

2026

Bezpečnost strojních zařízení – Bezpečnostní aspekty vztahující se k funkční bezpečnosti bezpečnostních řídicích systémů

ČSN
CLC IEC/TS 63074

33 2203

idt IEC/TS 63074:2023

Safety of machinery – Security aspects related to functional safety of safety-related control systems

Sécurité des machines – Aspects liés a la sureté relatifs a la sécurité fonctionnelle des systemes de commande relatifs
a la sécurité

Maschinensicherheit – Sicherheitsaspekte in Verbindung mit der funktionalen Sicherheit von sicherheitsrelevanten Steuerungssystemen

Tato norma je českou verzí technické specifikace CLC IEC/TS 63074:2024. Překlad byl zajištěn Českou agenturou pro standardizaci. Má stejný status jako oficiální verze.

This standard is the Czech version of the Technical Specification CLC IEC/TS 63074:2024. It was translated by the Czech Standardization Agency. It has the same status as the official version.

Národní předmluva

Upozornění na používání této normy

Tato norma přejímá technickou specifikaci CLC IEC/TS 63074:2024 vydanou v souladu s vnitřními předpisy CEN/
CENELEC, část 2.

Informace o citovaných dokumentech

EN IEC 62061:2021 zavedena v ČSN EN IEC 62061 ed. 2:2022 (33 2208) Bezpečnost strojních zařízení – Funkční bezpečnost řídicích systémů souvisejících s bezpečností

Související ČSN a TNI

ČSN EN 60204-1 ed. 3:2019 (33 2200) Bezpečnost strojních zařízení – Elektrická zařízení strojů – Část 1: Obecné požadavky

ČSN EN IEC 61496 (soubor) (33 2206) Bezpečnost strojních zařízení – Elektrická snímací ochranná zařízení

ČSN EN 61508-2 ed. 2:2011 (18 0301) Funkční bezpečnost

elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností –
Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související
s bezpečností

ČSN EN 61508-3 ed. 2:2011 (18 0301) Funkční bezpečnost
elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností –
Část 3: Požadavky na software

ČSN EN 61508-4 ed. 2:2011 (18 0301) Funkční bezpečnost
elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností –
Část 4: Definice a zkratky

ČSN EN IEC 62443 (soubor) (18 0304) Bezpečnost systémů pro průmyslovou automatizaci a řízení

ČSN EN IEC 62443-2-4 ed. 2:2019 (18 0304) Bezpečnost systémů pro průmyslovou automatizaci
a řízení –
Část 2-4: Požadavky na program bezpečnosti pro poskytovatele služeb IACS

ČSN EN IEC 62443-3-2:2021 (18 0304) Bezpečnost systémů pro průmyslovou automatizaci a řízení –
Část 3-2: Posouzení bezpečnostních rizik pro návrh systému

ČSN EN IEC 62443-3-3:2019 (18 0304) Průmyslové komunikační sítě – Bezpečnost sítě a systému –
Část 3-3: Požadavky na bezpečnost systému a bezpečnostní úroveň

ČSN EN IEC 62443-4-1:2018 (18 0304) Bezpečnost pro systémy průmyslové automatizace a řízení –
Část 4-1: Požadavky na životní cyklus vývoje bezpečného výrobku

ČSN EN 62745 (33 2209) Bezpečnost strojních zařízení – Požadavky na bezdrátové řídicí systémy
strojních zařízení

TNI POKYN ISO/IEC 51 (76 3503) Bezpečnostní hlediska – Směrnice pro jejich začlenění do norem

ČSN EN ISO 12100:2011 (83 3001) Bezpečnost strojních zařízení – Všeobecné zásady pro konstrukci –
Posouzení rizika a snižování rizika

ČSN EN ISO 13849-1 ed. 2:2017 (83 3205) Bezpečnost strojních zařízení – Bezpečnostní části
ovládacích systémů – Část 1: Obecné zásady pro konstrukci

ČSN EN ISO 13849-2:2013 (83 3205) Bezpečnost strojních zařízení – Bezpečnostní části ovládacích
systémů – Část 2: Ověřování platnosti

ČSN EN ISO 14119 (83 3315) Bezpečnost strojních zařízení – Blokovací zařízení spojená
s ochrannými kryty – Zásady pro konstrukci a volbu

Vysvětlivky k textu této normy

V případě nedatovaných odkazů na evropské/mezinárodní normy jsou ČSN uvedené v článku
„Souvisící ČSN a TNI“ nejnovějšími vydáními, platnými v době schválení této normy. Při používání
této normy je třeba vždy použít taková vydání ČSN, která přejímají nejnovější vydání nedatovaných
evropských/mezinárodních norem (včetně všech změn).

Informativní údaje z IEC/TS 63074:2023

Tuto technickou specifikaci vypracovala technická komise IEC/TC 44 *Bezpečnost strojních zařízení* –

Elektrotechnické aspekty.

Toto první vydání zrušuje a nahrazuje první vydání IEC/TR 63074 z roku 2019, jehož je technickou revizí.

Toto vydání obsahuje vzhledem k IEC/TR 63074:2019 tyto významné technické změny:

- a) novou kapitolu 6 o kybernetické bezpečnosti a funkčnímu zabezpečení strojních zařízení;
- b) nový obrázek A.1;
- c) nový článek C.3 Příklad 2 – Fáze použití stroje.

Text této technické specifikace se zakládá na těchto dokumentech:

Návrh	Zpráva o hlasování
44/964/DTS	44/987/RVDTS

Úplnou informaci o hlasování při schvalování této technické specifikace lze najít ve zprávě o hlasování ve výše uvedené tabulce.

Jazyk použitý při vypracování této technické specifikace je angličtina.

Tento dokument byl navržen v souladu se směrnicemi ISO/IEC, část 2, a byl vypracován v souladu se směrnicemi ISO/IEC, část 1, a se směrnicemi ISO/IEC, dodatkem IEC, dostupnými na www.iec.ch/members_experts/refdocs. Hlavní typy dokumentů vypracované v IEC jsou podrobněji popsány na www.iec.ch/standardsdev/publications.

Komise rozhodla, že obsah tohoto dokumentu zůstane nezměněn až do data příští prověrky (stability date) uvedeného na webových stránkách IEC (webstore.iec.ch) v údajích o tomto dokumentu. K tomuto datu bude dokument buď

- znovu potvrzen,
- zrušen,
- nahrazen zrevidovaným vydáním; nebo
- změněn.

UPOZORNĚNÍ – Publikace obsahuje barevný tisk, který je považován za potřebný k porozumění jejímu obsahu. Uživatelé by proto měli pro tisk tohoto dokumentu použít barevnou tiskárnu.

Wypracování normy

Zpracovatel odborného překladu: Ing. František Valenta, ELVAM, IČO 66051649

Technická normalizační komise: TNK 153 Bezpečnost elektrických zařízení a funkční bezpečnost strojních zařízení

Vydala: Česká agentura pro standardizaci, státní příspěvková organizace

Citované dokumenty a souvisící ČSN lze získat v e-shopu.

Česká agentura pro standardizaci je státní příspěvková organizace zřízená Úřadem pro technickou normalizaci, metrologii a státní zkušebnictví na základě ustanovení § 5 odst. 2 zákona č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších

předpisů.

ICS 13.110; 29.020

Bezpečnost strojních zařízení – Bezpečnostní aspekty vztahující se
k funkční bezpečnosti bezpečnostních řídicích systémů
(IEC/TS 63074:2023)

Safety of machinery – Security aspects related to functional safety
of safety-related control systems
(IEC/TS 63074:2023)

Sécurité des machines – Aspects liés a la sureté
relatifs a la sécurité fonctionnelle des systemes
de commande relatifs a la sécurité
(IEC/TS 63074:2023)

Maschinensicherheit – Sicherheitsaspekte
in Verbindung mit der funktionalen Sicherheit
von sicherheitsrelevanten Steuerungssystemen
(IEC/TS 63074:2023)

Tato technická specifikace byla schválena CENELEC dne 2024-01-22.

Členové CENELEC jsou povinni oznámit existenci této TS stejným způsobem jako u EN a umožnit,
aby TS byla v příslušné formě okamžitě dostupná na národní úrovni. Je dovoleno, aby zůstaly
v platnosti národní normy, které jsou s TS v rozporu.

Členy CENELEC jsou národní elektrotechnické komitety Belgie, Bulharska, České republiky, Dánska,
Estonska, Finska, Francie, Chorvatska, Irska, Islandu, Itálie, Kypru, Litvy, Lotyšska, Lucemburska,
Maďarska, Maltý, Německa, Nizozemska, Norska, Polska, Portugalska, Rakouska, Republiky Severní
Makedonie, Rumunska, Řecka, Slovenska, Slovinska, Spojeného království, Srbska, Španělska,
Švédska, Švýcarska a Turecka.



Evropský výbor pro normalizaci v elektrotechnice
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
Řídicí centrum CEN-CENELEC: Rue de la Science 23, B-1040 Brusel

© 2024 CENELEC Veškerá práva pro využití v jakékoliv formě a jakýmikoliv prostředky
jsou celosvětově vyhrazena členům CENELEC.

Ref. č. CLC IEC/TS

63074:2024 E

Evropská předmluva

Tento dokument (CLC IEC/TS 63074:2024) sestává z textu IEC/TS 63074:2023, který vypracovala technická

komise IEC/TC 44 *Bezpečnost strojních zařízení – Elektrotechnické aspekty*.

Upozorňuje se na možnost, že některé prvky tohoto dokumentu mohou být předmětem patentových práv. CENELEC nelze činit odpovědným za identifikaci jakéhokoliv nebo všech patentových práv.

Jakákoli zpětná vazba a otázky týkající se tohoto dokumentu mají být adresovány národnímu normalizačnímu orgánu uživatele. Úplný seznam těchto orgánů lze nalézt na webových stránkách CENELEC.

Oznámení o schválení

Text mezinárodní technické specifikace IEC/TS 63074:2023 byl schválen CENELEC jako evropská technická specifikace bez jakýchkoliv modifikací.

Úvod.....	9
1..... Rozsah platnosti.....	10
2..... Citované dokumenty.....	10
3..... Termíny, definice a zkratky.....	10
3.1..... Termíny a definice.....	10
3.2..... Zkratky.....	14
4..... Přehled bezpečnosti a zabezpečení.....	14
4.1..... Obecně.....	14
4.2..... Cíle zabezpečení.....	14
4.3..... Bezpečnostní cíle.....	14
5..... Bezpečnostní aspekty vztahující se k funkčnímu zabezpečení.....	16
5.1..... Obecně.....	16
5.1.1... Posouzení bezpečnostního rizika.....	16

5.1.2... Strategie odezvy na bezpečnostní riziko.....	17
5.2..... Bezpečnostní protipatření.....	18
5.2.1... Obecně.....	18
5.2.2... Identifikace a autentizace.....	19
5.2.3... Řízení používání.....	19
5.2.4... Systémová integrita.....	20
5.2.5... Důvěrnost dat.....	20
5.2.6... Omezený tok dat.....	20
5.2.7... Včasná odezva na události.....	20
5.2.8... Dostupnost zdrojů.....	20
6..... Kybernetická bezpečnost a funkční zabezpečení strojních zařízení.....	20
6.1..... Obecně.....	20
6.2..... Bezpečnostní opatření před poškozením.....	21
6.3..... Bezpečnostní protipatření před poškozením.....	21
6.3.1...	

Obecně.....	21
6.3.2... Potenciální zdroje kybernetických hrozeb.....	21
6.3.3... Vícefaktorová autentizace.....	21
6.3.4... Architektura sítě.....	22
6.3.5... Přenosná zařízení.....	22
6.3.6... Bezdrátová komunikace.....	22
6.3.7... Vzdálený přístup.....	22
6.3.8... Útok prostřednictvím přímého fyzického připojení.....	22
7..... Verifikace a údržba bezpečnostních protipatření.....	23
8..... Informace pro uživatele stroje (strojů).....	23
Příloha A (informativní) Základní informace vztahující se k hrozbám a metoda modelování hrozeb.....	24
A.1..... Hodnocení hrozeb.....	24
A.2..... Příklady hrozeb vztahujících se k bezpečnostním zařízením.....	25
Příloha B (informativní) Spouštěče posouzení bezpečnostního rizika.....	27
B.1..... Obecně.....	27

B.2..... Spouštěče řízené událostmi.....	
.....	27

Příloha C (informativní) Příklad toku informací mezi výrobcem zařízení, výrobcem stroje, integrátorem a uživatelem stroje..... 28

C.1..... Obecně.....	
.....	28

C.2..... Příklad 1 - Fáze návrhu stroje.....	
28	

C.3..... Příklad 2 - Fáze použití stroje.....	
28	

Bibliografie.....	
.....	30

Příloha ZA (normativní) Normativní odkazy na mezinárodní publikace a jim odpovídající evropské publikace..... 32

Obrázek 1 - Vztah mezi hrozbou (hrozbami), zranitelnostmi, následkem (následky) a bezpečnostním rizikem (riziky) pro SCS vykonávající bezpečnostní funkci (funkce).....	15
---	----

Obrázek 2 - Možné účinky bezpečnostního rizika (rizik) na SCS.....	16
--	----

Obrázek A.1 - Bezpečnostní zařízení a možné přístupy.....	26
---	----

Obrázek C.1 - Příklad toku obecných informací během fáze návrhu.....	28
--	----

Obrázek C.2 - Příklad toku obecných informací během fáze použití.....	29
---	----

Obrázek C.3 - Příklad toku informací během fáze použití v kontextu IEC 62443-2-4.....	29
---	----

Tabulka 1 - Přehled základních požadavků a možný dopad (dopady) na SCS.....	19
---	----

Úvod

Průmyslové automatizační systémy mohou být vystaveny bezpečnostním hrozbám zneužívajících zranitelností vzhledem k tomu, že:

- je možný přístup k řídicímu systému, například přeprogramování stroje (včetně zabezpečení);
- narůstá sbližování běžných systémů IT a průmyslových systémů;
- operační systémy se staly součástí vestavěných systémů, například protokoly založené na IP nahrazují proprietární síťové protokoly a data se vyměňují přímo ze sítě SCADA do kancelářského prostředí;
- software se vyvíjí opětovným použitím stávajících softwarových komponent třetích stran;
- vzdálený přístup dodavatelů se stal běžným způsobem provozu/údržby se zvýšeným rizikem kybernetické bezpečnosti z důvodu například neoprávněného přístupu, dostupnosti a integrity.

V kontextu stroje představuje řídicí systém stroje průmyslový automatizační systém.

Bezpečnostní řídicí systém strojů je součástí řídicího systému stroje, a proto může být také vystaven bezpečnostním hrozbám, které mohou vést ke ztrátě schopnosti udržovat bezpečný provoz stroje.

POZNÁMKA 1 Rizikový potenciál příležitostí k útoku je významný vzhledem k trendům a rozvojem hrozeb a množství známých zranitelností. Cíle zabezpečení jsou popsány zejména z hlediska důvěrnosti, integrity a dostupnosti, které budou obecně identifikovány a upřednostňovány pomocí přístupu založeného na riziku.

Cíle funkčního zabezpečení zohledňují riziko závažnosti újmy a pravděpodobnosti výskytu takovéto újmy. Účinky jakéhokoli rizika (nebezpečné události) určují požadavky na bezpečnostní integritu (úroveň bezpečnostní integrity (SIL)) v souladu s IEC 62061 pro bezpečnostní řídicí systémy nebo se souborem IEC 61508 pro elektrické/elektronické/programovatelné elektronické bezpečnostní systémy nebo úroveň výkonnosti (PL) v souladu s ISO 13849-1 pro bezpečnostní součásti řídicích systémů.

Co se týká bezpečnostní funkce, mohou bezpečnostní hrozby (vnitřní nebo vnější) ovlivňovat bezpečnostní integritu a celkovou dostupnost systému.

POZNÁMKA 2 Požadavky na bezpečnost („základní požadavky“) k zajištění bezpečnostních cílů, které má příslušný systém splňovat, definuje a doporučuje IEC 62443-3-3.

POZNÁMKA 3 Celková bezpečnostní strategie není předmětem tohoto dokumentu, další informace jsou uvedeny např. v souboru IEC 62443 nebo v ISO/IEC 27001.

Opatření k zabránění rozumně předvídatelnému chybnému použití fyzickou manipulací jsou řešena v některých normách funkčního zabezpečení strojních zařízení (např. v souboru IEC 61496 a ISO 14119).

POZNÁMKA 4 Opatření k zabránění rozumně předvídatelnému chybnému použití fyzickou manipulací nejsou stejná jako fyzická bezpečnost v souboru IEC 62443.

1 Rozsah platnosti

Tato technická specifikace identifikuje relevantní aspekty souboru IEC 62443 týkající se bezpečnostních hrozeb a zranitelností, které se zohledňují při návrhu a při implementaci bezpečnostních řídicích systémů (SCS), které mohou vést ke ztrátě schopnosti udržovat bezpečný provoz stroje.

Typické bezpečnostní aspekty týkající se stroje s potenciálním vztahem k SCS jsou:

- zranitelnosti SCS buď přímo nebo nepřímo prostřednictvím jiných částí stroje, které mohou být zneužity bezpečnostními hrozbami, jež mohou vést k bezpečnostním útokům (prolomení bezpečnosti);
- dopad na bezpečnostní charakteristiky a schopnost SCS vykonávat náležitě svoji funkci (funkce);
- definice typického případu použití a aplikace odpovídajícího modelu hrozeb.

Aspekty bezpečnostních hrozeb a zranitelností, které se netýkají zabezpečení, nejsou v tomto dokumentu zohledněny.

POZNÁMKA Části řídicího systému stroje, které se netýkají zabezpečení, mohou být také vystaveny bezpečnostním hrozbám s možným dopadem na provoz stroje, jako je produktivita, výkonnost nebo kvalita. Tyto aspekty viz soubor IEC 62443.

Tento dokument se zaměřuje na úmyslné škodlivé činnosti. Záměrná manipulace s hardwarem (např. zapojení, výměna komponent) nebo předvídané zneužití prostřednictvím fyzické manipulace s SCS (např. fyzický bypass) nejsou v tomto dokumentu zohledněny.

Tento dokument nezahrnuje bezpečnostní požadavky na produkty informační technologie (IT) a na návrh zařízení používaných v SCS (např. mohou být k dispozici normy specifické pro produkty, jako je IEC TS 63208).

Konec náhledu - text dále pokračuje v placené verzi ČSN.