad (publikationen leveres i kopi med et trykt DS-omslag)
- elektronisk (publikationen leveres på et elektronisk medie)

### **DS-betegnelse**

Alle DS-publikationers betegnelse begynder med DS efterfulgt af et eller flere præfikser og et nr., fx **DS 383**, **DS/EN 5414** osv. Hvis der efter nr. er angivet et **A** eller **Cor**, betyder det, enten at det er et **tillæg** eller et **rettelsesblad** til hovedstandard, eller at det er indført i hovedstandard.

DS-betegnelse angives på forsiden.

### **Overensstemmelse med anden publikation:**

Overensstemmelse kan enten være IDT, EQV, NEQ eller MOD

- **IDT:** Når publikationen er identisk med en given publikation.
- **EQV:** Når publikationen teknisk er i overensstemmelse med en given publikation, men præsentationen er ændret.
- **NEQ:** Når publikationen teknisk eller præsentationsmæssigt ikke er i overensstemmelse med en given standard, men udarbejdet på baggrund af denne.
- **MOD:** Når publikationen er modificeret i forhold til en given publikation.

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## EUROPÄISCHE NORM

July 2021

ICS 13.110; 25.040.99; 29.020

Supersedes EN 62061:2005 and all of its amendments  
and corrigenda (if any)

English Version

## Safety of machinery - Functional safety of safety-related control systems (IEC 62061:2021)

Sécurité des machines - Sécurité fonctionnelle des  
systèmes de commande relatifs à la sécurité  
(IEC 62061:2021)

Sicherheit von Maschinen - Funktionale Sicherheit  
sicherheitsbezogener Steuerungssysteme  
(IEC 62061:2021)

This European Standard was approved by CENELEC on 2021-04-26. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## Europæisk forord

Teksten i dokument 44/885/FDIS, den kommende 2. udgave af IEC 62061, som er udarbejdet af IEC/TC 44, Safety of machinery – Electrotechnical aspects, blev udsendt til parallel afstemning i IEC og CENELEC og godkendt af CENELEC som EN IEC 62061:2021.

Følgende datoer er fastsat:

- seneste dato, hvor dette dokument skal være implementeret nationalt ved publikation af en identisk national standard eller formel godkendelse (dop) 2022-01-26
- Seneste dato, hvor de nationale standarder, der er i modstrid med dette dokument, skal være trukket tilbage (dow) 2024-04-26

Dette dokument erstatter EN 62061:2005 og alle tilhørende tillæg og rettelserblade (hvis sådanne findes).

Der gøres opmærksom på, at indhold i dette dokument kan være underlagt patentrettigheder. CENELEC kan ikke drages til ansvar for at identificere sådanne patentrettigheder.

Dette dokument er udarbejdet af CENELEC i henhold til mandat fra Europa-Kommissionen og EFTA og understøtter væsentlige krav i et eller flere EU-direktiver.

Sammenhængen med ét eller flere EU-direktiver er angivet i det informative annekst ZZ, der er en integreret del af dette dokument.

Tilbagemeldinger og spørgsmål vedrørende dette dokument bør rettes til brugernes nationale komite. En fuldstændig liste over disse organisationer findes på CENELEC's hjemmeside.

## Godkendelse

Teksten i den Internationale Standard IEC 62061:2021 blev uden ændringer godkendt af CENELEC som Europæisk Standard.

I bibliografien i den officielle udgave skal følgende noter tilføjes for de angivne standarder:

IEC 60068(-serien)	NOTE	Harmoniseret som EN 60068(-serien)
IEC 60364-4-41:2005	NOTE	Harmoniseret som HD 60364-4-41:2017
IEC 60529	NOTE	Harmoniseret som EN 60529
IEC 60721(-serien)	NOTE	Harmoniseret som EN 60721-3-9:1993/A1(-serien)
IEC 60812	NOTE	Harmoniseret som EN ISO 60812
IEC 60947-4-1:2018	NOTE	Harmoniseret som EN IEC 60947-4-1:2019 (ikke ændret)
IEC 60947-5-1	NOTE	Harmoniseret som EN 60947-5-1
IEC 60947-5-3	NOTE	Harmoniseret som EN 60947-5-3
IEC 60947-5-5	NOTE	Harmoniseret som EN 60947-5-5
IEC 60947-5-8	NOTE	Harmoniseret som EN IEC 60947-5-8
IEC 61000-6-7	NOTE	Harmoniseret som EN 61000-6-7
IEC 61025:2006	NOTE	Harmoniseret som EN 61025:2007 (ikke ændret)
IEC 61131-2:2017	NOTE	Harmoniseret som EN 61131-2:2017 (ikke ændret), der skal udgives
IEC 61131-6:2012	NOTE	Harmoniseret som EN 61131-6:2012 (ikke ændret)

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

IEC 61140:2016	NOTE	Harmoniseret som EN 61140:2016 (ikke ændret)
IEC 61165	NOTE	Harmoniseret som EN 61165
IEC 61204-7:2016	NOTE	Harmoniseret som EN IEC 61204-7:2018 (ikke ændret)
IEC 61310(-serien)	NOTE	Harmoniseret som EN 61310(-serien)
IEC 61326-3-1	NOTE	Harmoniseret som EN 61326-3-1
IEC 61496(-serien)	NOTE	Harmoniseret som EN IEC 61496(-serien)
IEC 61508-1:2010	NOTE	Harmoniseret som EN 61508-1:2010 (ikke ændret)
IEC 61508-4:2010	NOTE	Harmoniseret som EN 61508-4:2010 (ikke ændret)
IEC 61508-5:2010	NOTE	Harmoniseret som EN 61508-5:2010 (ikke ændret)
IEC 61508-6:2010	NOTE	Harmoniseret som EN 61508-6:2010 (ikke ændret)
IEC 61508-7:2010	NOTE	Harmoniseret som EN 61508-7:2010 (ikke ændret)
IEC 61511(-serien)	NOTE	Harmoniseret som EN 61511(-serien)
IEC 61511-1:2016	NOTE	Harmoniseret som EN 61511-1:2017 (ikke ændret)
IEC 61511-1:2016/A1:2017	NOTE	Harmoniseret som EN 61511-1:2017/A1:2017 (ikke ændret)
IEC 61511-3:2016	NOTE	Harmoniseret som EN 61511-3:2017 (ikke ændret)
IEC 61649	NOTE	Harmoniseret som EN 61649
IEC 61709:2017	NOTE	Harmoniseret som EN 61709:2017 (ikke ændret)
IEC 61784-3(-serien)	NOTE	Harmoniseret som EN 61784-3(-serien)
IEC 61784-3:2016	NOTE	Harmoniseret som EN 61784-3:2016 (ikke ændret)
IEC 61800-5-2	NOTE	Harmoniseret som EN 61800-5-2
IEC 61810(-serien)	NOTE	Harmoniseret som EN 61810(-serien)
IEC 62443(-serien)	NOTE	Harmoniseret som EN IEC 62443(-serien)
IEC 62477(-serien)	NOTE	Harmoniseret som EN IEC 62477(-serien)
IEC 62502	NOTE	Harmoniseret som EN 62502
ISO/IEC 27001:2013	NOTE	Harmoniseret som EN ISO/IEC 27001:2017 (ikke ændret)
ISO 4413:2010	NOTE	Harmoniseret som EN ISO 4413:2010 (ikke ændret)
ISO 4414:2010	NOTE	Harmoniseret som EN ISO 4414:2010 (ikke ændret)
ISO 11161:2007	NOTE	Harmoniseret som EN ISO 11161:2007 (ikke ændret)
ISO 13850:2015	NOTE	Harmoniseret som EN ISO 13850:2015 (ikke ændret)
ISO 13851:2019	NOTE	Harmoniseret som EN ISO 13851:2019 (ikke ændret)
ISO 13855:2010	NOTE	Harmoniseret som EN ISO 13855:2010 (ikke ændret)
ISO 14118:2017	NOTE	Harmoniseret som EN ISO 14118:2018 (ikke ændret)
ISO 14119:2013	NOTE	Harmoniseret som EN ISO 14119:2013 (ikke ændret)
ISO/TR 22100-4:2018	NOTE	Harmoniseret som CEN ISO/TR 22100-4:2020 (ikke ændret)

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## Annex ZA (normativt)

### Normative referencer til internationale publikationer med de tilsvarende europæiske publikationer

Der er i teksten henvist til følgende dokumenter på en sådan måde, at noget eller alt indholdet udgør krav i dette dokument. For daterede referencer gælder kun den anførte udgave. For udaterede referencer gælder den nyeste udgave af det pågældende dokument (inklusive evt. tillæg).

NOTE 1 – Når en international publikation er ændret ved fælles ændringer, er dette angivet ved (mod), og den relevante EN/HD gælder.

NOTE 2 – Opdateret information om de nyeste udgaver af de Europæiske Standarder, der er anført i dette annex, kan fås her: [www.cenelec.eu](http://www.cenelec.eu).

<u>Publikation</u>	<u>Årstal</u>	<u>Titel</u>	<u>EN/HD</u>	<u>Årstal</u>
IEC 60204-1 (mod)	2016	Safety of machinery – Electrical equipment of machines – Part 1: General requirements	EN 60204-1	2018
IEC 61000-1-2	2016	Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena	EN 61000-1-2	2016
IEC 61508	serien	Functional safety of electrical/electronic/programmable electronic safety-related systems	EN 61508	serien
IEC 61508-2	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems	EN 61508-2	2010
IEC 61508-3	2010	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements	EN 61508-3	2010
ISO 12100	2010	Safety of machinery – General principles for design – Risk assessment and risk reduction	EN ISO 12100	2010
ISO 13849	serien	Safety of machinery – Safety-related parts of control systems	EN ISO 13849	serien
ISO 13849-1	2015	Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design	EN ISO 13849-1	2015
ISO 13849-2	2012	Safety of machinery – Safety-related parts of control systems – Part 2: Validation	EN ISO 13849-2	2012

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## Anneks ZZ (informativt)

### Sammenhæng mellem denne Europæiske Standard og de væsentlige krav i EU-direktiv 2006/42/EF [2006 OJ L 157], som efter hensigten skal være omfattet

Denne Europæiske Standard er udarbejdet i henhold til standardiseringsanmodning "M/396" fra Kommissionen for at tilvejebringe en frivillig metode til opfyldelse af væsentlige krav i Europa-Parlamentets og Rådets direktiv 2006/42/EF af 17. maj 2006 om maskinsikkerhed samt ændring af Direktiv 95/16/EF (omarbejdning) [2006 OJ L157].

Når denne standard er blevet omtalt i Den Europæiske Unions Tidende under dette direktiv, giver overensstemmelse med de normative punkter i denne standard, der er anført i tabel ZZ.1, en formodning om, at de tilsvarende væsentlige krav i det pågældende direktiv og tilsvarende EFTA-regulativer er opfyldt inden for denne standards anvendelsesområde.

**Tabel ZZ.1 – Sammenhæng mellem denne Europæiske Standard og bilag 1 til Direktiv 2006/42/EF [2006 OJ L 157]**

Væsentlige krav i Direktiv 2006/42/EF	Punkt(-er)/underpunkt(-er) i denne EN	Bemærkninger/noter
1.2.1	Pkt. 4, 5, 6, 7, 8, 9	
1.74.2 (e, g, i, r, s)	10.3	Dette underpunkt omhandler kun instruktionen vedrørende sikkerhedsfunktioner

**ADVARSEL 1:** Formodning om overensstemmelse er kun gyldig, så længe en henvisning til denne Europæiske Standard er anført i den liste, der er offentliggjort i Den Europæiske Unions Tidende. Brugere af denne standard bør hyppigt konsultere den nyeste liste, der er offentliggjort i Den Europæiske Unions Tidende.

**ADVARSEL 2:** Anden EU-lovgivning kan gælde for de produkter, som falder inden for denne standards anvendelsesområde.



# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

**Safety of machinery – Functional safety of safety-related control systems**

**Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité**



This is a preview of "DS/EN IEC 62061:2021". Click here to purchase the full version from the ANSI store.



**THIS PUBLICATION IS COPYRIGHT PROTECTED**

**Copyright © 2021 IEC, Geneva, Switzerland**

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

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

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

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

**About the IEC**

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

**About IEC publications**

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

**IEC publications search - [webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)**

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

**IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)**

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

**IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)**

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

**IEC online collection - [oc.iec.ch](http://oc.iec.ch)**

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

**Electropedia - [www.electropedia.org](http://www.electropedia.org)**

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

---

**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](http://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](http://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](http://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 online collection - [oc.iec.ch](http://oc.iec.ch)**

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

**Electropedia - [www.electropedia.org](http://www.electropedia.org)**

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



# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

---

**Safety of machinery – Functional safety of safety-related control systems**

**Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

---

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-9333-1

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

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## Indholdsfortegnelse

<b>FORORD</b> .....	8
<b>INDLEDNING</b> .....	10
<b>1 Anvendelsesområde</b> .....	11
<b>2 Normative referencer</b> .....	12
<b>3 Termer, definitioner og forkortelser</b> .....	13
3.1 Alfabetisk liste over definitioner .....	13
3.2 Termer og definitioner .....	15
3.3 Forkortelser .....	28
<b>4 Designprocessen for et SCS og functional safety-styring</b> .....	28
4.1 Formål .....	28
4.2 Designproces .....	29
4.3 Functional safety-styring ved hjælp af en functional safety-plan .....	31
4.4 Konfigurationsstyring .....	33
4.5 Ændring .....	33
<b>5 Specifikation af sikkerhedsfunktioner</b> .....	34
5.1 Formål .....	34
5.2 Specifikation af sikkerhedskrav (SRS) .....	34
5.2.1 Generelt .....	34
5.2.2 Oplysninger, der skal gives .....	34
5.2.3 Specifikation af funktionskrav .....	35
5.2.4 Vurdering af demand mode .....	35
5.2.5 Specifikation af sikkerhedsintegritetskrav .....	36
<b>6 Design af et SCS</b> .....	37
6.1 Generelt .....	37
6.2 Undersystemarkitektur baseret på top-down-nedbrydning .....	37
6.3 Grundlæggende metodik – Anvendelse af undersystemer .....	37
6.3.1 Generelt .....	37
6.3.2 Nedbrydning af SCS'et .....	38
6.3.3 Tilknytning til underfunktioner .....	39
6.3.4 Anvendelse af et præ-designet undersystem .....	39
6.4 Bestemmelse af SCS'ets sikkerhedsintegritet .....	40
6.4.1 Generelt .....	40
6.4.2 PFH .....	40
6.5 Krav til SCS'ets systematiske sikkerhedsintegritet .....	41
6.5.1 Krav til undgåelse af systematiske hardwarefunktionssvigt .....	41
6.5.2 Krav til styring af systematiske fejl .....	42
6.6 Elektromagnetisk immunitet .....	43
6.7 Softwarebaseret manuel parametrisering .....	43
6.7.1 Generelt .....	43
6.7.2 Påvirkning af sikkerhedsrelaterede parametre .....	43
6.7.3 Krav til softwarebaseret manuel parametrisering .....	44
6.7.4 Verifikation af parametriseringsværktøjet .....	45
6.7.5 Effektivitet i forbindelse med softwarebaseret manuel parametrisering .....	45
6.8 Sikkerhedsaspekter .....	45
6.9 Forhold vedrørende periodisk prøvning .....	46
<b>7 Udvikling og design af et undersystem</b> .....	46
7.1 Generelt .....	46

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

7.2	Design af undersystemarkitektur .....	47
7.3	Krav til valg og design af undersystemer og undersystemelementer.....	48
7.3.1	Generelt .....	48
7.3.2	Systematisk integritet .....	48
7.3.3	Fejlbetragtning og fejludelukkelse .....	51
7.3.4	Undersystemelementers funktionssvigtfrekvens.....	52
7.4	Undersystemers arkitekturmæssige begrænsninger .....	55
7.4.1	Generelt .....	55
7.4.2	Vurdering af andelen af ufarlige funktionssvigt ( <i>SFF</i> ) .....	56
7.4.3	SCS'ets opførsel ved detektion af en fejl i et undersystem.....	57
7.4.4	Realisering af diagnostiske funktioner .....	58
7.5	Arkitekturer til design af undersystemer.....	59
7.5.1	Generelt .....	59
7.5.2	Grundlæggende undersystemarkitekturer .....	59
7.5.3	Grundlæggende krav .....	61
7.6	Undersystemers <i>PFH</i> .....	62
7.6.1	Generelt .....	62
7.6.2	Metoder til vurdering af et undersystems <i>PFH</i> .....	62
7.6.3	Forenklet metode til vurdering af betydningen af fælles funktionssvigt med samme årsag ( <i>CCF</i> ) .....	62
<b>8</b>	<b>Software</b> .....	<b>62</b>
8.1	Generelt.....	62
8.2	Definition af softwareniveauer .....	63
8.3	Software – Niveau 1 .....	64
8.3.1	Softwareens sikkerhedslivscyklus – SW niveau 1 .....	64
8.3.2	Softwaredesign – SW-niveau 1 .....	65
8.3.3	Moduludvikling – SW-niveau 1 .....	67
8.3.4	Kodning – SW-niveau 1.....	67
8.3.5	Modultest – SW-niveau 1.....	68
8.3.6	Softwaretest – SW-niveau 1 .....	68
8.3.7	Dokumentation – SW-niveau 1 .....	69
8.3.8	Konfigurations- og ændringsstyringsprocessen – SW-niveau 1 .....	69
8.4	Softwareniveau 2.....	70
8.4.1	Softwareens sikkerhedslivscyklus – SW-niveau 2.....	70
8.4.2	Softwaredesign – SW-niveau 2.....	71
8.4.3	Softwaresystemudvikling – SW-niveau 2.....	73
8.4.4	Moduldesign – SW-niveau 2 .....	73
8.4.5	Kodning – SW-niveau 2.....	74
8.4.6	Modultest – SW-niveau 2.....	75
8.4.7	Softwareintegrationstest SW-niveau 2.....	75
8.4.8	Softwaretest – SW-niveau 2 .....	75
8.4.9	Dokumentation – SW-niveau 2 .....	76
8.4.10	Konfigurations- og ændringsstyringsprocessen – SW-niveau 2 .....	77
<b>9</b>	<b>Validering</b> .....	<b>77</b>
9.1	Valideringsprincipper.....	77
9.1.1	Valideringsplan .....	80
9.1.2	Anvendelse af lister over generiske fejl.....	80
9.1.3	Lister over specifikke fejl.....	80
9.1.4	Oplysninger til validering .....	81

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

9.1.5	Valideringsregistrering .....	81
9.2	Analyse som en del af valideringen.....	82
9.2.1	Generelt .....	82
9.2.2	Analyseteknikker.....	82
9.2.3	Verifikation af specifikationen af sikkerhedskrav (SRS).....	82
9.3	Prøvning som en del af valideringen.....	83
9.3.1	Generelt .....	83
9.3.2	Målenøjagtighed.....	83
9.3.3	Strengere krav.....	84
9.3.4	Prøveemner.....	84
9.4	Validering af sikkerhedsfunktionen.....	84
9.4.1	Generelt .....	84
9.4.2	Analyse og prøvning.....	85
9.5	Validering af SCS'ets sikkerhedsintegritet.....	85
9.5.1	Generelt .....	85
9.5.2	Validering af undersystem(-er) .....	85
9.5.3	Validering af foranstaltninger til imødegåelse af systematiske funktionssvigt .....	86
9.5.4	Validering af sikkerhedsrelateret software .....	86
9.5.5	Validering af kombination af sikkerhedsrelaterede undersystemer.....	87
<b>10</b>	<b>Dokumentation.....</b>	<b>87</b>
10.1	Generelt .....	87
10.2	Teknisk dokumentation.....	87
10.3	Brugervejledning til SCS'et.....	89
10.3.1	Generelt .....	89
10.3.2	Brugervejledninger udarbejdet af producenten af undersystemerne .....	89
10.3.3	Brugervejledning udarbejdet af SCS-integratoren .....	90
<b>Anneks A</b>	<b>(informativt) Bestemmelse af krævet sikkerhedsintegritet.....</b>	<b>92</b>
A.1	Generelt .....	92
A.2	Matrixtildeling for det krævede SIL-niveau .....	92
A.2.1	Identificering/angivelse af farer .....	92
A.2.2	Risikovurdering.....	92
A.2.3	Alvorlighed (Se) .....	93
A.2.4	Sandsynlighed for, at der sker skade.....	93
A.2.5	Kategori for skadesandsynlighed (CI) .....	96
A.2.6	Fastsættelse af SIL-niveau.....	96
<b>Anneks B</b>	<b>(informativt) Eksempel på metodik for design af SCS'er.....</b>	<b>99</b>
B.1	Generelt .....	99
B.2	Specifikation af sikkerhedskrav .....	99
B.3	Nedbrydning af sikkerhedsfunktionen.....	99
B.4	Design af SCS'et ved hjælp af undersystemer.....	100
B.4.1	Generelt .....	100
B.4.2	Design af undersystem 1 – "overvågning af afskærmningsdør" .....	100
B.4.3	Design af undersystem 2 – "vurderingslogik" .....	102
B.4.4	Design af undersystem 3 – "motorstyring" .....	103
B.4.5	Vurdering af SCS'et.....	103
B.4.6	PFH.....	104

This is a preview of "DS/EN IEC 62061:2021". Click here to purchase the full version from the ANSI store.

B.5	Verifikation .....	104
B.5.1	Generelt .....	104
B.5.2	Analyse .....	104
B.5.3	Prøvninger .....	105
<b>Anneks C</b>	<b>(informativt) Eksempler på <math>MTTF_D</math>-værdier for enkeltstående komponenter</b> .....	106
C.1	Generelt .....	106
C.2	Metode baseret på god teknisk praksis .....	106
C.3	Hydrauliske komponenter.....	106
C.4	Pneumatiske, mekaniske og elektromekaniske komponenters $MTTF_D$ .....	107
<b>Anneks D</b>	<b>(informativt) Eksempler på diagnostisk dækning (DC)</b> .....	109
<b>Anneks E</b>	<b>(informativt) Metode til vurdering af tilbøjelighed til fælles funktionssvigt med samme årsag (CCF)</b> .....	111
E.1	Generelt .....	111
E.2	Metodik .....	111
E.2.1	Krav til CCF .....	111
E.2.2	Vurdering af virkningen af CCF .....	111
<b>Anneks F</b>	<b>(informativt) Retningslinjer for softwareniveau 1</b> .....	114
F.1	Krav til softwaresikkerhed .....	114
F.2	Retningslinjer for kodning .....	115
F.3	Specifikation af sikkerhedsfunktioner .....	116
F.4	Specifikation af hardwaredesign .....	117
F.5	Specifikation af softwaresystemets design .....	119
F.6	Protokoller .....	121
<b>Anneks G</b>	<b>(informativt) Eksempler på sikkerhedsfunktioner</b> .....	124
<b>Anneks H</b>	<b>(informativt) Forenklede metoder til vurdering af et undersystems PFH-værdi</b> .....	125
H.1	Tabelfordelingsmetode .....	125
H.2	Forenklede formler til vurdering af $PFH$ .....	127
H.2.1	Generelt .....	127
H.2.2	Grundlæggende undersystemarkitektur A: Enkeltkanal uden diagnostisk funktion .....	127
H.2.3	Grundlæggende undersystemarkitektur B: Dobbeltkanal uden diagnostisk funktion .....	128
H.2.4	Grundlæggende undersystemarkitektur C: Enkeltkanal med diagnostisk funktion .....	128
H.2.5	Grundlæggende undersystemarkitektur D: Dobbeltkanal med én eller flere diagnostiske funktioner.....	133
H.3	Sammentællingsmetode .....	134
<b>Anneks I</b>	<b>(informativt) Functional safety-planen og designaktiviteterne</b> .....	135
I.1	Generelt .....	135
I.2	Eksempel på en maskines designplan, inklusive en sikkerhedsplan .....	135
I.3	Eksempel på aktiviteter, dokumenter og roller.....	135
<b>Anneks J</b>	<b>(informativt) Uafhængighed i forbindelse med gennemgange og prøvnings-/verifikations-/valideringsaktiviteter</b> .....	138
J.1	Softwaredesign.....	138
J.2	Validering.....	138
<b>Bibliografi</b>	.....	140

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

Figur 1 – Dette dokumentets anvendelsesområde.....	12
Figur 2 – Integration i risikonedsettelsesprocessen i ISO 12100 (uddrag) .....	29
Figur 3 – Iterativ proces i forbindelse med design af det sikkerhedsrelaterede styresystem .....	30
Figur 4 – Eksempel på en kombination af undersystemer, der udgør ét SCS.....	31
Figur 5 – Ved at aktivere en low demand sikkerhedsfunktion mindst én gang om året, kan den antages at være high demand .....	36
Figur 6 – Eksempler på typisk nedbrydning af en sikkerhedsfunktion i underfunktioner og funktionens tilknytning til undersystemer .....	39
Figur 7 – Eksempel på en sikkerhedsfunktions sikkerhedsintegritet baseret på tilknyttede undersystemer som ét SCS .....	40
Figur 8 – Undersystem A logisk afbildning .....	60
Figur 9 – Undersystem B logisk afbildning .....	60
Figur 10 – Undersystem C logisk afbildning .....	60
Figur 11 – Undersystem D logisk afbildning .....	61
Figur 12 – V-model for SW-niveau 1 .....	64
Figur 13 – V-model for softwaremoduler, som designeren har tilpasset SW-niveau 1 .....	64
Figur 14 – V-model for niveau 2-sofwarens sikkerhedslivscyklus. ....	70
Figur 15 – Oversigt over valideringsprocessen .....	79
Figur A.1 – Parametre anvendt ved risikovurdering .....	92
Figur A.2 – Eksempel på processen for fastsættelse af SIL-niveau .....	98
Figur B.1 – Nedbrydning af sikkerhedsfunktionen.....	100
Figur B.2 – Oversigt over design af SCS’ets undersystemer .....	100
Figur F.1 – Anlægstegning .....	116
Figur F.2 – Modularkitekturens overordnede design.....	119
Figur F.3 – Den primære designmetode til logisk vurdering .....	120
Figur F.4 – Eksempel på logisk illustration (programtegning).....	121
Figur H.1 – Undersystem A, logisk afbildning .....	127
Figur H.2 – Undersystem B, logisk afbildning .....	128
Figur H.3 – Undersystem C, logisk afbildning .....	128
Figur H.4 – Sammenhæng mellem undersystem C og den relevante fejlhåndteringsfunktion.....	129
Figur H.5 – Undersystem C med ekstern fejlhåndteringsfunktion.....	129
Figur H.6 – Undersystem C med ekstern fejlagnostik .....	131
Figur H.7 – Undersystem C med ekstern fejlreaktion .....	131
Figur H.8 – Undersystem C med intern fejlagnostik og intern fejlreaktion .....	131
Figur H.9 – Undersystem D, logisk afbildning .....	133
Figur I.1 – Eksempel på en maskines designplan, inklusive en sikkerhedsplan .....	135
Figur I.2 – Eksempel på aktiviteter, dokumenter og roller .....	136
Tabel 1 –Termer anvendt i IEC 62061 .....	13
Tabel 2 – Forkortelser anvendt i IEC 62061 .....	28
Tabel 3 – SIL-niveau og grænseværdier for <i>PFH</i> -værdier .....	36
Tabel 4 – Krævet SIL-niveau og <i>PFH</i> for et præ-designet undersystem .....	40
Tabel 5 – Relevant information for hvert undersystem .....	47

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

Tabel 6 – Et undersystems arkitekturmæssige begrænsninger: højeste SIL-niveau, som kan fordres for et SCS, der anvender undersystemet .....	56
Tabel 7 – Oversigt over grundlæggende krav og disses sammenhæng med grundlæggende undersystemarkitekturer.....	61
Tabel 8 – Forskellige niveauer af applikationssoftware .....	63
Tabel 9 – Dokumentation af SCS'er.....	88
Tabel A.1 – Klassifikation af skaders alvorlighed (Se).....	93
Tabel A.2 – Klassifikation af eksponeringsfrekvens og –varighed (Fr).....	94
Tabel A.3 – Klassifikation af sandsynlighed (Pr) .....	95
Tabel A.4 – Klassifikation af sandsynligheden for at undgå eller begrænse skade (Av) .....	96
Tabel A.5 – Parametre anvendt til at bestemme kategori for skadesandsynlighed (Cl).....	96
Tabel A.6 – Matrix til bestemmelse af det krævede SIL-niveau (eller PL <sub>r</sub> ) for en sikkerhedsfunktion.....	97
Tabel B.1 – Specifikation af sikkerhedskrav – eksempel på oversigt .....	99
Tabel B.2 – Systematisk integritet – eksempel på oversigt .....	104
Tabel B.3 – Verifikation ved prøvning .....	105
Tabel C.1 – Standardreferencer og $MTTF_D$ - eller $B_{10D}$ -værdier for komponenter.....	107
Tabel D.1 – Vurderinger af diagnostisk dækning (DC) (1 af 2) .....	109
Tabel E.1 – Kriterier for vurdering af CCF.....	112
Tabel E.2 – Kriterier for vurdering af CCF.....	113
Tabel F.1 – Eksempel på relevante dokumenter i forbindelse med den forenklede V-model.....	114
Tabel F.2 – Eksempler på retningslinjer for kodning.....	115
Tabel F.3 – Specificerede sikkerhedsfunktioner .....	117
Tabel F.4 – Relevant liste over input- og outputsignaler .....	118
Tabel F.5 – Eksempel på forenklet årsags- og virkningsmatrix .....	121
Tabel F.6 – Verifikation af specifikation af softwaresystemets design .....	122
Tabel F.7 – Gennemgang af softwarekode.....	122
Tabel F.8 – Softwarevalidering.....	123
Tabel G. – Eksempler på typiske sikkerhedsfunktioner .....	124
Tabel H.1 – Tildeling af $PFH$ -værdi til et undersystem .....	126
Tabel H.2 – Forholdet mellem $B_{10D}$ , drift og $MTTF_D$ .....	127
Tabel H.3 – Minimumværdi på $1/\lambda_{DFH}$ for anvendeligheden af $PFH$ -ligning (H.4).....	132
Tabel J.1 – Minimumniveauer for uafhængighed i forbindelse med gennemgang, prøvning og verifikation .....	138
Tabel J.2 – Minimumniveau af uafhængighed ved validering.....	138



## MASKINSIKKERHED –

### Functional safety i sikkerhedsrelaterede styresystemer

#### FORORD

- 1) IEC (International Electrotechnical Commission) er en verdensomspændende standardiseringsorganisation bestående af alle nationale elektrotekniske komiteer (nationale IEC-komiteer). IEC's formål er at fremme internationalt samarbejde inden for alle områder vedrørende standardisering på det elektriske og elektrotekniske område. Med dette for øje og som et supplement til andre aktiviteter udgiver IEC Internationale Standarder, Tekniske Specifikationer, Tekniske Rapporter, Offentligt Tilgængelige Specifikationer (PAS) og Vejledninger (i det følgende omtalt som "IEC-publikation(er)"). Udarbejdelsen varetages af tekniske komiteer. Enhver national IEC-komite, der har interesse i det behandlede emne, kan deltage i det forberedende arbejde. Internationale, statslige og ikke-statslige organisationer, der har en samarbejdsaftale med IEC, deltager ligeledes i dette arbejde. IEC har et tæt samarbejde med ISO (International Organization for Standardization) i henhold til betingelser, der er fastlagt ved aftale mellem de to organisationer.
- 2) IEC's formelle beslutninger eller aftaler om tekniske spørgsmål udtrykker så vidt muligt international konsensus om de pågældende emner, da alle interesserede nationale IEC-komiteer er repræsenteret i hver teknisk komite.
- 3) IEC-publikationer antager form af anbefalinger, der kan anvendes internationalt, og er godkendt af de nationale IEC-komiteer som sådanne. Selvom der træffes alle rimelige forholdsregler for at sikre, at det tekniske indhold i IEC-publikationer er nøjagtigt, kan IEC ikke gøres ansvarlig for den måde, hvorpå de anvendes, eller for fejlfortolkning af en slutbruger.
- 4) For at fremme international ensartethed forpligter de nationale IEC-komiteer sig til i videst muligt omfang at anvende IEC-publikationer på en gennemskuelig måde i deres nationale og regionale publikationer. Der skal i nationale eller regionale publikationer gøres tydeligt opmærksom på eventuelle afvigelser fra en IEC-publikation.
- 5) IEC udfører ikke selv attestering af overensstemmelse. Uafhængige certificeringsorganer udfører overensstemmelsesvurderingsydelser og giver i nogle tilfælde adgang til IEC-overensstemmelsesmærker. IEC er ikke ansvarlig for serviceydelser udført af uafhængige certificeringsorganer.
- 6) Alle brugere bør sikre, at de har den seneste udgave af denne publikation.
- 7) Der kan ikke gøres erstatningsansvar gældende over for IEC eller organisationens ledende medarbejdere, øvrige medarbejdere og ansatte eller andre befuldmægtigede, herunder eksperter og medlemmer af IEC's tekniske komiteer og nationale IEC-komiteer, for personskade, tingskade eller en hvilken som helst anden skade, hvad enten den er direkte eller indirekte, eller for omkostninger (herunder advokatsalærer) og udgifter som følge af offentliggørelse, anvendelse eller under påberåbelse af denne IEC-publikation eller andre IEC-publikationer.
- 8) Opmærksomheden henledes på de normative referencer, der er anført i denne publikation. Det er nødvendigt for korrekt brug af denne publikation at anvende de publikationer, der er henvist til.
- 9) Der gøres opmærksom på, at indhold i denne IEC-publikation kan være underlagt patentrettigheder. IEC kan ikke drages til ansvar for at identificere sådanne patentrettigheder.

IEC 62061 er udarbejdet af IEC teknisk komite 44: Safety of machinery – Electrotechnical aspects. IEC 62061 er en International Standard.

Denne 2. udgave ophæver og erstatter 1. udgave fra 2005, tillæg 1:2012 og tillæg 2:2015. Denne udgave er en teknisk revision.

Denne udgave indeholder følgende væsentlige tekniske ændringer i forhold til den tidligere udgave:

- opbygningen er ændret, og indholdet er opdateret, så det afspejler sikkerhedsfunktionens designproces
- standarden er udvidet, så den også omfatter ikke-elektriske teknologier
- definitionerne er opdateret, så de er passer til IEC 61508-4
- der er tilføjet en functional safety-plan, og konfigurationsstyringen er opdateret (pkt. 4)
- kravene til parametrisering er skærpet (pkt. 6)
- der er tilføjet en henvisning til krav til sikring (6.8)

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

- der er tilføjet krav om periodisk prøvning (6.9)
- der er foretaget forskellige forbedringer og en tydeliggørelse af arkitekturer og pålidelighedsberegninger (pkt. 6 og 7)
- "SILCL" er ændret til "maksimalt SIL-niveau" for undersystemer (pkt. 7)
- use cases for software er beskrevet, herunder krav (pkt. 8)
- der er tilføjet krav om uafhængighed i forbindelse med verifikation af software (pkt. 8) og om valideringsaktiviteter (pkt. 9)
- der er tilføjet et nyt informativt anneks med eksempler (anneks G)
- der er tilføjet nye informative annekser om typiske  $MTTF_D$ -værdier, diagnostik og beregningsmetoder for arkitekturerne (anneks C, anneks D og anneks H).

Teksten i denne Internationale Standard er baseret på følgende IEC-dokumenter:

Udkast	Afstemningsrapport
44/885/FDIS	44/888/RVD

De samlede oplysninger om afstemningen om godkendelse af denne standard kan findes i afstemningsrapporten anført i tabellen ovenfor.

Det sprog, der er anvendt i forbindelse med udviklingen af denne Internationale Standard, er engelsk.

Dette dokument er udarbejdet i overensstemmelse med ISO/IEC Directives, Part 2 og er udarbejdet i overensstemmelse med ISO/IEC Directives, Part 1 og ISO/IEC Directives, IEC Supplement, der er tilgængelige på [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs). De vigtigste dokumenttyper, der udvikles af IEC, er mere detaljeret beskrevet på [www.iec.ch/standardsdev/publications](http://www.iec.ch/standardsdev/publications).

Komiteen har besluttet, at denne publikations indhold forbliver uændret indtil den såkaldte "stability date", som er angivet på IEC's website under "<http://webstore.iec.ch>" i de data, der vedrører den pågældende publikation. På dette tidspunkt vil publikationen blive

- genbekræftet
- trukket tilbage
- erstattet af en revideret udgave eller
- ændret.

**VIGTIGT – Logoet for 'farve i dokumentet' på titelbladet på denne publikation angiver, at den indeholder farver, der anses for at være nyttige for korrekt forståelse af indholdet. Brugere bør derfor udskrive dette dokument på en farveprinter.**

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## INDLEDNING

Som resultat af automatisering, krav om øget produktion og lavere fysiske krav til operatøren spiller maskiners sikkerhedsrelaterede styresystemer (i det følgende benævnt SCS) en større rolle for opnåelse af en overordnet maskinsikkerhed. Derudover anvender SCS'er i stigende grad selv komplekse elektronisk teknologi.

I IEC 62061 specificeres kravene til design og implementering af sikkerhedsrelaterede styresystemer i maskineri. Dette dokument er maskinsektorspecifikt inden for rammerne af IEC 61508.

NOTE – Selvom der i IEC 62061 og ISO 13849-1 anvendes forskellige metoder til design af sikkerhedsrelaterede styresystemer, tager de sigte på at opnå samme risikonedsættelse.

Denne Internationale Standard er beregnet til at blive anvendt af maskindesignere og producenter og integratorer af styresystemer og andre, som er involveret i specifikation, design og validering af SCS'er. I den opstilles en metode og stilles krav for at opnå den nødvendige ydeevne, og den fremmer specifikationen af de sikkerhedsfunktioner, der har til formål at nedsætte risikoen.

Dette dokument indeholder maskinsektorspecifikke rammer for functional safety for maskiners SCS'er. Det dækker kun de aspekter i sikkerhedslivscyklussen, som er relateret til de stillede sikkerhedskrav frem til sikkerhedsvalidering. Der stilles krav om information om sikker anvendelse af maskiners SCS'er, information kan også blive relevant i senere faser af SCS'ers levetid.

Der er mange maskinsituationer, hvor SCS'er er en del af de sikkerhedsforanstaltninger, der har til formål at nedsætte risikoen. Et typisk eksempel er anvendelse af en tvangskoblet beskyttelsesforanstaltning, som, når den åbnes og tillader adgang i farezonen, giver signal til sikkerhedsrelaterede dele af maskinstyresystemet om at standse maskinens farlige drift. I forbindelse med automatisering bidrager maskinstyresystemet, som anvendes til at sikre, at maskinprocessen forløber korrekt, ofte til sikkerheden ved at nedsætte den risiko, der er forbundet med farer, der stammer direkte fra funktionssvigt i styresystemet. Dette dokument indeholder en fremgangsmåde og krav til at

- tildele den krævede sikkerhedsintegritet til hver sikkerhedsfunktion, der skal implementeres af SCS'et(-erne)
- gøre det muligt at designe det eller de egnede SCS'er, der passer til den eller de tildelte sikkerheds(kontrol)funktioner
- integrere sikkerhedsrelaterede undersystemer, der er designet i overensstemmelse med andre gældende functional safety-relaterede standarder (se 6.3.4)
- validere SCS'et(-erne).

Dette dokument er beregnet til at blive anvendt inden for rammerne af systematisk risikonedsættelse sammen med risikovurdering som beskrevet i ISO 12100. Forslag til metoder til tildeling af sikkerhedsintegritet er angivet i det informative anneks A.

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## MASKINSIKKERHED –

### Functional safety i sikkerhedsrelaterede styresystemer

## 1 Anvendelsesområde

Denne Internationale Standard fastsætter krav og giver anbefalinger til design, integration og validering af sikkerhedsrelaterede styresystemer (SCS) til maskiner. Den gælder for styresystemer, der anvendes enten enkeltvis eller i kombination til at udføre sikkerhedsfunktioner på maskiner, der ikke kan bæres i hånden under drift, herunder en gruppe af maskiner, der arbejder sammen på en koordineret måde.

Dette dokument er en maskinsektorspecifik standard inden for rammerne af IEC 61508 (alle dele).

Design af komplekse programmerbare elektroniske undersystemer eller undersystemelementer er ikke omfattet af dette dokument's anvendelsesområde. Disse emner er omfattet af anvendelsesområdet for IEC 61508 eller dermed forbundne standarder, se figur 1.

NOTE 1 – Elementer som fx systemer på chip- eller mikrocontrollerplader betragtes som komplekse programmerbare elektroniske undersystemer.

Den centrale del af denne sektorstandard indeholder generelle krav til design og verifikation af et sikkerhedsrelateret styresystem beregnet til anvendelse i high demand/continuous demand mode.

Dette dokument

- vedrører kun functional safety-krav, der har til formål at nedsætte risikoen i forbindelse med farlige situationer
- er begrænset til risici, der opstår direkte som følge af farerne ved selve maskinen eller fra en gruppe af maskiner, der arbejder sammen på en koordineret måde

NOTE 2 – Relevante sektorstandarder indeholder krav, der har til formål at nedsætte risici som følge af andre farer. For eksempel indeholder IEC 61511 yderligere information om situationer, hvor én eller flere maskiner er en del af en procesaktivitet.

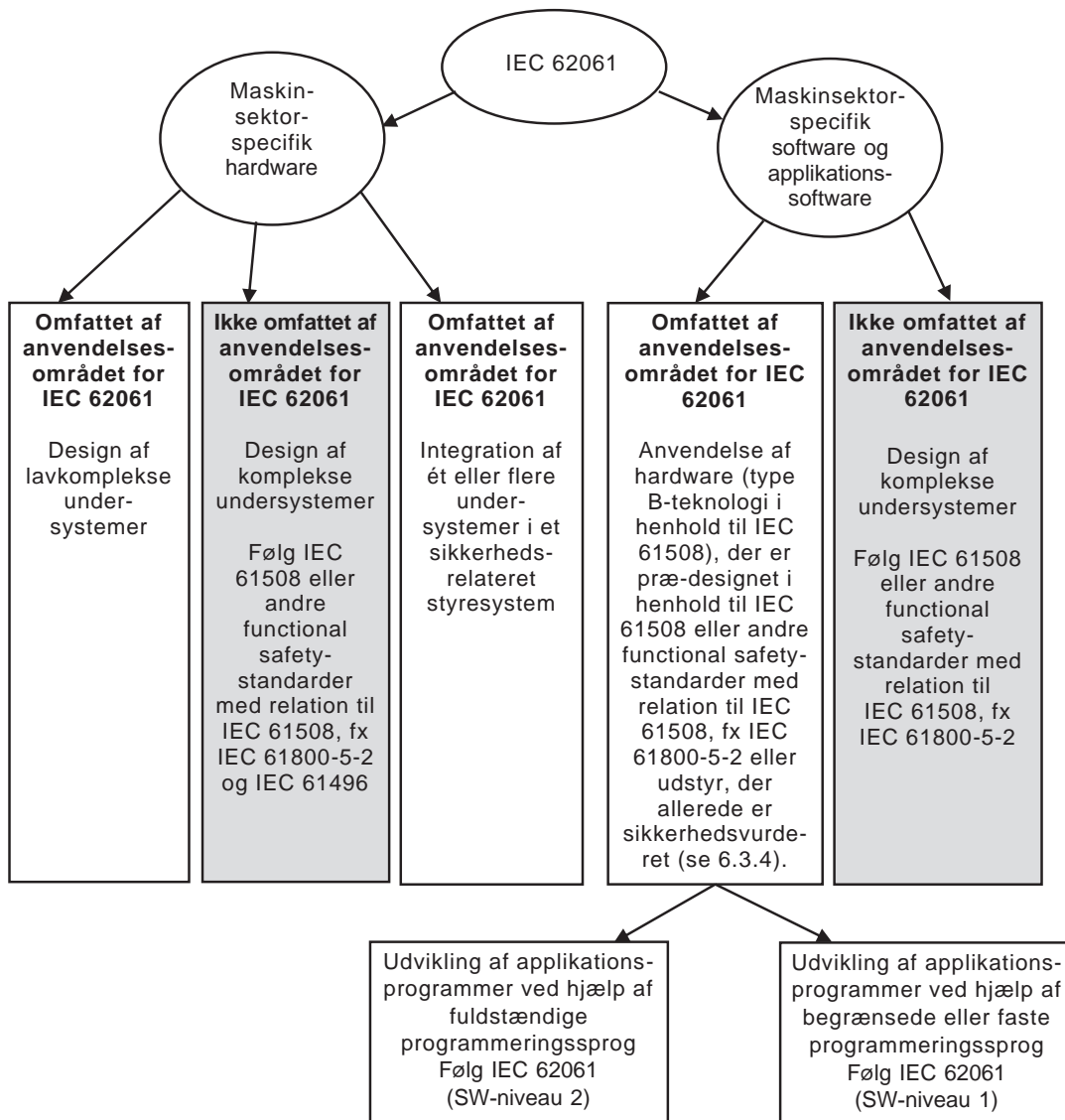
Dette dokument omfatter ikke

- elektriske farer, der opstår på grund af selve det elektriske styreudstyr (fx elektrisk stød – se IEC 60204-1)
- andre sikkerhedskrav, der er nødvendige på maskinniveau, som fx beskyttelsesforanstaltninger
- specifikke foranstaltninger vedrørende sikringsaspekter – se IEC TR 63074.

Dette dokument har ikke til formål at begrænse eller hindre teknologiske fremskridt.

Figur 1 illustrerer anvendelsesområdet for dette dokument.

This is a preview of "DS/EN IEC 62061:2021". Click here to purchase the full version from the ANSI store.



Figur 1 – Dette dokumentets anvendelsesområde

## 2 Normative referencer

Der er i teksten henvist til følgende dokumenter på en sådan måde, at noget eller alt indholdet udgør krav i dette dokument. For daterede referencer gælder kun den anførte udgave. For udaterede referencer gælder den nyeste udgave af det pågældende dokument (inklusive evt. tillæg).

IEC 60204-1:2016, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-1-2:2016, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61508 (alle dele), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

ISO 12100:2010, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

ISO 13849 (alle dele), *Safety of machinery – Safety-related parts of control systems*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)



Edition 2.0 2021-03

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

**Safety of machinery – Functional safety of safety-related control systems**

**Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité**

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)



**THIS PUBLICATION IS COPYRIGHT PROTECTED**  
**Copyright © 2021 IEC, Geneva, Switzerland**

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

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

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

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

**About the IEC**

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

**About IEC publications**

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

**IEC publications search - [webstore.iec.ch/advsearchform](http://webstore.iec.ch/advsearchform)**

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

**IEC Just Published - [webstore.iec.ch/justpublished](http://webstore.iec.ch/justpublished)**

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

**IEC Customer Service Centre - [webstore.iec.ch/csc](http://webstore.iec.ch/csc)**

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

**IEC online collection - [oc.iec.ch](http://oc.iec.ch)**

Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

**Electropedia - [www.electropedia.org](http://www.electropedia.org)**

The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 18 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

---

**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](http://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](http://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](http://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 online collection - [oc.iec.ch](http://oc.iec.ch)**

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

**Electropedia - [www.electropedia.org](http://www.electropedia.org)**

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



This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)



Edition 2.0 2021-03

# INTERNATIONAL STANDARD

# NORME INTERNATIONALE

**Safety of machinery – Functional safety of safety-related control systems**

**Sécurité des machines – Sécurité fonctionnelle des systèmes de commande relatifs à la sécurité**

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

COMMISSION  
ELECTROTECHNIQUE  
INTERNATIONALE

ICS 13.110; 25.040.99; 29.020

ISBN 978-2-8322-9333-1

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

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

CONTENTS

FOREWORD..... 8

INTRODUCTION..... 10

1 Scope..... 11

2 Normative references ..... 12

3 Terms, definitions and abbreviations ..... 13

    3.1 Alphabetical list of definitions..... 13

    3.2 Terms and definitions..... 15

    3.3 Abbreviations..... 28

4 Design process of an SCS and management of functional safety ..... 28

    4.1 Objective ..... 28

    4.2 Design process ..... 29

    4.3 Management of functional safety using a functional safety plan ..... 31

    4.4 Configuration management ..... 33

    4.5 Modification ..... 33

5 Specification of a safety function ..... 34

    5.1 Objective ..... 34

    5.2 Safety requirements specification (SRS) ..... 34

        5.2.1 General ..... 34

        5.2.2 Information to be available..... 34

        5.2.3 Functional requirements specification ..... 35

        5.2.4 Estimation of demand mode of operation ..... 35

        5.2.5 Safety integrity requirements specification..... 36

6 Design of an SCS ..... 37

    6.1 General..... 37

    6.2 Subsystem architecture based on top down decomposition ..... 37

    6.3 Basic methodology – Use of subsystem ..... 37

        6.3.1 General ..... 37

        6.3.2 SCS decomposition ..... 38

        6.3.3 Sub-function allocation ..... 39

        6.3.4 Use of a pre-designed subsystem ..... 39

    6.4 Determination of safety integrity of the SCS..... 40

        6.4.1 General ..... 40

        6.4.2 PFH..... 40

    6.5 Requirements for systematic safety integrity of the SCS ..... 41

        6.5.1 Requirements for the avoidance of systematic hardware failures ..... 41

        6.5.2 Requirements for the control of systematic faults..... 42

    6.6 Electromagnetic immunity ..... 43

    6.7 Software based manual parameterization..... 43

        6.7.1 General ..... 43

        6.7.2 Influences on safety-related parameters ..... 43

        6.7.3 Requirements for software based manual parameterization ..... 44

        6.7.4 Verification of the parameterization tool..... 45

        6.7.5 Performance of software based manual parameterization ..... 45

    6.8 Security aspects ..... 45

    6.9 Aspects of periodic testing ..... 46

7 Design and development of a subsystem ..... 46

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

7.1	General.....	46
7.2	Subsystem architecture design .....	47
7.3	Requirements for the selection and design of subsystem and subsystem elements .....	48
7.3.1	General .....	48
7.3.2	Systematic integrity .....	48
7.3.3	Fault consideration and fault exclusion .....	51
7.3.4	Failure rate of subsystem element .....	52
7.4	Architectural constraints of a subsystem .....	55
7.4.1	General .....	55
7.4.2	Estimation of safe failure fraction ( <i>SFF</i> ) .....	56
7.4.3	Behaviour (of the SCS) on detection of a fault in a subsystem .....	57
7.4.4	Realization of diagnostic functions.....	58
7.5	Subsystem design architectures.....	59
7.5.1	General .....	59
7.5.2	Basic subsystem architectures.....	59
7.5.3	Basic requirements .....	61
7.6	<i>PFH</i> of subsystems .....	62
7.6.1	General .....	62
7.6.2	Methods to estimate the <i>PFH</i> of a subsystem .....	62
7.6.3	Simplified approach to estimation of contribution of common cause failure ( <i>CCF</i> ).....	62
8	Software.....	62
8.1	General.....	62
8.2	Definition of software levels .....	63
8.3	Software – Level 1 .....	64
8.3.1	Software safety lifecycle – SW level 1 .....	64
8.3.2	Software design – SW level 1 .....	65
8.3.3	Module design – SW level 1.....	67
8.3.4	Coding – SW level 1 .....	67
8.3.5	Module test – SW level 1 .....	68
8.3.6	Software testing – SW level 1 .....	68
8.3.7	Documentation – SW level 1.....	69
8.3.8	Configuration and modification management process – SW level 1 .....	69
8.4	Software level 2 .....	70
8.4.1	Software safety lifecycle – SW level 2 .....	70
8.4.2	Software design – SW level 2 .....	71
8.4.3	Software system design – SW level 2 .....	73
8.4.4	Module design – SW level 2.....	73
8.4.5	Coding – SW level 2 .....	74
8.4.6	Module test – SW level 2 .....	75
8.4.7	Software integration testing SW level 2.....	75
8.4.8	Software testing SW level 2.....	75
8.4.9	Documentation – SW level 2.....	76
8.4.10	Configuration and modification management process – SW level 2.....	77
9	Validation .....	77
9.1	Validation principles.....	77
9.1.1	Validation plan.....	80
9.1.2	Use of generic fault lists .....	80

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

9.1.3	Specific fault lists .....	80
9.1.4	Information for validation .....	81
9.1.5	Validation record .....	81
9.2	Analysis as part of validation .....	82
9.2.1	General .....	82
9.2.2	Analysis techniques .....	82
9.2.3	Verification of safety requirements specification (SRS) .....	82
9.3	Testing as part of validation .....	83
9.3.1	General .....	83
9.3.2	Measurement accuracy .....	83
9.3.3	More stringent requirements .....	84
9.3.4	Test samples .....	84
9.4	Validation of the safety function .....	84
9.4.1	General .....	84
9.4.2	Analysis and testing.....	85
9.5	Validation of the safety integrity of the SCS .....	85
9.5.1	General .....	85
9.5.2	Validation of subsystem(s).....	85
9.5.3	Validation of measures against systematic failures .....	86
9.5.4	Validation of safety-related software .....	86
9.5.5	Validation of combination of subsystems .....	87
10	Documentation .....	87
10.1	General.....	87
10.2	Technical documentation .....	87
10.3	Information for use of the SCS .....	89
10.3.1	General .....	89
10.3.2	Information for use given by the manufacturer of subsystems .....	89
10.3.3	Information for use given by the SCS integrator .....	90
Annex A (informative)	Determination of required safety integrity .....	92
A.1	General.....	92
A.2	Matrix assignment for the required SIL.....	92
A.2.1	Hazard identification/indication .....	92
A.2.2	Risk estimation .....	92
A.2.3	Severity (Se) .....	93
A.2.4	Probability of occurrence of harm .....	93
A.2.5	Class of probability of harm (Cl).....	96
A.2.6	SIL assignment.....	96
A.3	Overlapping hazards .....	98
Annex B (informative)	Example of SCS design methodology .....	99
B.1	General.....	99
B.2	Safety requirements specification .....	99
B.3	Decomposition of the safety function.....	99
B.4	Design of the SCS by using subsystems .....	100
B.4.1	General .....	100
B.4.2	Subsystem 1 design – “guard door monitoring” .....	100
B.4.3	Subsystem 2 design – “evaluation logic” .....	102
B.4.4	Subsystem 3 design – “motor control” .....	103
B.4.5	Evaluation of the SCS.....	103
B.4.6	PFH.....	104

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

B.5	Verification.....	104
B.5.1	General .....	104
B.5.2	Analysis.....	104
B.5.3	Tests .....	105
Annex C (informative)	Examples of $MTTF_D$ values for single components .....	106
C.1	General.....	106
C.2	Good engineering practices method.....	106
C.3	Hydraulic components.....	106
C.4	$MTTF_D$ of pneumatic, mechanical and electromechanical components.....	107
Annex D (informative)	Examples for diagnostic coverage ( $DC$ ).....	109
Annex E (informative)	Methodology for the estimation of susceptibility to common cause failures (CCF).....	111
E.1	General.....	111
E.2	Methodology .....	111
E.2.1	Requirements for CCF .....	111
E.2.2	Estimation of effect of CCF .....	111
Annex F (informative)	Guideline for software level 1 .....	114
F.1	Software safety requirements.....	114
F.2	Coding guidelines .....	115
F.3	Specification of safety functions.....	116
F.4	Specification of hardware design .....	117
F.5	Software system design specification.....	119
F.6	Protocols .....	121
Annex G (informative)	Examples of safety functions.....	124
Annex H (informative)	Simplified approaches to evaluate the $PFH$ value of a subsystem .....	125
H.1	Table allocation approach .....	125
H.2	Simplified formulas for the estimation of $PFH$ .....	127
H.2.1	General .....	127
H.2.2	Basic subsystem architecture A: single channel without a diagnostic function .....	127
H.2.3	Basic subsystem architecture B: dual channel without a diagnostic function .....	128
H.2.4	Basic subsystem architecture C: single channel with a diagnostic function .....	128
H.2.5	Basic subsystem architecture D: dual channel with a diagnostic function(s) .....	133
H.3	Parts count method.....	134
Annex I (informative)	The functional safety plan and design activities .....	135
I.1	General.....	135
I.2	Example of a machine design plan including a safety plan .....	135
I.3	Example of activities, documents and roles.....	135
Annex J (informative)	Independence for reviews and testing/verification/validation activities .....	138
J.1	Software design .....	138
J.2	Validation.....	138
Bibliography	.....	140
Figure 1 – Scope of this document	.....	12

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

Figure 2 – Integration within the risk reduction process of ISO 12100 (extract) .....	29
Figure 3 – Iterative process for design of the safety-related control system .....	30
Figure 4 – Example of a combination of subsystems as one SCS.....	31
Figure 5 – By activating a low demand safety function at least once per year it can be assumed to be high demand .....	36
Figure 6 – Examples of typical decomposition of a safety function into sub-functions and its allocation to subsystems .....	39
Figure 7 – Example of safety integrity of a safety function based on allocated subsystems as one SCS .....	40
Figure 8 – Subsystem A logical representation .....	60
Figure 9 – Subsystem B logical representation .....	60
Figure 10 – Subsystem C logical representation .....	60
Figure 11 – Subsystem D logical representation .....	61
Figure 12 – V-model for SW level 1.....	64
Figure 13 – V-model for software modules customized by the designer for SW level 1 .....	64
Figure 14 – V-model of software safety lifecycle for SW level 2.....	70
Figure 15 – Overview of the validation process .....	79
Figure A.1 – Parameters used in risk estimation .....	92
Figure A.2 – Example proforma for SIL assignment process .....	98
Figure B.1 – Decomposition of the safety function.....	100
Figure B.2 – Overview of design of the subsystems of the SCS .....	100
Figure F.1 – Plant sketch .....	116
Figure F.2 – Principal module architecture design.....	119
Figure F.3 – Principal design approach of logical evaluation .....	120
Figure F.4 – Example of logical representation (program sketch) .....	121
Figure H.1 – Subsystem A logical representation .....	127
Figure H.2 – Subsystem B logical representation .....	128
Figure H.3 – Subsystem C logical representation.....	128
Figure H.4 – Correlation of subsystem C and the pertinent fault handling function .....	129
Figure H.5 – Subsystem C with external fault handling function .....	129
Figure H.6 – Subsystem C with external fault diagnostics .....	131
Figure H.7 – Subsystem C with external fault reaction .....	131
Figure H.8 – Subsystem C with internal fault diagnostics and internal fault reaction.....	131
Figure H.9 – Subsystem D logical representation.....	133
Figure I.1 – Example of a machine design plan including a safety plan .....	135
Figure I.2 – Example of activities, documents and roles .....	136
Table 1 – Terms used in IEC 62061 .....	13
Table 2 – Abbreviations used in IEC 62061.....	28
Table 3 – SIL and limits of <i>PFH</i> values.....	36
Table 4 – Required SIL and <i>PFH</i> of pre-designed subsystem .....	40
Table 5 – Relevant information for each subsystem .....	47
Table 6 – Architectural constraints on a subsystem: maximum SIL that can be claimed for an SCS using the subsystem .....	56

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

Table 7 – Overview of basic requirements and interrelation to basic subsystem architectures .....	61
Table 8 – Different levels of application software .....	63
Table 9 – Documentation of an SCS .....	88
Table A.1 – Severity (Se) classification .....	93
Table A.2 – Frequency and duration of exposure (Fr) classification .....	94
Table A.3 – Probability (Pr) classification .....	95
Table A.4 – Probability of avoiding or limiting harm (Av) classification .....	96
Table A.5 – Parameters used to determine class of probability of harm (Cl) .....	96
Table A.6 – Matrix assignment for determining the required SIL (or PL <sub>r</sub> ) for a safety function .....	97
Table B.1 – Safety requirements specification – example of overview .....	99
Table B.2 – Systematic integrity – example of overview .....	104
Table B.3 – Verification by tests .....	105
Table C.1 – Standards references and $MTTF_D$ or $B_{10D}$ values for components .....	107
Table D.1 – Estimates for diagnostic coverage ( $DC$ ) .....	109
Table E.1 – Criteria for estimation of CCF .....	112
Table E.2 – Criteria for estimation of CCF .....	113
Table F.1 – Example of relevant documents related to the simplified V-model .....	114
Table F.2 – Examples of coding guidelines .....	115
Table F.3 – Specified safety functions .....	117
Table F.4 – Relevant list of input and output signals .....	118
Table F.5 – Example of simplified cause and effect matrix .....	121
Table F.6 – Verification of software system design specification .....	122
Table F.7 – Software code review .....	122
Table F.8 – Software validation .....	123
Table G.1 – Examples of typical safety functions .....	124
Table H.1 – Allocation of $PFH$ value of a subsystem .....	126
Table H.2 – Relationship between $B_{10D}$ , operations and $MTTF_D$ .....	127
Table H.3 – Minimum value of $1/\lambda_D F_H$ for the applicability of $PFH$ equation (H.4) .....	132
Table J.1 – Minimum levels of independence for review, testing and verification activities .....	138
Table J.2 – Minimum levels of independence for validation activities .....	138

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**SAFETY OF MACHINERY –  
FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS**

FOREWORD

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

IEC 62061 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects. It is an International Standard.

This second edition cancels and replaces the first edition, published in 2005, Amendment 1:2012 and Amendment 2:2015. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- structure has been changed and contents have been updated to reflect the design process of the safety function,
- standard extended to non-electrical technologies,
- definitions updated to be aligned with IEC 61508-4,
- functional safety plan introduced and configuration management updated (Clause 4),
- requirements on parametrization expanded (Clause 6),
- reference to requirements on security added (Subclause 6.8),
- requirements on periodic testing added (Subclause 6.9),



This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

- various improvements and clarification on architectures and reliability calculations (Clause 6 and Clause 7),
- shift from "SILCL" to "maximum SIL" of a subsystem (Clause 7),
- use cases for software described including requirements (Clause 8),
- requirements on independence for software verification (Clause 8) and validation activities (Clause 9) added,
- new informative annex with examples (Annex G),
- new informative annexes on typical  $MTTF_D$  values, diagnostics and calculation methods for the architectures (Annex C, Annex D and Annex H).

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

Draft	Report on voting
44/885/FDIS	44/888/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at [www.iec.ch/members\\_experts/refdocs](http://www.iec.ch/members_experts/refdocs). The main document types developed by IEC are described in greater detail at [www.iec.ch/standardsdev/publications](http://www.iec.ch/standardsdev/publications).

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

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

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

## INTRODUCTION

As a result of automation, demand for increased production and reduced operator physical effort, Safety-related Control Systems (referred to as SCS) of machines play an increasing role in the achievement of overall machine safety. Furthermore, the SCS themselves increasingly employ complex electronic technology.

IEC 62061 specifies requirements for the design and implementation of safety-related control systems of machinery. This document is machine sector specific within the framework of IEC 61508.

NOTE While IEC 62061 and ISO 13849-1 are using different methodologies for the design of safety related control systems, they intend to achieve the same risk reduction.

This International Standard is intended for use by machinery designers, control system manufacturers and integrators, and others involved in the specification, design and validation of an SCS. It sets out an approach and provides requirements to achieve the necessary performance and facilitates the specification of the safety functions intended to achieve the risk reduction.

This document provides a machine sector specific framework for functional safety of an SCS of machines. It only covers those aspects of the safety lifecycle that are related to safety requirements allocation through to safety validation. Requirements are provided for information for safe use of SCS of machines that can also be relevant to later phases of the lifecycle of an SCS.

There are many situations on machines where SCS are employed as part of safety measures that have been provided to achieve risk reduction. A typical case is the use of an interlocking guard that, when it is opened to allow access to the danger zone, signals the safety related parts of the machine control system to stop hazardous machine operation. In automation, the machine control system that is used to achieve correct operation of the machine process often contributes to safety by mitigating risks associated with hazards arising directly from control system failures. This document gives a methodology and requirements to:

- assign the required safety integrity for each safety function to be implemented by SCS;
- enable the design of the SCS appropriate to the assigned safety (control) function(s);
- integrate safety-related subsystems designed in accordance with other applicable functional safety-related standards (see 6.3.4);
- validate the SCS.

This document is intended to be used within the framework of systematic risk reduction, in conjunction with risk assessment described in ISO 12100. Suggested methodologies for a safety integrity assignment are given in informative Annex A.

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

## SAFETY OF MACHINERY – FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

### 1 Scope

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related control systems (SCS) for machines. It is applicable to control systems used, either singly or in combination, to carry out safety functions on machines that are not portable by hand while working, including a group of machines working together in a co-ordinated manner.

This document is a machinery sector specific standard within the framework of IEC 61508 (all parts).

The design of complex programmable electronic subsystems or subsystem elements is not within the scope of this document. This is in the scope of IEC 61508 or standards linked to it; see Figure 1.

NOTE 1 Elements such as systems on chip or microcontroller boards are considered complex programmable electronic subsystems.

The main body of this sector standard specifies general requirements for the design, and verification of a safety-related control system intended to be used in high/continuous demand mode.

This document:

- is concerned only with functional safety requirements intended to reduce the risk of hazardous situations;
- is restricted to risks arising directly from the hazards of the machine itself or from a group of machines working together in a co-ordinated manner;

NOTE 2 Requirements to mitigate risks arising from other hazards are provided in relevant sector standards. For example, where a machine(s) is part of a process activity, additional information is available in IEC 61511.

This document does not cover

- electrical hazards arising from the electrical control equipment itself (e.g. electric shock – see IEC 60204-1);
- other safety requirements necessary at the machine level such as safeguarding;
- specific measures for security aspects – see IEC TR 63074.

This document is not intended to limit or inhibit technological advancement.

Figure 1 illustrates the scope of this document.

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

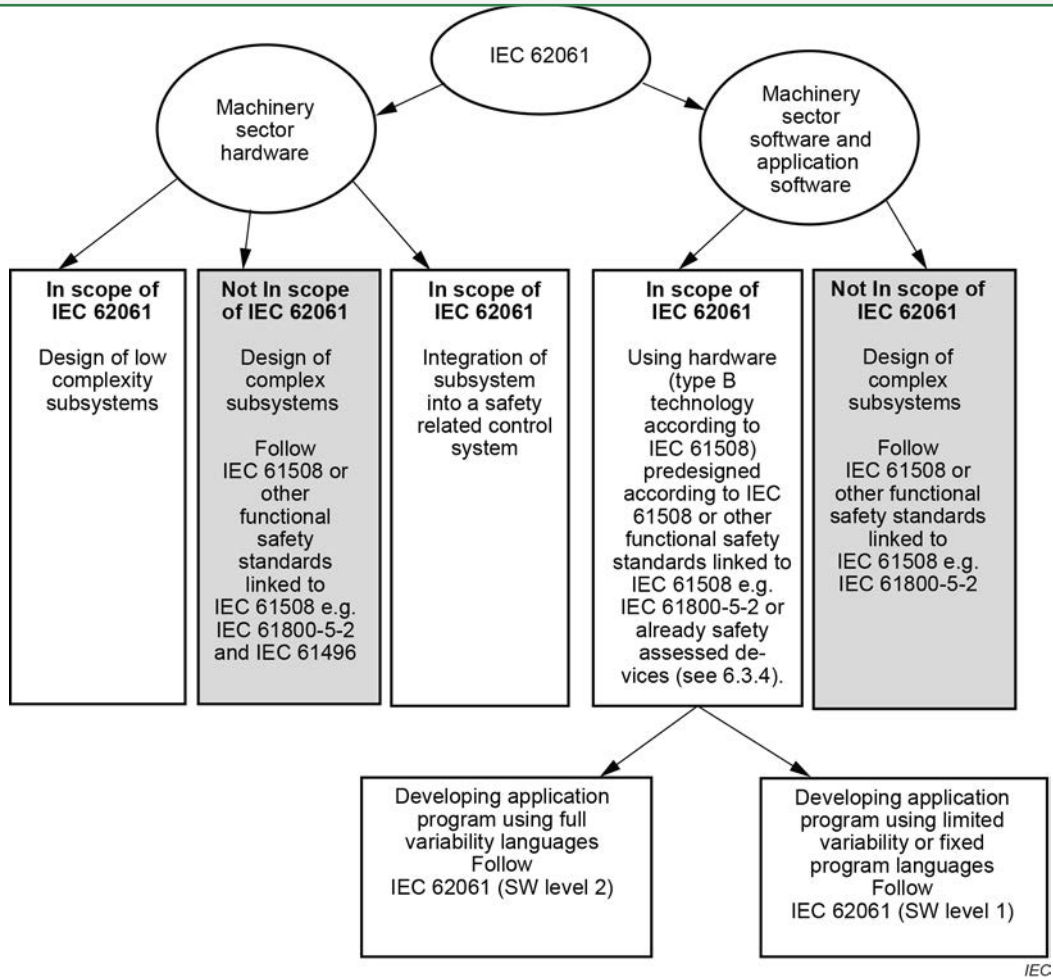


Figure 1 – Scope of this document

## 2 Normative references

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

IEC 60204-1:2016, *Safety of machinery – Electrical equipment of machines – Part 1: General requirements*

IEC 61000-1-2:2016, *Electromagnetic compatibility (EMC) – Part 1-2: General – Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena*

IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

IEC 61508-2:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

This is a preview of "DS/EN IEC 62061:2021". [Click here to purchase the full version from the ANSI store.](#)

ISO 12100:2010, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

ISO 13849 (all parts), *Safety of machinery – Safety-related parts of control systems*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13849-2:2012, *Safety of machinery – Safety-related parts of control systems – Part 2: Validation*