

# ČSN ISO/TS 15638-4 - Inteligentní dopravní systémy - Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel (TARV) - Část 4: Požadavky na zabezpečení systému

**Aplikační oblast:** [Systémy řízení nákladní dopravy](#), [Kooperativní systémy \(C-ITS\)](#)

**Rok vydání normy a počet stran:** Vydána 2020, 16 stran

**Rok zpracování extraktu:** 2021

**Skupina témat:** Vzdálená regulace nákladní dopravy

**Téma normy:** Inteligentní dopravní systémy – Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel (TARV) – Část 4: Požadavky na zabezpečení systému

**Charakteristika tématu:** Eliminace hrozeb C-ITS pro nákladní dopravu: ochrana dat, zabezpečení přenosu, přístup k datům, správa identity a důvěry a soukromí. Přeshraniční provoz a harmonizace

|                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Úvod, vysvětlení východisek</b>                                                                                                                                                         |
| Možné bezpečnostní hrozby a možnosti nástrojů pro zajištění zabezpečení systému TARV                                                                                                       |
| <b>Popis architektury, hierarchie, rolí a vztahů objektů</b>                                                                                                                               |
| Zabezpečení komplexního systému TARV a jeho kooperativních aplikací dle základní architektury ISO 15638-1 a možných upravených variant pro aplikace.                                       |
| <b>Popis procesu / funkce / způsobu použití</b>                                                                                                                                            |
| Obsahuje zabezpečení transakcí a dat TARV. Neobsahuje zabezpečení IVS (není zaměřením této technické normy).                                                                               |
| <b>Popis rozhraní / API / struktury systému</b>                                                                                                                                            |
| Zabezpečení transakcí a dat TARV v rámci „ohraničené zabezpečené spravované domény“ (BSMD) stanice ITS. Zabezpečení transakcí a dat TARV přenášených mimo BSMD s předem stanovenou adresou |
| <b>Definice protokolu / algoritmu / výpočtu</b>                                                                                                                                            |
| -                                                                                                                                                                                          |
| <b>Definice reprezentace dat / fyzikálního významu</b>                                                                                                                                     |
| -                                                                                                                                                                                          |
| <b>Definice konstant / rozsahů / omezení</b>                                                                                                                                               |
| -                                                                                                                                                                                          |

## Úvod

Nákladní doprava má zásadní hospodářský význam a současně se výrazně podílí na provozu na pozemních komunikacích, např. z pohledu plynulosti, bezpečnosti, zátěže infrastruktury i životního prostředí. Z těchto důvodů státy definují různá pravidla provozování nákladní dopravy, např. povinné přestávky v jízdě, mýtné, maximální zatížení náprav, omezení provozu v čase či vybraných oblastech. Současně státy musí zavést nějaký způsob kontroly dodržování těchto pravidel.

Soubor norem ISO 15638 ([TARV](#)) definuje možnou platformu pro řešení tohoto typu úloh. Platforma využívá univerzální palubní jednotku, spojenou se senzory na vozidle a infrastruktuře, vybavenou komunikačními kanály. Platforma také definuje organizační architekturu (uživatel, správní úřad, poskytovatel služby) a určuje související procesy (např. certifikaci a audit). Tato platforma umožňuje provozovat různé typy aplikací pro dálkové sledování dodržování pravidel, ale také pro podporu práce řidiče a podporu provozu nákladní dopravy.

[ISO 15638-4](#) (dále jen popisovaný dokument) se věnuje požadavkům na zabezpečení systému TARV tak, aby bezpečně poskytoval všechny požadované aplikační služby.

Poznámka: Extrakt uvádí vybrané kapitoly popisovaného dokumentu a přejímá původní číslování kapitol.

## Užití

Soubor norem ISO 15638 řeší platformu pro regulaci a státní dohled v nákladní dopravě. Tato platforma se v českém prostředí nyní nepoužívá, je však použitelná v případě, že vznikne poptávka veřejného sektoru po vyšší regulaci nákladní dopravy.

Pokud by státní správa tuto normalizovanou platformu zavedla, našla by uplatnění i v soukromém sektoru, protože umožňuje vytvářet a provozovat i komerční služby.

## 1. Předmět normy

ISO 15638-4 poskytuje obecné specifikace pro zabezpečení systému TARV, specifikace pro zabezpečení komunikace a dat TARV v rámci ohraničené zabezpečené spravované domény (BSMD) stanice ITS, a specifikace pro zabezpečení komunikace TARV. Pro případ komunikace mimo BSMD specifikuje i data.

Popisovaný dokument definuje požadavky na telematické aplikace pro regulovaná užitková vozidla pro:

- analýzu hrozeb, zranitelností a rizik
- správu zabezpečení
- služby zabezpečení

- architekturu zabezpečení
- správu identit
- správu důvěry
- řízení přístupu k zabezpečení
- služby vytvářející důvěru

Požadavky na zabezpečení jsou uvažovány hardwarové i softwarové pro:

- přenos dat TARV z [IVS](#) poskytovateli aplikačních služeb přes bezdrátové komunikační rozhraní
- přijetí pokynů od poskytovatele aplikačních služeb do IVS systému TARV
- komunikaci pro zpracování softwarových aktualizací pro IVS prostřednictvím bezdrátové komunikace

## 2. Související normy

Standardizace je nastavena tak, aby telematické aplikace mohly být integrovány do vestavěných systémů pro nákladní vozidla, již dostupných na trhu.

Popisovaný dokument doplňuje koncepty z [ISO 15638-1](#) ([extrakt](#)) popisující základní rámec a organizační architekturu TARV, a [ISO 15638-3](#) ([extrakt](#)) s požadavky na provoz aplikačních služeb TARV, procesy jejich schvalování a auditování, a vymáhání shody provozu nákladní přepravy s pravidly nastavenými správním úřadem.

V popisovaném dokumentu je uvedeno 9 norem v kapitole souvisejících norem, v bibliografii 34 norem. Z nich nejdůležitějšími jsou následující:

[ISO/TR 12859](#) ([extrakt](#)) stanoví aspekty soukromí v normách a systémech ITS. Soubor norem [ISO/IEC 15408](#) uvádí kritéria hodnocení zabezpečení IT.

Požadavky a cíle aplikace pro kooperativní systémy jsou v [ISO 17423](#) ([extrakt](#)).

Normy pro komunikaci ITS (dříve CALM) dokument uvádí [ISO 21210](#) ([extrakt](#)), [ISO 21212](#) ([extrakt](#)), [ISO 21213](#) ([extrakt](#)), [ISO 21217](#) ([extrakt](#)), [ISO 24102-3](#) ([extrakt](#)). Soubor norem [ISO 17427](#) pro kooperativní ITS popisují metodiku hodnocení rizik "core" systémů (ISO 17427-6), aspekty ochrany soukromí (ISO 17427-7), odpovědnosti (ISO 17427-8) a prokazování shody a vymáhání (ISO 17427-9).

[EUR 29634 EN](#) pro tzv. Point of Contact (CPOC) Protocol pro účely [C-ITS](#).

Dále normy ETSI pro zabezpečení: [ETSI TS 102 940](#) Architektura zabezpečení komunikace ITS a management zabezpečení, [ETSI TS 102 941](#) Management důvěry a soukromí, [ETSI TS 102 965](#) pro registraci identifikátoru aplikačního objektu (ITS-AID), a [ETSI TS 103 097](#) s hlavičkou zabezpečení a formáty certifikátu.

## 3. Termíny a definice

Základní sada termínů je uvedena v [ISO 15638-1](#) ([extrakt](#)), termíny k regulovaným službám v [ISO 15638-5](#) ([extrakt](#)) a [ISO 15638-6](#) ([extrakt](#)).

Popisovaný dokument uvádí 27 termínů. Nejdůležitějšími z nich pro tento extrakt jsou:

**aplikační služba** (*application service*) služba poskytovaná poskytovatelem služby, který má v regulovaném komerčním nákladním vozidle bezdrátový přístup k datům systému ve vozidle (IVS)

**regulované komerční nákladní vozidlo** (*regulated commercial freight vehicle*) vozidlo určené pro přepravu komerčního nákladu, které podléhá předpisům jurisdikce v oblasti užívání silničního systému dané jurisdikce a splnění zvláštních předpisů pro třídu komerčního nákladního vozidla, často prostřednictvím informací poskytovaných přes TARV

**schvalovací orgán/úřad** (*approval authority*) obvykle nezávislý orgán pro schvalování a audit poskytovatelů služeb

**správní úřad/jurisdikce** (*jurisdiction*) vládní, silniční nebo dopravní úřad, který vlastní regulativní aplikace

Příklad: Země, stát, městská rada, silniční úřad, ministerstvo (financí, dopravy) apod.

**stanice ITS; ITS-s** (*ITS-station*)

**systém IVS; systém ve vozidle** (*in-vehicle system; IVS*) entita v komunikační síti schopná komunikace s jinými podobnými entitami

Poznámka: Z abstraktního pohledu znamená "stanice ITS" množinu funkcí. Tímto termínem je často označována realizace těchto funkcí ve fyzické jednotce. Správný význam je většinou pochopitelný z kontextu. Správné označení pro fyzickou realizaci stanice ITS je [jednotka stanice ITS](#) (ITS-SU - ITS station unit).

**uzavřená zabezpečená řízená doména** (*bounded secure managed domain, BSMD*) – zabezpečené peer-to-peer komunikace mezi entitami (stanicemi ITS), které se mohou samy zabezpečit a vzdáleně spravovat

Poznámka: Uzavřená povaha je odvozena od požadavku, aby stanice ITS mohly komunikovat mezi sebou navzájem (peer-to-peer), i se zařízeními, která nejsou zabezpečena (dále jako „jiné stanice ITS“). Je třeba si uvědomit, že dosažení tohoto cíle vyžaduje často distribuci a skladování zabezpečovaného materiálu, který musí být chráněn v mezích stanic ITS. To vede k zabezpečené povaze entity. Existuje velká flexibilita k dosažení požadovaných komunikačních cílů a existuje požadavek, aby tato flexibilita byla řízena. V rámci C-ITS a ISO 21217 jsou takové stanice ITS definovány jako s provozem buďto v rámci BSMD nebo mimo BSMD.

**uživatel** (*user*) jednotlivec nebo strana, která se zapisuje a působí v rámci regulované nebo komerční aplikační služby TARV: [primární uživatel](#) a [sekundární uživatel](#)

Příklad: Řidič, dopravce, vlastník nákladu atd. (pozn.: nejčastějším uživatelem je dopravce).

Další termíny a zkratky z oboru ITS jsou obsaženy ve [slovníku ITS terminology](#).

## 4. Symboly a zkratky

Celkem popisovaný dokument uvádí 11 symbolů a zkratk. Zde jsou uvedeny pouze zkratky relevantní pro tento extrakt:

**BSMD** uzavřená zabezpečená spravovaná doména (*bounded secure managed domain*)

**C-ITS** kooperativní inteligentní dopravní systémy (*cooperative intelligent transport systems*)

**TARV** telematické aplikace pro regulaci komerčních nákladních vozidel (*telematics applications for regulated commercial freight vehicles*)

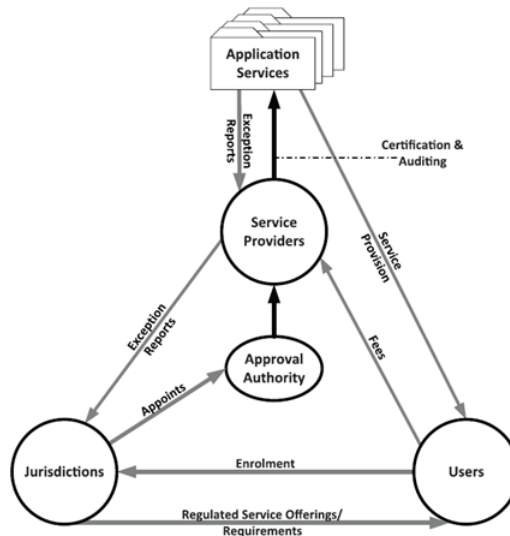
Další termíny a zkratky z oboru ITS jsou obsaženy ve slovníku ITS ([www.itsterminology.org](http://www.itsterminology.org)).

Další termíny a zkratky v anglické verzi jsou dostupné online na IEC Electropedia (<http://www.electropedia.org/>) a ISO Online browsing platform (<http://www.iso.org/obp>).

## 5 Obecný přehled a rámec

Základní informace o TARV obsahují části normy ISO 15638-1 až ISO 15638-7. Od ISO 15638-8 jsou části normy zaměřeny na jednotlivé aplikační služby TARV.

Kapitola (rozsah 2 strany) odkazuje na základní části normy ISO 15638 a předměty jejich řešení. Následující obrázek 1 ukazuje organizační architekturu systému TARV s klíčovými aktéry a jejich vztahy se vzájemnou komunikací, tedy subjekty zabezpečení.



Obrázek 1 (obr. 1 normy) – Základní architektura s rolemi v TARV (zdroj: ISO 15638-1)

Dále kapitola uvádí seznam všech částí souboru norem TARV.

## 6 Požadavky

Kapitola (rozsah 5,5 strany) je jádrem popisovaného dokumentu. V této kapitole se rozebírají postupně aspekty spojené se zabezpečením a nyní dostupné nástroje.

Článek Analýza hrozeb, zranitelností a rizik, vycházející ze souboru norem [ISO/IEC 15408](#), specifikuje požadavky na funkční komponenty pomocí evaluace zabezpečení (Targets Of Evaluation, TOEs) a sady komponent zajištění zabezpečení. Jsou definována kritéria evaluace pro profily ochrany (Protection Profiles, PP) a bezpečnostní cíle (Security Targets, ST). ISO/IEC 15408 uvádí stupnici, která se nazývá úrovněmi jistoty ohodnocení ([Evaluation Assurance Levels, EAL](#)), jež má hodnoty EAL1 až EAL7.

Cíli zabezpečení TARV jsou:

- Aktéři TARV. Předpokládají se dle [ISO 15638-1](#) (extrakt). Pokud jde o aktéry v obecném smyslu kooperativních ITS, uvažují se dle [ISO 17427-1](#).
- Funkce a výkon palubního zařízení. Ty jsou především otázkou konstrukce IVS, která není předmětem souboru norem ISO 15638.
- Zabezpečení aplikační služby TARV. To je zásadní rolí poskytovatele aplikační služby, ale není předmětem souboru norem ISO 15638.

Funkční požadavky na zabezpečení jsou definovány v následujících bodech:

- Funkční požadavky na TOE
- Obecné specifikace pro zabezpečení systému TARV
- Přenosy dat s nízkým zabezpečením prostřednictvím stanice ITS
- Přenosy dat prostřednictvím stanice ITS se zabezpečením C-ITS v BSMD
- Přenosy dat TARV včetně definovaného zabezpečení mimo BSMD

Další články se odkazují především na normy [ETSI TS 102 940](#) a [ISO TR 12859](#) (extrakt). Pro identifikaci vozidla a přenos identifikačních údajů přípojného vozidla (trailer ID, TID) je uveden odkaz na normu [ISO 15638-3](#) (extrakt).

Pro přeshraniční provoz a harmonizaci nejsou uvedena žádná ustanovení. Dokument neobsahuje žádné zvláštní požadavky na kvalitu služeb (kapitola 7), zkoušení (kapitola 8) a značení, označování a balení (kapitola 9). Tyto kapitoly obsahují pouze toto prohlášení o neuvedení požadavků.

## Příloha A (informativní): Příklad zabezpečení TARV v regulační doméně

Příloha A (rozsah 0,5 strany) nabízí pouze krátký přehled tří nástrojů zabezpečení:

- kořen důvěry (root of trust; RoT) a infrastrukturu správy a distribuce veřejných klíčů (public key infrastructure; PKI); odkazuje na EUR 29634 EN a [ETSI TS 102 940](#)
  - aplikační certifikáty; dle [ETSI TS 103 097](#)
- aplikační identifikátor ITS (ITS application identifier; ITS AID) a identifikátor služby poskytovatele (provider service identifier; PSID); s odkazem na [ETSI TS 103 097](#), [IEEE 1609.12](#) a [ETSI TS 102 965](#)

## Souvisící normy

- [ČSN ISO 15638-1 - Inteligentní dopravní systémy – Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel \(TARV\) – Část 1: Rámec a architektura](#)
- [ČSN ISO 15638-2 - Inteligentní dopravní systémy – Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel \(TARV\) – Část 2: Parametry společné platformy používající CALM](#)
- [ČSN ISO 15638-3 - Inteligentní dopravní systémy – Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel \(TARV\) – Část 3: Provozní požadavky, postupy certifikace a opatření dohledu nad poskytovateli regulovaných služeb](#)
- [ČSN ISO 15638-5 - Inteligentní dopravní systémy – Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel \(TARV\) – Část 5: Generické informace o vozidle](#)
- [ČSN ISO 15638-6 - Inteligentní dopravní systémy – Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel \(TARV\) – Část 6: Regulované aplikace](#)
- [ČSN ISO 15638-7 - Inteligentní dopravní systémy – Rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel \(TARV\) – Část 7: Ostatní aplikace](#)
- [ISO 12859 - ITS - Aspekty ochrany dat systémů ITS](#)
- [CEN ISO TS 17423 - Inteligentní dopravní systémy – Kooperativní systémy – Požadavky a cíle aplikace ITS na výběr komunikačních profilů](#)
- [CEN ISO TS 17427 - Inteligentní dopravní systémy – Kooperativní systémy – Role a odpovědnosti pro systémy založené na architektuře C-ITS](#)
- [ISO/TR 17427-6 - Inteligentní dopravní systémy – Kooperativní ITS – Část 6: Metodika hodnocení rizik základních systémů](#)
- [ISO 12859 - ITS - Aspekty ochrany dat systémů ITS](#)
- [ISO 24102-3 - Inteligentní dopravní systémy – Komunikační infrastruktura pro pozemní mobilní zařízení \(CALM\) – Management ITS stanic – Část 3: Přístupové body služby](#)
- [ISO 21217 - Inteligentní dopravní systémy – Architektura stanice a komunikační architektura](#)
- [ISO 21213 - Inteligentní dopravní systémy – Komunikační infrastruktura pro pozemní mobilní zařízení \(CALM\) – Přenosy v mobilních sítích 3.generace](#)
- [ISO 21212 - Inteligentní dopravní systémy – Komunikační infrastruktura pro pozemní mobilní zařízení \(CALM\) – Přenosy v mobilních sítích 2.generace](#)
- [ISO 21210 - Inteligentní dopravní systémy – Komunikační infrastruktura pro pozemní mobilní zařízení \(CALM\) – Část 1: Síťové protokoly pro internetové připojení](#)

## Souvisící termíny

- [kooperativní ITS; kooperativní inteligentní dopravní systémy](#)
- [rámec pro kooperativní telematické aplikace pro regulaci komerčních nákladních vozidel](#)
- [aplikační služba](#)
- [poskytovatel aplikační služby](#)
- [systém IVS; systém ve vozidle](#)
- [stanice ITS](#)
- [cíl zabezpečení](#)
- [bezpečnost; zabezpečení](#)
- [zabezpečení](#)
- [bezpečnostní doména](#)