Univerzita Pardubice
Dopravní fakulta Jana Pernera

Ověření naplnění výchozích funkčních požadavků na implementaci ETCS L2 v podmínkách dané železniční infrastruktury

Bc. Daniel Kolář

Diplomová práce
2018

Univerzita Pardubice
Dopravní fakulta Jana Pernera
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Daniel Kolář**
Osobní číslo:	**D16387**
Studijní program:	**N3708 Dopravní inženýrství a spoje**
Studijní obor:	**Elektrotechnické a elektronické systémy v dopravě**
Název tématu:	**Ověření naplnění výchozích funkčních požadavků na implementaci ETCS L2 v podmínkách dané železniční infrastruktury.**
Zadávající katedra:	**Katedra elektrotechniky, elektroniky a zabezpečovací techniky v dopravě**

Zásady pro vypracování:

Funkční požadavky na železniční zabezpečovací systém - účel, význam, charakteristika, atributy.
Analýza a rozklad funkčních požadavků, vazba na další podrobnější úrovně specifikací.
Identifikace minimální úrovně realizace systému ETCS L2 (integrace jeho jednotlivých komponent a subsystémů) nutné pro provedení relevantních ověření naplnění funkčních požadavků testovými metodami.
Aplikace metod testového ověření uplatněním konkrétního postupu na množinu vybraných funkčních požadavků v podmínkách odpovídajících reálnému provozu ETCS L2.

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

AŽD Praha s.r.o. Funkční požadavky na aplikaci ETCS L2 na infrastruktuře SŽDC : RBC ETCS [soubory formátu *.doc]. 2017. Neveřejný dokument.
ČSN EN 50 128 ed. 2. Drážní zařízení - Sdělovací a zabezpečovací systémy a systémy zpracování dat - Software pro drážní řídicí a ochranné systémy. Praha : Český normalizační institut, 2012.
Boulanger, J.-L. CENELEC 50128 and IEC 62279 Standards. 1. vyd. ISTE Ltd et John Wiley & Sons, Inc, 2015. 352 s. ISBN: 978-1-84821-634-1
Rierson, L. Developing Safety-Critical Software: A Practical Guide for Aviation Software and DO-178C Compliance. 1. vyd. CRC Press. 2013. 565 s. ISBN 978-1-4398-1369-0
Wiegers, K., E. Požadavky na software: Od zadání k architektuře aplikace. 1. vyd. Brno: Computer Press, a. s., 2008. 448 s. ISBN 978-80-251-1877-1. ČSN EN 50 126. Drážní zařízení - Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS). Praha : Český normalizační institut, 2001.
TNŽ 34 2620. Železniční zabezpečovací zařízení - Staniční a traťové zabezpečovací zařízení. Olomouc : České dráhy, s.o., 2002.

Vedoucí diplomové práce: **Ing. Jan Ouředníček, Ph.D.**
AŽD Praha

Datum zadání diplomové práce: **15. listopadu 2017**
Termín odevzdání diplomové práce: **18. května 2018**

doc. Ing. Libor Švadlenka, Ph.D.
děkan

L.S.

Ing. Dušan Černák, Ph.D.
vedoucí katedry

V Pardubicích dne 12. března 2018

Prohlášení autora

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury. Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 18. 5. 2018 Daniel Kolář

Poděkování

Tímto bych chtěl poděkovat vedoucímu práce panu Ing. Janu Ouředníčkovi, Ph.D. za konzultace nad popsanými metodami a postupy i za odborné vedení této práce. Rovněž děkuji kolegovi Tomáši Zapletalovi za spoluúčast při měřících jízdách motorového vozu a za asistenci během získávání videozáznamů klíčových pro vyhodnocení výsledků.

Anotace

Práce se zabývá tvorbou a ověřením funkčních požadavků na interoperabilní vlakový zabezpečovací systém ETCS. Obsahuje poznatky a nabyté zkušenosti při tvorbě dokumentované specifikace chování systému ETCS včetně vysvětlení smyslu dalších atributů funkčních požadavků potřebných ke kvalitnímu vedení projektu. Po provedení analýzy a popisu charakteru funkčních požadavků bylo provedeno uplatnění metod testového ověření naplnění několika vybraných funkčních požadavků.

Klíčová slova

funkční požadavky, metody ověření, vlakový zabezpečovací systém, ETCS L2

Title

Verification of ETCS L2 High-level Functional Requirements implementation in conditions of the particular Railway infrastructure

Annotation

This work deals with creation and verification of functional requirements for interoperable train control system ETCS. It contains knowledges and gained experiences with creation documented specification of system ETCS behavior including explanation meaning of other functional requirement attributes which are necessary to effective project leading. After analyzing and describing the nature of functional requirements, the application of test verification methods was evaluated several selected functional requirements.

Keywords

functional requirements, verification methods, train control system, ETCS L2

Obsah

Úvod

Funkční požadavky tvoří stejně jako kód implementace v SW zařízení důležitou součást hotového systému, jenž předává uživateli nebo zákazníkovi informaci o tom, jak se bude systém vůči svému okolí chovat, jak bude reagovat na změny stavů svých i stavů připojených systémů a komponent.

Při porovnávání významu tvorby požadavků s vlastní realizací kódu implementace by se na první pohled mohlo zdát, že se jedná méně významnou práci s menším vlivem na výsledek, než je vlastní tvorba HW a kódování SW systému, ale to je omyl, neboť i vývojář a programátor uvažují při návrhu systému podle toho, co má systém vlastně dělat a co se po něm požaduje, byť tyto poznatky cíleně dokumentačně nezachytí.

Nejde pouze o potřebu prostého zdokumentování současného systému, ale také o materiál, jenž můžeme dále rozšiřovat, zdokonalovat a využít pro potřeby budoucího vývoje nových systémů ať už přímo spolupracujících nebo inovujících stávající systém. Může být podkladem k porovnání dvou konkurenčních (z hlediska obchodního, technického, či z hlediska účelu) systémů. Po zavedení změn do požadavků lze rozhodnout, jaké změny je nutné provést i ve vlastní realizaci systému. Rovněž lze díky této dokumentaci požadavků na systém rychleji vytvořit materiály pro školení zaměstnanců a uživatelů, jenž se s tímto systémem setkávají poprvé a je potřeba je seznámit s chováním systému.

Obecně lze požadavky rozdělit na funkční a parametrické (v angl. literatuře označované jako Non-functional) (*Wiegers 2008*). Zatímco funkční požadavky specifikují chování systému z hlediska změn stavu systému, parametrické specifikují jiné vlastnosti jako např. výkonnost nebo parametry RAMS (bezpečnost, spolehlivost, udržitelnost, dostupnost) a jsou limitovány omezeními při návrhu, vývoji a konstrukci výsledného produktu (systému).

1 Systém ETCS

European Train Control System (ETCS) je vlakový zabezpečovací systém nasazovaný v Evropě jako interoperabilní systém s cílem pokrýt železniční infrastruktury jednotlivých států jednotným vlakovým zabezpečovačem a umožnit tak plnohodnotný provoz vozidel vybavených mobilní částí tohoto systému i v cizích zemích, ve kterých jsou dosud instalované pouze národní vlakové zabezpečovače specifické pro každý stát. Nasazení tohoto zabezpečovače s sebou až na výjimky přináší vůči stávajícím systémům také zvýšení úrovně dohledu jízdy vozidel na úplnou kontrolu rychlosti. Z hlediska aplikačních úrovní ETCS byla na síti SŽDC po zkušenostech zvolena instalace ETCS L2.

Interoperability je dosaženo dodržením jednotných principů, procesů a prostředků přenosu informace k zajištění dohledu nad jízdou vozidla, jež jsou náplní systémových požadavků ze souboru specifikací (tzv. SUBSETů) vydávaných European Union Agency for Railways (dříve European Railway Agency). V době vzniku této práce (duben 2018) jsou vydané tři ETCS specifikace platné současně:

- ETCS Baseline 2,
- ETCS Baseline 3,
- ETCS Baseline 3 release 2.

Tyto specifikace jsou diskutovány zástupci všech zainteresovaných subjektů (výrobců, správců infrastruktury, provozovatelů drážní dopravy, …) železničních zabezpečovacích zařízení a jejich znění je doplňováno, upřesňováno a modifikováno pomocí tzv. change requests. Příslušné specifikace jsou jedním z klíčových zdrojů pro vytvoření funkčních požadavků na vytvářený systém ETCS i v podmínkách české železniční infrastruktury, která je pod správou SŽDC.

Systém ETCS se skládá ze stacionární části a mobilní části. Mobilní část je umístěná na vozidle a je tím subsystémem, který přímo vykonává dohled nad jízdou vozidla podle přijatých povolení a dalších informací, kterými disponuje samo vozidlo (změna módu, odměřování vzdálenosti, atd.). Stacionární část systému ETCS (v úrovni L2) vyhodnocuje polohu vozidla spolu s podmínkami na infrastruktuře a zásobuje mobilní část povoleními k jízdě a dalšími informacemi o stavu infrastruktury.

Pro účely dohlížení jízdy vozidla bylo nadefinováno 17 módů mobilní části, které se liší rozsahem, jakým je jízda vozidla dohlížena a možnostmi jakými vozidlo disponuje. Vozidlo se

může v jednom okamžiku nacházet pouze v jednom módu. Informaci o svém stavu mobilní část předává stacionární části typicky periodickým odesíláním zprávy č. 136: Train Position Report (dále jen PR).

Zatímco mobilní část tohoto systému je jednotná pro všechny státy, stacionární část musí být navržena a vybudována nad stávajícím zabezpečovacím zařízení, které je pro každý stát specifické, tak aby bylo dosaženo (interoperabilních) principů bezpečného dohlížení jízdy vozidel.

ETCS specifikace dále definují rozhraní mezi:

- stacionární a mobilní částí systému ETCS (zprávy a pakety pro komunikaci mobilní části s RBC a naopak);
- mobilní částí systému ETCS a strojvedoucím vozidla prostřednictvím jednotného zobrazení dispozic vydaných vozidlu na DMI aktivního ovládacího pultu.

1.1 Dohlížení jízdy vozidel

Mezi dohledové informace zařazujeme povolení k jízdě (MA) a SR autorizaci. Pokud vozidlo nemá platnou dohledovou informaci, není mu umožněno pokračovat v jízdě s výjimkou případů, kdy strojvedoucí vědomě vykonal činnost na mobilní části s následkem převzetí zodpovědnosti od systému. Stacionární část systému ETCS má k dispozici informaci o poloze čela vozidla nahlášeného v PR od mobilní části a jelikož je tato informace zprostředkována jako interval, v němž se má skutečné čelo vozidla v době vytvoření této informace na vozidle nacházet, pracuje systém ETCS s různým typem čela (uvažuje jeden nebo druhý konec intervalu) v různých požadavcích.

1.1.1 Dohledová informace MA FS, vozidlo v módu FS

Vozidlo přijme dohledovou informaci MA FS, pokud má systém ETCS informace o vyhrazení jízdní dráhy pro dané vozidlo a zároveň vylučuje přítomnost jiného vozidla před čelem vozidla v rámci takové jízdní dráhy. Rychlost vozidla jedoucího v módu FS je omezena rychlostními profily, jenž jsou součástí dohledové informace MA. V případě, že je mobilní část vozidla v módu FS, zodpovídá systém ETCS plně za bezpečnost jízdy vozidla.

1.1.2 Dohledová informace MA OS, vozidlo v módu OS

Vozidlo přijme dohledovou informaci MA OS, pokud má systém ETCS informace o vyhrazení jízdní dráhy pro dané vozidlo, ale nemůže vyloučit přítomnost jiného vozidla před čelem

vozidla v rámci vyhrazené jízdní dráhy. Rychlost vozidla jedoucího v módu OS je, nad rámec ostatních rychlostních profilů, omezena národní hodnotou.

1.1.3 SR autorizace, vozidlo v módu SR

Vozidlo přijme SR autorizaci, pokud systém ETCS nemá informace k vyhrazení jízdní dráhy pro dané vozidlo a rovněž nemůže vyloučit přítomnost jiného vozidla před čelem vozidla. Rychlost v módu SR je omezena národní hodnotou. Neuplatňuje se dohled dle rychlostních profilů, ale rychlost ke konci SR autorizace je omezena brzdnými křivkami. Dále rozlišujeme 3 druhy SR autorizací, podle délky na kterou umožní jízdu vozidla.

Nulová SR autorizace neumožňuje jízdu vozidla, slouží k zajištění stojícího vozidla v případech, kdy není vyloučena jízda vozidla na téže koleji v opačném směru.

Omezená SR autorizace vymezuje vzdálenost, na kterou se může vozidlo pohybovat vpřed na koleji. Odesílá se jako preventivní opatření snižující riziko projetí zakazující návěsti na hlavním návěstidle, kdy nelze umožnit jízdu v FS ani v OS módu.

Neomezená SR autorizace umožňuje jízdu vozidla vpřed bez délkového omezení, přičemž se uvažuje, že dojde ke kontaktování BG a možnosti odeslat dohledovou informaci MA v OS či FS módu.

1.1.4 Vozidlo v ostatních módech

Ostatní módy jsou voleny strojvedoucím, nebo do nich provádí přechod samotná mobilní část na základě okolností (např. přechod do módu TR, který proběhne společně s aktivací nouzového brzdění po projetí konce dohledové informace čelem vozidla). Aktuální mód vozidla je indikován strojvedoucímu na DMI aktivního ovládacího pultu.

Každý mód má svá specifika použití a charakteristické vlastnosti. Specifikace ETCS předurčují použití těchto módů a definují zodpovědnosti osob a systému pro každý mód zvlášť.

NP (No Power)	UN (Unfitted)
SB (Stand-By)	TR (Trip)
PS (Passive Shunting)	PT (Post Trip)
SH (Shunting)	SF (System Failure)
LS (Limited Supervision)	IS (Isolation)
SL (Sleeping)	SN (National system)
NL (Non-Leading)	RV (Reversing)

Tab. 1 Přehled ostatních módů mobilní části ETCS

2 Funkční požadavky

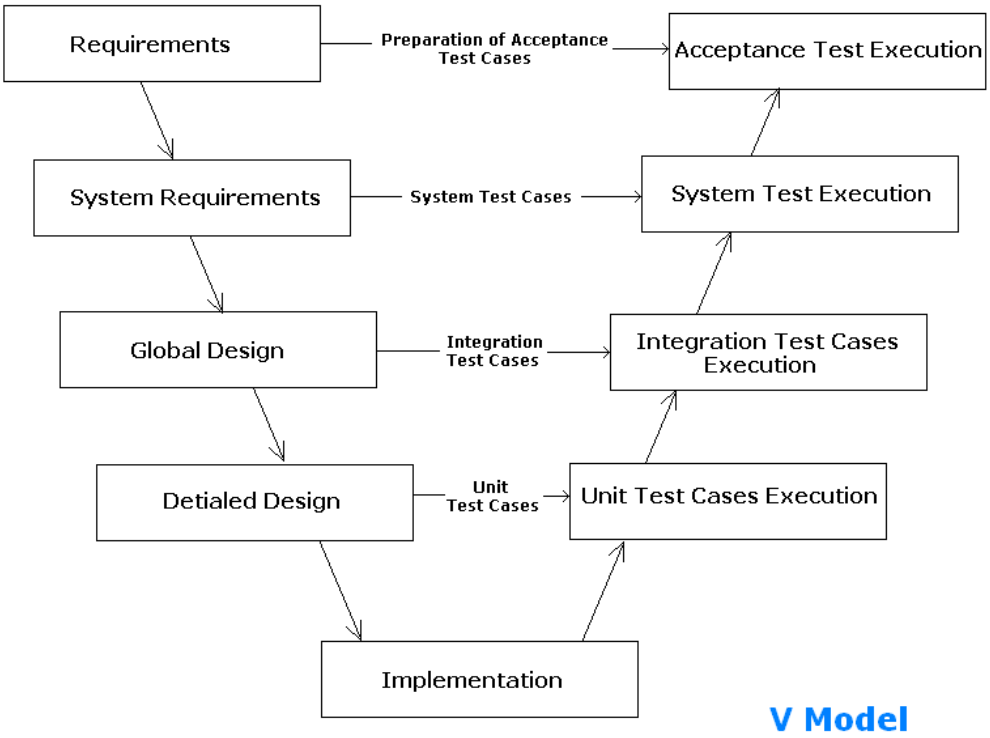
Podnětem pro vznik požadavků na systém je vytvoření specifikace systému zahrnující popis všech požadovaných vlastností a chování systému při rozličných stavech systému, resp. kombinace takových okolních podmínek a vnitřních stavů systému, které by měly vyvolat známou, předem definovanou reakci systému. Účelem požadavků je předejít nenaplnění očekávání zákazníka při a po realizaci projektu.

Např. dokument DO-178C Software Considerations in Airborne Systems and Equipment Certification (Certifikace leteckých systémů a vybavení) dále pracuje s pojmy High-Level požadavek, Low-Level požadavek, softwarový požadavek a odvozený požadavek. Kromě toho se specifikací softwarových požadavků zabývá i norma pro drážní zařízení ČSN EN 50128 ed. 2. Oba dokumenty vyžadují zavedení trasování požadavků na své zdroje a cíle.

Členění softwarových požadavků podle DO-178C:

- Softwarový požadavek – *„popisuje, co má být produkováno softwarem při daných vstupech a omezeních. Softwarové požadavky jsou High-Level i Low-Level“ (Rierson 2013).*
- High-Level požadavek – *„softwarový požadavek vyplývající z analýzy systémových požadavků, požadavků na bezpečnost a systémovou architekturu“ (Rierson 2013).*
- Low-Level požadavek – *„softwarový požadavek vyplývající z High-Level požadavků, odvozených požadavků a omezení návrhu, který může být přímo implementován bez dalších informací“ (Rierson 2013).*
- Odvozený požadavek – *„požadavek vytvořený při vývoji softwaru, který není přímo trasovatelný na High-Level požadavky a/nebo specifikuje chování za systémovými požadavky“ (Rierson 2013).*

Funkční požadavky nemají za úkol popisovat konkrétní realizaci implementace požadovaného chování. Požadavky jednak slouží k ověření, že konkrétní realizace není v konfliktu s požadovaným chováním, dále aby podle jejich znění následně vzešel návrh realizace v dalších nižších úrovní požadavků.



Obr. 1 V-model (V-model (Software Development Life Cycle) 2012)

Jedním z průmyslově využívaných typů životních cyklů (vedení projektu) je tzv. V-model, který přehledně odděluje požadavkovou fázi, implementační fázi a verifikační s validační fází. V levé části modelu se nachází požadavky, vůči kterým se ve stejné úrovni řešení (v jednom řádku V-modelu) nachází v pravé části modelu testové ověření těchto požadavků. V časovém okně mezi těmito dvěma procesy probíhá tvorba požadavků stále nižších úrovní a to až do implementace. Po implementaci se postupně ověřují požadavky stále vyšších úrovní prostřednictvím příslušných testů v rámci stejné úrovně řešení. Dílčí části V-modelu mohou být tvořeny prováděním menších V-modelů uvnitř.

Vůči funkčním požadavkům probíhá dokázání naplnění požadovaného chování prostřednictvím testových případů. Díky těmto testovým případům můžeme provést ověření funkčního chování celého systému ETCS.

Výchozí funkční požadavky na systém by měly být definovány ještě před vlastním návrhem systému, což jde sice proti přání vytvořit „něco“ v co nejkratším čase, ale funkční požadavky představují dokumentovanou vizi (chování systému) a umožňují kontrolu nad následnou vlastní realizaci systému (implementací softwaru). Tvorba požadavků na systém rovněž předchází

etapě „návrhu včetně implementace a výroby a zavedení“ v životním cyklu, který doporučuje norma ČSN EN 50126.

Dobrý popis funkčního chování do funkčních požadavků na počátku projektu umožní odhalení nesprávného chování systému ještě v době, kdy jeho opravy budou stát minimum nákladů v porovnání s pozdější eliminací chyb odhalených ve fázi testování téměř hotového systému. Studie prokazují, že až 30% chyb v realizaci systému vzniká v důsledku špatně vytvořených požadavků. (Wiegers 2008, Rierson 2013).

2.1 Zápis funkčních požadavků

Funkční požadavky lze zapsat v přirozeném jazyce, matematické podobě (rovnice), grafických (vývojových) diagramech. S ohledem na charakter výstupů ze systému ETCS, které vždy zaujímají určitý slovně popsatelný stav více subsystémů (např. dohledová informace vozidla – mód a indikace zobrazené strojvedoucímu na subsystému DMI po naplnění funkčního požadavku + indikace na subsystému HMI RBC), a dosavadní praxe v oblasti zabezpečovací techniky v ČR, byl (i přes svou omezenou jednoznačnost u složitých systémů) zvolen textový popis požadavků v přirozeném jazyce v unifikovaných tabulkových strukturách, v nichž jsou atributy požadavků rozděleny do buněk. Vzhledem k rozsáhlosti požadovaného funkčního chování systému ETCS byly funkční požadavky rozděleny hierarchicky podle svého významu do několika samostatných dokumentů.

Správa požadavků se skládá z:

- vyhledání / získání požadavků od všech zúčastněných stran,
- diskuze požadavků se zákazníkem,
- dokumentace požadavků,
- verifikace požadavků.

Primárním zdrojem požadavků je zákazník, resp. všechny zúčastněné strany, které sdělují své připomínky k výsledné podobě systému. Dalším původcem funkčních požadavků jsou samotní řešitelé systému, kteří přicházejí s návrhem systému a v průběhu vývoje před nimi vyvstávají nové požadavky ze zkušeností s realizací. Velice důležité je průběžné projednávání a odsouhlasení požadovaného chování systému se zákazníkem s ohledem na jeho realizovatelnost, přínos a na omezení daná konstrukcí výsledného systému (výkonnost, investiční nákladnost, atd.).

Mezi zdroje pro funkční požadavky na systém ETCS tak patří:

- dokumenty ETCS specifikace, tj. systémové požadavky (system requirement specification) vydávané European Union Agency for Railways standardizující principy, procesy a prostředky k dosažení interoperability systému ETCS;
- ZTP SŽDC, tj. zvláštní technické podmínky zákazníka a uživatele systému na konkrétní projekt (např. Kolín – Břeclav st. hr.);
- případy užití obsahující vybrané scénáře funkčního chování systému projednané se zástupci zákazníka, tj. uživatele systému, jakožto jedna z technik získávání požadavků;
- analýzy a diskuze řešitelů vytvářené v reakci na aplikování požadavků z předchozích bodů na systém zabírající důsledky a návrhy řešení v konkrétních podmínkách.

Požadavky zákazníka (ZTP SŽDC) jsou nejvyšší úrovní požadavků, ovšem často tyto požadavky nejsou napsané ve formě, v níž by byly přímo ověřitelné provedením testů systému, nýbrž ve formě očekávání zákazníka a cíle, které má systém splňovat. Zároveň platí, že požadavky zákazníka nesmí být v rozporu s technickými normami železnic (např. TNŽ 34 2620) a souborem specifikací ETCS (SUBSET).

Množství funkčních požadavků vznikne v důsledku odvození od požadavků, které předloží zúčastněné strany typicky pro konkrétní provozní situace. Tyto požadavky pokrývají ve specifikaci systému např. situace, které nebyly známy při zadání výchozí specifikace systému.

Typová charakteristika požadavků není v žádné literatuře normativně definována. *„Různí pozorovatelé mohou tutéž větu popsat jako uživatelský požadavek, softwarový požadavek, funkční požadavek, systémový požadavek, technický požadavek.“ (Wiegers 2008).* Pojem funkční požadavek využívá např. směrnice Aerospace Recommended Practice ARP4754.

Stejně jako systém se i funkční požadavky na systém v průběhu času vyvíjejí tak, jak jsou diskutovány a realizovány. Pro zvládnutí a kontrolu budoucích změn je důležité udržet kompaktnost celé specifikace požadavků ve smyslu dopadu změny specifikace jednoho funkčního požadavku na jiné příbuzné funkční požadavky a požadavky nižších úrovní. Kromě normy ČSN EN 50128 ed. 2 na vývoj softwaru pro drážní řídící a ochranné systémy, která sama vyžaduje trasovatelnost požadavků na software, se i z uvedených předchozích důvodů mezi funkčními požadavky zavádí vazba trasování.

Specifikace musí být rovněž schopna přijmout nový požadavek (novou funkční vlastnost – např. odeslání nového upozornění strojvedoucímu) v průběhu vývoje systému i po dobu jeho nasazení v provozu. Specifikace by proto měla být verzována tak, jak jsou v ní změny aplikovány.

Skupinu funkčních požadavků se stejným významem výstupu systému lze označit za funkční vlastnost, kterou má systém poskytovat. V dokumentech funkčních požadavků na systém ETCS je společná funkční vlastnost využita k organizaci dokumentů a nachází se přímo v názvu kapitoly funkčních požadavků např. prodloužení MA FS na staniční kolej. Díky tomu je udržena v celé specifikaci větší přehlednost.

2.2 Atributy funkčních požadavků

V případě, že jsme pro popis funkčních požadavků zvolili textovou formu, lze k funkčnímu požadavku (jeho specifikaci) připojit další vlastnosti neboli atributy, které vysvětlují jeho význam, příčinu, dopad na systém atd. Vedle atributu specifikace samotného funkčního požadavku tak definujeme i další atributy, jejichž změny mohou být v průběhu vývoje s výhodou vyhodnocovány samostatně. Chceme-li však vyhodnocovat změny samostatných atributů požadavků, musíme vytvořit strukturu funkčního požadavku (šablonu), v níž jsou všechny atributy od sebe navzájem odděleny – jako vhodné se jeví tabulkové uspořádání funkčního požadavku.

Identifikace požadavku		
Verze systému	Baseline	Projekt
Specifikace požadavku		
Poznámky		
Vyplývá z	Rodič, potomek	
Případy užití	Odkazy	
Závaznost		
Bezpečnostní relevance		
Kritéria splnění požadavku		

Tab. 2 Šablona funkčního požadavku

2.2.1 Identifikace

Identifikace požadavku musí být unikátní v celém projektu a po případném zániku požadavku v budoucnu, nesmí být jeho identifikátor využit pro jiný požadavek z důvodů potenciální změny významu takového požadavku při zapomenutých vazbách z jakékoliv části dokumentace projektu na tento požadavek nebo rizik spojených s obnovou původního požadavku a následnou duplicitou.

Identifikátor funkčních požadavků na systém ETCS se skládá z unikátního čísla, k němuž je připojen suffix naznačující funkční vlastnost, jíž požadavek popisuje.

2.2.2 Baseline

Jak již bylo vysvětleno v kapitole 1, v současné době existuje několik vedle sebe uznávaných specifikací systému ETCS tzv. baseline. Příkladem jak mohou být baseline rozdílné je např. paket 39: Track Condition Change of traction system, který v baseline 2 obsahuje proměnnou M_TRACTION o délce 8bitů, která jednoznačně identifikuje trakční systém, jenž může být použit na dané trati. V baseline 3 release 2 ten samý paket udává trakční systém prostřednictvím dvou proměnných – M_VOLTAGE reprezentující hodnotu napětí a NID_CTRACTION nesoucí národní identifikátor trakčního systému.

2.2.3 Verze systému

Udává systémovou verzi ETCS, které odpovídá navržená část systému ETCS (stacionární nebo mobilní). Systém ETCS se stále vyvíjí a tak vznikají nové baseline, přičemž každá baseline obsahuje několik systémových verzí. V provozu se tak mohou potkávat vozidla a stacionární část s různými systémovými verzemi. Náplní tohoto atributu je definice, jakých systémových verzí se tento požadavek týká.

2.2.4 Projekt

Tento atribut udává projekty, ke kterým se vztahuje implementace příslušného funkčního požadavku. Znění funkčních požadavky vyplývají z toho, co požaduje zákazník ve svých zadáních. Pokud si zákazník bude přát v novém projektu implementovat novou funkční vlastnost, protože to je např. specifikum daného projektu, vytvoří se nové funkční požadavky pouze pro daný projekt.

2.2.5 Specifikace požadavku

Specifikace funkčního požadavku je jeho hlavní část, která definuje požadované chování systému. Strukturálně se může skládat z popisu úvodního stavu, v němž se vozidlo nachází, který následují podmínky, po jejichž splnění má systém zareagovat požadovaným způsobem.

Jednotlivé podmínky funkčního požadavku mohou být plněny současně (využíváme spojení podmínek slovy „a zároveň“), nebo sekvenčně („a následně“), v takovém případě je pro uplatnění požadavku nutné dodržet pořadí, ve kterém jsou podmínky požadavku splňovány.

Požadavky by měly být napsány stručně a výstižně, aby nedocházelo k vytvoření odlišného vlastního výkladu čtenáře, než v jakém je funkční požadavek psán. Vysvětlující souvislosti jsou proto velice důležité pro pochopení problematiky, ale je vhodné je spíše oddělit formou poznámek pod textem než tvorbou složitých souvětí.

Specifikaci požadavků se snažíme psát v přítomném čase a omezit minulý čas na nezbytné minimum, jelikož se bez dalšího rozvinutí může jevit jako příliš vágní – např. formulace „systém ETCS disponoval informací o volnosti“.

2.2.6 Odkazy

V tomto atributu se nacházejí identifikátory požadavků, které popisují realizaci systému, resp. požadavky nižší úrovně, které řeší daný funkční požadavek. Do odkazů nezařazujeme identifikátory původců vzniku funkčního požadavku, protože těm je věnován samostatný atribut „vyplývá z“.

2.2.7 Případy užití

Případy užití tvoří nižší úroveň specifikace (obsahuje i prostředky, kterými je systém realizován), která je však často předchůdcem samotného funkčního požadavku, jelikož požadavek vzniknul po projednání scénářů ve znění případu užití se zástupci zákazníka.

2.2.8 Vazby vyplývá z

Funkční požadavky vyplývají zejména z požadavků zákazníka. Každý funkční požadavek musí z něčeho vyplývat, aby bylo vůbec možné určit příčinu a účel vytvoření funkčního požadavku. Pokud se v tomto atributu nachází odkaz na jinou formu specifikace (analýzy), pak je to z důvodu, že se jedná o detailnější určení příčiny toho, proč vlastně takový požadavek vznikl.

2.2.9 Rodič/potomek

Tento atribut obsahuje identifikátory rodičovských požadavků nebo potomků tohoto požadavku. Ty tvoří hierarchii požadavků v rámci dané úrovně požadavků, tj. funkčních požadavků, nikoliv vazby na nižší (jiné) úrovně specifikace. Vazby mezi požadavky podrobněji uvádí Kolář (2018).

2.2.10 Závaznost

Závaznost představuje prioritu, s jakou má být celý požadavek implementován ve výsledném systému, nikoliv prioritu s jakou se má do systému implementovat v průběhu vývoje z časového hlediska. Bezpečnostně kritické požadavky pro vydání dohledové informace vozidlu musí být označeny nejvyšší prioritou, neboť se jedná o hlavní vlastnost systému, bez níž by neměl přílišný přínos a mohlo by dojít ke snížení bezpečnosti. Opakem jsou požadavky, které slouží k předání doplňující informace strojvedoucímu, jež sice ovlivní úsudek strojvedoucího v dané situaci, nicméně dohled nad jízdou vozidla prostřednictvím vlakového zabezpečovač zajistí, že bezpečnost jízdy vozidla není ani v případě, kdy strojvedoucí není spraven o stavu okolností, ohrožena.

Funkční požadavky na systém ETCS mají nadefinovány 4 kategorie závaznosti:

a) Povinný (Mandatory) – klíčové požadavky k dosažení cílových vlastností celého systému;
b) Vysoce doporučený (High Recommended) – požadavky, jejichž implementace je předpokládaná v řešení systému a případné zásadní důvody k tomu požadavek neimplementovat musí být dokumentovány – dohledatelnou písemnou formou;

c) Doporučený (Recommended) – požadavky, jejichž implementace je předpokladem k dosažení efektivní činnosti celého systému, nicméně jejich případné neimplementování nemá zásadní vliv na bezpečnost;
d) Volitelný/nepovinný (Optional) – případné neimplementování těchto požadavků nemá zásadní dopad na efektivní činnost systému ani na bezpečnost.

2.2.11 Bezpečnostní relevance

Bezpečnostní relevance udává jakým způsobem je požadavek spojen s bezpečností vozidla, důvody jak a proč se tento požadavek přičiní o zvýšení bezpečnosti jízdy vozidla. V tomto atributu se rovněž nacházejí odkazy na požadavky, které s příslušným požadavkem souvisí a vyvozují další funkční chování systému v případě nenaplněného požadovaného chování systému nebo strojvedoucího.

Zdrojem k těmto informacím jsou mj. i specifikace systému ETCS, které popisují zodpovědnost zúčastněných stran při jízdě vozidla v daném módu.

2.2.12 Kritéria naplnění požadavku

Tato část požadavku poskytuje možnost ověření implementace požadavku. Cílem není popsat všechny stavy systému a způsoby, kterými má být dosaženo požadované reakce systému, ale uvést jednoduchý příkladný postup, jehož provedením by měl být požadavek naplněn. Slouží i k rámcovému ujištění, že požadavek je testovatelný ještě před samotnou tvorbou testových případů, a ujištění čtenáře, že požadavek správně chápe.

Tento atribut je prázdný u rodičovského požadavku, jehož naplnění zajišťují jeho potomci, protože rodičovský požadavek je příliš abstraktní, než abychom ho mohli prohlásit za naplněného při provedení určitého příkladného postupu.

3 Charakteristika funkčních požadavků

Pro tvůrce systému představují funkční požadavky, následující požadavky na systém od zúčastněných stran, druhou nejvyšší úroveň požadavků s maximální možnou mírou abstrakce pro provedení testového ověření jejich naplnění. Tyto požadavky jsou ověřovány při nahlížení na systém ETCS rozdělený na subsystémy (RBC, OBU, …) jejichž funkční projev se projevuje jak na rozhraní k obsluze, tak situacemi vozidla v kolejišti.

Projevy naplnění funkčního požadavku musí být detekovatelné zákazníkem (uživatelem), aniž by bylo nutné sledovat vnitřní stavy systému, které nejsou dostupné jinak, než pomocí speciálních technických prostředků (např. vyčtení a prohlížení logů). Ke sledování projevu a příčin funkčního chování systému ETCS jsou tedy využita stávající zabezpečovací zařízení a jejich obslužná pracoviště a pak samozřejmě rozhraní zajišťující indikace a ovládání systému ETCS. Strojvedoucímu ke komunikaci se systémem ETCS slouží DMI. Dispečerovi umožní vedle sledování informací o vozidlech a stavu infrastruktury také ovlivnění činnosti ETCS rozhraní HMI RBC.

Funkční požadavky, které vyžadují složitější popis rozložení prvků a topologie kolejiště v okolí vozidla, obsahují kromě slovního popisu i křížový odkaz na ilustrační nákres dané situace obsahující i naznačené aktivity a reakce systému ETCS.

3.1 Postup při tvorbě nových funkčních požadavků

Jeden požadavek by měl obsahovat pouze jedno „má“ (ekvivalent anglického „shall“) – ve smyslu „má provést“, „má vykonat“. Jsou-li splněny podmínky, má systém ETCS zareagovat požadovaným způsobem. Tuto zásadu samozřejmě nelze brát doslovně, dochází-li k projevu chování systému na více subsystémech najednou (HMI RBC, DMI, …), ale principiálně pokud na toto chování bezprostředně navazuje další podmínka a systém má provést něco dalšího (nabízí se doplnit do požadavku „a pokud navíc“), je nutné v takovém případě vytvořit pro toto chování nový funkční požadavek, který přebírá stav předchozího. Snahou je dosažení relativně jednoduchých a zejména jednoznačných testovatelných požadavků.

Požadavky lze za cílem extrahování některé části (myšlenky nebo principu), která se opakuje ve specifikaci více požadavků, uspořádat do hierarchie rodič-potomek, v níž rodič představuje popis oné extrahované části a potomek pak konkrétnější užití rodiče. Společně jsou rodičovský požadavek a potomek testovatelný. V dosavadní tvorbě funkčních požadavků se rodič stal

netestovatelným požadavkem, jelikož je příliš abstraktní, než aby na základě jeho znění mohl vzniknout testovací případ.

Před aplikováním zamýšlených změn ve funkčním chování systému, tj. přepsání stávajících funkčních požadavků nebo vytvoření nových, se provádí tzv. non-regresní analýza. *„Non-regresní analýza se skládá z určení souboru testů k demonstrování, že modifikace, která bude provedena, nemá efekt na zbytek softwarové aplikace“ (Boulanger 2015, s. 149).*

Tato analýza tedy určí, které testové případy se budou muset opakovat.

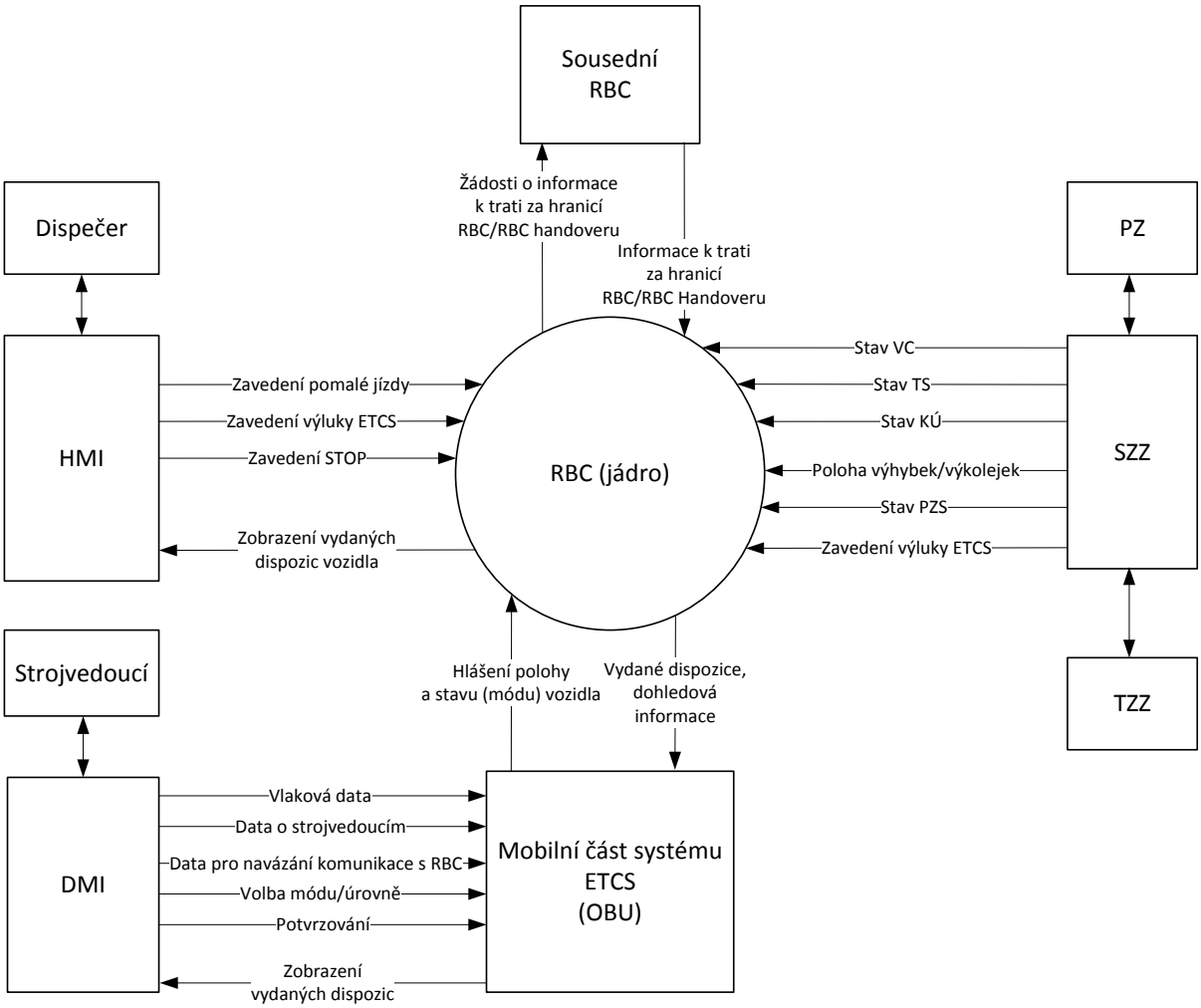
Při tvorbě funkčních požadavků musíme znát aktéry a komponenty, které tvoří koncové činitele systému, na nichž se projevuje funkční chování a které budou vystupovat i ve specifikaci požadavků. K tomuto účelu lze sestavit kontextový diagram.

3.1.1 Kontextový diagramu systému ETCS L2

Kontextový diagram (Data Flow Diagram) zobrazuje hranice mezi systémem a uživateli nebo zařízeními, které systému poskytují nebo od něj přijímají data a dále ovlivňují jeho činnost.

Systém ETCS je v zobrazení Obr. 2 dále rozdělen na jednotlivé subsystémy – RBC (jádro), HMI RBC, mobilní část systému ETCS a DMI. Datové toky jsou definovány směrem šipky a obecným popisem informací přenášených těmito daty. Komunikace systému ETCS s uživateli probíhá prostřednictvím rozhraní DMI a HMI RBC. Tyto části systému tedy slouží k převodu povelů do datových toků a opačným směrem z datových toků na indikaci stavu systému ETCS.

Stanovení hranic systému a jeho definice je současně vyžadováno normou ČSN EN 50126 pro vytvoření požadavků na RAMS.



Obr. 2 Kontextový diagram systému ETCS

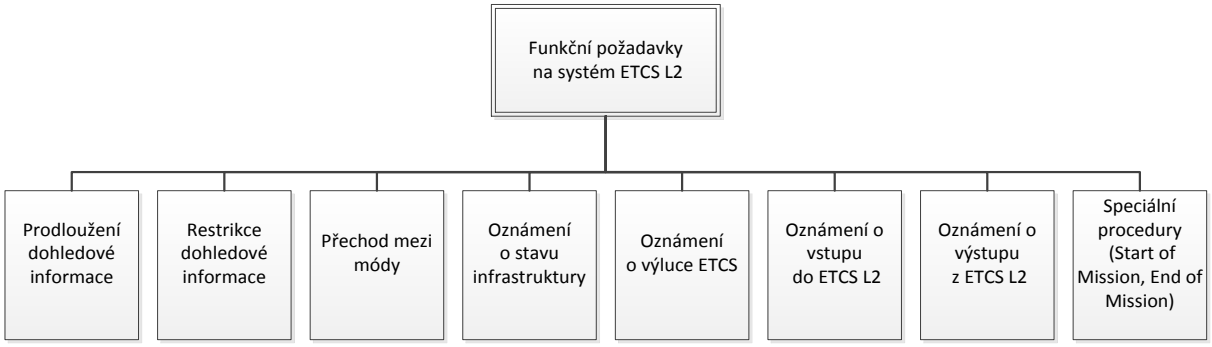
3.1.2 Vytvoření datového slovníku

Terminologie a věty, které se vyskytují ve funkčních požadavcích, by měly být pro lepší pochopení problematiky, co nejvíce výstižné a pokud možno unifikované, protože se jedná o diskrétní informace, které systém získává nebo odesílá na svá rozhraní, popř. vnitřní stavy systému, jenž vyplývají z předchozího sledu událostí.

Způsoby jakými lze dosáhnout takových vnitřních stavů mají být uvedeny v datovém slovníku, který vysvětluje význam zavedených pojmů. Příkladem je např. „systém ETCS disponuje nekompletní informací o poloze čela vozidla na staniční koleji“. To samo o sobě čtenáři nic moc neříká, ale díky datovému slovníku se dozví, co tato věta znamená, tj. že „na základě informace o předchozí jízdě vozidla nemůže systém ETCS vyloučit polohu čela vozidla na jiné staniční koleji v případech, kdy vozidlo provádělo posun a měnilo směr jízdy“.

4 Analýza funkčních požadavků

Podle typu přenášené informace mezi stacionární a mobilní částí systému ETCS, která se ve výsledku projeví určitým způsobem na vysílající nebo přijímací straně funkčně, lze funkční požadavky rozřadit do následujících skupin:



Obr. 3 Rozdělení funkčních požadavků podle přenášené informace

a) vozidlo pokračuje ve stávajícím módu (prodlouží se dohledová informace);
b) vozidlo přijme restrikci stávající dohledové informace;
c) vozidlo provádí přechod do jiného módu (systém může vyžadovat např. potvrzení od strojvedoucího vozidla);
d) strojvedoucímu vozidla se odešle oznámení o stavu infrastruktury (návěstidlo v poruše při svícení náhradní návěsti, PZS v poruše, nutná procedura Override, …);
e) strojvedoucímu vozidla se odešle oznámení o výluce ETCS;
f) strojvedoucímu vozidla se odešle oznámení o vstupu vozidla do úrovně ETCS L2;
g) strojvedoucímu vozidla se odešle oznámení o výstupu vozidla z úrovně ETCS L2;
h) mezi vozidlem a stacionární částí systému se odešle informace v rámci provedení procedur zahájení a ukončení mise atd.

Zařazení požadavků pod tyto skupiny může usnadnit rozhodování, jakou závaznost by měl daný požadavek splňovat, byť je třeba u každého požadavku individuálně zohlednit i specifické okolnosti. Nabízené kategorie závaznosti jsou popsány v kapitole 2.2.10.

Požadavky ze skupin a), c) můžeme klasifikovat jako vysoce doporučené. Pokud některý požadavek není naplněn, není zcela vyloučena funkčnost systému, ale je nutné, aby byly splněny ostatní požadavky nabízející východisko z dané situace (např. volba Override EoA).

Požadavky ze skupiny b) tvoří reakci systému na výskyt možného nebezpečí před vozidlem. Ve většině těchto požadavků je nežádoucí, aby nedošlo k jejich implementaci, a je jim tedy obvykle přiřazena nejvyšší závaznost – povinná.

Požadavky ze skupiny h) je nezbytné naplnit, aby vůbec došlo k zahájení nebo ukončení dohledu systému nad jízdou vozidla a z tohoto důvodu je jejich implementace nezbytná a závaznost označena jako povinná.

Skupiny d), e), f), g) obsahují zpravidla požadavky na zobrazení textových zpráv a jiné indikace na DMI a HMI RBC. Tyto požadavky jsou většinou volitelné.

Požadavky lze podle Easy Approach to Requirements Syntax (EARS), 2009 označit za typ:

- state-driven, který je uplatňován tehdy, když systém setrvává v určitém stavu, resp. jeho vstupy;
- event-driven, který je uplatněn bezprostředně po samotné události v systému (změna stavů).

State-driven požadavek má být tedy naplňován **po celou dobu**, kdy má splněné podmínky, zatímco event-driven požadavek má být naplněn **v jednom okamžiku** po samotné změně stavu.

Dále lze funkční požadavky na systém ETCS kategorizovat podle charakteru, jakým ovlivňují jízdu vozidla.

4.1 Požadavky na vydání dohledové informace vozidlu

Tyto požadavky jsou typu state-driven. Vozidlu se vydává dohledová informace MA nebo SR autorizace podle stavu infrastruktury před vozidlem, který analyzuje stacionární část systému ETCS – funkční požadavky lze tedy kategorizovat podle toho, v jaké její části se vozidlo aktuálně nachází:

- vozidlo na staniční koleji,
- vozidlo na traťové koleji,
- vozidlo ve zhlaví/záhlaví,

respektive kam až je vydána dohledová informace obdržená vozidlem:

- k návěstidlu na konci staniční koleje,
- k oddílovému návěstidlu,
- … jinému místu na infrastruktuře.

Do této skupiny spadají i požadavky na interakci systému se strojvedoucím za účelem získání nové informace, kdy se systém ETCS dotazuje strojvedoucího na situaci na infrastruktuře, kterou aktuálně nezískává technickými prostředky, a po potvrzení dotazu mobilní část tuto informaci následně odešle stacionární části, která vyhodnocuje podmínky před vozidlem, čili tyto požadavky jsou vázány k určitým částem infrastruktury.

Mezi tyto požadavky patří např. potvrzení TAF k hlavnímu návěstidlu.

4.2 Požadavky na interakci systému se strojvedoucím po přijetí dohledové informace

Do této skupiny patří požadavky na potvrzení oznámení zobrazeného na DMI vozidla strojvedoucímu, např. potvrzení přechodu do módu OS – strojvedoucí potvrzením fakticky od systému ETCS přebírá zodpovědnost za kontrolu volnosti koleje před čelem vozidla. Tyto požadavky navazují na požadavky řešící vydání dohledové informace, ale nejsou vztaženy ke konkrétnímu místu na infrastruktuře, nýbrž právě např. ke stavu, kdy vozidlo disponuje dohledovou informací MA OS, ale nemá informaci o tom, že strojvedoucí je srozuměn s tím, že byl přechod do OS proveden. Následkem toho vyplývá, že jde o požadavky typu state-driven.

Jedná se o funkční požadavky, v jejichž specifikaci figuruje pouze mobilní část systému ETCS, která si má, v případě že strojvedoucí nepotvrdí, sama zajistit případné omezení jízdy vozidla (např. aktivace provozní brzdy).

4.3 Požadavky na informování strojvedoucího

Tato skupina obsahuje funkční požadavky na zobrazení textové zprávy pro informování strojvedoucího o stavu infrastruktury před čelem vozidla (např. zpráva o poruše vnějších prvků zabezpečovacího zařízení umístěných v kolejišti). Tyto požadavky nemají charakter přímo ovlivňující dohled jízdy vozidla, ale mohou obsahovat důležité informace, které ovlivňují další chování strojvedoucího (např. zpráva o nutnosti provedení volby Override EoA) a jejichž přijetí je předpokladem k plynulé jízdě vozidla. Informace má být strojvedoucímu poskytována po celou dobu, kdy je prvek v poruchovém stavu, jde tedy o požadavky state-driven.

Na druhou stranu i požadavky na zobrazení informace, která odvolává předchozí zprávu (např. přejezd se opět ocitl v bezporuchovém stavu), je třeba naplňovat po dobu trvání stavu, kdy se vozidlo stále nachází před daným prvkem (přejezdem), proto jsou také typu state-driven.

4.4 Požadavky na restrikce – zkrácení dohledové informace / nouzové zastavení

Příčinami restrikcí jsou zpravidla změny na infrastruktuře, které mohou ohrozit bezpečnost jízdy vozidla, jelikož se staly na místě, do kterého již vozidlo disponuje dovolující dohledovou informací, resp. v místech kde se vozidlo podle dostupných informací právě nachází. Tyto požadavky specifikují, kde dojde k vyvolání potřeby odeslání restrikce vozidlu, ale po jejich naplnění obvykle nelze stanovit, kde vozidlo po naplnění požadavku, typicky po přijetí příkazu k nouzovému zastavení nebo vypršení časové platnosti poslední přijaté dohledové informace, zastaví. Z tohoto důvodu již nelze predikovat, v jakém stavu se po naplnění požadavku vozidlo a infrastruktura nachází. Při testování systému bude třeba zanalyzovat konkrétní situaci a vybrat, jaký požadavek a testový případ se má dále testovat.

Na první pohled by se mohlo zdát, že požadavek na zkrácení dohledové informace MA, bude mít jednoznačně definovaný stav vozidla po naplnění požadavku, ale nelze s jistotou určit, že po přijetí zkrácené dohledové informace MA, nebude toto vozidlo již tak blízko konci této dohledové informace MA, že vzápětí dojde k aktivaci nouzového brzdění a naplnění požadavku na přechod do módu TR po projetí EoA čelem vozidla.

Pokud se jedná o:

- odeslání příkazu k nouzovému zastavení vozidla (CEM nebo UEM);
- zkrácení dohledové informace MA;
- odeslání MA s nulovou délkou nebo SR autorizace s nulovou délkou *.

dochází k uplatnění těchto požadavků v důsledku události – změny stavu infrastruktury před vozidlem, který předtím vozidlu umožňoval více (např. vydání dohledové informace MA do dotčeného úseku infrastruktury). Typ těchto požadavků je tedy většinou event-driven. Stavy, kdy omezující podmínky na trati přetrvávají a kdy není žádoucí, aby jimi bylo vozidlo ohroženo, pokryjí požadavky na vydání dohledové informace (viz požadavky v kapitole 4.1).

* Zvláštním případem je požadavek na vydání SR autorizace s nulovou délkou vozidlu v módu SB nebo PT, kdy je v těchto módech mobilní částí systému ETCS zajištěno, že se vozidlo nepohybuje a tedy samotné přijetí SR autorizace s nulovou délkou pro ně nepředstavuje žádné omezení navíc vůči stávajícímu stavu. Samotná událost, která zapříčinila odeslání SR autorizace s nulovou délkou (postavení VC opačného směru vůči orientaci tohoto vozidla), mohla nastat již předtím, než se vozidlo ocitlo v módu SB (např. provedením Start of Mission)

a naplňování tohoto požadavku je požadováno po celou dobu, kdy trvá příslušný stav. Tím pádem je tento požadavek state-driven.

4.5 Požadavky na interakci strojvedoucího se systémem ETCS iniciované strojvedoucím

Tyto požadavky specifikují, jak má systém ETCS reagovat na provedení volby strojvedoucím, resp. zadání dat na DMI vozidla. Obecně takové aktivity mohou nastat kdekoliv, neboť se jedná o procedury, jejichž iniciátorem je strojvedoucí. Tyto požadavky mají být naplňovány po celou dobu, kdy nedošlo ke změně stavu, jedná se tedy o požadavky typu state-driven. Konkrétně se jedná se o požadavky na:

- zahájení mise (Start of Mission);
  - Těmito požadavky začíná dohled systému ETCS nad jízdou vozidla, sekvence provedení úkonů a zadávání dat na DMI strojvedoucím je stanovena specifikacemi ETCS, z nichž vyplývá, že pokud následně strojvedoucí provede volbu START, odešle mobilní část žádost o dohledovou informaci do stacionární části, která uděluje vozidlu dohledovou informace podle informace o poloze vozidla a dále dle podmínek (stavu infrastruktury) před vozidlem.
- ukončení mise (End of Mission);
- volbu módu strojvedoucím (SH, NL) a změnu aplikační úrovně ETCS (LSTM/L0, L1);
- aktivovanou proceduru Override EoA;
  - Provedením volby Override EoA strojvedoucí ovlivní mód vozidla – vozidlo má s výjimkou jízdy v módu SH provést přechod do módu SR a umožnit po omezenou dobu jízdu na omezenou vzdálenost. Tato procedura je určena k umožnění jízdy vozidla za konec dohledové informace (nejčastěji za hlavní návěstidlo se zakazující návěstí), případně uvedení vozidla do pohybu, pokud vozidlu nebyla dosud vydána dohledová informace.

4.6 Požadavky na délku dohledové informace MA FS

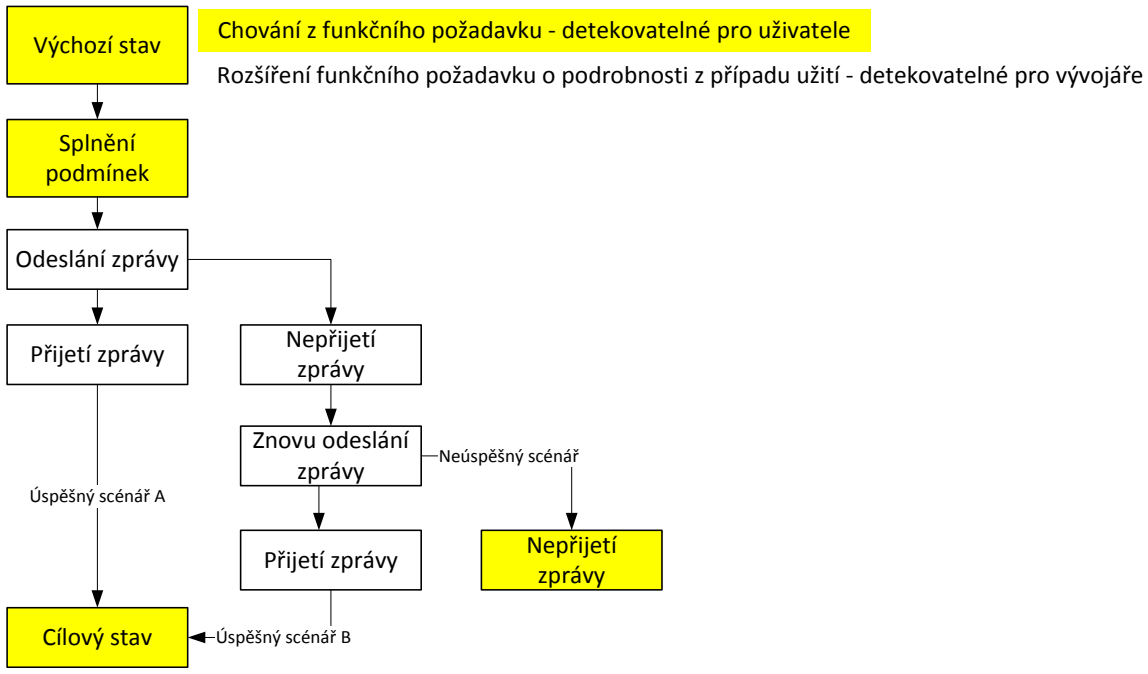
Délka dohledové informace MA FS představuje parametr, který by měl být dodržován a při testování sledován po celou dobu jízdy vozidla v módu FS, což je mód vozidla (stav), který je předpokladem k naplnění těchto state-driven požadavků. Naplnění se tedy vyhodnocuje v průběhu celého testování, pokud jsou splněny podmínky pro MA FS (infrastruktura před

vlakem umožňuje prodloužení dohledové informace MA FS), které popisují požadavky na samotné vydání dohledové informace vozidlu. Požadavek na minimální délku MA FS musí být dodržen i při jízdě přes hranici RBC/RBC Handover, která je specifická tím, že dochází k výměně informací mezi RBC odevzdávající vozidlo a RBC přijímající vozidlo. Znalost těchto hranic na reálném projektu je při ověřování naplnění požadavku nezbytná pro výběr správného testového případu příslušného požadavku na délku MA FS, který řeší prodloužení přes hranici.

5 Vazby požadavků na další úrovně specifikací

Návrh konkrétní realizace systému, jehož chování má odpovídat funkčním požadavkům, je popsán v nižších úrovních specifikace. Prvním typem dokumentace vázané na funkční požadavky jsou tzv. **případy užití.**

Jeden požadavek může být navázán k více případům užití, které podrobněji rozvádějí přípustné (uvažované) scénáře chování vozidla a systému ETCS během plynutí času. Rozšíření spočívá např. ve vytvoření alternativního scénáře pro případ, kdy vozidlo nepřijme zprávu, která nese informaci potřebnou pro projevení změny stavu. Pokud má dojít k dosažení stejné výstupní charakteristiky jako při provedeném úspěšném scénáři, ve kterém daná zpráva dorazila, má být naplněn i požadavek, který vznikl z tohoto úspěšného scénáře. Případ užití již umožňuje určit, **jakým způsobem došlo k naplnění požadavku** (na Obr. 4 scénář A nebo scénář B), jelikož má definované mezistavy, které můžeme vyhodnotit při nahlédnutí do toku zpráv mezi mobilní a stacionární částí ETCS.



Obr. 4 Skladba případu užití s popisy chování systému - detekce právě procházející větve scénáře

Druhým typem dokumentace spojeným s funkčními požadavky jsou **systémové požadavky na trať ovou část ETCS L2** označené jako SRS ETCS L2 (System Requirement Specification).

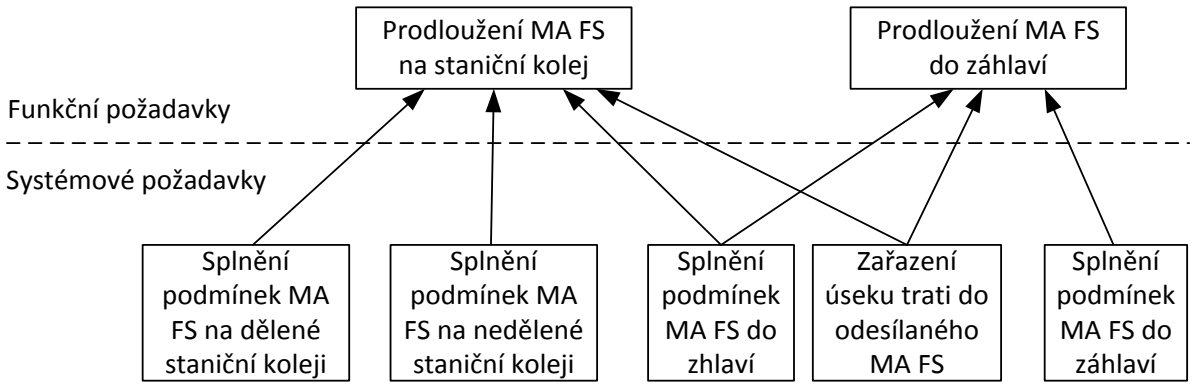
Požadavky SRS ETCS L2 dnes tvoří popis aktuálního stavu realizace systému tzv. „state of the art“, ze kterého společně s dosavadními zkušenostmi s jejich tvorbou těží funkční požadavky. Nicméně příčiny ke vzniku a obsahu specifikace konkrétních funkčních požadavků je nutné hledat jinde – u požadavků od všech zúčastněných stran (viz kapitola 2.2.8).

Ve specifikaci požadavků SRS ETCS L2 se tvůrci systému zmiňují (na rozdíl od funkčních požadavků) o konkrétní podobě realizace systému včetně popisu zpráv, paketů a proměnných ETCS jazyka využitých k naplnění požadované funkční vlastnosti systému.

Požadavky SRS ETCS L2 tvoří požadavky na umístění nových komponent v kolejišti (např. balíz), požadavky na komunikaci s ostatními zabezpečovacími zařízeními a zejména také softwarové požadavky na RBC, čili funkční chování, které se odehrává uvnitř RBC a projevuje se ve výsledku zejména navenek, ale samotné naplnění jednoho požadavku SRS ETCS L2 se v některých situacích projevuje pouze změnou vnitřních stavů RBC.

Výsledkem naplnění jednoho nebo několika SRS požadavků jsou pak splněny podmínky nutné k naplnění dílčích částí funkčních požadavků na systém ETCS (např. odeslání zprávy 3 „Movement Authority“ z RBC je nutnou podmínkou, aby vozidlo mohlo přejít do módu FS nebo OS), nicméně nelze pomocí SRS ETCS L2 požadavků prokazovat funkční chování celého systému ETCS ve všech jeho aspektech, neboť na funkčním chování se podílejí kromě traťové části ještě další subsystémy ETCS (OBU, komunikační řetězec,…).

Jeden požadavek FRS pokrývá vlastnosti, které jsou na úrovni SRS popsány více požadavky SRS ETCS L2. Zároveň jsou tyto SRS ETCS L2 požadavky více všestranné, tj. například se vztahují k dílčím strukturám kolejiště (zhlaví, staniční kolej,…) a nelze je přiřadit jako implementaci pouze k jednomu funkčnímu požadavku (prodloužení MA FS do vjezdové vlakové cesty).



Obr. 5 Příklad vazeb mezi funkčními a systémovými požadavky

Pokud se podíváme na příklad citace části požadavku SRS ETCS L2: „RBC eviduje splněné podmínky pro generování MA FS ve zhlaví“, jeví se požadavky SRS ETCS L2 jako více univerzální vůči funkčním požadavkům a řeší problematiku požadovaného funkčního chování systému ETCS na takové úrovni, jejíž správná funkce je ověřitelná často pouze nepřímo skrze posouzení hodnot proměnných při běhu spuštěného kódu funkčních algoritmů, resp. přímo ověřitelná, pokud ovšem testujeme naplnění více požadavků současně. Samotné požadavky SRS ETCS L2 jsou tedy obtížně testovatelné, nicméně **představují důležitý popis realizace celé traťové části systému ETCS potřebné k dosažení naplnění funkčních požadavků na celý systém**, ještě před tím než dojde k rozdělení funkcí a úloh mezi další subsystémy, jenž mají své požadavky nižší úrovně vůči SRS ETCS L2, např. tzv. požadavky SSRS pro zobrazení na HMI RBC. Bez těchto požadavků se obejít nelze. Z požadavků SRS ETCS L2 vyplývají i pokyny k projektování traťové části systému ETCS, např. rozmístění balíz v kolejišti obsahující příslušného pakety dat v telegramech potřebných k naplnění funkčních požadavků nebo počet RBC pokrývajících část infrastruktury, na které je systém ETCS nasazen.

Z hlediska vazeb požadavků by měly v budoucnu testovatelné požadavky SRS představovat popis implementace funkčních požadavků, přičemž by se měla zavést trasovatelnost na funkční požadavky (vazbou „vyplývá z“, která bude směřovat od požadavků vyšší úrovně – funkčních požadavků).

6 Ověření naplnění funkčních požadavků

Jednou z důležitých vlastností funkčních požadavků je jejich testovatelnost (ověřitelnost jejich naplnění), díky které můžeme provést ověření naplnění funkčních požadavků prostřednictvím jednoho nebo více testových případů. Jeden testový případ obsahuje scénář, po jehož provedení by mělo dojít k takovému projevu funkčního chování, aby bylo možné vyhodnotit naplnění jednoho nebo více funkčních požadavků.

K funkčnímu požadavku se váže příznak neotestovaný / otestovaný.

Funkční požadavek je označen za otestovaný, pokud byly provedeny všechny testové případy, které se k němu vážou a zároveň u těchto testových případů bylo dosaženo cílového stavu do požadované doby od zahájení testu (provedením všech úkonů v postupu scénáře z výchozího stavu testového případu). Problematice vyhodnocení testových případů se věnuje Kolář (2018).

6.1 Verifikace a validace požadavků

Ověření neboli verifikace požadavků je proces, jenž slouží k ujištění, že systém je realizován v podobě, která poskytuje funkce vyžadované v jeho specifikaci, tedy i funkčním požadavkům. Pro verifikaci se kromě ověření naplnění požadavků otestují i případy, kdy požadavky nejsou naplněny. V normě ČSN EN 50128 ed.2 je pojem verifikace popsán jako: *„proces zkoumání následovaný rozhodnutím založeným na důkazech, že výstupní položky (proces, dokumentace, software nebo aplikace) určité vývojové etapy naplňují požadavky této etapy s ohledem na úplnost, správnost a konzistenci“*

Validací se rozumí proces, jenž ověří naplnění očekávání zákazníka, tj. systém plní požadovaný účel (podle očekávání zákazníka). Norma ČSN EN 50128 ed.2 zavádí pojem validace jako: *„proces analýzy následovaný rozhodnutím založeným na důkazech za účelem rozhodnout, zda položky (např. proces, dokumentace, software nebo aplikace) odpovídají potřebám uživatelů, zejména s ohledem na bezpečnost a kvalitu a s důrazem na vhodnost jejich činnosti v souladu s jejich účelem v zamýšleném prostředí“*.

Pro tuto práci zabývající se aplikací metod ověření naplnění funkčního chování není podstatné rozlišovat pojmy verifikace a validace ve spojení s funkčními požadavky. Dále pracujeme s jedním pojmem – ověření naplnění požadavků, který má za cíl zkontrolování realizovaného systému vůči chování ve funkčních požadavcích.

6.2 Sestavení testových scénářů

Každý požadavek má definovaný výchozí stav systému ETCS a jeho komponent – např. poloha a mód dohlíženého vozidla. Zároveň platí, že dosáhnout takového výchozího stavu lze pouze po naplnění některých funkčních požadavků popř. jiné definované procedury v předchozím kroku.

Pokud před námi stojí úkol ověřit co nejvíce funkčních požadavků v co nejkratším období, aby mohl být systém bez dlouhých prodlev využit v provozu, a zároveň dosáhnout účinného ověření funkčních požadavků, neboť ty se de facto ověřují nepřetržitě po spuštění systému, je na místě provést analýzu funkčních požadavků a stanovit, která ověření funkčních požadavků na sebe mohou časově navazovat.

Pro dosažení efektivního výběru následujících testových případů ověřujících naplnění funkčních požadavků do tzv. testového scénáře byly vytvořeny dvě matice, v nichž jsou booleovsky (TRUE = x / FALSE = -) vyplněny návaznosti mezi příslušnými funkčními požadavky. Člověk, jenž provádí testování (dále označovaný jako tester), a případně i softwarový nástroj, který tyto matice může zpracovávat, tak má informaci, které ověřované požadavky na sebe reálně mohou navazovat a usnadní jim to orientaci při vyhledávání konkrétního dále ověřovaného požadavku. Každý funkční požadavek je v testovém scénáři ověřován prostřednictvím zvoleného konkrétního testového případu, který je/bude prováděn, z testových případů, které jsou na příslušný požadavek trasovány.

Matice podmíněného zařazení ověření funkčního požadavku do scénáře je vytvořená zvlášť:

a) pro zařazení funkčních požadavků z kapitoly 4.1 (požadavky na vydání dohledové informace vozidlu);
b) pro zařazení funkčních požadavků z kapitoly 4.2 (požadavky na interakci systému se strojvedoucím po přijetí dohledové informace).

		POSLEDNÍ POŽADAVEK ZAŘAZENÝ VE SCÉNÁŘI							
	mód po naplnění požadavku	FS	FS	FS	FS	FS	FS	FS	FS
		Prodloužení FS na SK				Prodloužení FS do záhlaví		Prodloužení FS na TK	SR → FS ze SK
Vyžadovaný aktuální mód vozidla	popis požadavku	VC/VCO na SK	VCRP na SK	vjezdová VC/VCO na SK ve výluce	vjezdová VCRP na SK ve výluce	VC ze SK - vstřícná náv. v záhlaví	VC ze SK - nevstřícná náv. v záhlaví	volný oddíl	VC ze SK na trať nebo na SK
popis požadavku	číslo pož.	0103101	0103102	0103103	0103104	0103111	0103112	0103121	0102201
FS	MA FS, VC/VCO na SK	0103101	x	-	x	-	-	-	x	x
FS	MA FS, VCRP na SK	0103102	x	-	x	-	-	-	x	x
FS	MA FS, vjezdová VC/VCO na SK ve výluce	0103103	-	-	-	-	-	-	x	-
FS	MA FS, vjezdová VCRP na SK ve výluce	0103104	-	-	-	-	-	-	x	-
FS	MA FS, VC ze SK - vstřícná náv. v záhlaví	0103111	x	-	x	-	-	-	-	x
FS	MA FS, VC ze SK - nevstřícná náv. v záhlaví	0103112	x	-	x	-	-	-	-	x
FS	MA FS, volný oddíl	0103121	-	-	-	-	x	x	x	x
SR	MA FS, VC ze SK na trať nebo na SK	0102201	-	-	-	-	-	-	-	-
SR	MA FS, VC na SK	0102222	-	-	-	-	-	-	-	-
SR	MA FS, bez VC, vozidlo bylo v záhlaví	0102242	-	-	-	-	-	-	-	-
OS	MA FS, pot. TAF - VC, VCO, VCRP ze SK na trať nebo na SK	0102401	-	-	-	-	-	-	-	-
OS	MA FS, pot. TAF - uvolnění oddílu	0102421	-	-	-	-	-	-	-	-
OS	MA FS, pot. TAF - VC/VCO/VCRP na SK	0102422	-	-	-	-	-	-	-	-
OS	MA FS, pot. TAF - vstřícná náv. v záhlaví	0102441	-	-	-	-	-	-	-	-
OS	MA FS, pot. TAF - nevstřícná náv. v záhlaví	0102442	-	-	-	-	-	-	-	-
FS	Výstup do LSTM/L0 - MA FS za oddíl.náv.	0105401	-	-	-	-	x	x	x	x
UN/SN	vstup z LSTM/L0 - MA FS za oddíl. náv.	0105021	-	-	-	-	-	-	-	-
UN/SN	vstup z LSTM/L0 - MA FS za vjezd. náv.	0105121	-	-	-	-	-	-	-	-
UN/SN	vstup z LSTM/L0 - MA FS před prvním oddíl. náv. - zastave	0105304	-	-	-	-	-	-	-	-

Obr. 6 Náhled do matice podmíněného zařazení ověření požadavku na vydání dohledové informace

Na Obr. 6 je znázorněna dvourozměrná matice z bodu a) o *n* řádcích a *n* sloupcích (daný požadavek se vyskytuje jak v řádku, tak i ve sloupci), přičemž pro požadavky v řádcích stanovují vyznačené symboly návaznosti (X) takové požadavky ve sloupcích, které následně zařazovanému požadavku v sestaveném testovém scénáři mohou bezprostředně předcházet.

		POSLEDNÍ POŽADAVEK ZAŘAZENÝ VE SCÉNÁŘI							
		FS → OS na SK	FS → OS na TK	FS → OS v záhlaví		FS → OS na SK	požadavek na nepotvrzení		
		přechod do OS ve VCRP na SK	obsazený další oddíl	obsazený 1. oddíl - vstřícná náv. v záhlaví	obsazený 1. oddíl - nevstřícná náv. v záhlaví	VZEOA na SK, přechod do OS	nepotvrzení OS před náv.	nepotvrzení OS do 5 s po minutí náv. - aktivace brzd	nepotvrzení OS před začátkem KU
požadavek na potvrzení		0104001	0104101	0104121	0104122	0104011	0104521	0104532	0104561
potvrzení OS před náv.	0104511	-	x	x	x	-	-	-	-
nepotvrzení OS před náv.	0104521	-	x	x	x	-	-	-	-
potvrzení OS do 5 s po minutí náv.	0104531	-	-	-	-	-	x	-	-
nepotvrzení OS do 5 s po minutí náv. - aktivace brzd	0104532	-	-	-	-	-	x	-	-
potvrzení OS za 5 s po minutí náv. - deaktivace brzd	0104533	-	-	-	-	-	-	x	-
potvrzení OS před KU	0104551	x	-	-	-	-	-	-	-
nepotvrzení OS před KU	0104561	x	-	-	-	-	-	-	-
potvrzení OS do 5 s po vjetí do KU	0104571	-	-	-	-	-	-	-	x
nepotvrzení OS do 5 s po vjetí do KU - aktivace brzd	0104572	-	-	-	-	-	-	-	x
potvrzení OS za 5 s po vjetí do KU - deaktivace brzd	0104573	-	-	-	-	-	-	-	-
potvrzení do 5 s po přechodu do OS	0104021	-	-	-	-	x	-	-	-
nepotvrzení do 5 s po přechodu do OS - aktivace brz	0104022	-	-	-	-	x	-	-	-
potvrzení za 5 s po přechodu do OS - deaktivace brz	0104023	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z LSTM (SN) u oddíl. náv.	0105002	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z L0 (UN) u oddíl. náv.	0105003	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z LSTM (SN) u vjezd. náv.	0105102	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z L0 (UN) u vjezd. náv.	0105103	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z LSTM (SN) u prvního oddíl.	0105302	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z L0 (UN) u prvního oddíl. ná	0105303	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z LSTM (SN) na konci SK	0105342	-	-	-	-	-	-	-	-
Přepnutí OBU do L2 (FS) z L0 (UN) na konci SK	0105343	-	-	-	-	-	-	-	-

Obr. 7 Náhled do matice podmíněného zařazení ověření požadavku na interakci systému se strojvedoucím

Na Obr. 7 je dvourozměrná matice z bodu b) o *x* řádcích a *y* sloupcích, přičemž pro požadavky v řádcích stanovují vyznačené symboly návaznosti (X) takové požadavky ve sloupcích, které následně zařazovanému požadavku v sestaveném testovém scénáři mohou bezprostředně předcházet. Požadavky ve sloupcích ovšem v této matici tvoří i funkční požadavky z kapitoly 4.1 (požadavky na vydání dohledové informace vozidlu).

Pro požadavky z kapitol 4.3, 4.4, 4.5 a 4.6 není výhodné tyto vztahy do matice definovat, jelikož potřeba jejich naplnění může nastat téměř kdykoliv (např. odeslání UEM při zadání generálního stop z HMI RBC) nebo se jedná o požadavky, po jejichž zařazení do scénáře není známo, kde se vozidlo bude po naplnění požadavku na infrastruktuře nacházet (např. přechod do módu TR po projetí EoA – např. pokud vozidlo zastaví ve zhlaví bude systém ETCS reagovat jinak než kdyby zastavilo až v záhlaví). V případě potřeby ověření takových požadavků je pro zjednodušení vytvoření a udržování aktuálních matic výhodnější, aby tester vybral podle skutečných podmínek k ověřování adekvátní požadavek, než zařazovat tyto požadavky do výběru uvažovaných následujících ověřovaných požadavků. Pokud tester bude potřebovat v daném okamžiku ověřit naplnění požadavku na restrikce, nic mu v tom nebrání, ale předpokládá se, že takovou restrikcí se stávající scénář ukončí a pro další jízdu začne vytvářet scénář nový podle toho, jaký byl stav po uplatnění nebo neuplatnění restrikce.

Scénář jízdy vytváří tester na základě toho, co mu nabízí matice jako následující možný požadavek k ověření, resp. pokud takový požadavek není v maticích nijak podmíněn, zařadí ho individuálně na základě vyhodnocení aktuálního stavu.

Průběh testů s vytvořeným testovým scénářem je závislý na skutečném funkčním chování systému při ověřování:

a) Pokud dochází k naplnění funkčních požadavků (dosažení cílového stavu), je vytvořená posloupnost testových případů ponechána v původní podobě.
b) Pokud nedojde k naplnění některého funkčního požadavku v průběhu scénáře (tj. test byl vyhodnocen jako neúspěšný), musí se nadefinovat nový výchozí stav (tj. vybrat první ověřovaný požadavek, resp. testový případ), ve kterém se vozidlo a infrastruktura nachází, aby tím následně byl prostřednictvím matice zúžen počet funkčních požadavků, jejichž ověřování dále připadá v úvahu, a mohli jsme tak vytvořit nový testový scénář jízdy. V případě, že dochází k častému nenaplnění funkčních požadavků, klesá využitelnost matice, ale zároveň to ukazuje, že systém nesplňuje všechny funkční požadavky na něj kladené.

Testový scénář lze sestavit i před jeho samotným provedením jako postup testování, podle kterého se má postupovat, což se jeví jako vhodný způsob při testování v laboratorních podmínkách, kde provádění testů není ovlivněno okolním drážním provozem, nýbrž pouze naší aktivitou, a není ani nijak časově omezeno.

Primárním cílem je však ověření naplnění funkčních požadavků v plných provozních podmínkách. Toho lze dosáhnout provedením testovací jízdy na vozidle v delším úseku železniční infrastruktury a sestavením testového scénáře až po provedení jízdy s následným zpětným důkladným vyhodnocením naplnění všech požadavků podle pořízeného záznamu z jízdy. Testovací jízda je totiž mnohdy ovlivněna jízdami ostatních drážních vozidel, což ovšem nemusí být na škodu, neboť se jedná o prostředí, ve kterém bude běžně provozován.

Pokud jsou k tomu vhodné podmínky, lze provést ověření naplnění vybraných funkčních požadavků přímo při testovacích jízdách, ovšem dlouhodobější jízda podle scénáře není vzhledem k možnostem v reálném drážním provozu realizovatelná a s ohledem na čas potřebný k důkladnému vyhodnocení všech požadavků ani přímo při jízdě vyhodnotitelná (ani ne tak jejich výsledný projev jako spíše ověření naplnění všech podmínek daného konkrétního testového případu).

Proces ověřování naplnění funkčních požadavků může obsahovat samotný jeden požadavek v rámci testování, kdy po ověření naplnění požadavku testování ukončíme. V praxi je však při provádění testovacích jízd (v laboratoři na simulátoru i na reálném vozidle) výhodné ověřovat plnění více funkčních požadavků v rámci celé jízdy pod dohledem systému ETCS. Předpokládá se, že většina těchto ověřovaných požadavků se bude zaměřovat na jízdu vozidla v módu FS a jeho prodlužování, což ale není na škodu, neboť jízda podle dohledové informace MA FS je to, co se od tohoto systému v reálném provozu očekává. Do těchto jízd však lze zanést i ověření požadavků, které budou nastávat sice méně často, ale jejich naplnění je důležité např. z důvodu umožnění přechodu vozidla do módu FS (mobilní část v současné implementaci ETCS po Start of Mission neobdrží dohledovou informaci MA FS, protože musí být nejprve zjištěna poloha vozidla – systém ETCS musí znát poslední kontaktovanou referenci na infrastruktuře, tj. balízovou skupinu, a zároveň systém ETCS musí mít informaci, že se před vozidlem, které má vyhrazenou část infrastruktury, nenachází jiné vozidlo).

Pokud ověření jednoho funkčního požadavku navazuje na předchozí ověřovaný požadavek, pak při testovací jízdě můžeme analyzovat, zda nějaké funkční požadavky na systém ETCS ve specifikaci úplně nechybí – jedná se o chybějící nepopsané kombinace vstupních parametrů, při níž by systém měl vykazovat nebo již vykazuje projev nějaké funkce. V testovém scénáři se tím pádem vyskytne prázdné místo, které není možné vyplnit žádným ověřením dosavadního funkčního požadavku.

Vybíráme-li ověřované požadavky do testového scénáře na základě návazností v matici, kde se výběr provádí podle posledního zařazeného ověřovaného funkčního požadavku, může dojít k situaci, kdy bychom za tento poslední požadavek potřebovali zařadit na další místo ve scénáři více požadavků současně (a tedy současně začít ověřovat jejich naplnění – viz požadavky 4. a 4a. v Obr. 10). Evidentně se musí jednat o požadavky jiného charakteru (v Obr. 10 to je přijetí dohledové informace MA OS a potvrzení přechodu do OS před minutím návěstidla), jinak by to znamenalo chybu ve funkční specifikaci – protismyslné požadavky.

Z tohoto vyplývá, že je potřeba rozlišovat charakter jednotlivých požadavků (viz kapitola 4). Podklady pro vytvoření testových scénářů tvoří:

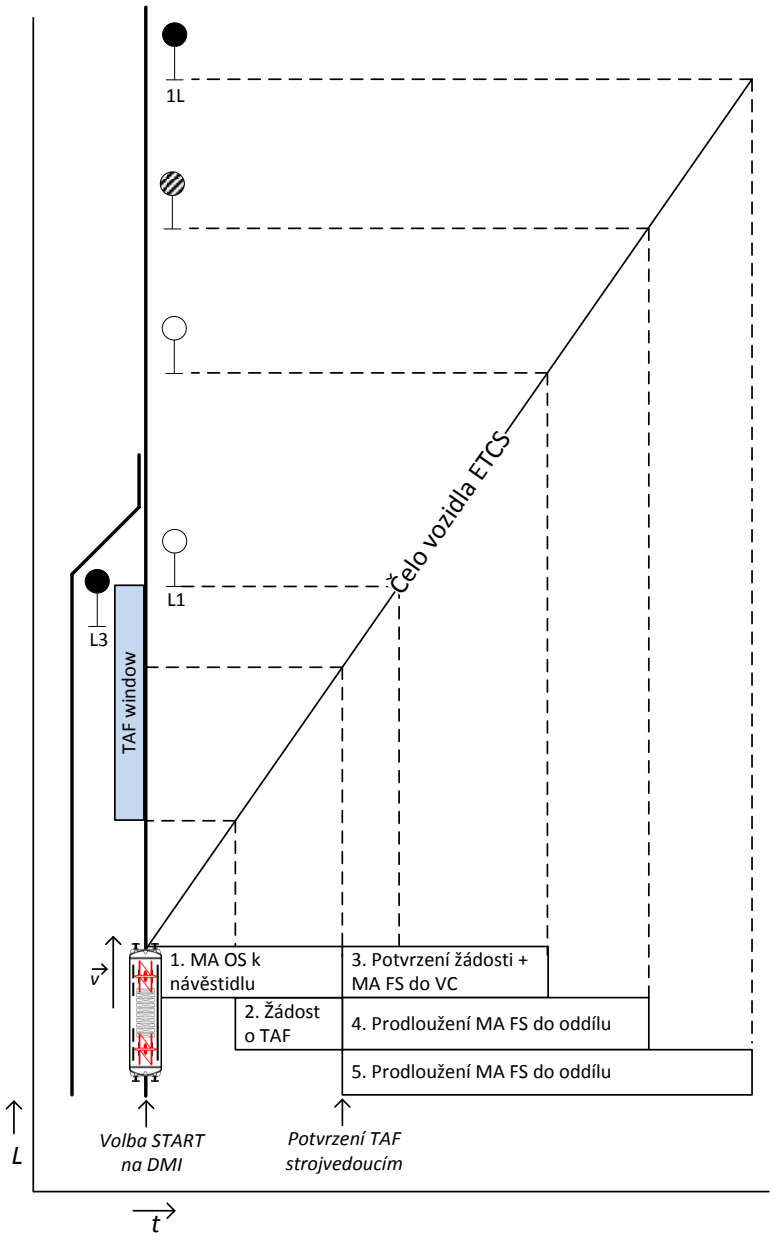
a) množina funkčních požadavků,
b) množina testových případů,
c) matice podmíněného zařazení funkčního požadavku do scénáře.

Princip ověřování naplnění funkčních požadavků v sestaveném scénáři je ilustrován na následujících obrázcích (jedná se o příklad požadavků na vydání dohledové informace).

V obrázcích, jenž jsou součástí této práce, je každý požadavek ve scénáři reprezentován obdélníkem. Číslované pořadí požadavků označuje pořadí, ve kterém jsou/byly zařazovány do scénáře. Doba ověřování naplnění jednoho funkčního požadavku je vystižena délkou obdélníku požadavku.

Obdélníky testů ověření požadavků na vydání dohledové informace MA jsou vpravo ukončeny u potenciálního EoA nebo místa změny módu vozidla (přechod z módu OS do FS), resp. obecně do okamžiku, kdy se začne ověřovat požadavek jiný, ovšem stejného charakteru (např. vydávání dohledové informace), který se má uplatňovat na úkor požadavku předchozího (kdyby strojvedoucí nepotvrdil přechod z módu OS do FS, ověřoval by se stále původní požadavek na vydání MA OS až do dojetí k EoA).

Délka dohledové informace MA FS a další parametrické požadavky na systém ETCS zajistí stanovení konečného počtu požadavků v aktuálním kontrolovaném řetězci složeném z několika současně ověřovaných funkčních požadavků na vydání dohledové informace v případě, že jsou splněny podmínky k vydání dohledové informace na větší vzdálenost, která by již překročila požadovanou minimální délku dohledové informace.



Obr. 8 Scénář přechodu vozidla z módu OS do FS

Scénář složený pouze z testů ověřujících požadavky na vydávání dohledové informace – prodlužování dohledové informace umožňující jízdu vozidla s přechodem z módu OS do FS je zobrazen na Obr. 8. Nastává potřeba určit, jak, kdy a po jakou dobu se má ověřovat naplnění funkčních požadavků.

Pozice začátků obdélníků požadavků vyplývají z textu specifikací požadavků (např. vozidlo disponuje dohledovou informací k hlavnímu návěstidlu na začátku prostorového oddílu – následující požadavek na prodloužení MA FS do prostorového oddílu je ověřován od tohoto návěstidla).

Může se ověřovat naplnění více požadavků současně – např. na Obr. 8 jsou do okamžiku označeného šipkou „Potvrzení TAF strojvedoucím“ současně ověřovány funkční požadavky 1. a 2. Od tohoto okamžiku se dále ověřují požadavky 3., 4., a 5.

Konec ověřování požadavku může být definován:

- místem na infrastruktuře;
    - návěstidlem jakožto potenciálním koncem dohledové informace u požadavku na vydání dohledové informace na část infrastruktury,
    - začátkem kolejového úseku,
    - polohou přejezdu,
    - … jiným místem vyplývajícím ze specifikace požadavku,
- okamžikem, kdy uživatel (strojvedoucí nebo dispečer) provedl volbu;
    - potvrzení přijetí informace na DMI,
    - Override EoA,
    - provedení generálního STOP,
    - … jinou aktivitou obsluhy vedoucí k ověřování naplnění jiného funkčního požadavku na úkor předchozího,
- okamžikem, kdy přestanou být splněny podmínky pro naplnění požadavku – např. splnění podmínek k naplnění více dovolujícího požadavku;
    - postavením vlakové cesty ze staniční koleje (viz Obr. 9),
    - uvolněním kolejového úseku,

V případě, že jsou viditelně splněny podmínky pro naplnění požadavku, musíme pro stanovení okamžiku resp. místa, odkud se má začít naplňovat funkční požadavek, zohlednit na vozidle dobu, o kterou se zpozdí zpracování a zobrazení informace na vozidle od okamžiku vzniku informace ve stávajícím zabezpečovacím zařízení (typicky rozsvícením dovolující návěsti na hlavním návěstidle).

Tato doba dále závisí na dalších okolnostech mezi, které patří:

- provádění prodloužení dohledové informace MA FS, přičemž oblast, kde došlo ke změně podmínek, leží za hranicí RBC/RBC Handoveru (v takovém případě je k výpočtům nutné přičíst dobu zpoždění vlivem předání informace o stavu trati za hranicí RBC/RBC Handoveru z RBC do RBC);

- charakter změny podmínek může být více omezující nebo více dovolující (filosofie – restrikce se má mobilní části odeslat bez prodlení, zatímco vylepšení podmínek může počkat na další plánované obnovení dohledové informace).

Následující hodnoty časů jsou převzaty z dokumentu AŽD Praha s.r.o. (2017b).

Maximální doba *t* je stanovena na:

$$t_{max} = t_{ETS-RBC\_max} + t_{EC\_RBC\_max} + t_{GSM-R\_max} + t_{EC\_EVC\_max}$$
$$t_{max} = 7 + 0{,}8 + 2 + 0{,}5 = 10{,}3\ s \qquad (1)$$

Kde:

$t_{ETS\text{-}RBC\_max}$ … maximální doba od vzniku informace ve stávajícím zabezpečovacím zařízení do projevu této změny ve funkčních algoritmech RBC

$t_{EC\_RBC\_max}$ … maximální doba zpracování informace v RBC

$t_{GSM\text{-}R\_max}$ … maximální doba přenosu informace mezi RBC a vozidlem

$t_{EC\_EVC\_max}$ … maximální doba zpracování informace v EVC

Minimální doba *t* je stanovena na:

$$t_{min} = t_{ETS-RBC\_min} + t_{EC\_RBC\_min} + t_{GSM-R\_min} + t_{EC\_EVC\_min}$$
$$t_{min} = 0{,}785 + 0{,}4 + 0{,}5 + 0{,}25 = 1{,}935\ s \qquad (2)$$

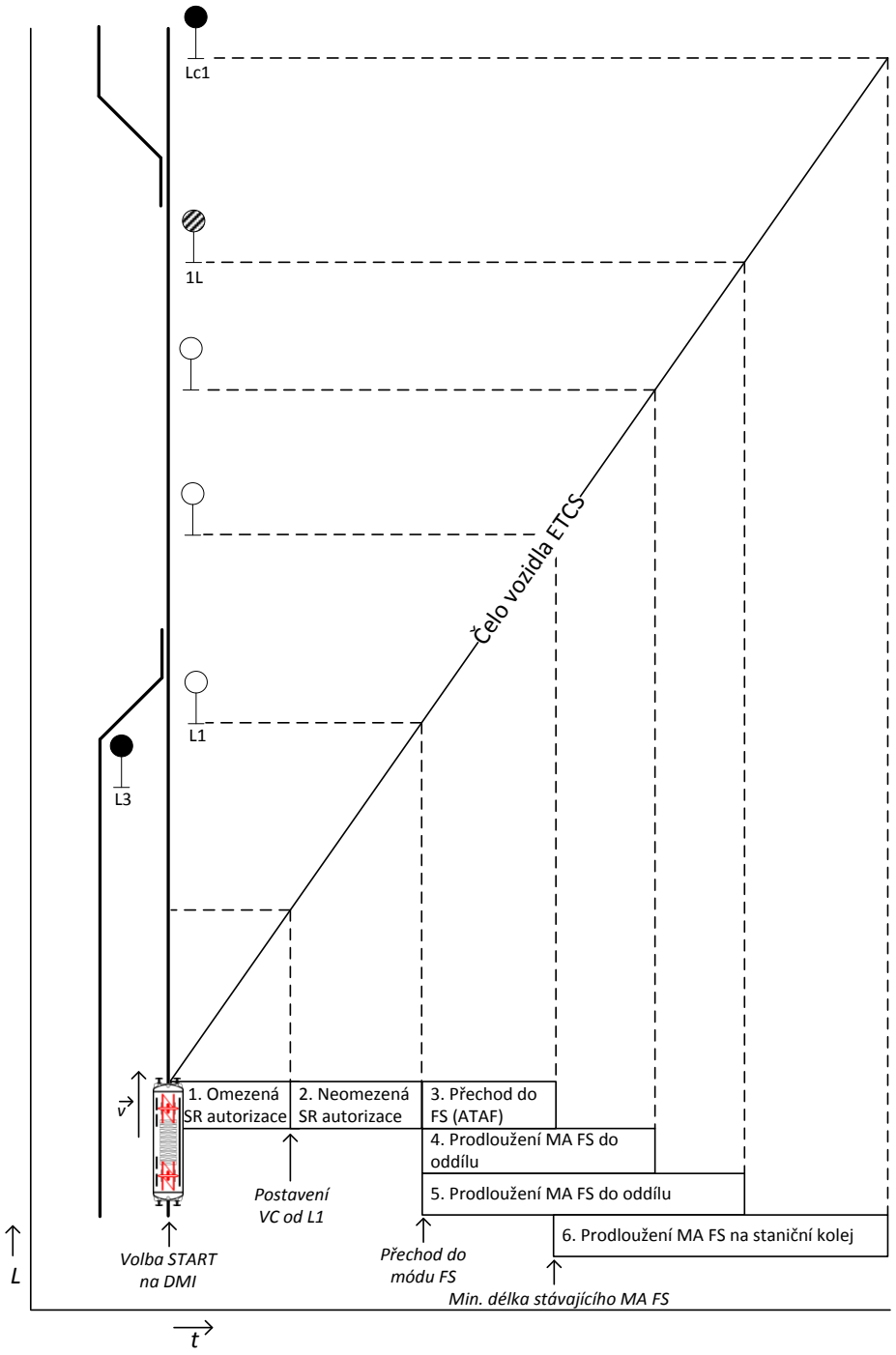
Kde:

$t_{ETS\text{-}RBC\_min}$ … minimální doba od vzniku informace ve stávajícím zabezpečovacím zařízení do projevu této změny v FA RBC

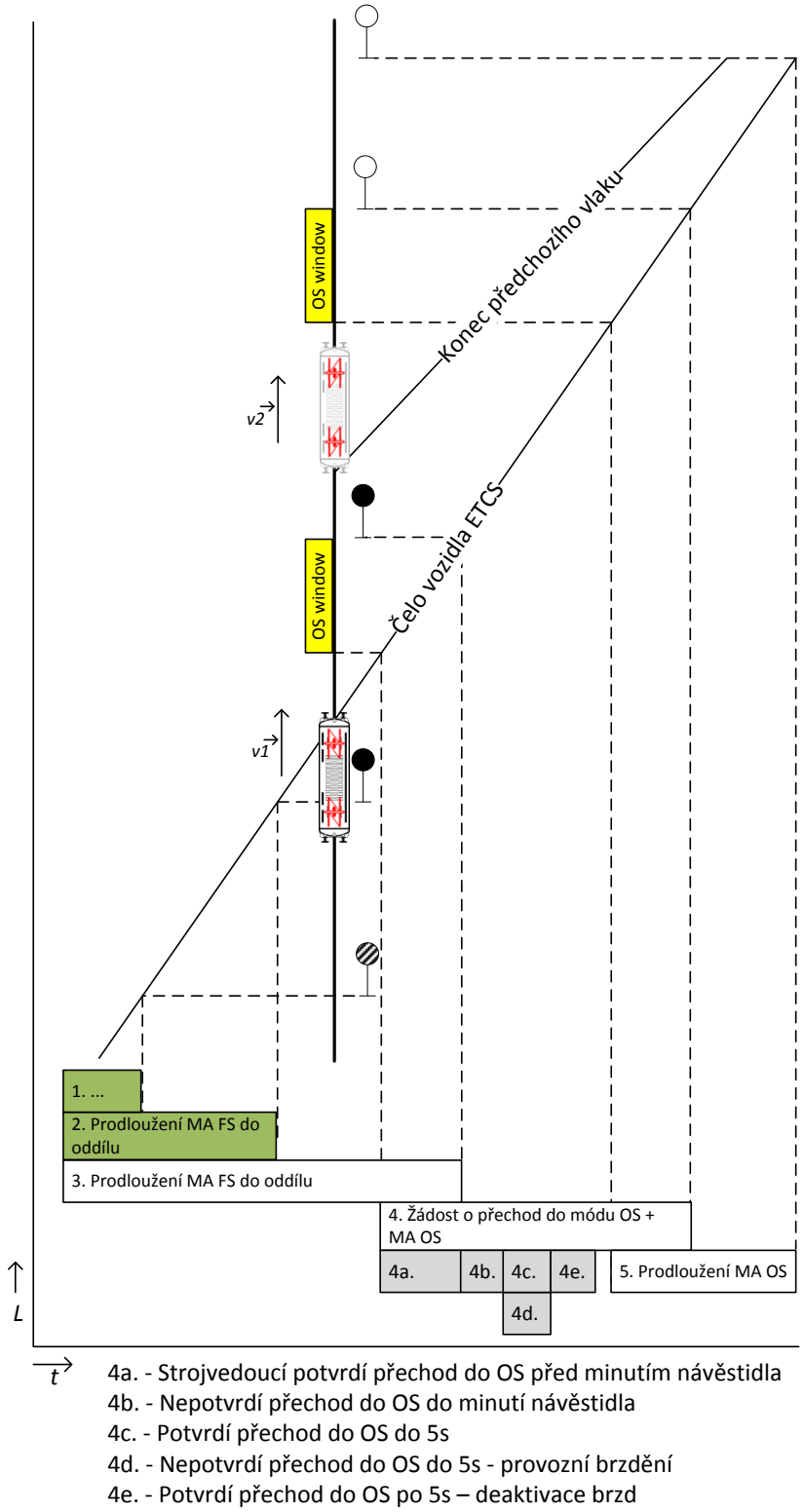
$t_{EC\_RBC\_min}$ … minimální doba zpracování informace v RBC

$t_{GSM\text{-}R\_min}$ … minimální doba přenosu informace mezi RBC a vozidlem

$t_{EC\_EVC\_min}$ … minimální doba zpracování informace v EVC



Obr. 9 Scénář jízdy po provedení Start of Mission a volbě START na DMI

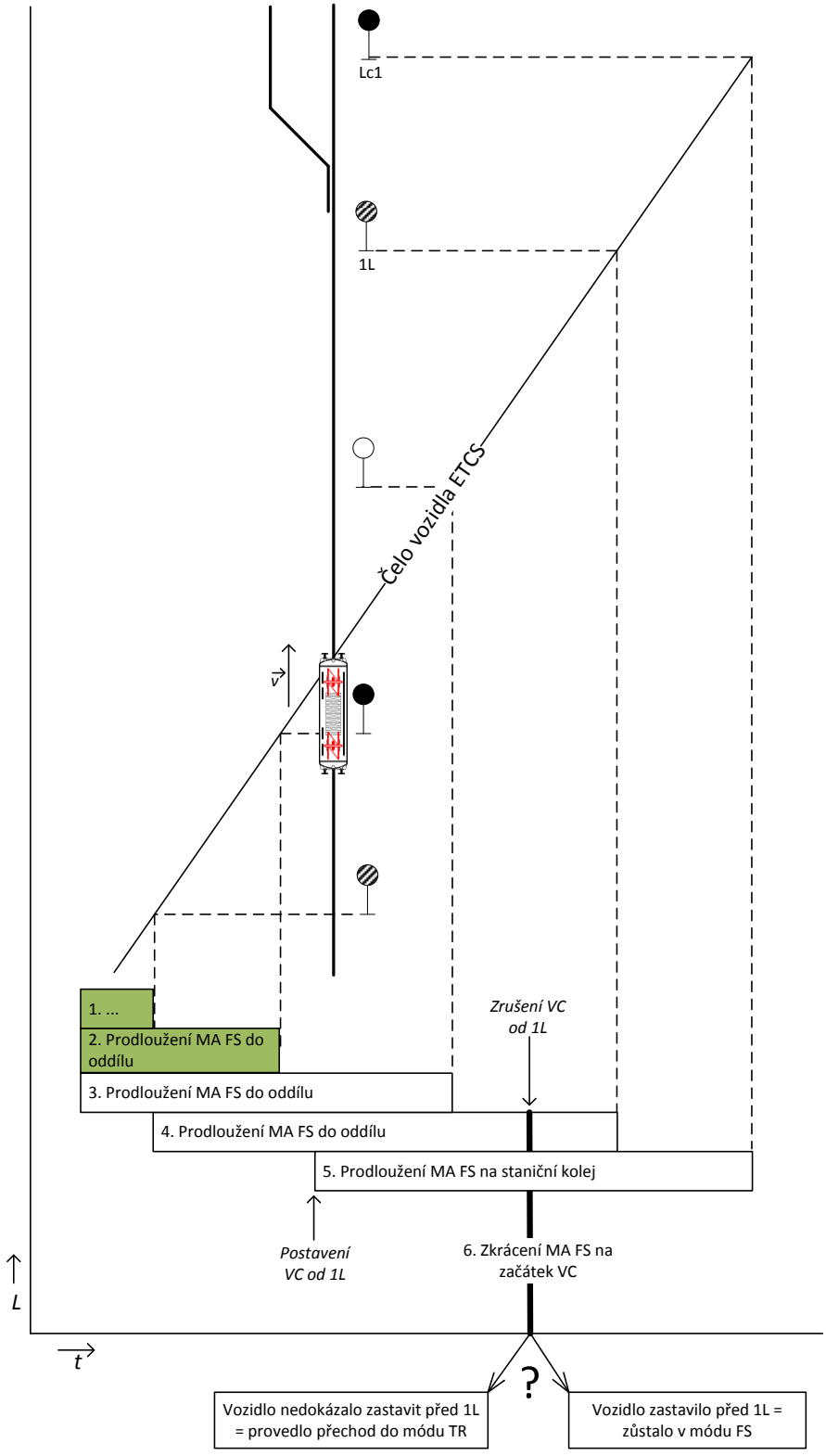


Obr. 10 Scénář přechodu vozidla z módu FS do OS

Obr. 10 znázorňuje scénář složený z požadavků na vydávání dohledové informace i požadavků na interakci se strojvedoucím po přijetí nové dohledové informace (potvrzení přechodu vozidla

do módu OS). Zeleně jsou v tomto obrázku zvýrazněny ty požadavky, jejichž ověřování již skončilo, jelikož byly uplatňovány v oblasti, kterou vozidlo již celou projelo, tudíž se nachází za aktuální polohou čela vozidla.

Pokud se před vozidlem nachází obsazený prostorový oddíl, vybere se k ověření požadavek „4. Žádost o přechodu do módu OS + MA OS“, kterého může ve scénáři následovat ověření požadavku na potvrzení přechodu do OS (4a, 4b, 4c, 4d, 4e). Jeho nebo jejich zvolení ovšem neovlivní umožnění výběru dalšího ověřovaného požadavku „5. Prodloužení MA OS“, jelikož v tomto případě již vozidlo přijalo MA OS (je zobrazeno na HMI RBC) a čeká se pouze na potvrzení strojvedoucím, které umožní další jízdu v módu OS (RBC očekává přijetí PR s informací, že se vozidlo nachází v módu OS). Pokud strojvedoucí přechod do módu OS zatím nepotvrdil (čili k ověření nebyl zvolen žádný požadavek na potvrzení), pak zřejmě čeká na změnu podmínek, tj. uvolnění následujícího prostorového oddílu a prodloužení MA FS. I tento požadavek tedy musí být součástí požadavků umožněných k výběru následujícího požadavku k ověření po požadavku „4. Žádost o přechod do módu OS + MA OS“.



Obr. 11 Scénář s restrikcí dohledové informace

Na Obr. 11 je zachyceno vydání restrikce představující omezení dohledové informace, příp. i vymazání dohledové informace a přechod do mód TR. Další jízda vozidla závisí na tom, jakým

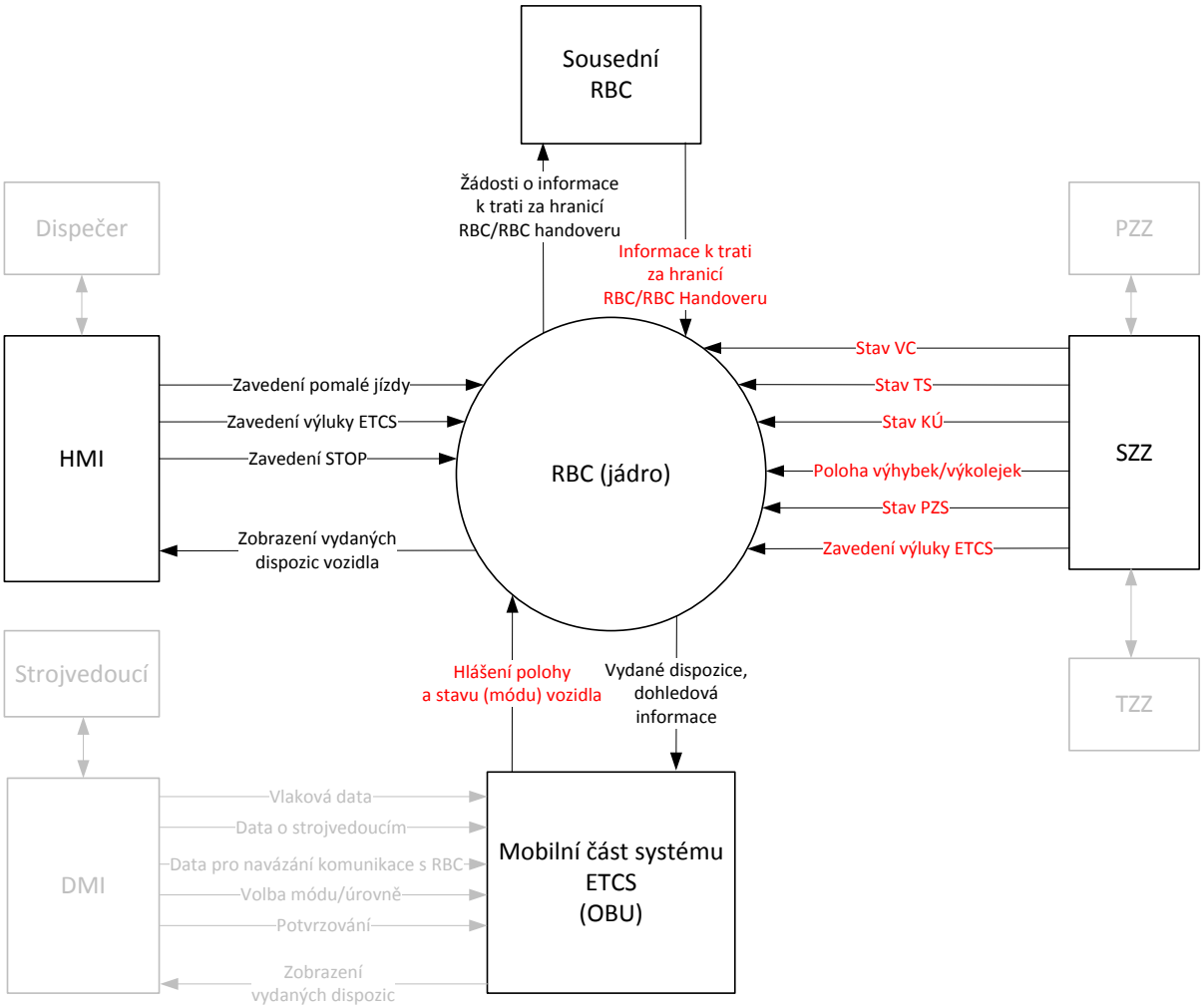
způsobem byla jízda vozidla restrikcí ovlivněna. Požadavek „6. Zkrácení MA FS na začátek VC“ je typu event-driven a proto je v testovém scénáři označen pouze čarou, neboť u tohoto požadavku se při jeho ověřování spokojíme s tím, že dohledová informace byla dostatečně včas zkrácena k novému EoA. Pokud by vzápětí byla dohledová informace MA FS opět prodloužena, ačkoliv by dle očekávání neměla (stav se nezměnil), jednalo se o chybu ve specifikaci požadavku na vydání dohledové informace (v tomto případě by oním požadavkem byl „5. Prodloužení MA FS na staniční kolej“).

V případě, že vozidlo v módu FS obdrží zkrácené MA FS a v okamžiku jeho uplatnění bude od nového EoA ve vzdálenosti takové, že dokáže zastavit ještě před ním, zůstává mobilní část v módu FS a má stále dohledovou informaci MA FS. Naopak pokud již vozidlo před novým EoA zastavit nedokáže, dojde po projetí EoA k přechodu mobilní části do módu TR a dále bude obtížné dopředu určit, v jaké části infrastruktury vozidlo skutečně zastaví, což má, po splnění podmínek pro další jízdu vozidla, vliv na budoucí vydanou dohledovou informaci, která by umožňovala jízdu vozidla. Tímto okamžikem tento testový scénář končí a vybereme nový první ověřovaný požadavek.

6.3 Minimální úroveň realizace systému ETCS pro testování

Tato kapitola je určena k identifikaci potřebných komponent a subsystémů nutných k ověření naplnění funkčních požadavků. Některé takové komponenty systému ETCS vystupují už v samotném textu specifikace požadavků (DMI, HMI RBC, …), další komponenty vyplývají z návrhu řešení a implementace systému.

Pokud je známé chování komponent a subsystémů, které zajišťují vytvoření vstupních dat, s nimiž dále pracuje RBC a které mají na základě znění požadavků vést k reakci RBC, lze tyto části systému pro účely testování funkčního chování nahradit jejich simulacemi. V úvahu připadají simulace některých komponent a subsystémů, které poskytují RBC informace o stavu infrastruktury a vozidla.



Obr. 12 Červeně zvýrazněný možný simulovaný tok dat v kontextovém diagramu systému ETCS

6.3.1 Navázané staniční zabezpečovacího zařízení

Systém ETCS v dosavadní implementaci neovlivňuje vlastní chod SZZ. Informace ze SZZ jsou v RBC využívány pro identifikaci podmínek bezpečnostně relevantních k sestavování dohledové informace pro vozidlo vybavené mobilní částí systému ETCS. Mezi informace přijímané ze SZZ patří nejen informace z dopravny, kterou SZZ ovládá (stavy vlakových cest, informace o volnosti kolejových úseků), ale i informace o podmínkách na trati od TZZ, informace o bezporuchovém stavu PZS atd.

Vstupní informace od známého SZZ schváleného k provozu je třeba pro samotnou implementaci do systému ETCS i pro jejich nasimulování patřičně zanalyzovat a uvést do aplikačních podmínek v jakých můžeme RBC (systém ETCS) provozovat.

Systém ETCS aplikační úrovně L2 lze provozovat tam, kde je SZZ umožněno získat zejména informace o:

- návěstech hlavních návěstidel dovolujících jízdu vlaku,
- volnosti kolejových úseků,
- závěru vlakové cesty,
- stavech PZ a úvazky TZZ se SZZ.

Tyto požadované vlastnosti zpravidla splňují SZZ 3. kategorie.

V souvislosti s instalací stacionární části systému ETCS bylo nutné tato stavědla upravit tak, aby umožnila odesílání dat do RBC. V případě reléového SZZ došlo k vytvoření tzv. provizorní úvazky, tj. systém ETCS lze plnohodnotně provozovat (umožňuje jízdu vozidla v plném dohledu – módu FS) na vybraných staničních kolejích.

6.3.2 Mobilní část systému ETCS

V úvahu připadá částečná simulace mobilní části omezená na funkční chování, které vytváří informace přijímané RBC od vozidla jako například hlášení polohy, potvrzování zpráv, přenášené do stacionární části (RBC). Zprávy a pakety přenášené z mobilní části do RBC jsou dané ETCS specifikacemi, čili lze uvažovat, že tyto informace od reálné mobilní části budou ve svém složení těmto specifikacím odpovídat.

Interoperabilní vlakový zabezpečovací systém ETCS, lépe řečeno jeho stacionární část, by měla být kompatibilní se všemi mobilními částmi ETCS v rámci kompatibilních systémových verzí ETCS (více se kompatibilitě věnuje Marek, 2015), nicméně v době ověřování naplnění funkčních požadavků na systém ETCS je k dispozici pouze omezený počet mobilních částí splňující požadavky na fázi testování podle SŽDC (2010).

SŽDC dále pro každý typ mobilní části v souladu s předpisy plánuje provedení testů kompatibility mobilní části s vybudovanou stacionární částí ETCS L2 (SŽDC 2017).

V době ověřování naplnění funkčních požadavků na systém ETCS není žádná mobilní část považována za subsystém s referenčním chováním. Mobilní části různých typů (výrobců) mají svá specifika, ale všechny by měly odpovídat příslušné specifikaci ETCS. V případě, kdy jsou dostupné mobilní části od malého počtu výrobců, je výhodné provádět další simulaci mobilní části v laboratoři i přes své systematické chyby, protože i simulace představuje další zdroj dat pro analýzu výsledného funkčního chování stacionární části. V budoucnu bude zřejmě různých

typů mobilních částí přibývat a spolu s tím bude i vzrůstat důvěra v to, že všechny tyto mobilní části dohromady představují referenční chování.

Činnost mobilní části je ovlivněna, kromě přijetí dohledové informace, také pohybem vozidla, chováním strojvedoucího provádějícího volby na DMI a kontaktováním balíz umístěných v kolejišti. Pro potřeby vytvoření simulace jejího chování zbývá určitá náhodnou velikost zpoždění, s jakým jsou zprávy obsahující tyto informace přenášeny mezi vozidlem a RBC – doba přenosu a zpracování informace od svého vzniku je ovlivněna vlastnostmi přenosového prostředí mezi vozidlem a RBC a zpráva nemusí být z různých důvodů doručena v pořádku do RBC. Je tedy potřeba stanovit minimální i maximální dobu a při testování aplikovat různé hodnoty uvnitř tohoto intervalu.

Simulovat v laboratoři plně funkční chování mobilní části, tedy i zpracovávání informace od RBC a provádění zásahu do jízdy vozidla nebo indikace na DMI, není žádoucí, jelikož tím dochází k samotnému návrhu funkčního chování mobilní části, která stejně není schválená k provozu ani certifikovaná vůči specifikacím ETCS. Podoba projevů funkčního chování mobilní části je ovlivňována i testovaným subsystémem (RBC), které je v současné podobě určené pouze k provoznímu ověřování požadovaného chování. V případě, že by bylo simulováno úplné funkční chování mobilní části, mohlo by se nesprávné funkční chování RBC zamaskovat za nesprávné chování simulace (obsahující systematické chyby) a ve výsledku by systém mohl mylně naplňovat funkční požadavky.

Využití reálných mobilních částí schválených k provozu na vozidlech při testování systému ETCS je nutným předpokladem k ověření kompatibility dat přenášených z RBC na mobilní část na vozidle a celkově k ověření naplnění funkčních požadavků na celý systém ETCS z hlediska zásahu vlakového zabezpečovače do jízdy vozidla. Cílem je ověřovat funkční chování s větším počtem reálných mobilních částí, čímž dosáhneme širšího ověření funkčního chování systému ETCS.

6.3.3 HMI RBC

HMI RBC představuje rozhraní k ETCS resp. k RBC pro obsluhu jeho stacionární části. Slouží k indikaci funkčního chování systému ETCS a jeho ovládání prostřednictvím povelů.

HMI RBC je součástí testované RBC, takže projevy funkčního chování, které můžou tvořit část funkčního požadavku (např. indikace délky vydané dohledové informace na HMI RBC), lze ověřit už při laboratorním testování funkčního chování se simulovanými vstupy.

6.3.4 Prostředky pro přenos informace na vozidlo

Přenosu informací na vozidlo se účastní balízové skupiny i radiová síť GSM-R (prostřednictvím Euroradia).

Přenos informace z balízy na mobilní část systému ETCS se provádí prostřednictvím tzv. balízových telegramů. Umístění balízových skupin do kolejiště je třeba provést jak z hlediska ověření obsahu balízového telegramu a jeho správné interpretace mobilní části systému ETCS, tak i ověření správného rozmístění BG na infrastruktuře.

RBC jsou podle rozmístění balíz odesílána hlášení polohy (PR) s příslušnými hodnotami vzdálenosti a nepřesností měření od poslední balízové skupiny. Větší četnost balízových skupin v kolejišti vede ke zpřesňování informace o poloze vozidla. Z hlediska funkčních požadavků, dochází k naplnění některých z nich právě po přijetí příslušného paketu obsaženého v balízovém telegramu. Jedná se např. o funkční požadavek na provedení přechodu do úrovně L2 vozidla, které kontaktovalo BG na hranici oblasti ETCS L2. Umístění balízové skupiny rozhoduje o tom, kdy a kde dojde jakýmkoliv způsobem k projevu kontaktování BG a přijetí balízového telegramu. Funkční požadavky předpokládají určité rozmístění balíz (např. v záhlaví za poslední výhybkou směrem ze stanice), jenž jsou nutné pro uvažované nabytí nové informace o poloze vozidla v okolí vybraného místa. Z funkčních požadavků tedy nepřímo skrze požadavky SRS ETCS L2 vyplynuly pokyny k projektování balíz, jenž by měly stanovit pravidla v umísťování balíz do kolejiště.

Pokud uvažujeme instalaci ETCS aplikační úrovně L2 nebo L3, pak je pokrytí dotčených železničních tratí digitální rádiovou sítí GSM-R nezbytným předpokladem k nasazení tohoto systému, neboť v těchto úrovních je využit pro přenos dohledové informace na vozidlo a opačným směrem k hlášení polohy a stavů vozidel.

Euroradio tvoří subsystém (část protokolové struktury) poskytující vedení komunikační relace mezi RBC a mobilní částí systému ETCS L2 a proto musí být při ověření naplnění požadavků uvažována zpoždění přenosu způsobená tímto přenosovým prostředkem.

Euroradio je rovněž využito pro komunikaci RBC mezi sebou. Význam této komunikace spočívá při aktivní transakci RBC/RBC Handover např. v odesílání tzv. Route Related Information – informací důležitých pro vydání dohledové informace do oblasti infrastruktury řízené sousední RBC. Strojvedoucí vozidla s dohledovou informací MA FS nebo MA OS by podle požadovaného chování neměl být nijak zvlášť informován o jízdě přes hranici oblastí

RBC. Jízda vozidla přes hranici oblastí RBC se projeví dispečerům na HMI RBC, kde je tato hranice označena v reliéfu kolejiště.

6.3.5 Radiobloková centrála ETCS (jádro)

RBC je centrálou stacionární části systému ETCS, která vytváří dispozice vydávané mobilní části systému ETCS (vozidlu). Platí obecný princip vlakového zabezpečovače – co není dovoleno, to je zakázáno – v tomto případě vozidlu v úrovni L2 bez přijaté platné dohledové informace není umožněn další pohyb bez dalších aktivit konaných vědomě strojvedoucím vozidla (např. Override EoA).

Účelem RBC v systému ETCS je vyhodnocení podmínek, ve kterých se vozidlo nachází a podle nich připravit dispozice (dohledové informace), které tomuto vozidlu odešle ve formátu zpráv, k nimž jsou přidružovány pakety s daty, odpovídajícím specifikacím ETCS.

Softwarové vybavení RBC tvoří z hlediska implementace funkčního chování zejména část generické aplikace tzv. systémový SW a část specifické aplikace tzv. adresný software (konfigurační data), který reprezentuje data potřebná pro znalost své oblasti infrastruktury (topologie kolejiště, …), aby mohla být vydána dohledová informace v oblasti řízené z této RBC. Každá RBC je zodpovědná za dohled jízdy vozidla ve své oblasti, přičemž pokud vozidlo jede v delším úseku trati a vjede z oblasti řízené z RBC do oblasti řízené z jiné RBC, přebírá RBC, která přijímá vozidlo (při aktivní komunikace se sousední RBC), zodpovědnost za jízdu vozidla odesláním zprávy „Take Over Responsibility“ sousední RBC.

Samotné jádro RBC ve znění funkčních požadavků nijak nevystupuje – je z uživatelské pohledu na systém v pozadí jako entita, která tvoří část logiky systému, ale přímo na sobě neindikuje žádné projevy funkčního chování zjistitelné pro dispečera nebo strojvedoucího a teprve HMI RBC, které tvoří subsystém celé RBC, toto umožní.

6.3.6 Sousední Radiobloková centrála pro RBC/RBC Handover

Zajistit spolupráci dvou reálných RBC případně jejich simulací je potřeba k ověření funkčních požadavků, při nichž je prováděn RBC/RBC Handover (plynulé předání zodpovědnosti za dohled nad vozidlem) v případě, kdy je vyžadována komunikace mezi RBC a sousední RBC při jízdě vozidla z oblasti řízené jednou RBC do oblasti řízené druhou RBC (RBC/RBC Handover). Při RBC/RBC Handoveru probíhá přenos dat mezi RBC prostřednictvím zpráv definovaných ve specifikacích ETCS a stejně jako v případě komunikace s mobilní částí vozidla, tak i zde je třeba při simulacích počítat s různými zpožděními v komunikaci, které by

mohly zpozdit vydání dohledové informace a následně způsobit nenaplnění požadavků na prodloužení dohledové informace vozidlu jedoucímu přes hranici RBC/RBC Handoveru.

7 Aplikace metod testového ověření naplnění funkčních požadavků

Z kapitoly 6.3 vzešly dva způsoby, jakými lze ověřovat naplnění funkčních požadavků – prostřednictvím simulátoru a prováděním testů na měřícím voze. Oba způsoby mají své výhody a nevýhody.

7.1 Testování na simulátoru

Toto testování je výhodné s ohledem na možnost navození takřka jakékoliv provozní situace, v níž se může vybavené vozidlo nacházet, bez omezení daným okolním provozem. Limitováni jsme pouze schopnostmi simulátoru.

Tester spouští simulaci SZZ, mobilní části systému ETCS a funkční algoritmy RBC a vybírá adresný software podle oblasti infrastruktury, kterou má testovat. Do kolejiště v simulaci následně umístí vozidlo a zahájí proceduru navázání spojení s RBC. Od tohoto okamžiku je vozidlo dohlíženo podle podmínek, které tester navolí na HMI RBC a JOP SZZ stejným způsobem, jakými by byly dosaženy v reálném provozu dispečerem. Funkce, které vykonává strojvedoucí – uvedení vozidla do pohybu, potvrzení TAF u návěstidla, provedení volby Override EoA jsou dostupné v panelu simulace OBU. V simulátoru není implementované kompletní funkční chování mobilní části systému ETCS (zobrazování na DMI) a proto v něm není možné ověřit naplnění některých požadavků – např. požadavky na potvrzení přijetí dohledové informace MA OS strojvedoucím. Omezené jsou i možnosti testování restrikcí na traťové koleji související s obsazením kolejového úseku na traťové koleji vlivem nemožné simulace některých provozních stavů reálného TZZ.

Funkční chování RBC se v simulátoru projevuje na monitoru simulovaného HMI RBC a na panelu, který simulace vyplňuje informacemi o vysílání zpráv z RBC do OBU a naopak. Kromě časového údaje odeslání / přijetí zprávy v RBC a samotného čísla zprávy má tester možnost nahlédnout do obsahu dané zprávy.

Výhodou tohoto testování je dále nepřetržitá informace o přesné (číselné hodnotě) vzdálenosti čela vozidla od EoA, čehož lze využít při ověřování délky dohledové informace a správného umístění EoA při naplnění funkčních požadavků na prodlužování dohledové informace MA FS nebo MA OS, jelikož jejich ověření na vozidle je problematické a na větší vzdálenosti (více než cca 4 km) méně přesné (viz kapitola 7.2).

V případě, že jsou k ověření vybrány požadavky na restrikce, je simulátor vhodný z toho důvodu, že ani po naplnění takového požadavku nedojde k omezení skutečného okolního drážního provozu.

7.2 Testování na vozidle

Strojvedoucímu se funkční chování systému ETCS projevuje zobrazením informací, které vozidlo přijme od RBC, na DMI aktivního ovládacího pultu vozidla. Protože je ETCS interoperabilní vlakový zabezpečovač, musí být i zobrazování na DMI provedeno výrobcem mobilní části tak, aby odpovídalo příslušným specifikacím ETCS.

Obr. 13 Zobrazení na DMI podle specifikace ETCS

Mezi informace indikované systémem ETCS strojvedoucímu patří:

- aktuální maximální dovolená rychlost;
- budoucí maximální dovolená rychlost (od místa snížení rychlosti);
- aktuální rychlost vozidla;
- délka dohledové informace MA v podobě bargrafu, který je upraven tak, aby oznamoval místa změn rychlosti ze statického rychlostního profilu, jenž je součástí poslední obdržené dohledové informace MA;
- vzdálenost do cíle – k nejbližší změně rychlosti nebo ke konci dohledové informace MA indikována pomocí bargrafu i číselně (to však pouze pokud se vozidlo přiblíží k EoA a

dostane se do oblasti brzdných křivek – na méně než cca 1900 m pro rychlost MV AŽD 110 km/h);

- mód a úroveň, v nichž se mobilní část vozidla aktuálně nachází;
- textová hlášení, žádosti o potvrzení, aktivované procedury (typicky Override EoA);
- číslo vlaku;
- aktuální čas nastavený na mobilní části.

7.2.1 Postup ověření dílčího chování ETCS na mobilní části (měřícím voze)

Možnosti testového ověření naplnění dílčího chování ETCS na vozidle byly vyzkoušeny na I. tranzitním železničním koridoru v oblasti ETCS L2 na motorovém voze 851 026-5 (dále MV AŽD) vybaveném mobilní částí ETCS od výrobce Bombardier Transportation umožňující dohled jízdy v aplikačních úrovních ETCS L2, L1, LSTM a L0.

Ve zvoleném úseku trati byla na DMI vozidla průběžně odečítána délka dohledové informace MA FS společně s aktuálním časovým údajem z DMI (ve formátu hh:mm:ss) za účelem ověření naplnění funkčních požadavků z informací, které má k dispozici strojvedoucí a které ovlivní jeho činnost při řízení drážního vozidla.

Pokud RBC vydalo a následně vozidlo přijalo prodlouženou dohledovou informaci MA FS, došlo k naplnění funkčního požadavku na prodloužení MA FS do dané části infrastruktury z hlediska jeho požadovaného výstupu pohledem na DMI, na němž se prodloužila vyznačená oblast na bargrafu. Z DMI byl v témže okamžiku odečten aktuální časový údaj zobrazení prodloužené dohledové informace MA strojvedoucímu.

Stupnice zobrazené délky dohledové informace MA FS vyznačené v bargrafu je logaritmická. Jízdou vozidla dochází k postupnému přibližování vozidla k místu, kde je podle MA snížena rychlost, resp. k místu EoA tohoto MA, a zvětšování rozlišitelnosti zbývající vzdálenosti a tedy i k přesnějšímu odečtu pohledem strojvedoucího. Strojvedoucí má možnost zvolit rozsah zobrazené vzdálenosti na DMI z několika variant (32 km, 16 km, 8 km, 4 km). Pod určitou vzdálenost od EoA, při které se vozidlo dostane do oblasti brzdných křivek (cca 1900 m pro rychlost MV AŽD 110 km/h), dochází navíc k zobrazení číselné hodnoty vzdálenosti čela vozidla od EoA na samotném bargrafu vzdálenosti do cíle. V takové vzdálenosti tedy již může strojvedoucí na DMI přesně odečíst, jak daleko se nachází čelo vozidla od EoA a přizpůsobit tomu jízdu vozidla, aby do brzdění nemusela zasáhnout samotná mobilní část systému ETCS.

Spolu se sledováním projevu funkčního chování na DMI byla současně monitorována i poloha vozidla prostřednictvím GPS lokátoru umístěném při jízdě v interiéru vozidla na stanovišti strojvedoucího. Účelem zařízení GPS bylo zaznamenávat souřadnice (zeměpisné šířky a zeměpisné délky) aktuální polohy vozidla na trati s časem výskytu v dané poloze s cílem přiřazení okamžiku funkčního projevu systému k aktuální poloze vozidla a k možnému určení EoA přijatého MA po ujetí odečtené délky z bargrafu. Výhodou této metody je, že po součtu dílčích délek mezi naměřenými body GPS, dojde k provedení dalšího nezávislého měření délky dohledové informace MA.

Je zřejmé, že hodnoty času hodin z GPS lokátoru a DMI se mohou lišit vlivem nepřesného nastavení těchto zařízení. Proto byl před zahájením měření a po ukončení měření vypočítán rozdíl mezi hodnotou času GPS lokátoru a času DMI, aby bylo možné k sobě data o MA FS a exportovaná data souřadnic GPS v daném čase přiřadit.

Skutečná délka přijaté dohledové informace MA byla odměřována pomocí výpočtu ujeté vzdálenosti z vyexportovaných průjezdních bodů GPS uložených do souborů typu XML označených příponou *.GPX.

Pro lepší prezentaci ujeté vzdálenosti ve vztahu k infrastruktuře byla stanovena počáteční hodnota kilometráže v grafech pomocí známé polohy venkovních prvků v kolejišti (návěstidla, přejezdy, …), jejichž kilometrická poloha je zaměřena v situačních schématech, přičemž stejně lze polohu těchto prvků popsat pomocí zeměpisných souřadnic GPS. Pokud těmto dvěma popisům polohy přiřadíme jedno společné místo, získáme referenční bod, ke kterému můžeme přičítat přírůstky vypočítaných vzdáleností mezi body GPS.

Kilometrická poloha míst EoA (hlavních návěstidel) přijatých MA FS do grafu byla vypočítána z přírůstků vypočítané vzdálenosti ujeté vůči místu, kde vozidlo přijalo prodloužené MA FS. Tento přírůstek mohl být definitivně stanoven až při průjezdu vozidla (GPS lokátoru) kolem daného potenciálního EoA.

Vlastní měření tedy probíhalo nezávisle na další kilometráži trati (kterou lze použít jako orientační údaj pro ověření smysluplnosti naměřené vzdálenosti, nikoliv k jejímu stanovení nebo zpřesnění).

Naměřená a také skutečná ujetá vzdálenost se od té určené na první pohled z hektometrovníků / kilometrovníků bude lišit (nemají vliv na účel měření kilometráže, protože jde o orientační záležitost), neboť naměřená vzdálenost zohledňuje i jízdu vozidla do odboček a kolejových

spojek a fakticky měří délku, kterou vozidlo ujede, byť ne spojitě. Nepřesnost do měření vnáší chyba souřadnic GPS, hustota naměřených souřadnic bodů na infrastruktuře (čím kratší bude vzdálenost naměřených bodů, tím přesněji bude trajektorie z GPS kopírovat skutečnou trajektorii zejména v obloucích) a použitá metoda výpočtu vzdálenosti mezi body (viz dále).

Dílčí vzdálenost ujetá mezi dvěma změřenými body GPS (při zkušebních jízdách činila řádově jednotky metrů) byla vypočtena pomocí Haversinova vzorce, který nahrazuje elipsoidní tvar Země koulí o středním poloměru 6371 km (Freiberger 2014).

Nadmořské výška dvou sousedních bodů je ve výpočtech zanedbána.

$$\Delta ZD_n = ZD_{n+1} - ZD_n$$
$$\Delta Z\check{S}_n = Z\check{S}_{n+1} - Z\check{S}_n$$
$$\Delta s_n = 2 \cdot R \cdot \sin^{-1} \sqrt{\sin^2 \frac{\Delta Z\check{S}_n}{2} + \cos Z\check{S}_n \cdot \cos Z\check{S}_{n+1} \cdot \sin^2 \frac{\Delta ZD_n}{2}} \qquad 3$$

Kde:

R … střední poloměr Země, 6371 km

$Z\check{S}_n$ … zeměpisná šířka bodu n

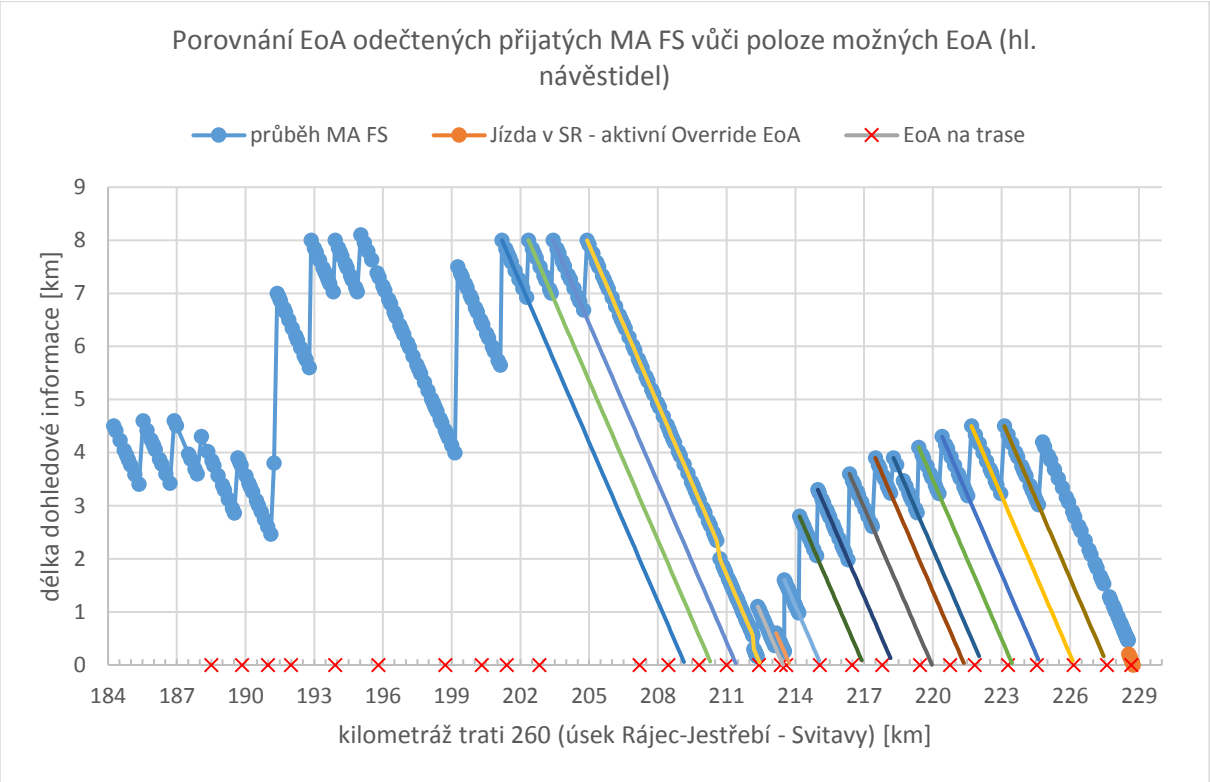
ZD_n … zeměpisná délka bodu n

$Z\check{S}_{n+1}$ … zeměpisná šířka bodu n+1

ZD_{n+1} … zeměpisná délka bodu n+1

Δs_n … vzdálenost bodu n+1 od bodu n

Při měření bylo zjištěno, že vzhledem k nepřesnosti odečtu délky dohledové informace z bargrafu při uvažovaných délkách MA FS až okolo 7 km, bylo možné i přes nastavení optimálního rozsahu zobrazené vzdálenosti na DMI (8 km) bezpečně určit pouze fakt, že **MA bylo vozidlu prodlouženo dále dle požadavků**, protože to se viditelně projevilo skokovou změnou vyznačené oblasti na bargrafu DMI.

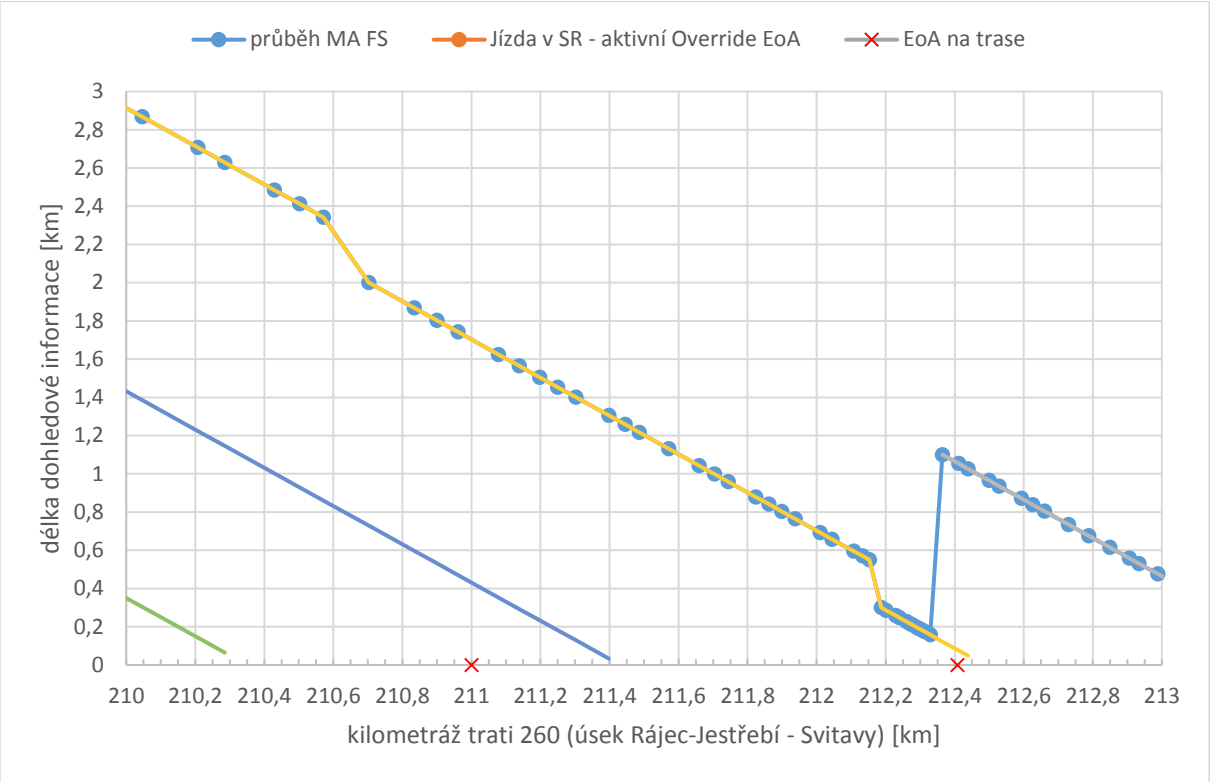


Graf 1 Změřené délky dohledových informací při jízdě motorového vozu

Jak je patrné z Graf 1, pokud nebylo MA FS přijaté v km 204,9 prodlužováno, nýbrž pouze obnovováno (platnost MA je časově omezená) stále ke stejnému EoA, bylo možné délku MA postupně zpřesňovat (provedením dalších odečtů z bargrafu DMI) a díky tomu spolehlivě určit k jakému EoA bylo toto MA vydáváno. Způsobem, kdy nejsou splněny podmínky k prodloužení MA FS, lze tedy bezpečně detekovat, že **MA bylo vozidlu vydáno k EoA podle požadavku.**

Pokud bylo vozidlu MA FS prodlužováno, mohlo být EoA původního MA FS stanoveno při další jízdě kolem tohoto EoA aproximací ujeté původní délky MA. Tyto aproximace znázorňují jednotlivé křivky ekvidistantní s „obálkou“, která reprezentuje aktuální délku MA vozidla.

Podmínky, při nichž by nemělo být vozidlu MA FS dále prodlužováno, lze přivodit např. jízdou vozidla ke staničnímu návěstidlu, od kterého není postavena vlaková cesta, nebo jízdou vozidla k hlavnímu návěstidlu na začátku obsazeného prostorového oddílu na traťové koleji.



Graf 2 Detail na zpřesnění odečtené délky přijaté dohledové informace pří přibližování k EoA

7.2.2 Ověření naplnění požadavků na prodloužení MA FS při jízdě přes hranici RBC/RBC Handoveru

Za účelem ověření metod z této práce proběhly 16. 5. 2018 jízdy MV AŽD pod dohledem ETCS na trase Kolín – Česká Třebová. Zaznamenávány byly tentokrát projevy funkčního chování systému ETCS na vozidle i na HMI RBC v CDP Praha. K ověření podmínek pro naplnění funkčního požadavku bylo sledováno zobrazení na HMI RBC. Pro komplexnější ověření těchto podmínek (ověření správnosti zobrazených stavů na HMI RBC) je možné při testech dále zaznamenávat indikace na ZPC JOP, nicméně toto dosud neproběhlo z důvodu nežádoucího rušení dispečera při řízení železničního provozu. K vyhodnocení korelace projevů na DMI i HMI RBC byly pořízeny videozáznamy obou zařízení spolu s jejich hodinami. Funkční chování by ze své podstaty mělo být okamžitě vyhodnotitelné, ovšem videozáznamy umožní hlubší analýzu příčin funkčního chování a přináší výhodu v podobě neomezené doby vyhodnocení naplnění funkčních požadavků. Obzvláště pokud ověřujeme naplnění více funkčních požadavků současně, je nežádoucí některý z nich opomenout kvůli nedostatku času.

Pro synchronizaci dat z měření bylo potřeba určit:

- odchylku hodin obou videokamer před a po provedení jízd MV AŽD;
- odchylku hodin videokamery snímající HMI RBC vůči hodinám HMI RBC;
- odchylku hodin videokamery snímající DMI vůči hodinám DMI;
- odchylku hodin GPS lokátoru vůči hodinám videokamery na DMI.

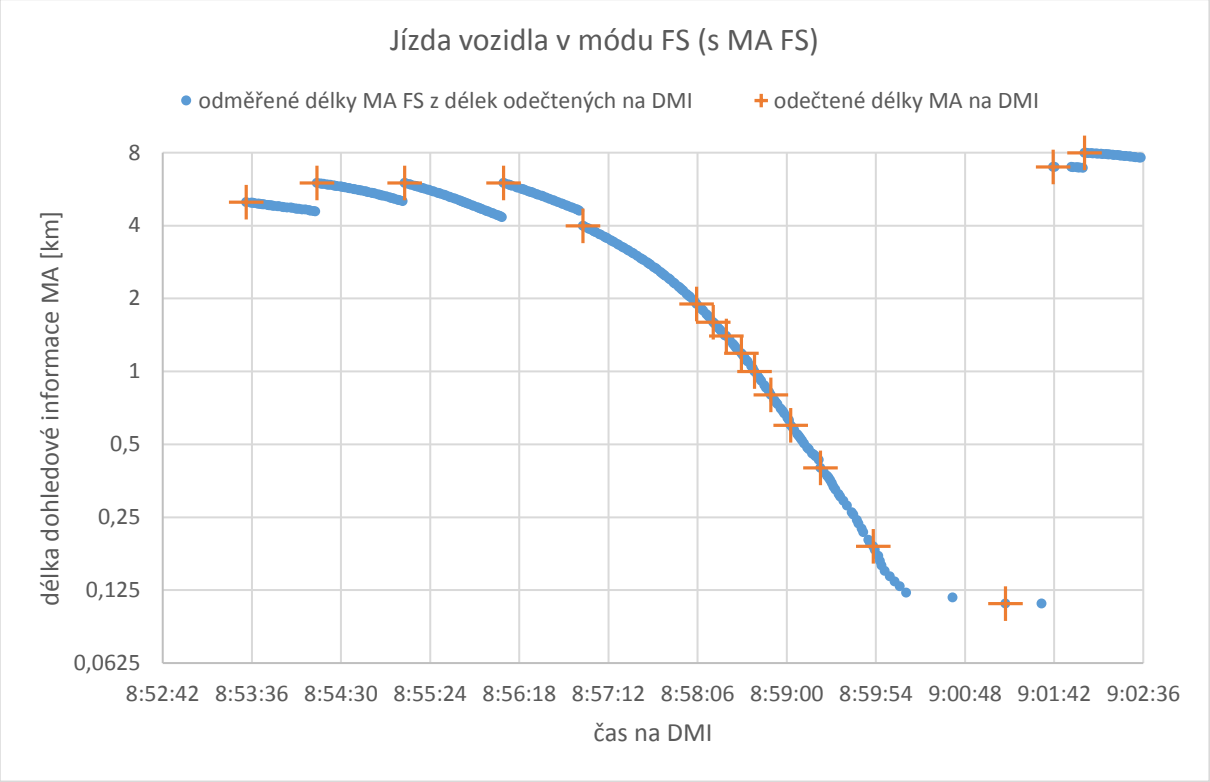
Změna rychlosti přírůstku času hodin DMI nebo HMI vůči časům příslušných videokamer, které jsou směrodatné pro synchronizaci, nebyla při testovací jízdě explicitně měřena. Předpokládá se, že tato odchylka by byla detekovatelná z odlišné délky pořízeného videozáznamu a času hodin DMI na prvním a posledním snímku videozáznamu, což lze provést i po ukončení testovacích jízd. Neočekává se, že stanovení odchylek bude dosaženo s velkou přesností na desetiny sekundy, nýbrž s přesností na několik málo sekund (2, max. 3 s), což zhruba odpovídá rozlišitelné schopnosti strojvedoucího a dispečera.

Pro účely srozumitelnější interpretace výsledků funkčního chování systému ETCS je v dalších vyhodnoceních všechna činnost systému ETCS vztažena (tj. případně přepočítána) na čas hodin DMI vozidla.

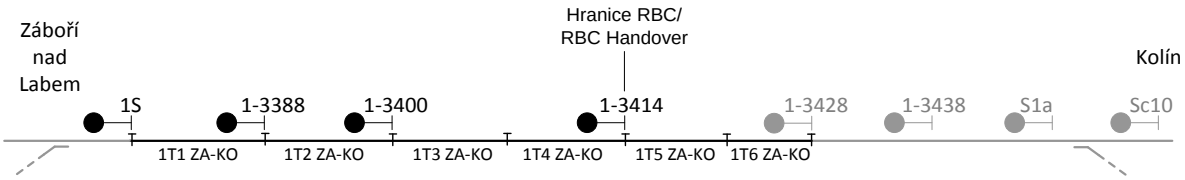
K aktivaci dohlížení jízdy vozidla systémem ETCS došlo poté, co obsluha vozidla provedla proceduru SoM na 10. SK v žst. Kolín (zadání vlakových dat a nastavení pro zahájení komunikace se stacionární částí systému ETCS). Protože systém ETCS neměl po SoM k dispozici kompletní informaci o poloze čela vozidla (nebylo možné vyloučit výskyt tohoto vozidla na jiné koleji), byla vozidlu po postavení odjezdové vlakové cesty (s rozsvícenou dovolující návěstí „Rychlost 40 a volno“ na cestovém návěstidle Sc10) z 10. SK v žst. Kolín udělena neomezená SR autorizace, která umožnila uvést vozidlo do pohybu.

Po vjezdu vozidla do vlakové cesty bylo následně na základě naplněného funkčního požadavku na přechod z módu SR do FS v čase 8:53:28 (čas DMI) na HMI RBC indikováno odeslání dohledové informace MA FS vozidlu, které jej zobrazilo v čase 8:53:32 na DMI a současně provedlo vozidlo přechod do módu FS dle příslušného testového případu #11_FS_SK_TEST, který je uveden v příloze A ověřující naplnění funkčního požadavku. Podle zobrazené délky dohledové informace MA FS bylo patrné, že došlo současně k naplnění více funkčních požadavků, jelikož MA FS se vydalo i do několika navazujících kolejových úseků. Při analýze o jaké funkční požadavky se mohlo jednat, využijeme matice podmíněného zařazení požadavku do scénáře.

Poté, co jsme určili aktuálně naplňované funkční požadavky, ověříme, zda k jejich naplnění skutečně došlo v tolerované době (obsahující i nepřesnost synchronizace času hodin) po splnění všech nutných podmínek uvedených v požadavku prostřednictvím vybraného testového případu, který se na danou situaci v kolejišti vztahuje. Pokud je testový případ vyhodnocen jako úspěšný (viz Kolář 2018) a to po celou dobu ověření naplnění požadavku a stejně tak i ostatní testové případy ověřující naplnění tohoto požadavku, je zároveň i funkční požadavek označen jako otestovaný. Pro dokumentaci provedení testového případu je vytvořen testový report, který se na testový případ trasuje.



Graf 3 Prodlužování MA FS po odjezdu vozidla z žst. Kolín



Obr. 14 Situační nákres odjezdu z žst. Kolín

Při této testovací jízdě bylo již první MA FS, které bylo indikované na HMI RBC v čase 8:53:28 a na DMI v čase 8:53:32, prodlouženo k hranici RBC/RBC Handover (na konec kolejového úseku 1T5 ZA-KO k oddílovému návěstidlu 1-3414). První kolejový úsek za touto hranicí (1T4

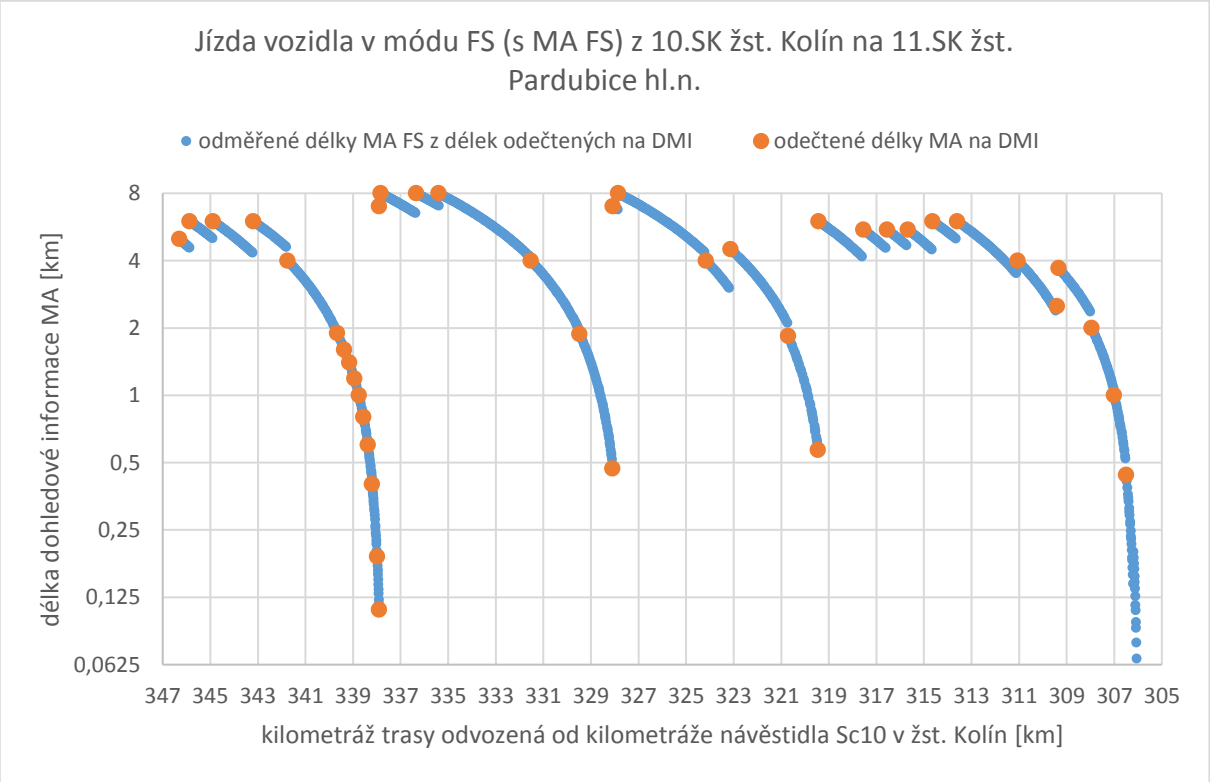
ZA-KO) byl v daném okamžiku indikován na HMI RBC jako obsazený předchozím vozidlem. Odečtená délka MA FS v době jejího přijetí na vozidle byla 5 km. Můžeme tedy vyhodnotit provedení testového případu #03_PRODL_FS _TK_TEST uvedeného v příloze B. Všechny podmínky tohoto testového případu byly splněny a proto je vyhodnocen jako úspěšný – na základě jakéhokoliv vyhodnocení tohoto testového případu vzniknul testový report #01_TESTREPORT uvedený v příloze E.

V okamžiku, kdy došlo k ukončení indikace obsazení kolejového úseku 1T4 ZA-KO na HMI RBC za hranicí RBC/RBC Handover, zůstal tento kolejový úsek na HMI RBC indikován jako kolejový úsek, přes který je vydáno MA OS, ačkoliv na DMI vozidla byla stále správně zobrazena dohledová informace MA FS k původnímu EoA (návěstidlu 1-3414), jelikož kolejový úsek 1T3 ZA-KO, jenž je součástí jednoho prostorového oddílu společně s 1T4 ZA-KO, byl stále obsazený. Toto chování bylo způsobeno indikací vyhodnocených podmínek udělení MA za hranici RBC/RBC Handover, ovšem zároveň nebyly splněny podmínky, aby toto MA bylo možné odeslat vozidlu.

Stejná situace se opakovala i po ukončení indikace obsazení dalšího navazujícího kolejového úseku 1T3 ZA-KO (v témže prostorovém oddílu) a to po dobu ještě cca 1 s, než došlo ke změně indikací obou dotčených kolejových úseků v čase 8:54:07 a prodloužení dohledové informace MA FS za hranici RBC/RBC Handoveru k následujícímu oddílovému návěstidlu (1-3400) na konci kolejového úseku 1T3 ZA-KO dle požadavků a to jak na HMI RBC, tak po uplynutí 7 s na DMI vozidla. Délka MA odečtená z bargrafu byla v okamžiku přijetí prodlouženého MA FS 6km.

V čase 8:55:01 byla na HMI RBC ukončena indikace obsazeného kolejového úseku 1T2 ZA-KO (samotného v prostorovém oddílu) a zároveň bylo na HMI RBC indikováno prodloužení MA FS do tohoto kolejového úseku, na jehož konci je oddílové návěstidlo 1-3388. O 7 s později se projevilo prodloužení MA i na DMI vozidla. V 8:55:59 došlo na HMI RBC k indikaci dalšího prodloužení MA FS (bezprostředně po uvolnění kolejového úseku 1T1 ZA-KO) k vjezdovému návěstidlu 1S žst. Záboří nad Labem. Vozidlo prodloužené MA přijalo v čase 8:56:08 a s tímto obnovovaným MA pokračovalo v jízdě k vjezdovému návěstidlu, aniž by mu bylo dále viditelně prodlužováno. Dále byl zaznamenán okamžik, kdy strojvedoucímu zobrazená délka MA dosáhla 4000 m pro zpřesnění informace o vzdálenosti čela vozidla od EoA dosud určené předchozí odečtenou délkou MA v době jejího prodloužení. Vozidlo zastavilo až v místě, odkud byla na DMI indikována vzdálenost 110m od konce tohoto MA. Po postavení vlakové cesty

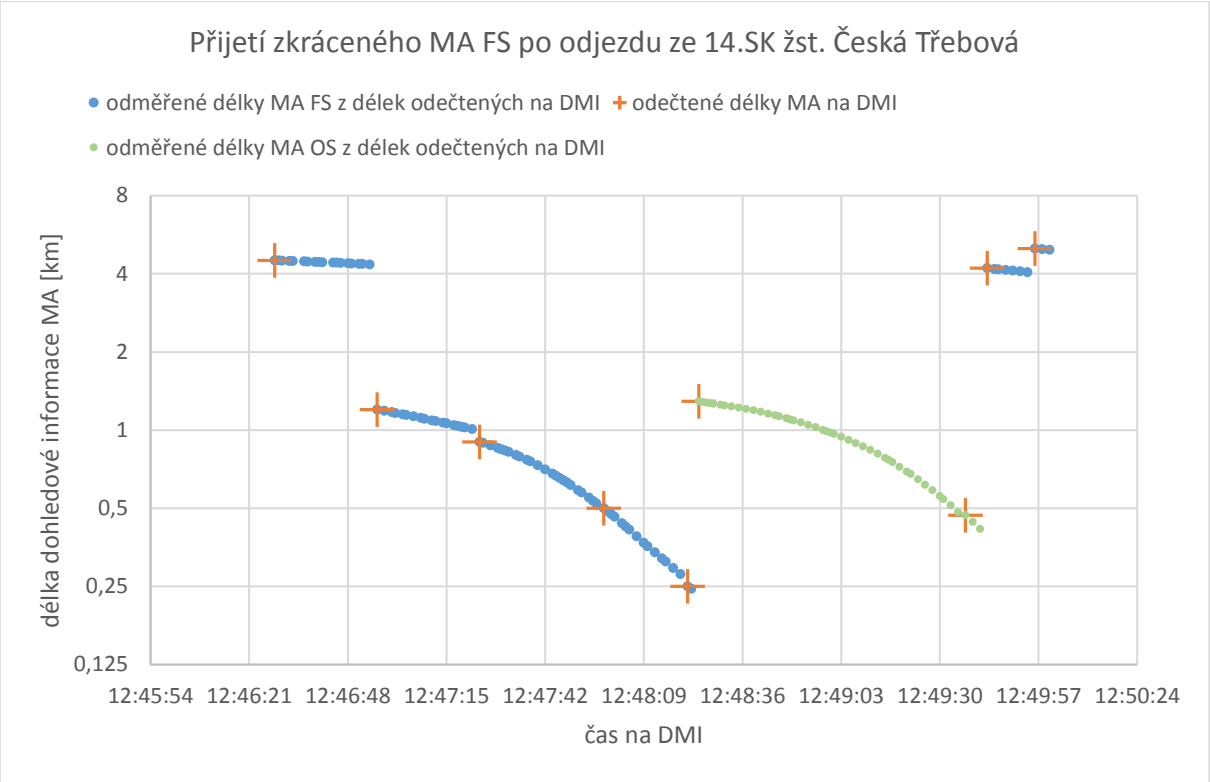
byla vozidlu umožněna další jízda za vjezdové návěstidlo 1S a na DMI dosáhlo MA FS odečtené délky 7 km. V čase 9:02:06 vozidlo minulo vjezdové návěstidlo. Vzdálenost ujetá dle GPS od okamžiku zastavení (se zobrazenou vzdáleností 110 m od EoA) do minutí vjezdového návěstidla, byla vypočítána na 126 m. Rozdíl mezi vzdálenostmi tedy činil 16 m. Kilometrická poloha návěstidla 1S žst. Záboří nad Labem je v situačních schématech označena jako km 337,774, přičemž vozidlo podle výpočtů z GPS toto návěstidlo minulo v km 337,772.



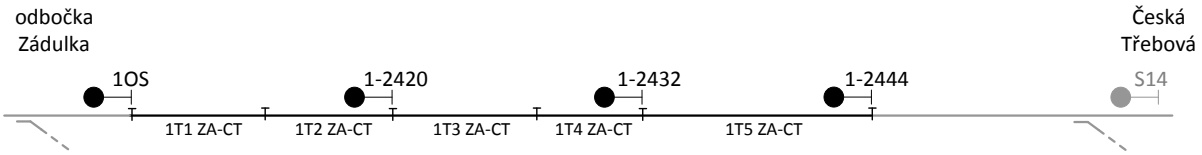
Graf 4 Naměřené pozice na trase při prodlužování MA FS při jízdě z žst. Kolín do žst. Pardubice hl.n.

7.2.3 Ověření naplnění požadavků na zkrácení MA

Ověření naplnění funkčního požadavku na zkrácení dohledové informace MA FS při poruše podmínek v prostorovém oddílu před vozidlem, který je součástí vydané dohledové informace, jíž vozidlo disponuje, proběhlo plánovaně při jízdě mezi žst. Česká Třebová a odbočkou Zádulka.



Graf 5 Zkrácení MA FS a přechod do/z módu OS po odjezdu z žst. Česká Třebová



Obr. 15 Situační nákres odjezdu z žst. Česká Třebová

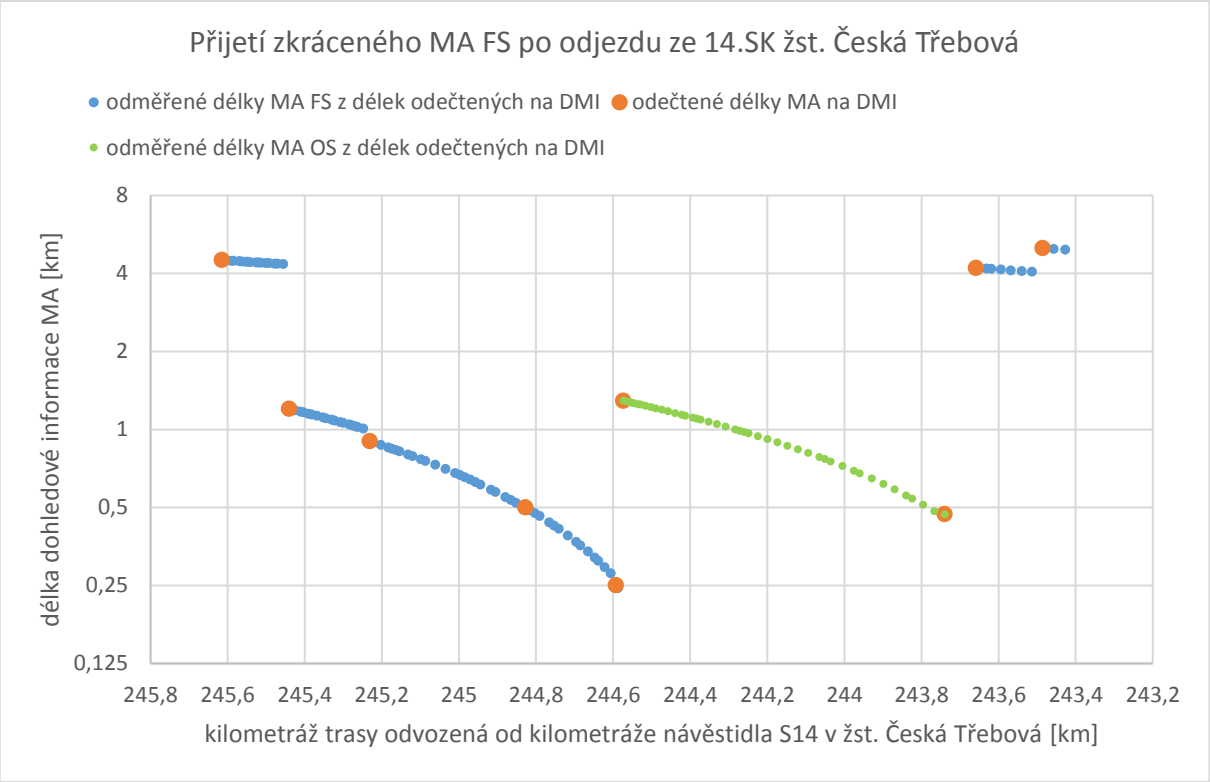
Vozidlo v módu SR vjelo do vlakové cesty postavené ze 14.SK (na jejímž konci je návěstidlo S14) žst. Česká Třebová a v čase 12:46:28 indikovalo na bargrafu DMI přijaté MA FS s odečtenou délkou 4,5 km. Na HMI RBC bylo zobrazeno MA FS vydané přes kolejové úseky až po návěstidlo 1OS v odbočce Zádulka. Na HMI RBC zatím nebylo indikováno postavení vlakové cesty od tohoto hlavního návěstidla.

V čase 12:46:52 došlo na HMI RBC k indikaci obsazeného kolejového úseku 1T5 ZA-CT, důsledkem čehož bylo okamžitě zkráceno MA FS k hlavnímu návěstidlu před tímto kolejovým úsekem (1-2444). Zkrácené MA FS vozidlo přijalo a indikovalo v čase 12:46:56 na DMI s délkou MA odečtenou na 1,2 km, jehož délka se při hodnotě 900 m začala indikovat i číselně.

V okamžiku, kdy bylo čelo vozidla vzdálené méně než 300 m od EoA (konkrétně při hodnotě 250 m), došlo na DMI k zobrazení žádosti o přechod do módu OS. Obsluha vozidla posléze tuto žádost potvrdila a vozidlo provedlo přechod do módu OS. Změna módu se projevila i na

HMI RBC změnou indikace u čísla vlaku. Vozidlo pokračovalo v jízdě v kolejovém úseku 1T5 ZA-CT s MA OS k návěstidlu na konci tohoto kolejového úseku (1-2432). Kolejový úsek 1T3 ZA-CT před vozidlem, ležící mezi návěstidly 1-2432 a 1-2420, byl na HMI RBC indikován jako volný. Vozidlo se přibližovalo k návěstidlu 1-2432 a poté, co indikovaná zbývající délka MA OS dosáhla 500 m (hodnota CZ_D_TAFREQDISP), zobrazila se na DMI žádost o potvrzení TAF v souladu s testovým případem #01_OS_TK_TEST v příloze C.

Následovalo provedení testového případu #01_FS_TK_TEST v příloze D, podle něhož obsluha vozidla po kontrole volnosti potvrdila TAF, a po uplynutí dalších 5 s vozidlo přijalo a indikovalo MA FS na vzdálenost 4,2 km, neboť krátce před potvrzením TAF došlo k postavení vlakové cesty od návěstidla 1OS odbočky Zádulka.



Graf 6 Naměřené pozice na trase při zkrácení MA FS a přechod do/z módu OS po odjezdu z žst. Česká Třebová

Závěr

Diplomová práce provedla čtenáře zákulisím tvorby funkčních požadavků na vlakový zabezpečovací systém ETCS, jehož nasazení do provozu, které přispěje ke zvýšení bezpečnosti železniční dopravy v našich krajinách, se jistě kvapem blíží a tak je důležité co nejdříve stanovit účinné metody ověření naplnění požadovaného chování systému, které je použitelné v různých provozních situacích. Náplní práce bylo mimo jiné také vyzdvihnout důležitost samotných funkčních požadavků pro realizaci finální podoby systému v takové podobě, aby zákazník nebyl nemile překvapen.

Obsáhlá část práce se věnuje rozboru charakteru funkčních požadavků, jejich popisu a využití těchto informací z analýzy při ověřování naplnění. Dále byly popsány vazby těchto požadavků na další úrovně dosavadních specifikací systému ETCS a předloženy argumenty proč je důležité sledovat příčinu vzniku funkčního požadavku a nepřehlédnout přání zákazníka.

Uvedeny jsou popisy subsystémů a komponent, jejichž realizace je potřebná k ověření naplnění funkčních požadavků na vlakový zabezpečovací systém ETCS aplikační úrovně L2. Zanalyzovány byly i možnosti nahrazení chování těchto subsystémů a komponent simulacemi pro účely ověření funkčního chování.

Podařilo se provést měřící jízdy MV AŽD na I. tranzitním železničním koridoru a ověřovat tak funkční chování systému přímo nejideálnějším způsobem, jak jej vidí strojvedoucí a dispečer. Na závěr této práce je shrnut podrobný popis průběhu těchto jízd, dále pak dříve uvedených metod uplatněných k získání informací potřebných k vyhodnocení funkčního chování a samotné vyhodnocení provedených testů ověřujících naplnění funkčních požadavků zejména na dohled jízdy vozidla v módu FS, protože dosažení plného dohledu jízdy v co možná nejkratším čase je bezpečnostním cílem systému ETCS L2.

V této práci je v konkrétně uvedených metodách využito dalšího nezávislého technického prostředku k ověření naplnění funkčních požadavků – globálního polohového systému, jehož přesnost a dostupnost se v praxi jeví jako dostatečná pro tyto účely. Snahou ověření naplnění funkčních požadavků je dokázat korektní funkční chování prostřednictvím indikací a ovládání na uživatelské úrovni aniž by muselo být využito nějaké další nadstandardní diagnostiky.

Literatura a zdroje

AŽD Praha s.r.o. Funkční požadavky na aplikaci ETCS L2 na infrastruktuře SŽDC : RBC ETCS [soubory formátu *.doc]. 2017a. *Neveřejné dokumenty.*

AŽD Praha s.r.o. Parametry specifické aplikace RBC pro KP ETCS a další hodnoty použité v analýzách [soubor formátu *.doc]. 2017b. *Neveřejný dokument.*

AŽD Praha s.r.o. RBC ETCS – Specifikace systémových požadavků na traťovou část ETCS L2 [soubor formátu *.doc]. 2017c. *Neveřejný dokument.*

ČSN EN 50128 ed. 2. Drážní zařízení – Sdělovací a zabezpečovací systémy a systémy zpracování dat – Software pro drážní řídicí a ochranné systémy. Praha : Český normalizační institut, 2012.

BOULANGER, Jean-Louis. *Cenelec 50128 and iec 62279 standards*. Hoboken, NJ: ISTE Ltd/John Wiley and Sons, 2015. ISBN 978-1-84821-634-1.

RIERSON, Leanna. *Developing safety-critical software: a practical guide for aviation software and DO-178c compliance*. Boca Raton: CRC Press/Taylor & Francis Group, 2013. ISBN 9781439813683.

WIEGERS, Karl Eugene. *Požadavky na software*. Brno: Computer Press, 2008. ISBN 978-80-251-1877-1.

ČSN EN 50126. Drážní zařízení – Stanovení a prokázání bezporuchovosti, pohotovosti, udržovatelnosti a bezpečnosti (RAMS). Praha : Český normalizační institut, 2001.

TNŽ 34 2620. Železniční zabezpečovací zařízení – Staniční a traťové zabezpečovací zařízení. Olomouc : České dráhy, s.o., 2002.

PALUMBO, Maurizio. *Requirements Management for Safety Critical Systems* [online]. 25 Jun 2015, 1-7 [cit. 2018-05-15]. Dostupné z: http://www.railwaysignalling.eu/wp-content/uploads/2015/06/Req_mgt_safety_critical_system_MPalumbo.pdf

MAVIN, Alistair, Philip WILKINSON, Adrian HARWOOD a Mark NOVAK. Easy Approach to Requirements Syntax (EARS). *2009 17th IEEE International Requirements Engineering Conference* [online]. IEEE, 2009, 2009, 317-322 [cit. 2018-05-15]. DOI: 10.1109/RE.2009.9. ISBN 978-0-7695-3761-0. Dostupné z: http://ieeexplore.ieee.org/document/5328509/

MAREK, Jakub. Informace z UNISIG, aktuální stav specifikací a další rozvoj ETCS_2015_ETCS_Marek.pdf. In: *ACRI* [online]. AŽD Praha, 2. června 2015 [cit. 2018-05-15]. Dostupné z: http://www.acri.cz/uploads/acri-akademie/15-06%20ETCS/2015_ETCS_Marek.pdf

SŽDC, s.o. *Pokyn provozovatele dráhy k zajištění plynulé a bezpečné drážní dopravy č. X/2017: Věc: Testy kompatibility palubních a traťových částí systému ERTMS/ETCS úrovně 2* [online]. SŽDC, s.o., 2017, 15. 12. 2017, 1-63 [cit. 2018-05-15]. Dostupné z: provoz.szdc.cz/Portal/Show.aspx?oid=1521400

SŽDC, s.o. *Technické požadavky pro implementaci ERTMS/ETCS L2 na české části Koridoru E* [online]. SŽDC, s.o., 2010, 10. 6. 2010, 1-40 [cit. 2018-05-15]. Dostupné z: http://www.szdc.cz/soubory/ertms/technicke-pozadavky.doc

KOLÁŘ, Daniel. *Ročníkový projekt II: Funkční požadavky na železniční zabezpečovací systémy – uplatnění SW nástroje pro správu požadavků a pro podporu testování jejich naplnění*. Pardubice, 2018. Ročníkový projekt. Univerzita Pardubice, Dopravní fakulta Jana Pernera. Vedoucí práce Jan Ouředníček.

FREIBERGER, Marianne. Lost but lovely: The haversine. *Plus.maths.org* [online]. Cambridge: Freiberger, 2014, 4 July 2014 [cit. 2018-05-15]. Dostupné z: https://plus.maths.org/content/lost-lovely-haversine

V-model (Software Development Life Cycle). *Software Testing Class - Complete website for Softare Testing Folks* [online]. 2012, 29 May 2012 [cit. 2018-05-17]. Dostupné z: http://www.softwaretestingclass.com/v-model/

Seznam zkratek

BG	Balise Group – balízová skupina
CDP	Centrální dispečerské pracoviště
CEM	Conditioned Emergency Stop – podmíněné nouzové zastavení
DMI	Driver Machine Interface – rozhraní na ovládacím pultu vozidla
EoA	End of Authority – konec oprávnění k jízdě
ETCS	European Train Control System
EVC	European Vital Computer – počítač mobilní části
GPS	Global Positioning System – globální polohový systém
HMI RBC	Human Machine Interface – rozhraní mezi dispečerem a systémem
JOP	Jednotné obslužné pracoviště
MA	Movement Authority – oprávnění k jízdě
MV AŽD	Měřící vůz společnosti AŽD Praha s.r.o.
OBU	On Board Unit – mobilní část systému ETCS na vozidle
PR	Position Report – hlášení polohy vozidla
PZ	Přejezdové zabezpečovací zařízení
PZS	Přejezdové zabezpečovací zařízení světelné
RAMS	Reliability, Availability, Maintainability, Safety vlastnosti systému
RBC	Radio Block Center – Radiobloková centrála ETCS
SoM	Start of Mission – Zahájení mise
SRS ETCS L2	Systémové požadavky na traťovou část ETCS L2
SZZ	Staniční zabezpečovací zařízení
SŽDC	Správa železniční dopravní cesty, státní organizace
TAF	Track Ahead Free – volnost koleje před vozidlem
TZZ	Traťové zabezpečovací zařízení
UEM	Unconditioned Emergency Stop – nepodmíněné nouzové zastavení
ZTP	Zvláštní technické podmínky

Seznam obrázků

Seznam tabulek

Seznam grafů

Příloha A

#11_FS_SK_TEST	
Testované požadavky:	#@trace 0102201_FRS_L2_MAFS_SK
Výchozí stav:	Čelo vozidla je na staniční koleji. Čelo vozidla se nachází v nedostatečné vzdálenosti (D_DOSTAT) od hlavního návěstidla na konci staniční koleje. Systém ETCS disponuje kompletní informací o poloze čela vozidla. Od hlavního návěstidla na konci staniční koleje je postavena vlaková cesta. OBU je v módu SR. OBU disponuje „Neomezenou SR autorizací“
Postup scénáře:	Vozidlo vjede do prvního kolejového úseku za hlavním návěstidlem.
Cílový stav:	Na DMI je indikováno, že vozidlo je v módu FS, je indikována povolená vzdálenost udávajícím vzdálenost zbývající k místu konce dohledové informace MA FS a je indikována povolená rychlost pro jízdu v módu FS. Na HMI RBC je v seznamu vlaků a v kolejišti u symbolu příslušného vlaku indikováno, že je vozidlo v módu FS a délka dohledové informace MA FS.

Příloha B

#03_PRODL_FS _TK_TEST	
Testované požadavky:	#@trace 0103121_FRS_L2_MAFS_TK
Výchozí stav:	OBU je v módu FS. OBU nedisponuje dohledovou informací MA FS k návěstidlu na začátku daného prostorového oddílu. Daný prostorový oddíl za hlavním návěstidlem, ke kterému je vydána dohledová informace MA FS, je volný.
Postup scénáře:	OBU disponuje dohledovou informací MA FS k návěstidlu na začátku prostorového oddílu.
Cílový stav:	Na DMI je indikováno prodloužení dohledové informace MA FS k oddílovému návěstidlu na konci daného prostorového oddílu. Na HMI RBC je indikováno prodloužení dohledové informace MA FS k oddílovému návěstidlu na konci daného prostorového oddílu.

Příloha C

#01_OS_TK_TEST	
Testované požadavky:	#@trace 0102321_FRS_L2_TAF_TK
Výchozí stav:	Čelo vozidla je na traťové koleji v prostorovém oddílu, za kterým následuje ve směru aktivního ovládacího pultu další prostorový oddíl. OBU je v módu OS. OBU disponuje dohledovou informací MA OS. Následující prostorový oddíl je volný.
Postup scénáře:	Čelo vozidla je od hlavního návěstidla ve vzdálenosti menší než je hodnota CZ_D_TAFREQDISP
Cílový stav:	Na DMI je zobrazena „Žádost o potvrzení TAF“.

Příloha D

#01_FS_TK_TEST	
Testované požadavky:	#@trace 0102421_FRS_L2_MAFS_TK
Výchozí stav:	Čelo vozidla je na traťové koleji před oddílovým návěstidlem. OBU je v módu OS. OBU disponuje dohledovou informací MA OS. Na DMI zobrazena „Žádost o potvrzení TAF“
Postup scénáře:	Strojvedoucí potvrdí na DMI „Žádost o potvrzení TAF“.
Cílový stav:	Na DMI je indikováno, že vozidlo je v módu FS, je indikována povolená vzdálenost udávajícím vzdálenost zbývající k místu konce dohledové informace MA FS a je indikována povolená rychlost pro jízdu v módu FS. Na HMI RBC je v seznamu vlaků a v kolejišti u symbolu příslušného vlaku indikováno, že je vozidlo v módu FS a délka dohledové informace MA FS.

Příloha E

#01_TESTREPORT			
Testový případ:	#03_PRODL_FS _TK_TEST	*Lokalita:* Kolín, 1T5 ZA-KO, 1T6 ZA-KO *Čas:* 16. 5. 2018, 8:53:28	
Výchozí stav:	OBU je v módu FS. OBU nedisponuje dohledovou informací MA FS k návěstidlu na začátku daného prostorového oddílu. Daný prostorový oddíl za hlavním návěstidlem, ke kterému je vydána dohledová informace MA FS, je volný.		OK OK OK
Předchozí testový případ:	#00_TESTREPORT		
Postup scénáře:	OBU disponuje dohledovou informací MA FS k návěstidlu na začátku prostorového oddílu.		OK
Cílový stav:	Na DMI je indikováno prodloužení dohledové informace MA FS k oddílovému návěstidlu na konci daného prostorového oddílu. Na HMI RBC je indikováno prodloužení dohledové informace MA FS k oddílovému návěstidlu na konci daného prostorového oddílu.		OK OK
Vyhodnocení:	Úspěšný		