



AŽD Praha s.r.o.

Součinnost manažerů infrastruktury, členských států a dodavatelů

Peter Gurník, Štěpán Klapka a kol.

Závod Technika

Osnova

- Součinnost evropského železničního sektoru při definici budoucího železničního systému
- Iniciativa EULYNX
- Stav evropských specifikací a jejich časová perspektiva
- Výzvy pro uplatnění specifikací EULYNX v praxi
- Rozhraní SCI, SDI, SMI, SSI
- Protokol RaSTA
- Závěr

Součinnost evropského železničního sektoru při definici budoucího železničního systému



Evropský železniční sektor poprvé společně navrhuje jednotnou systémovou architekturu budoucího železničního systému v rámci **System Pillar Europe's Rail** – „generického systémového integrátora“ a architekta budoucího evropského železničního systému.

- *Architekt budoucího systému* – vytváří jednotný operační koncept a funkční, bezpečnou a kyberneticky zabezpečenou systémovou architekturu.
- *Koordinační platforma sektoru* – sdružuje zástupce správců infrastruktury, dopravců, dodavatelů, výrobců vozidel, autorit a asociací do jednoho koordinačního rámce.
- *Most ke standardizaci* – připravuje jednotné specifikace a architektonické principy, které následně vstupují do TSI a evropské normalizace (ERA, CENELEC atd.).
- *Sjednocuje různé iniciativy* (EULYNX, RCA, OCORA apod.) pod jeden koordinační rámec, aby výsledek byl součástí jednotného evropského referenčního systému.

Iniciativa EULYNX

- Iniciativa (dnes stálá organizace) evropských správců infrastruktury, která od roku 2014 standardizuje technická rozhraní staničních zabezpečovacích zařízení s cílem multi-dodavatelského řešení a snížení životních nákladů.
- Od roku 2024 část specifikací EULYNX vzniká v pracovních skupinách Systémového pilíře (Pracovní skupiny: Trackside Assets a Transversal Functions). Pro tuto část specifikací je Systémový pilíř systémovou autoritou, má sektorovou podporu a perspektivu stabilního uplatnění.
 - EULYNX Baseline Set 4 Release 3 a zejména Release 4 jsou společně vydané EULYNX + Europe's Rail, přičemž Release 4 je plně integrován do Systémového pilíře
- Zbylé části specifikací (hlavně oblast systémových rozhraní) konsultuje konsorcium EULYNX s dodavatelskou asociací (UNIFE), ale její připomínky pro ni nejsou závazné (často se jimi neřídí).
- Železnice vyžadují uplatnění specifikací EULYNX ve formě požadavků soutěžní dokumentace ke stavbě.

Stav evropských specifikací a jejich časová perspektiva

■ **STIP (Standardisation and TSI Input Plan)**

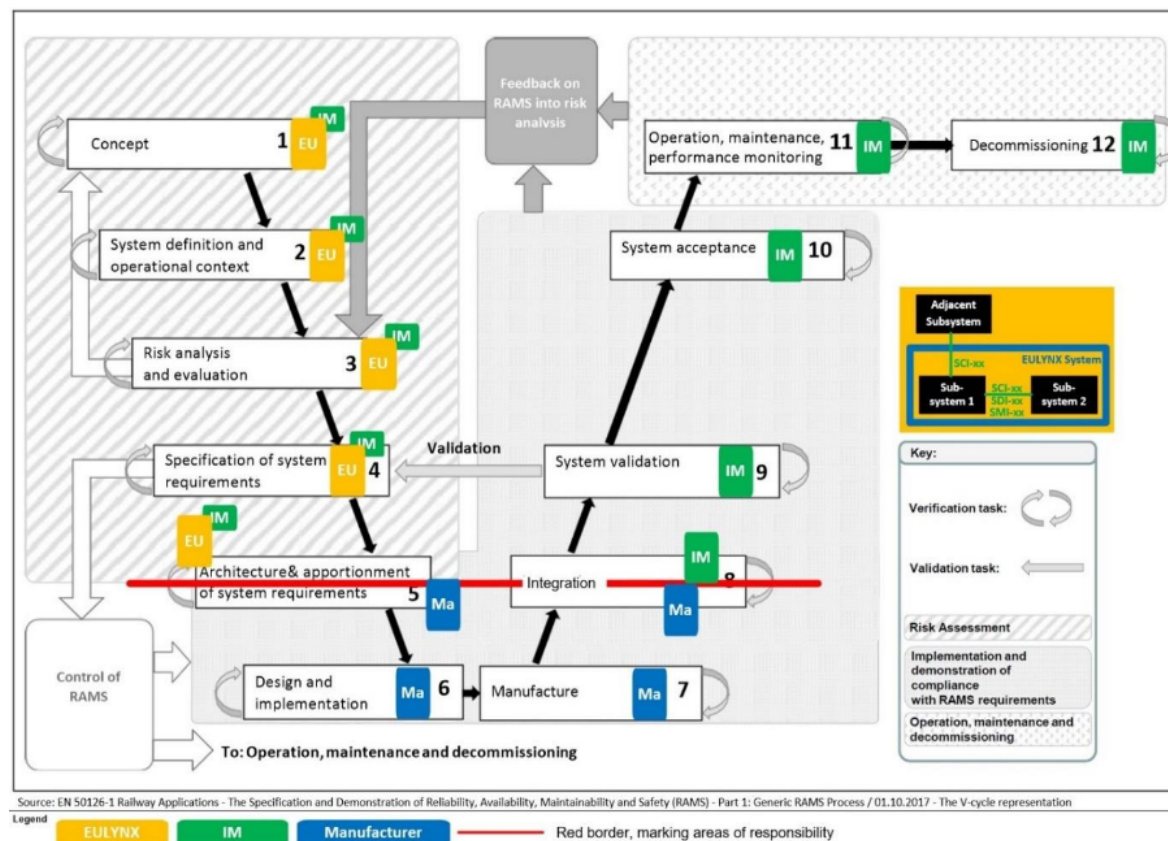
- Je v podstatě “**úřední řád**” pro evropské specifikace – říká, *co se má standardizovat, jakou cestou (TSI, EN, „SP dokument“), kdy zhruba a z jakých výstupů vzejde.*
- **STIP je koordinován Systemovým pilířem** a schvaluje ho System Pillar Steering Group spolu s Evropskou Komisí, ERA a standardizačními orgány (CEN/CENELEC, SFR, RASCOP).

■ **Časová perspektiva STIP**

- Krátkodobý horizont (cca do 2026): „údržba“ stávajících TSI, zejména CCS a OPE, uvedení FRMCS, První specifikace digitálního spřáhla.
- Střednědobý horizont (cca 2027–2030): Cílová architektura CCS, jednotné datové modely a rozhraní, systematická kyberbezpečnost
- Dlouhodobý horizont (po 2030): Plná specifikace ATO GoA3/4, automatizované posuny, migrace FRMCS, propojení řízení provozu

Výzvy pro uplatnění specifikací EULYNX v praxi (1) INTEGRACE

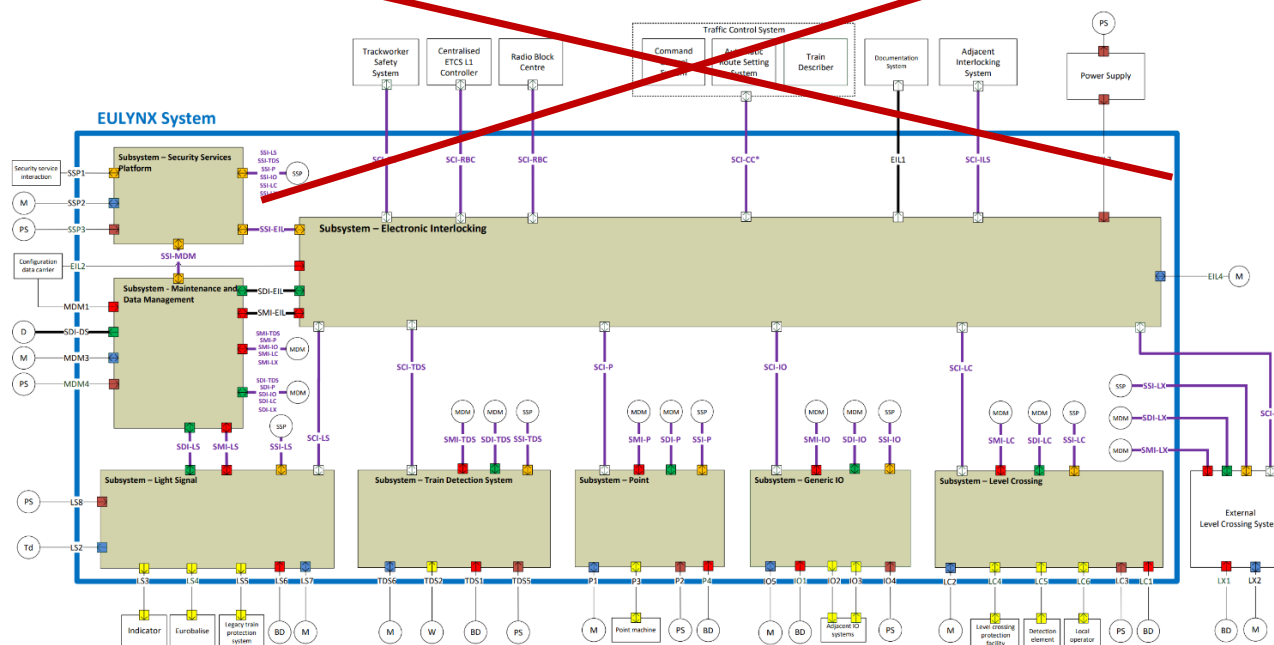
- Implementace rozhraní musí být validována v souladu s ČSN EN 50126/50716/50129
- Správy železnic musí doplnit požadavky nad rámec těch v EULYNX specifikacích, definujících konkrétní národní/aplikační kontext.
- Ověření vhodnosti implementace pro konkrétní aplikaci je v odpovědnosti správce infrastruktury.
- Pro každou aplikaci používající rozhraní EULYNX je nutné identifikovat bezpečnostně kritické funkce a doložit jejich implementaci -> dopad na kompatibilitu.



Výzvy pro uplatnění specifikací EULYNX v praxi (2) SYSTÉMOVÁ ROZHRANÍ

- Funkční specifikace systémových rozhraní EULYNX (stavědlo, řídicí systémy, RBC, TZZ,..) nejsou podporovány Systémovým pilířem z důvodu pravděpodobné nekompatibility s budoucí standardizací architektury CCS.
- Specifikace systémových rozhraní jsou ve velké většině přizpůsobené pro konkrétního uživatele (formou tzv. „národních kódů“) a navzájem nekompatibilní.
- Malé využití a uplatnění i mezi členy EULYNX (nižší jednotky národních kódů oproti cca 20 členům konsorcia)

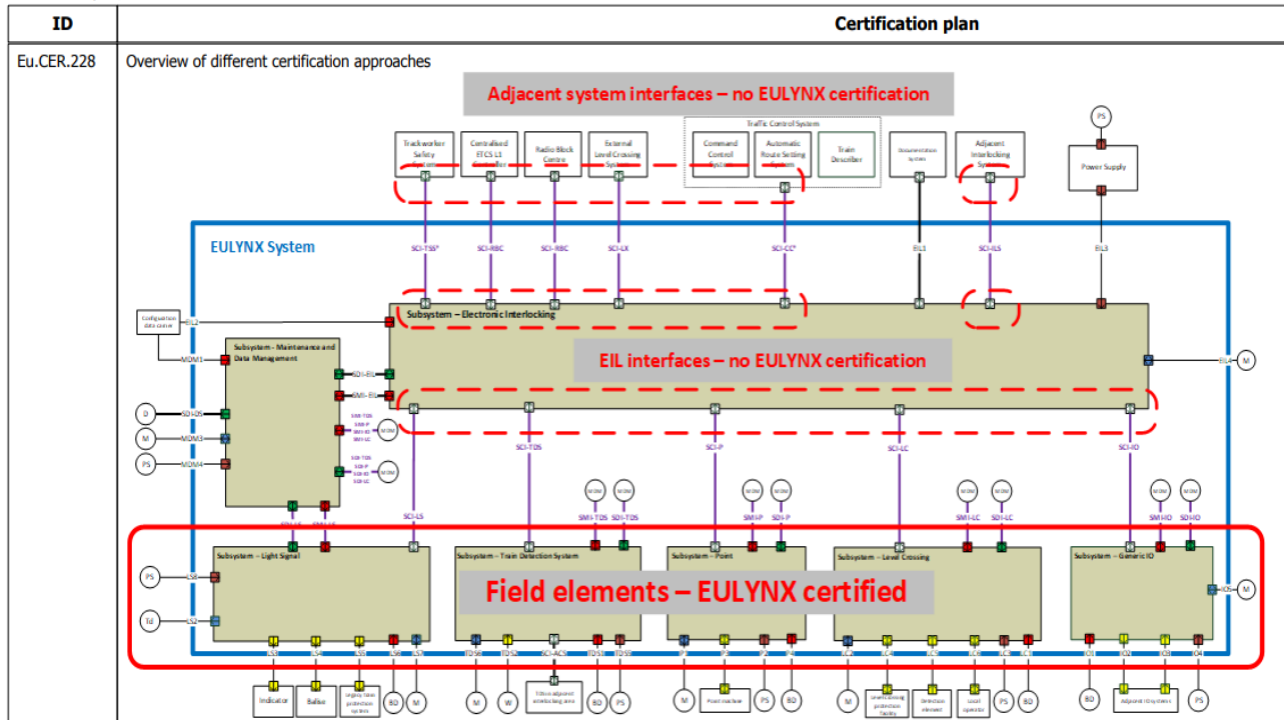
Není široká shoda na dlouhodobém rozvoji



Výzvy pro uplatnění specifikací EULYNX v praxi (3) CERTIFIKACE A KOMPATIBILITA SPECIFIKACÍ

- EULYNX certifikace poskytuje důkaz o správné implementaci specifikací EULYNX v rozhraní konkrétního dodavatele.
- EULYNX certifikace **negarantuje** vzájemnou kompatibilitu rozhraní mezi různými dodavateli (nezohledňuje nutné doplnění vyplývající z požadavků integrace)
- EULYNX certifikace je podporována jen pro objektové kontroléry, ne pro systémová rozhraní.
- Kompatibilita EULYNX specifikací různých verzí není zaručena. Je v odpovědnosti konkrétního správce železnic, aby soutěžil dodávku zařízení s kompatibilními verzemi EULYNX požadovaných rozhraní.

Certification plan, current

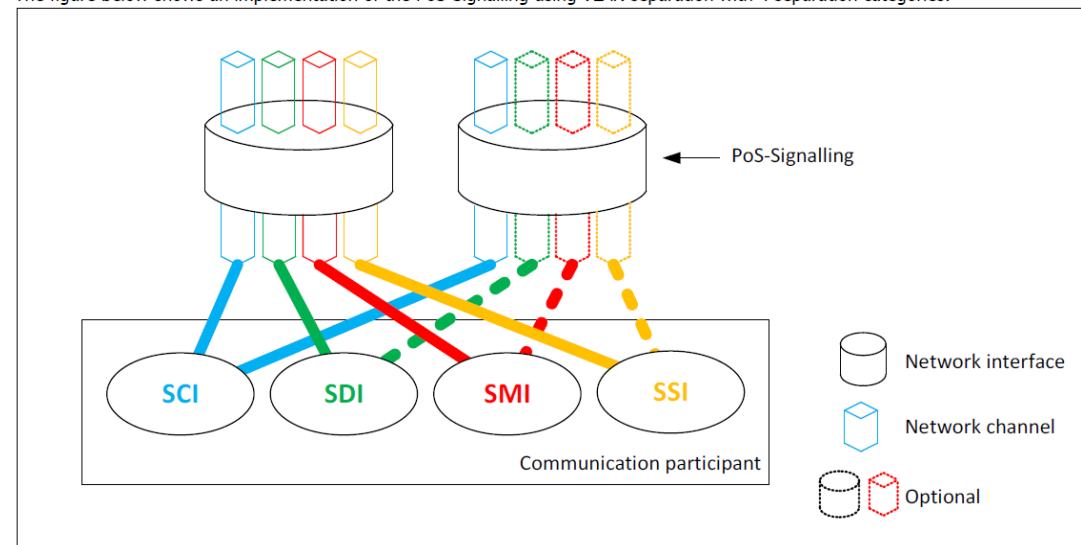


- EULYNX specifikace kybernetické bezpečnosti navazují na specifikace publikované **Systémovým pilířem** v únoru 2025 a odkazuje se na ni.
- EULYNX **definuje** cílovou úroveň bezpečnosti (SL-T = 3) pro svou architekturu, a následně vyžaduje, aby **implementující strany (zejména Správce infrastruktury)** zajistily a prokázaly, že je této úrovni dosaženo v konkrétní aplikaci.
- EULYNX poskytuje jak **povinné požadavky/opatření**, tak i **procesní rámec** s tím, že **konkrétní správce železnic** musí provést vlastní analýzu rizik pro konkrétní aplikaci a navrhnout opatření v kontextu celkového konceptu kybernetické bezpečnosti v oblasti své působnosti.
- Některé požadavky jdou nad rámec současné praxe v ČR: Příkladem může být např. požadavek na použití multifaktorové autentizace (MFA) pro rozhraní s obsluhujícím personálem.
- Z důvodu zajištění kybernetické bezpečnosti v case (vlivem tzv. eroze bezpečnosti), je na konkrétním správci železnic, aby zajistil další technická a organizační opatření pro prostředí národní infrastruktury s možným dopadem na kompatibilitu rozhraní EULYNX.

Výzvy pro uplatnění specifikací EULYNX v praxi (5) EULYNX KOMUNIKACE – rozhraní SCI/SDI/SMI/SSI

- 4 kategorie rozhraní
 - SCI – Standard Communication Interface,
 - SDI – Standard Diagnostic Interface,
 - SMI – System Maintenance Interface,
 - SSI – Standard Security Interface
- Rozhraní SCI-XX
 - Mandatorní zálohování – 2xPoS
 - Logika komunikace (událostní přístup) je značně rozdílná od koncepce uplatňované v ČR – dopady na funkční chování systémů spolupracujících na úrovni EULYNX rozhraní.

The figure below shows an implementation of the PoS-Signalling using VLAN separation with 4 separation categories.



Protokolové vrstvy pro rozhraní SDI-XX a SMI-XX

Figure of the protocol stack of the SDI-XX in the EULYNX System (for service function Time synchronisation, see [SP-SEC-ServSpec])

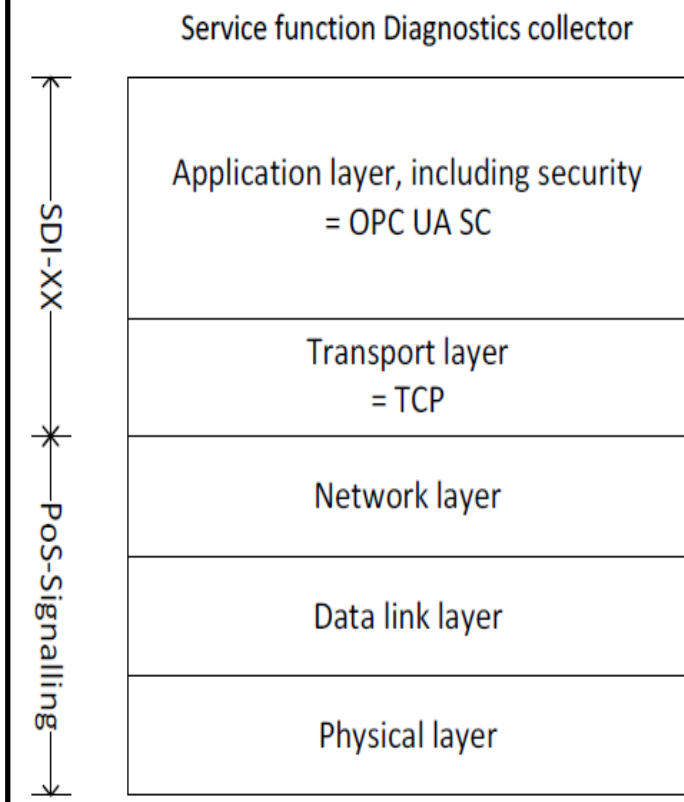
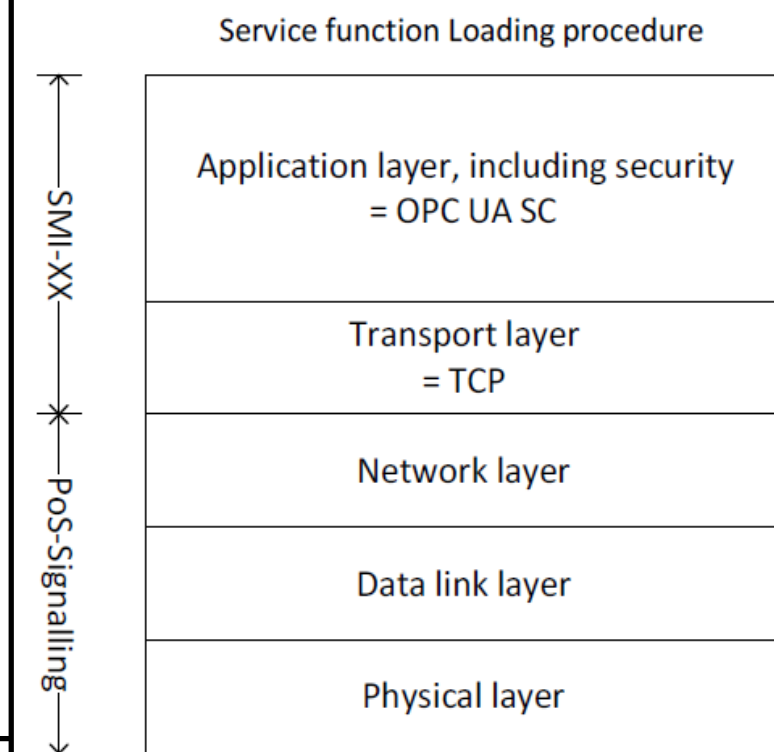
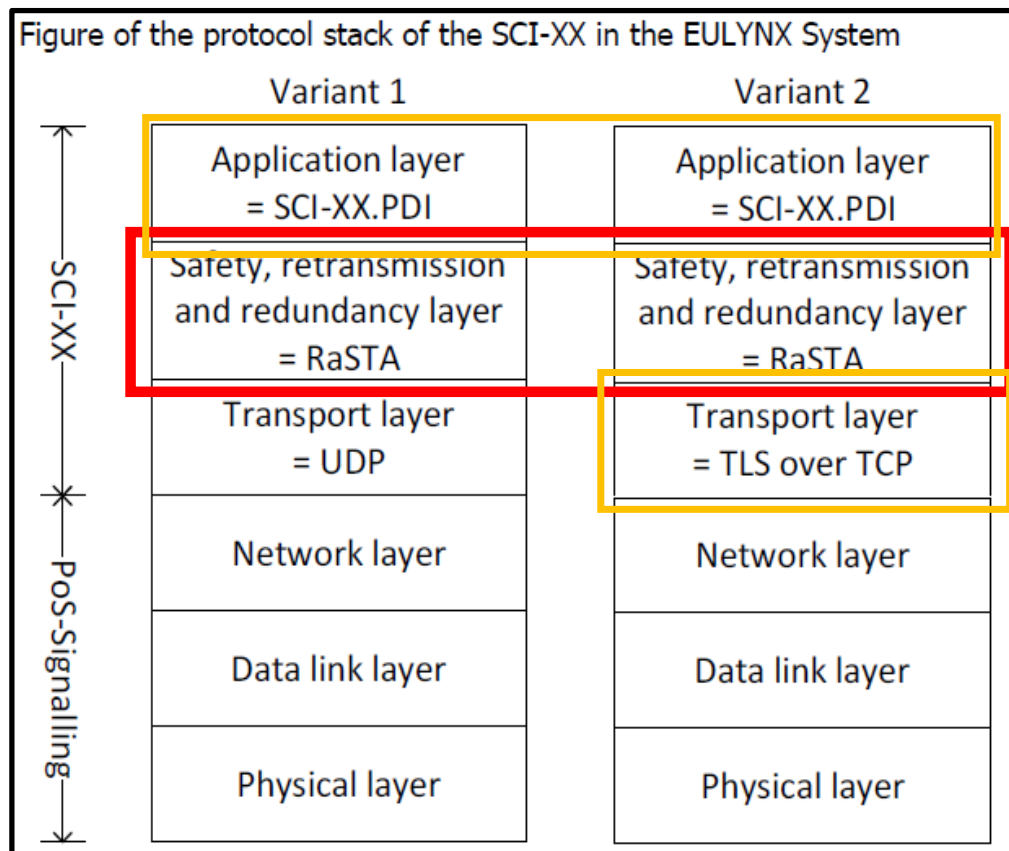


Figure of the protocol stack of the SMI-XX in the EULYNX System



Protokolové vrstvy pro rozhraní SCI-XX



PDI - Proces Data Interface protokol

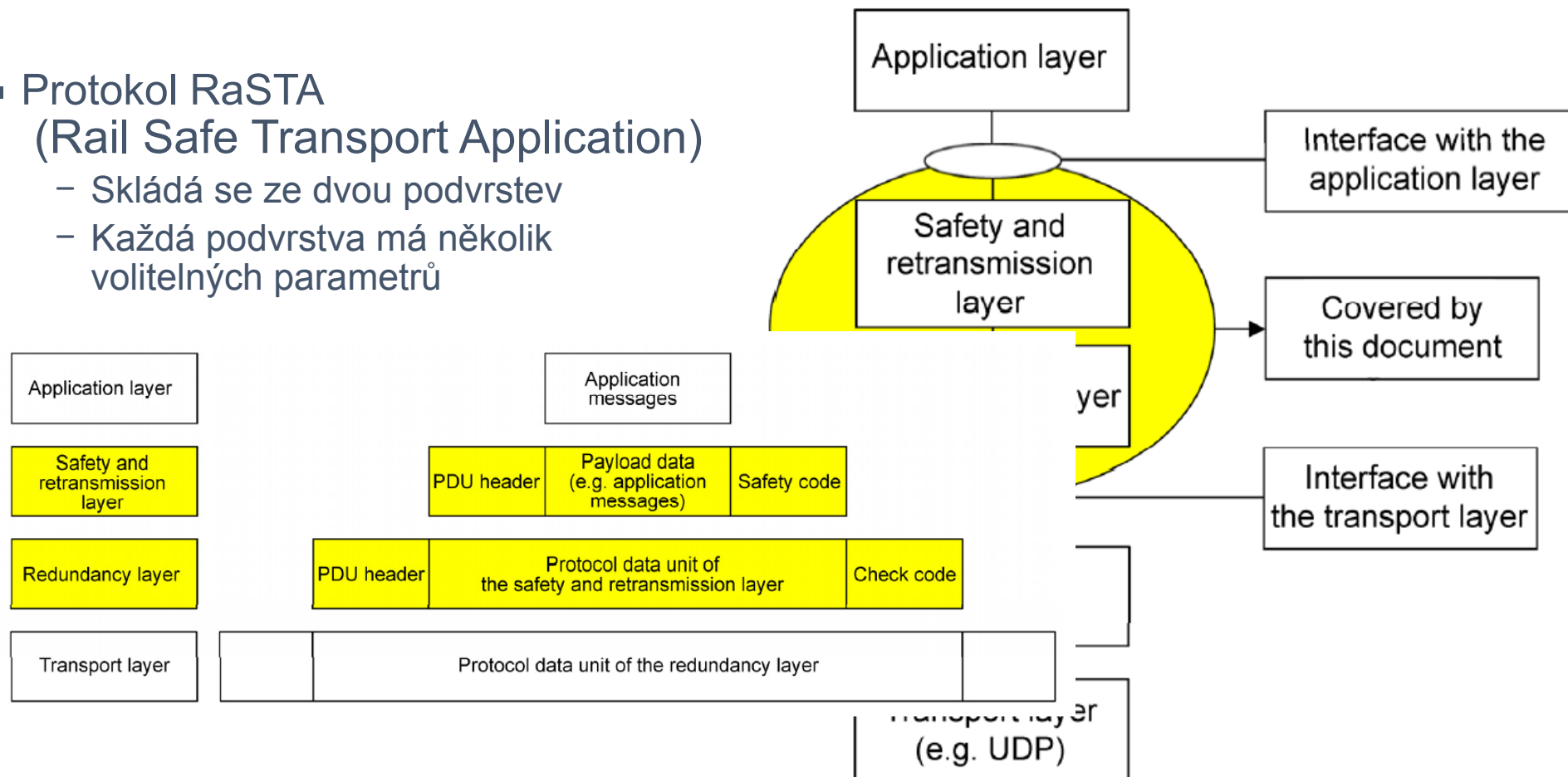
popisuje specifikace/standard DIN VDE V 0831-200

Nově doplněna varianta pro TLS přes TCP – 3 profily

Protokol RaSTA (1)

■ Protokol RaSTA (Rail Safe Transport Application)

- Skládá se ze dvou podvrstev
- Každá podvrstva má několik volitelných parametrů



Použitě parametry protokolu RaSTA pro EULYNX

■ Specifikuje dokument „20250620 Interface definition SCI Eu.Doc.92

7.2 Safety and retransmission layer

Table 23 – Configuration parameters of the safety and retransmission layer

| Option | Description | Subclause |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| T_{max} | Maximum accepted age of a message | 5.5.6 |
| T_h | Time period for sending heartbeats | 5.5.7 |
| Safety code | 1) No safety code; 2) Lower half of MD4 with a projected initial value; 3) Full MD4 with a projected initial value. | 5.3.11 |
| MWA | Maximum number of received, unconfirmed messages. This value shall be less than $N_{sendmax}$. | 5.5.9 |
| $N_{sendmax}$ | Maximum number of messages which the communication party may send without receiving a confirmation. This value is exchanged when the connection between the two communication parties is established and can be interpreted as the minimum size of the receive buffer. | 5.5.9 |
| $N_{maxPacket}$ | The maximum packetization factor states how many messages of one user may at maximum be combined to form a message of the safety and retransmission layer. | 5.5.10 |
| $N_{diagWindow}$ | The value $N_{diagWindow}$ defines the size of the measurement window for the channel quality measurement. | 5.5.6.4 |

7.3 Redundancy layer

Table 24 – Configuration parameters of the redundancy layer

| Option | Description | Subclause |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Number of physical channels | 1 – n | 6.1 |
| Check code | a) None; b) CRC32 with polynomial 0x EE5B42FD; c) CRC32 with polynomial 0x 1EDC6F41; d) CRC16 with polynomial 0x 1021; e) CRC16 with polynomial 0x 8005. | 6.3.6 |
| T_{seq} | Time period indicating how long a message is buffered that was received outside the sequence. | 6.6 |
| $N_{diagnosis}$ | Measurement window for diagnosis reports of the redundancy layer | 6.6.3.2 |
| $N_{deferQueueSize}$ | Maximum number of entries in the waiting queue deferQueue | 6.6 |

| | | |
|-----------|------|----------------------------------------------------------------------------------------------------|
| Eu.SCI.48 | Head | 3.2.1.1.1 T_{max} |
| Eu.SCI.49 | Info | T_{max} is the maximum accepted age of a message. |
| Eu.SCI.50 | Req | $T_{max} = 1800$ ms |
| Eu.SCI.54 | Head | 3.2.1.1.3 Safety Code |
| Eu.SCI.56 | Req | SafetyCode = option 2 (lower half of MD4) The initialisation value for MD4 is project specific. |

| | | |
|-----------|------|---------------------------------------|
| Eu.SCI.73 | Head | 3.2.1.2.2 Check code |
| Eu.SCI.75 | Req | Check code = option a (no check code) |

MD4

- Algoritmus MD4 Message-Digest je kryptografická hash (otisk) funkce vyvinutá Ronaldem Rivestem v roce 1990. Délka otisku je 128 bitů. Algoritmus ovlivnil pozdější návrhy, jako jsou algoritmy MD5, SHA-1 a RIPEMD.
- Bezpečnost MD4 byla vážně narušena. První úplný kolizní útok proti MD4 byl publikován v roce 1995 a od té doby bylo publikováno několik novějších útoků. Existuje také teoretický útok na předobraz.
- Bezpečnost - Slabiny MD4 byly demonstrovány Den Boerem a Bosselaersem v článku publikovaném v roce 1991. První úplný kolizní útok na MD4 objevil Hans Dobbertin v roce 1995, jehož provedení trvalo v té době pouze několik sekund. V srpnu 2004 Wang et al. objevili velmi účinný kolizní útok, spolu s útoky na pozdější návrhy hashových funkcí v rodině MD4/MD5/SHA-1/RIPEMD. Tento výsledek byl později vylepšen Sasaki et al., (Klíma) a generování kolize je nyní stejně levné jako její ověření (několik mikrosekund).
- V roce 2011 RFC 6150 uvedl, že RFC 1320 (MD4) je historický (zastaralý).
- Nalezené kolize prokazují, že minimální vzdálenost MD4 je $H_d=1$. To znamená, že existují data, kde MD4 nerozpozná ani změnu v jenom bitu! Díky nelinearitě kódu nelze vypočítat váhové rozložení a pravděpodobnost selhání detekce (viz požadavky EN 50159).

Doporučení změn v protokolu RaSTA Safety Code, Check Code

- Stanovit kvantitativní cíle (TFFR) pro kontrolu integrity v rozhraních EULYNX. Z těchto cílů odvodit kvantitativní požadavky na pravděpodobnost selhání kontroly integrity.
- Posoudit, zda kvantitativní požadavky na detekci jsou prokazatelné pro nějaký set parametrů kontroly integrity v protokolu RaSTA.
- Doplnit protokol RaSTA o další možnosti v kontrole integrity
 - Safety Code založený na otisku MD4 rozšířit a použít konstrukci s využitím CRC, která umožní doložení kvality detekce pro kvantitativní cíle.
 - Check Code doplnit o další varianty CRC, které by se Safety Code umožnily větší škálovatelnost detekčních vlastností pro použití EULYNX ve velkých datových centrech.

Závěr

- Systémový pilíř společně s procesem STIP a jeho podporou na úrovni evropského železničního sektoru definují cestovní mapu k cílové architektuře, systémovým rozhraním a časovému plánu změn TSI.
- EULYNX je jednou z iniciativ, která vstupuje do Systémového pilíře; zároveň dále samostatně rozvíjí prvky, v nichž se se Systémovým pilířem nekryje.
- Specifikace EULYNX je vždy nutné doplnit o národní/aplikační kontext, ověřit integraci specifickou pro každý projekt, navrhnout koncept kybernetické bezpečnosti a dlouhodobý přístup k zajištění kompatibility verzí – tato odpovědnost leží na správcích železniční infrastruktury.
- Rizikem uplatnění EULYNX zůstávají požadavky, které mohou vést k nekompatibilitě s budoucími evropskými standardy.
- Výzvou při uplatnění specifikací EULYNX u konkrétního správce infrastruktury je jejich převedení do realistických, udržitelných a bezpečných řešení v souladu s vizí dlouhodobého rozvoje konkrétního železničního systému.



Děkuji za pozornost



© AŽD Praha s.r.o., 2021 All rights reserved.
Žirovnická 3146/2, Záběhlice, 106 00 Praha 10, Czech Republic

www.azd1.cz